A Text book of Research Papers on Fingerprint Recognition & Hash code Techniques

Dr. Krishna Prasad K.

Faculty, Department of Computer science,
College of Computer and Information Sciences
Srinivas University, Mangalore, INDIA

Srinivas Publication
(A Unit of Srinivas University)

First Edition, 2018

A Text book of Research Papers on Fingerprint Recognition & Hash code Techniques

Dr. KRISHNA PRASAD K.

Faculty, Department of Computer science,

College of Computer and Information Sciences

Srinivas University, Mangalore, INDIA

Srinivas Publication

(A Unit of Srinivas University)

Srinivas University, Mangalore, INDIA

First Edition, 2018

ISBN: 978-81-938040-3-2

Dedicated to

My Family & My Teachers

Foreword

I am happy to note that the Book entitled "A Text book of Research Papers on Fingerprint Recognition & Hash code Techniques" by **Dr. Krishna Prasad K.,** is having enriched information on the latest technology of Photonics and being published by Srinivas Publication, Srinivas University, Mukka, Mangalore.

Srinivas University is striving hard through its contribution for qualitative improvement in the level of education, environment, and economy of the country. We have a visionary mission to contribute to multidimensional growth and development of the society in general and all-round development of the students in particular. We hope that the inspiring students, under the guidance of dedicated teachers and a far-sighted leadership of the top administration would lend this University to a coveted and recognized position in the galaxy of higher education in the world. We aspire our University to be an excellent centre of excellence, innovation, honor, integrity, and outstanding quality and service. Our prime objective is to enrich and support the individual in his/her Endeavour towards the attainment of knowledge and wisdom to apply that knowledge in coherence with the aims and ambitions of the individuals in particular, and for the greater good of humankind in general.

I am happy to write a foreword to this book and glad that **Dr. Krishna Prasad K.,** is making a considerable effort in bringing out this book under Advances in Technology Series. The book contains research articles related to Fingerprint image enhancement, recognition and Hash code generation methods. This book also contains applications of Multifactor authentication model using Fingerprint Hash code, OTP and Password and compares this new model with existing similar systems. These papers published already in peer-reviewed International Journals. This Book has written with an intention to get all papers together under one roof, which will benefit all the researchers of related areas.
Congratulations to the Authors for their determined efforts in bringing out this Book.

CA. A. Raghavendra Rao
Chancellor, Srinivas University,
President, A. Shama Rao Foundation

CONTENTS

PREFACE

In this information and communication technology era, human beings are every now and again requested checks of their identity. Regularly, this is done using passwords while seeking activities like public security, access control, surveillance, and application sign on, and so on. In an organization, educational institutions, political and government offices, security has become crucial aspect and more and more research is carried out for the purpose of verification or identification. The issue of normal framework security involves the assurance of framework components. Therefore, this security can be easily breached when a password is divulged, a card is stolen or through social engineering. Besides, a great many people utilize a similar password crosswise over various applications; an impostor, after deciding or accessing a single password, would now be able to get to different applications. Basic passwords can be easily hacked while troublesome passwords might be difficult to review, and passwords easily broken by dictionary attacks. The requirement for solid client validation procedures has expanded in the wake of uplifted worries about security and quick development in systems administration, correspondence, and portability. These constraints related to the utilization of passwords improved by the joining of better strategies for client confirmation.

The recent innovative researchers significantly concentrate on cell phones. Cell phones have turned into a critical gadget of human life. Clients get to their messages, informal organizations, financial balances, and different sites by means of cell phones. Mobile manufacturers or developers and application engineers take an assortment or mixture of safety efforts because of the individual, private as well as the touch sensitive nature of the data put away in cell phones. The utilization of biometric authentication on cell phones began with cameras. From the last few years, cell phone producers have included biometric validation frameworks like the increasingly well-known unique fingerprint recognition highlight. This is a more secure and handy answer for recognizable proof on cell phones. The unique fingerprint traits of a man are exceptionally exact and are special to a person. Authentication frameworks in light of unique fingerprints have demonstrated to create low false acceptance rate and false rejection rate, alongside other favourable circumstances like simple and easy usage strategy. Additionally, the unique fingerprint ordinarily stays unaltered from birth until death. Aside from being extraordinary and constant, fingerprints accumulated in a non-obtrusive way with no symptom.

The current fingerprint technology is quite mature to identify or verify human using various diverse types of matching or comparing the process with already stored features or templates. One of the potential threats in a biometric framework is the compromise of the biometric template, which may prompt genuine security and protection dangers. Almost all fingerprint template protection methods neglects to meet all the coveted necessities of a viable biometric framework like revocability, security, protection, and high coordinating precision. Specifically, ensuring the fingerprint formats has been a troublesome issue because of huge intra-client varieties (e.g., turn, interpretation, nonlinear twisting, and partial fingerprint image). So there is a huge necessity of building a highly secured and not reversible or revocable fingerprint template protection and recognition system, which can serve the need of diverse applications in information, communication, surveillance and security fields. Consequently, the present research means to build up an Automatic Partial Unique Fingerprint Recognition System, which also takes care of template protection to validate a person.

Fingerprint Hash code does not gives full security or authentication purpose but combined with other security elements like password or OTP in order to enhance security. Fingerprint Hash code acts as a key, which can uniquely identify every person. Therefore, it can be replaceable with user-id or username and can work along with text-based, picture based, or pattern based passwords.

This book contains research articles related to Fingerprint image enhancement, recognition and Hash code generation methods. This book also contains applications of Multifactor authentication model using Fingerprint Hash code, OTP and Password and compares this new model with existing similar systems. These papers published already in peer-reviewed International Journals. This Book has written with an intention to get all papers together under one roof, which will benefit all the researchers of related areas.

ABOUT THE AUTHOR

Mr. Krishna Prasad K**.** is belonging to Mangaluru, India born on **25th May 1983**. He received his **M.Sc.** (5 years Integrated Course) degree in Information Science from Mangalore University in 2006, **M.Phil.** Degree in Computer Science from Madurai Kamaraj University in 2009 and **M.Tech.** in Information Technology from Karnataka State Open University (KSOU) in 2013 respectively. Presently he is doing his part time **Ph.D.** in the field of Biometric Fingerprint Hash code generation methods in Srinivas University, Mangaluru, India. Since June 2006, he is working in College of Computer and Information Sciences, Srinivas University, City Campus, Pandeshwar, Mangaluru and designated as Assistant Professor in 2014. He is having 12 years of teaching experience in different Computer Science subjects for BCA and MCA courses.

Currently he is working as **Assistant Professor** in College of Computer and Information Sciences, Srinivas University, City campus, Pandeshwar, Mangaluru, India. He has conducted many Guest Lectures in **Vedic Mathematics** and **Shortcut tricks for Competitive Examinations** in and around Dakshina Kannada District of Karnataka State, India. His research interest includes **Fingerprint Hash Code Generation Methods and Multifactor Authentication Model.** He was member of BOE of BCA in Mangalore University for six months in 2013 and for one year in 2017 and Paper setter and Evaluator in Mangalore University.

Mr. Krishna Prasad K. has published **31** research papers in referred international journals with more than 85 Google Scholar citations and Ranked **29** in Elsevier SSRN elibrary journal papers of last 12 months updated on 01 March 2018. He has also presented **18** papers in conferences, out of which **2** were International Conferences and remaining were National Conferences.

ACKNOWLEDGEMENTS

First of all, I derive immense pleasure in placing on record my deep sense of appreciation, gratitude and indebtedness to my research supervisor, **Prof. Dr. P. Sreeramana Aithal**, Vice Chancellor, Srinivas University, Mukka, Mangalore, for his all-round help in suggesting the problem, sustaining the interest, motivating, inspiring, and extending valuable guidance.

I am happy for the love and support I have had from **Sumana S**., my wife and **Abheeshta Krishna**, my son through the years of dreams, and making life truly exciting. I would like to thank my parents who have blessed me with great tolerance. I would like to thank my **Father-in-law**, **Mother-in-law**, and **Brother-in-law**, for their continuous support and motivation for completing my research work and for publishing same as a Book. I would like to thank my **brother** and **his family** for moral support. Without you all, things would have so much harder. I am wholeheartedly grateful to Sri. **CA. A. Raghavendra Rao**, President, A. Shama Rao Foundation, Mangalore and also Chancellor, Srinivas University, Mukka, Mangalore, for encouraging me by providing all facilities to carry out this work. I wish to express my sincere thanks to **Dr. P. Srinivas Rao**, Vice-president, A. Shama Rao Foundation, Mangalore and also Pro-Chancellor, Srinivas University, Mukka, Mangalore, for their support.

I am thankful to **Prof. P. Sridhara Acharya**, Coordinator, College of Computer and Information Sciences, Pandeshwar, Mangaluru, for moral support and encouragement. I am wholeheartedly thankful to **Mr. Mangesh Nayak**, Faculty, College of Computer and Information Sciences, Pandeshwar, Mangaluru for designing the cover page of my Book.

I also thank all my colleagues at Srinivas College, Pandeshwar, Mangalore, for their kind help and encouragement.

Last but not the least; I thank Almighty, who has made my life blissful. May his name be exalted, honored and glorified.

Chapter 1

A Conceptual Study on Image Enhancement Techniques for Fingerprint Images

Biometrics is an emerging field of research in recent years and has been devoted to the identification of individuals using one or more intrinsic physical or behavioral traits. Fingerprints are the prominent and widely acceptable biometric features compared to face, speech, iris, and other types of biometrics. Fingerprint characteristic or features are unique for everyone and which cannot change throughout the lifetime. Fingerprint biometrics is having applications in diverse fields like attendance system, criminology, mobile applications and logical access control system. This is the purpose behind the popularity of fingerprints as the biometric identifier. The biometric image captured through mobile supportive devices like the mobile camera or USB Fingerprint contains low-quality images. In fingerprint recognition system the quality of the image plays a very important role while matching two fingerprints. Most of the fingerprint recognition systems result in poor matching due to impurity or noisy images. So there is high necessity and scope for image preprocessing and enhancement techniques in order to improve the quality of fingerprint image and to obtain high accuracy in the matching process. In this paper, we discuss some approaches and methods for reducing noise or impurities and to improve the quality of the image before matching them. These techniques help the fingerprint recognition system to become robust and to obtain high quality in the matching process.

Keywords: Fingerprint, Ridge, Pattern, Enhancement, Thinning, Binarisation, Filtering.

1.1 INTRODUCTION

Biometrics is unique metrics related to human characteristics, which can be used for identification or authentication purpose as individual's claimed identity. Every human being can be recognized through observation of particular characteristics, which mainly involves different types as visual biometrics, chemical biometrics, auditory biometrics, behavioral biometrics, Olfactory or odor biometrics and spatial biometrics [1]. The qualities utilized for human distinguishing proof on the premise of their all inclusiveness, uniqueness, perpetual quality, quantifiability, and agreeableness. There are different biometric identifiers however fingerprints are the most broadly utilized among them. Fingerprints have two properties that are utilized for distinguishing proof:

i) Uniqueness: This property says that everybody has one of a kind fingerprint. No two people regardless of the possibility that they are twins can have same fingerprints. No two fingerprints on the same hand have ever been observed to be similar. The example of edges and valleys are distinctive for each person and for each finger.

ii) Permanence: This property says that the fingerprints of a man are changeless i.e. they don't change all through the lifetime of that individual. Regardless of the possibility that there is a scar on the finger of a man than the outline of the edges and valleys will recuperate after some time.

1.1.1 Definition of Fingerprint

A fingerprint is the pattern of lines called ridges and some special structures on the surface of finger called furrows. Ridges are combinations of ridge flow, ridge characteristics and ridge structure, which is common elements in all fingerprints and ride characteristics are unique called minutiae.

1.1.2 Features of Fingerprint

Fingerprint identification is one of the most important biometric technologies compared to other biometrics due to its popularity and widely available technologies, which has drawn a considerable amount of interest recently [2-3]. The unique feature of the fingerprint is determined by the local ridge characteristics called minutiae, which are one of the most important criteria used in fingerprint recognition system [4]. There are more than 150 minutiae characteristics are identified in the literature. These local ridge characteristics are not equally distributed. Minutiae are classified into two types based on minutiae points as ridge ending and bifurcation. Ridge ending starts at a point and ends in another point suddenly [5]. Bifurcation is the feature in which ridge starts from an arbitrary point and moves in a path and at any, some other arbitrary point splits into two paths or simply ridge forks. A good quality fingerprint image comprises of at least 50-100 minutiae.

Ridge ending and Ridge Bifurcation overlaid in fingerprint image Automatic fingerprint matching algorithm compares these local ridge characteristics (minutiae) and their relationship to obtain scores at the time of personal identification and verification. Two ridges are separated by low lines called valleys. The valleys and ridges are usually represented by white and black lines or colors in fingerprint images. There are another two characteristics of minutiae core and delta, which are used for matching of fingerprints. Core represents the

center from which ridge ending and ridge bifurcation or simply pattern are made. Delta is the point on friction ridge, at or nearest to the point of divergence of ridge ending and ridge bifurcation and which looks like the shape of delta symbol. Delta is also pointed from which Loop pattern, Whorl Pattern, and Arch pattern deviate. These are shown in Figure 1.1 and 1.2 respectively.

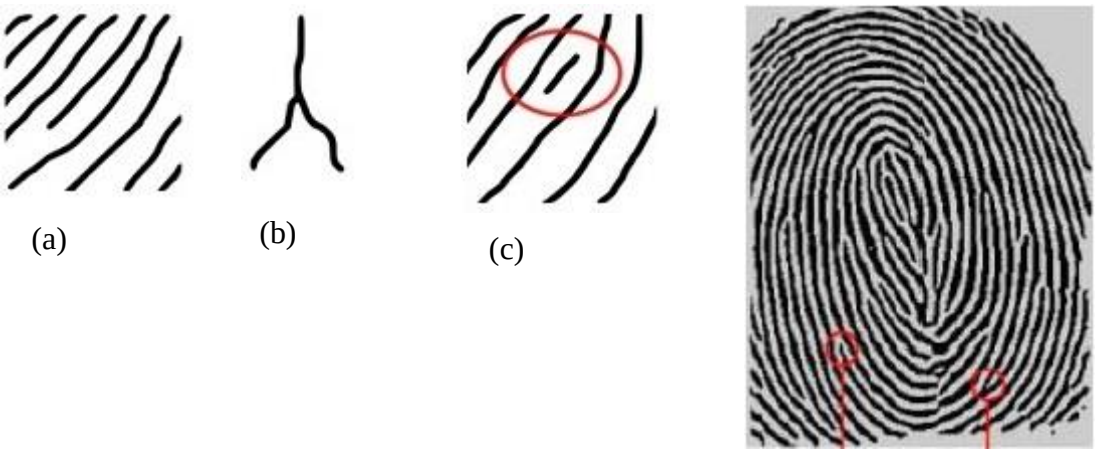


Figure 1.1: (a) Ridge ending (b) Bifurcation (c) Short Ridge (Dot) (d) Ridge ending and Ridge Bifurcation overlaid in fingerprint image

Loop pattern: Ridges enters from either side of the impression or pattern, re-curves or touches an imaginary line drawn from delta to the core and terminates on the same side from where it's originated.

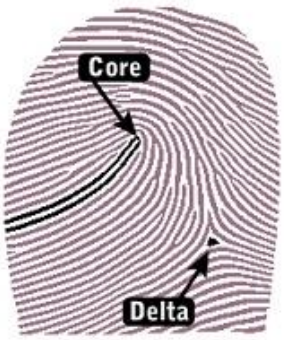


Figure 2: Core and delta of fingerprint image

There are two types of Loop patterns; they are Ulnar Loop patterns and Radial Loop patterns. Ulnar Loop patterns are like a waterfall flowing towards the right with triangular points.

Radial Loop patterns are opposite to Ulnar Loop patterns flowing towards left and shape is like a waterfall. In Arch, pattern ridges start from one side of the fingerprint pattern to another side without doing backward turn. Tented Arch is like a camping tent with sharp endings. Delta is not involved in Arch patterns. Whorl pattern consists of series of circles which starts from an arbitrary point and ends at the same point. In Concentric Whorl designs line begins from the focal point of the little circle, the lines on the fingertip gives off an impression of being little circles and spreads out like concentric circles with two triangle points.

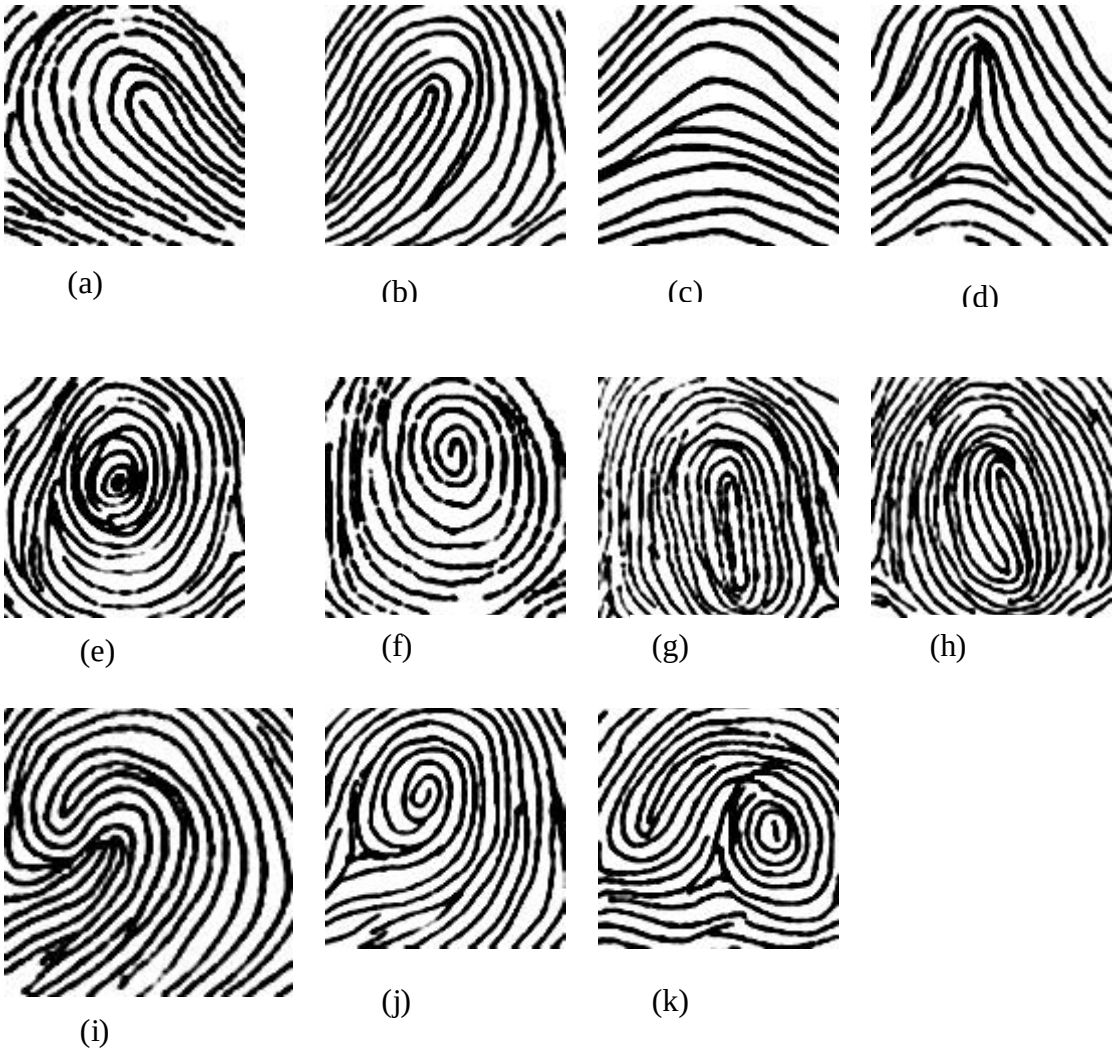


Figure 1.3: Basic patterns of fingerprints- (a) Ulnar Loop (b) Radial Loop (c) Simple Arch (d) Tented Arch (e) Concentric Whorl (f) Spiral Whorl pattern (g) Press Whorl (h) Imploding Whorl (i) Composite Whorl (j) Peacock's Eye (k) Variant pattern

A spiral Whorl pattern consists of a winding model beginning from the inside and moves outward, has two triangular focuses. In Press Whorl patterns, like the whorl design, yet the circle transforms into a long oval shape, has two triangular focuses. Imploding Whorl patterns contains jujitsu or spiral like patterns in the center, encompassed by multi-layers of the circle. Composite Whorl patterns are similar to imploding Whorl without multi layered

circle surrounding it. Peacock's Eye pattern from the inside would appear that a peacock's eyes and lips; the middle comprises of more than one circle or winding, the finish of each ring is associated in a straight line. It has two triangular focuses; one further and the other nearer to the inside. Variant pattern frequently has the mix of at least two of whorls, ulnar circles, or basic curves, with at least two triangle focuses. Basic pattern of Fingerprint image are shown in Figure 1.3.

1.1.3 Fingerprint Recognition

Fingerprint recognition system utilizes two types datasets called as training data set and test datasets. The training dataset is used for training purpose, initially, the fingerprint image is preprocessed and enhanced and later features are extracted and stored as a template. In test datasets, the same process is repeated but the template is not stored and just compared with the already stored template and matching score is calculated by utilizing an automated computer system. The stored features are compared for one to one match called verification and one-to many called as identification [6].

1.2 RELATED WORK

L. Hong et al. [7] proposed a fast fingerprint enhancement algorithm, which depended on ridge orientation and frequency and through that, they can able to obtain more clear ridge and valley structure of the initial fingerprint image. They have evaluated the performance of fingerprint enhancement algorithm using goodness index and found that incorporating enhancement algorithm improves verification accuracy. Sharat S. Chikkerur et al. [8] proposed a new approach for fingerprint enhancement based on Short Time Fourier Transform (STFT) Analysis, mainly used for non-stationary properties. The algorithm evaluated all inherent features of the fingerprint image and found that performance of the algorithm improved slightly better. The Three inherent features are foreground region mask, local ridge orientation, and local frequency orientation. Sebastian et al. [9] proposed an algorithm for fingerprint minutiae based on CLAHE (Contrast Limited Adaptive Histogram Equalization). Their primary intention was to know the performance of combining Clip Limit, standard deviation, and sliding neighborhood, three techniques for the fingerprint enhancement. Through a simulated investigation, paper stimulates for developing thinning process and enhancement of the image. S.Greenberg et al. [10] compare the detection and analysis of minutiae through fingerprint image binarisation and direct extraction of minutiae from gray scale fingerprint images. They used Histogram equalization, Wiener filtering, and image binarisation as first method and unique anisotropic filter for direct gray scale enhancement as the second method in order to compare binarisation and direct extraction of minutiae from gray scale image techniques with an ultimate goal to achieve image enhancement. They found that both methods show significant improvements in terms of efficiency and execution time.

Y. He et al. [11] studied, analyzed and proposed a new algorithm based on orientation fields for image enhancement. In order to reduce noise and to obtain a high-quality image and to obtain better matching results, image enhancement and minutiae matching are two important

steps in auto computer assisted fingerprint recognition system. D. K. Misra et al. [12] developed a method for fingerprint image enhancement based on Fourier cosine transform and matching of fingerprint image based on region and line structure that live between minutiae pairs.

Jianwei Yang et al. (2002) [13] improved the existing algorithm for fingerprint feature extraction by extracting minutiae directly from an original gray level image without undergoing steps of binarisation and thinning and obtained considerable better performance in efficiency. Jianwei Yang et al. (2003) [14] introduced novel filter design method for fingerprint image enhancement using Traditional Gabor Filter (TGF) of the invention to overcome drawbacks in image dependent parameter selection strategy. They have modified existing Traditional Gabor Filter as Modified Gabor Filter (MGF). Their algorithm achieved a remarkable advantage in preserving fingerprint image structure and in image enhancement consistency. C. Lee et al. (2006) [15] studied recognition of fingerprint image captured by a mobile camera. In segmentation of fingerprint regions from background images, they concentrated on three aspects which include texture, color, and size information. They proposed a robust regression method to overcome the drawbacks of gradient based filtering inability to remove outliers. In the pre-processing stage, they divided the fingerprint images into small blocks and verified blocks quality using good or bad quality regions. Their pre-processing algorithm and experimental results showed good performance compared to conventional ones.

1.3 IMAGE ENHANCEMENT TECHNIQUES

Fingerprint image enhancement techniques mainly focus on reducing noises as much as possible in training datasets image or selected image and to obtain high scores in the matching process. The accuracy of the test datasets image directly depends on the quality of the image in training dataset. Because of this purpose, the good quality image is an essential and basic requirement for the improved results of matching. But this is not so easy or possible to obtain a good quality image almost all the time due to skin problems, scars on fingers. These wounds or cuts may end up with false minutiae results even in the good quality image. The error or noisy fingerprint image cannot able to provide all features at the time of feature extraction, either it may give wrong data or may not give required features only. Looking into all these aspects, fingerprint image pre-processing or enhancement becomes necessary and essential. There are many fingerprint enhancing techniques are available in the literature, an overview of these techniques are explained in this paper [17].

1.3. A. Histogram Modeling:

The histogram of the fingerprint image represents, how often or number of times a gray level occurs in a group of total gray levels of the image. The output image produced by the histogram contains noisy in terms of intensity levels. Histogram equalization is a special technique to adjust intensity or brightness and to enhance the contrast of the image. With the help of histogram equalization, we can get a uniform or identical histogram for the output

image. This technique is mainly used for improvement in contrast of an image by adjusting the individual gray level of the image. The results of the histogram are shown in Figure 1.4.

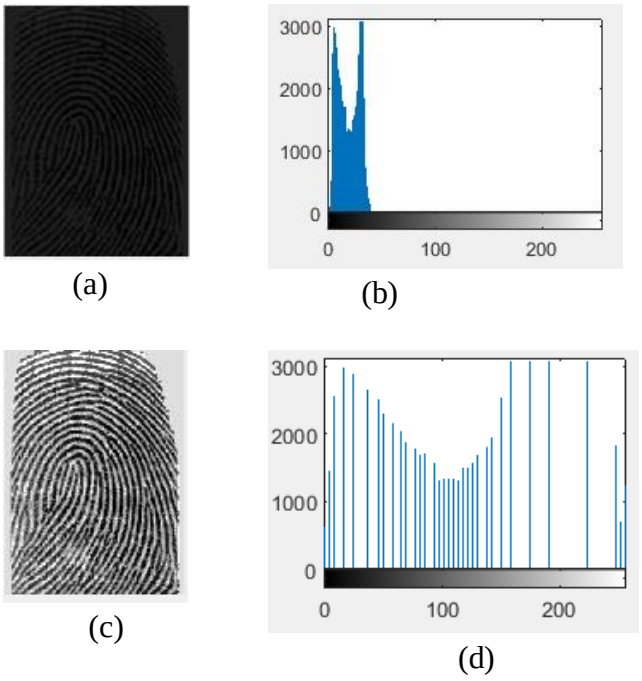
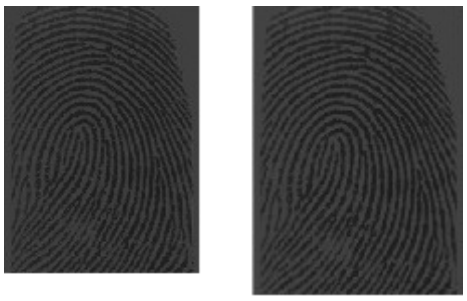


Figure 1.4: (a) Original image (b) Histogram of original image (c) Histogram equalized image (d) Histogram of equalized image

1.3. B. Filtering Methods

In fingerprint image recognition system, many filtering methods are available in the literature. These filtering methods ultimate purpose is to remove all types of error encountered in input or initial image and to improve the image recognition capacity in all aspects. Few methods are discussed below;

Median Filtering: Median filtering considers statistical median of the pixels contained in a window around the pixel and it is a nonlinear filtering process used to remove impulsive noise and to enhance the fingerprint image quality. Median filtering is shown in Figure 1.5.



(a) **(b)**

Figure 5: (a) Image before median filtering (b) Image after applying median filtering

Median is calculated as follows

$$V(m, n) = \text{median}\{y(m-k, n-1), (k,1) \epsilon W\}$$

Where W is the chosen Window. As like statistical figures, median filtering requires pixel values of the window should be arranged in order.

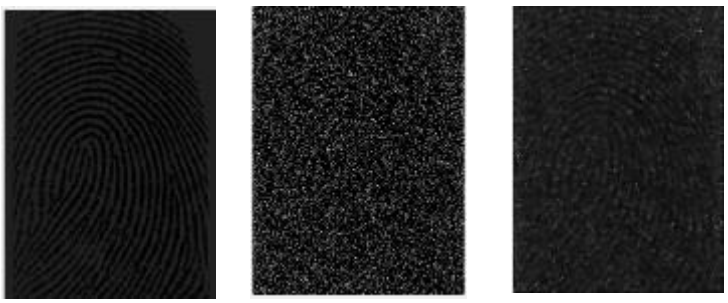
High Pass filtering: High pass filtering is basically used to extract edges of the images. High pass filter helps to improve the quality of the image by sharpening the edges of the fingerprint image. Due to this reason, it is always good practice to do high pass filtering for the original image. The high pass filtering simply removes or the blurred image from the original image. High Pass filtering is shown in Figure 1.6.

(a) (b)

Figure 6: (a) Image before High pass filtering (b) Image after applying High pass filtering

Weiner Filtering:

Weiner filtering produces a good quality image by removing additive noises even when the image is having blur or low intensity. It minimizes maximum error in the process of noise smoothing, to improve the quality of the image. Figure 1.6 shows Weiner Filtering.



(a) (b) (c)

Figure 1.6: (a) Original image (b) Image after applying Noise (c) Image after applying Weiner Filter

Gabor Filtering: Gabor channel is a linear channel whose impulse reaction is characterized by a harmonic function and the result is multiplied by a Gaussian function. Gabor filter ideally catches both local orientation and frequency information from a fingerprint image. Once the ridge orientation and ridge frequency are calculated, at that point they are utilized to build the Gabor filter. In fingerprint enhancement, Gabor filter can be aligned to a particular frequency and orientation values. Gabor filter can improve the ridges towards local orientation. Figure 1.5 shows Gabor filtering.

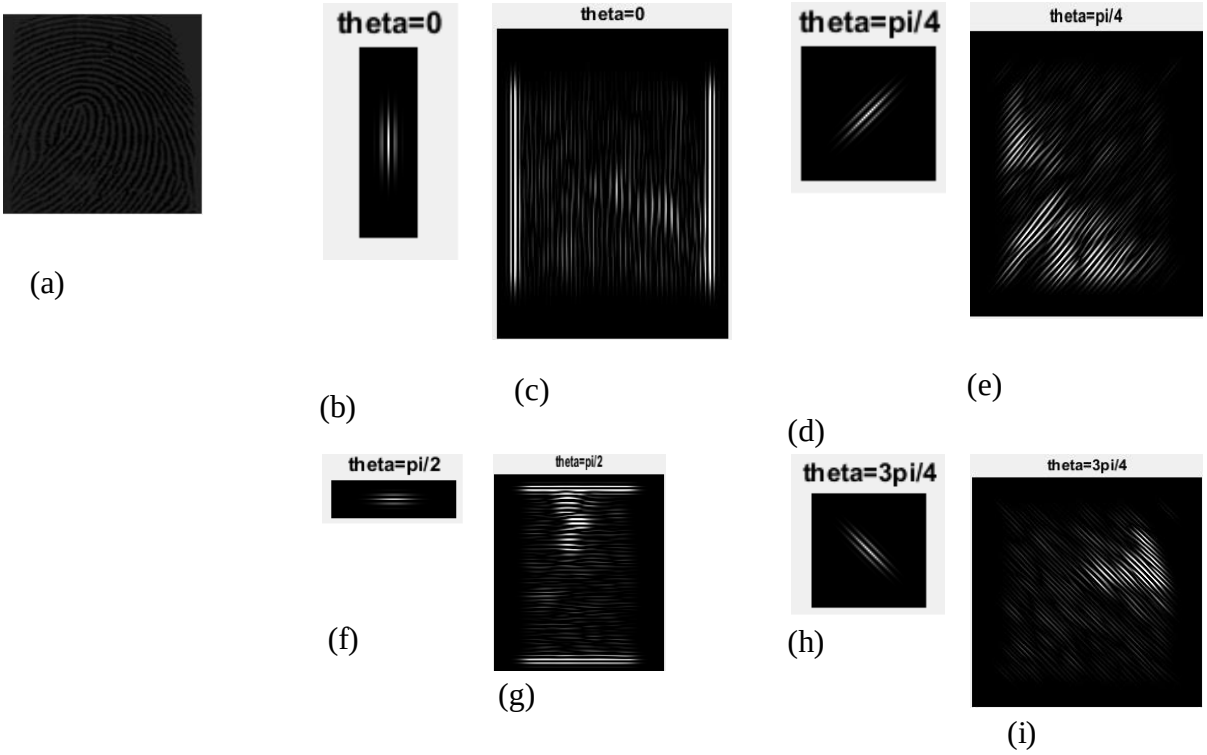


Figure 1.7: Gabor filtering size 7 × 7 and 4 orientations: - (a) Original Image (b) orientation-theta=0 (c) orientation-theta=$\frac{\pi}{4}$ applied to original image (d) orientation-theta=$\frac{\pi}{4}$ (e) orientation-theta=$\frac{\pi}{4}$ applied to original image (f) orientation-theta=$\frac{\pi}{2}$ (e) orientation-theta=$\frac{\pi}{2}$ applied to original image (f) orientation-theta=$\frac{3\pi}{4}$ (e) orientation-theta=$\frac{3\pi}{4}$ applied to original image

1.3. C. Binarisation and Thinning

Binarisation is one of the preprocessing stages in automatic fingerprint recognition systems. If the input image is a color image, first it should be converted into gray scale image. From the gray scale image, a binary image is obtained by considering only two states as zero for ridges, which are represented by black color and one for the valley, which is represented by white color. In binarisation, we preset some threshold for pixels and pixel which is lower and higher than is threshold is represented by white and black color respectively.

Thinning is a special process that consecutively wears away the foreground pixels and finally produces lines that are almost one-pixel width. The first and foremost condition for thinning is input image should be a binary image and produces output as a binary image. Thinning is a final prior step to minutiae extraction in automatic fingerprint recognition system. Thinning is not achieved in a single step but it achieved through an iterative process. The connectivity of ridges and bifurcation can be reproduced from the thinning, means it preserves the basic structure of the image without affecting its original structure. Figure 1.8 shows binarization and thinning process of original fingerprint image.

(a) (b) (c)

Figure 1.8: (a) Original image (b) Image after Binarisation (c) Thinning Image

1.4 CONCLUSION

In this paper, we have discussed basic concepts of fingerprint images and made a conceptual study on fingerprint image enhancement techniques. The diagram shown here are obtained by writing and running code in MATLAB. The fingerprint recognition system greatly affected by the quality of input image and if we apply image enhancement techniques on the input image, the noised can be reduced and also recognition system performance improved. Wish this paper could play an active role in image enhancement process in automatic fingerprint recognition system.

REFERENCES

[1] Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. IEEE security & privacy, 99(2), 33-42.

[2] Lee, H. C., Ramotowski, R., & Gaensslen, R. E. (Eds.). (2001). Advances in fingerprint technology. CRC press.

[3] Newham, E. (1995). The biometric report. SJB services, 733.

[4] Moenssens, A. A. (1975). Fingerprint techniques. Chilton.

[5] Lee, C., Lee, S., Kim, J., & Kim, S. J. (2006, January). Preprocessing of a fingerprint image captured with a mobile camera. In International Conference on Biometrics, Springer, Berlin, Heidelberg. 348-355.

[6] Krishna Prasad, K. and Aithal, P. S.(2017). A Conceptual Study on User Identification and Verification Process Using Face Recognition Techniques. International Journal of Applied Engineering and Management Letters (IJAEML), (ISSN Applied), 1(1), 6-17. DOI:http://doi.org/10.5281/zenodo.810343

[7] Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: Algorithm and performance evaluation. IEEE transactions on pattern analysis and machine intelligence, 20(8), 777-789.

[8] Chikkerur, S., Govindaraju, V., & Cartwright, A. (2005). Fingerprint image enhancement using STFT analysis. Pattern Recognition and Image Analysis, 20-29.

[9] Sepasian, M., Balachandran, W., & Mares, C. (2008, October). Image enhancement for fingerprint minutiae-based algorithms using CLAHE, standard deviation analysis and sliding neighborhood. In Proceedings of the World congress on Engineering and Computer Science 22-24.

[10] Greenberg, S., Aladjem, M., Kogan, D., & Dimitrov, I. (2000). Fingerprint image enhancement using filtering techniques. Proceedings of IEEE 15th International Conference on Pattern Recognition, 3, 322-325.

[11] He, Y., Tian, J., Luo, X., & Zhang, T. (2003). Image enhancement and minutiae matching in fingerprint verification. Pattern recognition letters, 24(9), 1349-1360.

[12] Misra, D. K., Tripathi, S. P., & Singh, A. (2012). Fingerprint image enhancement, thinning and matching. International Journal of Emerging Trends & Tech in Comp Science (IJETTCS), 1(2), 17-21.

[13] Yang, J., Liu, L., Jiang, T., & Fan, Y. (2002, August). An improved method for extraction of fingerprint features. In Proc. the 2nd Int. Conf. Image and Graphics, Anhui, PR China, 552-558.

[14] Yang, J., Liu, L., Jiang, T., & Fan, Y. (2003). A modified Gabor filter design method for fingerprint image enhancement. Pattern Recognition Letters, 24(12), 1805-1817.

[15] Lee, C., Lee, S., Kim, J., & Kim, S. J. (2006, January). Preprocessing of a fingerprint image captured with a mobile camera. In International Conference on Biometrics, Springer, Berlin, Heidelberg, 348-355.

[16] Misra, D. K., Tripathi, S. P., & Singh, A. (2012). Fingerprint image enhancement, thinning and matching. In International Journal of Emerging Trends & Tech in Comp Science (IJETTCS), 1(2), 17-21.

[17] Saini, A. (2012). Image enhancement techniques for fingerprint images. *International Journal of Emerging Trends and Technology in Computer Science*, 1(3), 215-17.

****

Chapter 2

Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image

Biometrics is the one most popular property in human distinguishing proof based on physical or behavioral features. The different physiological characteristics are Fingerprint, DNA, Face, hand, retina, ear features, and odor, where as behavioral characteristics or features are typing rhythm, gait, gesture, and voice with the basic premise that all are unique and all human beings are identified by these intrinsic traits. In the physiological traits, Fingerprint is most commonly utilized the biometric feature in diverse fields for identification and verification purpose. Fingerprint features can be separated into three noteworthy classifications in view of the granularity at which they are removed as level 1, level 2, and level 3 features. Level 1 feature contains macro details, which are easily extractable and include orientation filed, ridge frequency filed and pattern configuration. Only these global features or Level 1 features are not sufficient to uniquely identify or recognize, but if these features are used along with level 2 or level 3 features, that can make the fingerprint recognition system more robust and secure. Level1 features are used for image enhancement and orientation purpose. In this paper, we survey the existing literature on Level 1 features and try to analyze other researcher's contribution to this field.

Keywords: *Fingerprint Recognition, Ridge Orientation, Ridge Ending, Bifurcation, Level 1 Features*

2.1 INTRODUCTION

Fingerprint recognition is one of the interesting and complex image processing problems, which requires a constant and continuous contribution to new research from the research community. Even though the face recognition is automatic pattern recognition system and controlled by the computer, the performance of the system is directly dependent on the quality of the fingerprint images and the quality of the image capturing device [1]. Partial fingerprint image captured by the image acquisition device is yet another problem faced by the automatic fingerprint pattern recognition system. Level1 details may include general outlier structure of ridges like ridge flow and ridge pattern configuration [2]. Level 1 feature comprises of the orientation of the fingerprint, core-center from which ridge ending and ridge pattern is made named and delta location-point on the friction ridge and distinction of finger versus palm. As shown in figure 1, Level1 Features example includes Simple Arch, Tented Arch, Right Loop, Left Loop, Composite Whorl, Concentric Whorl, Imploding Whorl, Press Whorl, Spiral Whorl, Peacock's- Eye Whorl and Variant Whorl [3]. Loop pattern Ridges enters from either side of the impression or pattern, re-curves or touches an imaginary line drawn from delta to the core and terminates on the same side from where it's originated. In Arch, pattern ridges start from one side of the fingerprint pattern to another side without doing backward turn. Whorl pattern consists of series of circles which starts from an arbitrary point and ends at the same point [3]. With only Level 1 features, fingerprint recognition systems neither recognize the image nor identify or verify the image [4]. Level 1 feature is mainly used for classification, verification, filtering, and enhancement purpose and is shown in Figure 2.1.

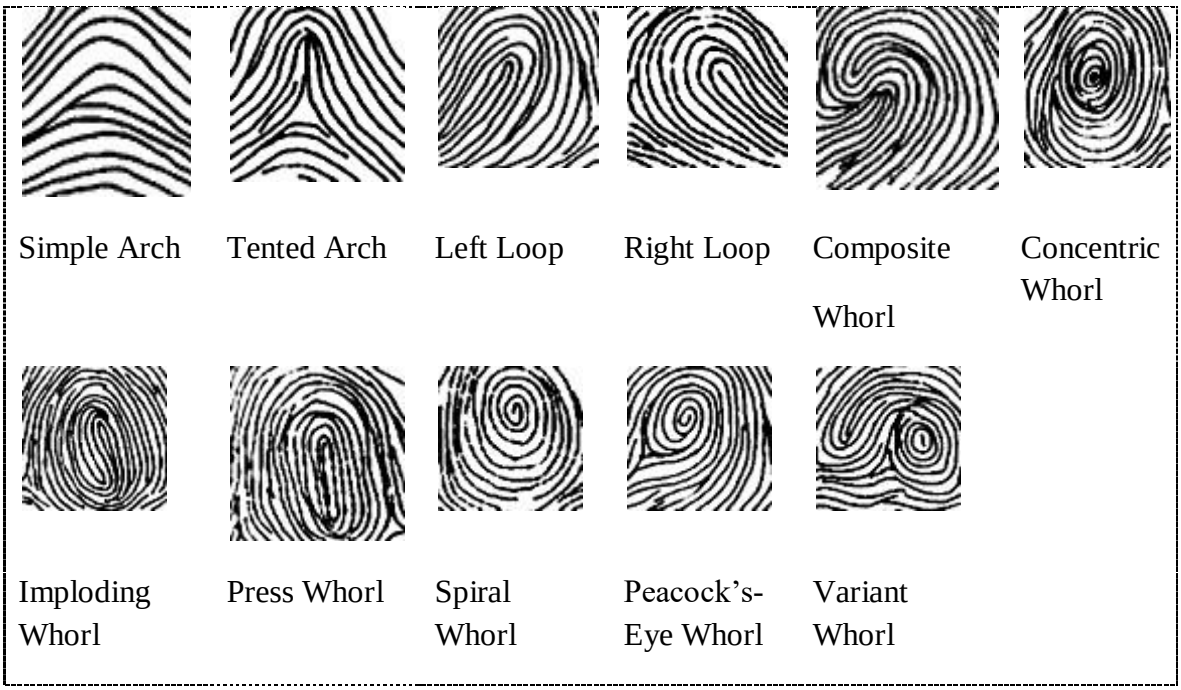
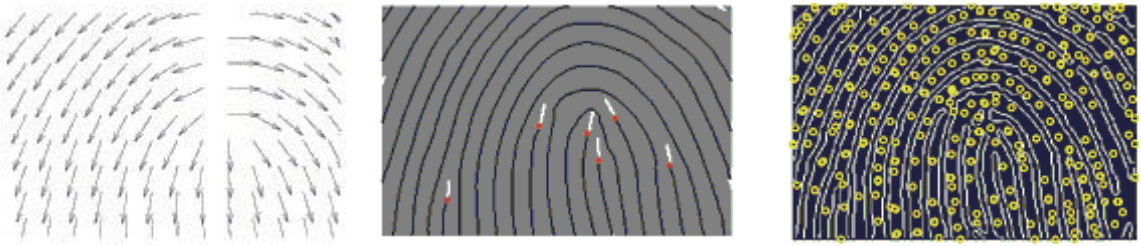


Figure 2.1: Fingerprint Level 1 Features-Examples [2-3]

The main purpose of Level 1 features- ridge pattern or flow and orientation are mainly used for image enhancement and orientation purpose, which will improve the quality of fingerprints. If the image contains noisy regions, it's difficult to define the orientation of the

image. Image enhancement techniques are essential or necessary due to the fact that, the image captured through sensor or optical device is not assured quality [4]. Fingerprint image enhancement is technically done by improving the quality of ride pattern or increasing the consistency of ridge orientation, which literally means level 1 feature, is exposed and analyzed. Ridge ending and ridge bifurcation or minutiae points are level 2 features. Micro details like pore and ridge contours form level 3 features. Figure 2.2 shows fingerprint features in terms of level 1, level 2, and level 3.



Level 1 **Level 2** **Level 3**

Figure 2.2: Three Levels Features of Fingerprint [5]

A fingerprint has several features, which are island (a line that runs or flows alone without touching other lines or regions), dot (an independent ridge which looks like a dot and equal in length and width), bridge or crossover (a small ridge which connects two parallel ridges), core (centre of the fingerprint pattern) and delta (a point from which fingerprint pattern alters or deviates). The unique features of a ridge, from which different pattern occurs are called minutiae. Ridge ending and ridge bifurcation are the two types of minutiae. A ridge ending is nothing but where ridge terminates or discontinue. Ridge bifurcation is a feature where a ridge splits or diverges, like a fork. From ridge ending and bifurcation, we can define several other features. The lake or enclosure is a feature in this ridge diverges and soon converges and becomes single ridge. Spur is yet another feature in which short ridge branching off a long ridge. Still, some other features like line unit, line fragment, eye, and hook also can be extracted and studied, which are referred as fingerprint low-level features. The low-level features are shown in figure 2.3.

Figure 2.3: Low- level Features of Fingerprint image [5]

Level 2 features show various ways ridge points can be irregular. Minutiae are most reliable features, which are permanent and unique for every human being unless and until some

wound or permanent damage occurs. The number of minutiae points collected should be more to get high efficiency. Examples of level 2 features are shown in Figure 2.4.

Figure 2.4: Examples of Level 2 features of fingerprint [6]

In this paper, we discuss the contribution of other researchers in feature extraction process of fingerprint images using Level 1 or Level 2 features or sometimes both, and how these features are helpful in broad classification of fingerprint images or in the enhancement of images by reducing noise. We also do a quantitative analysis of fingerprint image enhancement using a table which lists Author name, Exposed feature level, Approaches/ Techniques used, and Benefits as its columns.

2.2 LITERATURE REVIEW

This section narrates work done by other researchers to Fingerprint enhancement through classification using Level 1 or Level 2 features or sometimes both. In this section, the contributions of all researchers to the field of fingerprint image enhancement using Level1 features are summarized.

Sherlock et al. (1994) [7] proposed image enhancement algorithm based on nonstationary directional Fourier domain filtering. The directional filter used first and foremost to smooth the input image whose orientation in all fields matched to the local ridge orientation. The output of this stage is reduced noise image or high-quality image compared to the input image. Fourier Domain filtering mainly uses local ridge patterns and local ridge parameters, directional band pass filters, and local ridge spacing. To implement the filtering techniques in the digital computer the image must be spatially sampled and the continuous function used in Fourier Transform is replaced by discrete functions. All images were sampled at a low resolution of 512 by 512 pixels and edge effects of discrete Fourier Transform were reduced to 10% using separable split-cosine window. The result of the enhancement used for various classifications of the input images. A comparison is made between enhancements used in automated fingerprint identification system developed by the UK home office and enhancements made based on this filter method and the later one showed significant advances in speed, accuracy, and efficiency of the automated fingerprint identification system. Chikkerur et al. (2005) [8] proposed fingerprint enhancement using Short Term Fourier Transforms (STFT), which is based on not stationary signals. In this paper, researchers extended the properties of STFT to two dimensional (2D) fingerprint images. They proposed a new algorithm for image enhancement process based on contextual filtering in Fourier domain. The new algorithm simultaneously yields local ridge orientation and local ridge frequency level 1 feature. The intrinsic features of the fingerprint image can be computed using single unified approach rather than multiple algorithms. Compare to other image

processing algorithm like local/windowed processing, more formal approach for analyzing the non-stationary fingerprint image.

Hsieh, C. T. et al. (2003) [9] proposed an effective and efficient algorithm for fingerprint image enhancement, which not only improves the quality of the clarity of the image but also improves the continuity of the ridge structure based on global texture and local orientation. The global texture is exposed using multi resolution analysis and local orientation through wavelet transforms. In wavelet based fingerprint analysis first input image is converted into normalized image. Normalized image is decomposed using wavelet decomposition. Wavelet decomposition image is processed again using global texture filtering. Next Local directional compensation is done and finally, wavelet reconstruction process is achieved. Normalization, Wavelet decomposition, Global texture filtering, Local directional compensation, wavelet reconstruction are the flowchart components of proposed enhancement algorithm. Their Experiment results show that enhanced image using wavelet based enhancement algorithm out performed in terms of efficiency and execution time in improving minutiae detection. Paul & Lourde (2006) [10] proposed the new method for image enhancement using the applications of wavelet transforms. Before the inventions of these techniques, popular other techniques were Gabor filtering and Fourier filtering. The new method outperformed compared to this method in terms of efficiency and execution time.

Ye et al., 2007 [11] additionally utilized a 2D discrete wavelet transform to digitally compress fingerprint and to reconstruct the original image, whenever necessary using some reconstructing attributes. Few quantitative measurements are used to evaluate the quality of wavelet transform, which helps in image enhancement process. In this paper researcher also used a different measure to evaluate the performance of wavelet transform and obtained higher efficiency. Farina et al., (1999) [12] worked on a binary image, the input is either already taken as a binary image or converted into binary from the grayscale image and also the image is skeletonized. Due to differences in a number of minutiae occur in real, there is a necessity of post pre-processing, in order to maintain the consistency of image and to reduce the computational cost. They also proposed a new method for ridge cleaning based on ridge positions. In order to validate endpoints and bifurcation, they used two novel approaches and related algorithm. The presented minutiae extraction algorithm performs well in dirty areas and on the backgrounds.

Maio and Maltoni, 1997 [13] focused on the extraction of ridge ending and bifurcation called as minutiae directly from the gray-scale image rather than converting it into the binary image and then extracting minutiae. The new techniques were based on ridge line following algorithms and algorithm follows or goes parallel along with ridge line until ridge ending or bifurcation occurs. They compared their algorithm with those known approaches, which converts the original image into binary image and new method showed superiority in terms of efficiency and robustness.

Hong et al. (1998) [14] presented a fast fingerprint enhancement algorithm based on level features like fingerprint ridge pattern and orientation and substantially improve the quality of

ridge and furrow structures on the estimated local ridge orientation and frequency. This is one of most cited journal paper in image enhancement process. They have evaluated the performance of the image enhancement algorithm using goodness index evaluation criteria of minutiae and by comparing the accuracy of online fingerprint system for verification purpose. They used Gabor filter to tune local ridge orientation and ridge frequency.

Gabor Filters (Gabour, 1946 [15]) combines both frequency domain and spatial domain with a better-combined resolution by utilizing both frequencies selective and orientation selective. Gabor filters help to retain the true valley and ridge structure and also helps to remove maximum noise involved in the input image. Hong et al. (1996) [16] proposed new fingerprint enhancement algorithm which comprises of different phases as orientation filed estimation, ridge extraction, and minutiae extraction and preprocessing. These phases help to decompose input image to set of filtered image. Yang et al. (2003) [17], authors proposed novel filter method for fingerprint image enhancement by considering traditional Gabor Filtering as the inspiration for their work. They mainly developed with the intention to overcome the flaws encountered in traditional Gabor filter and name it as Modified Gabor Filter (MGF) with parameter selection scheme is image independent. Experimental results showed that MGF reduces False Rejection Rate (FRR) by 2% and False Acceptance Rate (FAR) of 0.01%.

Greenberg et al. (2000) [18] proposed two methods for fingerprint image enhancement, out of which one method is histogram equalization and the other one is an anisotropic filter for direct grayscale enhancement without converting to a binary image. The result achieved is compared with some other similar image enhancement algorithm, and new algorithm outperformed in terms of efficiency and time required. Wu et al. (2004) [19] proposed a new method for image enhancement, by integrating Anisotropic filter and Directional Median Filter (DMF). Anisotropic filter and DMF are used to reduce Gaussian distributed noise and impulse noise. DMF helps to join broken fingerprint ridges, corrects the holes of fingerprint images, and smoothes irregular ridges. In order to implement and test the algorithm, FVC2000 database were used. They compared their new algorithm with the already existing similar algorithm and results showed good performance in efficiency and execution time.

Teddy and Martin (2002) [20] demonstrated spatial analysis techniques for latent fingerprint image enhancement. The latent fingerprint is not good in quality which includes some degrade quality like blurred, incomplete or partial and also their spatial definition is not clear. In order improve the quality and thereby by achieving classification or comparison, they used some nonlinear filters and frequency domain filters along with high-pass Butterworth filter with the aid of adaptive fast Fourier transform for enhancement of the degraded image. Fingerprint captured using ink or live scan usually requires only spatial filtering like brightness, contrast, and color map adjustment to examine the level 2 features.

E-Kyung and Bae (2006) [21] proposed an adaptive filter according to different conditions of the input image which are oil, dry, and neutral instead of the uniform image. To identify oil/dry/neutral image five features are used which are mean, variance, block directional

difference, ridge and valley thickness ratio, and orientation change. In adaptive filtering first, several features of the image are extracted and then it is fed into clustering module and then adaptive filtering is applied on clustering to produce a good quality image. For clustering wards clustering method is used. After clustering, once the image is processed depending on the image characteristics, for oily images valleys are improved by expanding thin and detached one, for dry images ridges are enhanced by extracting their center lines and removing white pixels.

Chengpu et al. (2008) [22] proposed an effective robust algorithm for fingerprint enhancement and firstly, used contrast stretching approach to improve the clarity between foreground and background of the fingerprint image. Secondly, to improve the orientation estimation utilized the structure of the tensor property. Finally, in order to take the advantages both Gabor filter and diffusion filter, they are combined and adopted low pass filter at the direction that is parallel to the ridge and used band pass filter at the direction perpendicular to the ridge. Wang, Li, Huang, & Feng, 2008 [23] introduced log Gabor filter in order to overcome drawbacks of the traditional Gabor filter and to promote and improve fingerprint enhancement performance. The result showed good performance and efficiency compare to traditional Gabor filter. Yuanyuan (2012) [24] proposed new image enhancement algorithm based on elliptical Gabor filter. The ridge information on the fingerprint is used for determining the range of filtering dynamically. Estimating the degree of curvature and the frequency of fingerprint ridge in local areas are used for accomplishing elliptical Gabor filter. To correct errors in the input image and to obtain more precise enhancement, elliptical Gabor filter is used. The experimental results show that the precision of minutiae extraction is significantly improved and which results in good and higher accuracy rate of the subsequent operations are also improved.

Babatund (2012) [25] modified some of the existing sub-models mathematical algorithms for fingerprint image enhancement and obtained new version. The different sub models of the new version are segmentation, normalization, ridge orientation estimation, ridge frequency estimation, Gabor filtering, and Binarization and Thinning. In order to test this new version, the author used windows vista home basic operating system and Matrix Laboratory (Matlab) as Frontend engine. Synthetic fingerprint and real fingerprint were used while testing in FVC2004 fingerprint database DB3. The new version performed well in terms of efficiency and some other commonly used performance evaluation matrices.

Saatci & Tavsanoglu (2003) [26] concentrated on the segment by segment analysis of the fingerprint pattern results in various ridge directions and frequencies. To match ridge features at each point authors used directional filter along with correct filter parameters and which resulted in effective fingerprint ridge enhancement. Researchers used main technique or method for image enhancement is Cellular Neural Network (CNN) Gabor type filters. He, Tian, Luo, & Zhang, (2003) [27] developed fingerprint image enhancement algorithm based on orientation fields with three aspects as ridge information for minutiae matching process in a simple and effective way, use of variable sized boundary boxes, and use of simpler alignment method. The first aspect overcomes the problem of reference point per selection

with low computational cost. The second aspect makes the algorithm more robust to nonlinear deformation between fingerprints. The third approach reduces the complexity of alignment.

2.3 QUALITATIVE ANALYSIS OF FINGERPRINT LEVEL 1 AND LEVEL 2 FEATURES ENHANCEMENT

Fingerprint image enhancement is one of the main process or stage of Automatic Fingerprint Recognition System. The performance of fingerprint recognition system is depending on the quality of the input image. Partial fingerprint draws special attention for fingerprint image enhancement, due to its inherent properties like broken, cut, damage or noisy. So there is a great necessity of image enhancement process in order to enhance the performance of automatic fingerprint recognition system. This section presents different approaches to image enhancement using level 1 or level 2 or both features of the fingerprint image. Table 1 gives a detailed description of fingerprint image enhancement algorithms or methods. Most of the algorithms consider either Level 1 or Level 2 or both features for image enhancement purpose. The Table 2.1 narrates Author name, Exposed Features, Approaches/Techniques, and Benefits, of fingerprint image enhancement algorithms.

Table 2.1: Comparative Analysis of Fingerprint Image Enhancement by extracting Level 1 and Level 2 Features

Authors	Exposed Features (Level/s)	Approaches /Techniques	Benefits
Sherlock et al. (1994) [7]	Level 1	Directional Fourier Domain Filtering	Demonstrates the usefulness of position-dependent Fourier domain in processing of images Significant improvements in the speed and accuracy of AFIS
Chikkerur et al. (2005) [8]	Level 1	Short Term Fourier Transforms, Contextual filtering in Fourier domain	Fingerprint image can be computed using single unified approach. More formal approach for analyzing the non-stationary fingerprint image.
Hsieh, C. T. et al. (2003) [9]	Level 1 & Level 2	Wavelet Transform, Gabor Filters	Enhanced image using wavelet based enhancement algorithm out performed in terms of efficiency and execution time in improving minutiae detection. Images are normalized and reduced noise.
Paul & Lourde (2006) [10]	Level 1 & Level 2	Wavelet Transform, Gabor Filters,	Enhanced performance, efficiency, and execution time compared to traditional Gabor filter and Fourier filter

Ye et al., 2007 [11]	Level 1 & Level 2	Wavelet Transform, Gabor Filters,	Quantitative measurements used to evaluate the quality of wavelet transform helps in image enhancement process. Enhanced performance and efficiency
Farina et al., (1999) [12]	Level 2 & Level 1 (partially)	Binarisation	Reduced computational cost due to post pre-processing. Ridge cleaning based on ridge positions
Maio and Maltoni, 1997 [13]	Level 2	Gray scale image is directly processed	Compared to known approaches, which converts the original image into binary image and new method showed superiority in terms of efficiency and robustness.
Hong et al. (1998) [14]	Level 1	Ridge pattern and orientation, Goodness Index, Gabor Filter	Fast fingerprint enhancing algorithm. Local ridge orientation and ridge frequency which improves the performance of the matching process.
Gabour, 1946 [15])	Level 1 & Level 2	Gabor filter, frequency domain, spatial domain	Helps to retain the true valley and ridge structure and also helps to remove maximum noise involved in the input image.
Hong et al. (1996) [16]	Level 1 & Level 2	Gabor Filter	Helps to decompose input image to set of filtered image. Comprises of different phases as orientation filed estimation, ridge extraction, and minutiae extraction and preprocessing.
Yang et al. (2003) [17]	Level 1 & Level 2	Modified Gabor Filter (MGF)	MGF reduces False Rejection Rate (FRR) by 2% and False Acceptance Rate (FAR) of 0.01%.
Greenberg et al. (2000) [18]	Level 1 & Level 2	histogram equalization and Anisotropic filter	Direct grayscale enhancement without converting to a binary image. New algorithm outperformed in terms of efficiency and time required.
Wu et al. (2004) [19]	Level 1 & Level 2	Anisotropic filter and Directional Median Filter (DMF).	Reduced Gaussian distributed noise and impulse noise. DMF helps to join broken fingerprint ridges, corrects the holes of fingerprint images, and smoothes irregular ridges. Showed good performance in efficiency and execution time compared to the similar type of algorithms.
Teddy and Martin	Level 1 & Level 2	Nonlinear filters, Frequency	Handles efficiently images of a type like blurred, incomplete or partial and un

(2002) [20]		domain filter, High pass Butterworth filter, adaptive fast Fourier transform	clear spatial definition.
E-Kyung and Bae (2006) [21]	Level 1	Adaptive Filtering, mean, variance, block directional difference, ridge and valley thickness ratio, and orientation change	Able to recognize and enhance different conditions of input image, which are oil, dry, and neutral instead of uniform image.yu
Chengpu et al. (2008) [22]	Level 1	Contrast stretching, tensor property, Gabor filter and diffusion filter	Improves the clarity between foreground and background of the fingerprint image. Improves the orientation estimation. Takes the advantages of both Gabor filter and diffusion filter.
Wang, Li, Huang, & Feng, 2008 [23]	Level 1 & Level 2	Log Gabor filter	Overcomes the drawbacks of traditional Gabor filter Improves fingerprint enhancement performance.
Yuanyuan (2012) [24]	Level 1 & Level 2	Elliptical Gabor filter	The experimental results show that the precision of minutiae extraction is significantly improved. Improved quality minutiae result in good and higher accuracy rate of the subsequent operations are also improved.
Babatund (2012) [25]	Level 1	Modified sub-models of mathematical model- Segmentation, Normalization, Ridge orientation estimation, Ridge frequency estimation, Gabor filtering, and Binarisation and Thinning	The new version of modified sub-models of mathematical models performed well in terms of efficiency and some other commonly used performance evaluation matrices.
Saatci &	Level 1	Segmentation,	Resulted in effective fingerprint ridge

Tavsanoglu (2003) [26]		Directional filter, Cellular Neural Network (CNN) Gabor type filters	enhancement. High performance.
He, Tian, Luo, & Zhang, (2003) [27]	Level 1 & Level 2	Orientation fields as ridge information, variable sized boundary boxes, simple alignment method	Orientation fields as ridge information, variable sized boundary boxes, simple alignment method are three important aspects. Overcomes the problem of reference point per selection with low computational cost. Robust to nonlinear deformation between fingerprints. Reduces the complexity of alignment.

2.4 CONCLUSION

Fingerprint image enhancement is one of the important steps in Automatic Fingerprint Identification System. The fingerprint recognition system performance always depends on the quality of fingerprint input image. Fingerprint image enhancement is technically done by improving the quality of ride pattern or increasing the consistency of ridge orientation, which literally means level 1 feature, is exposed and analyzed. Ridge ending and ridge bifurcation or minutiae points are level 2 features, which is also sometimes exposed and analyzed for enhancement purpose. In this paper, we have surveyed earlier works in fingerprint image enhancement of about 21 authors. The different methods used for image enhancement are wavelet transform, Gabor Filter, Log Gabor filter, Directional filter, Elliptical Gabor filter, Adaptive Filtering and much more similar types of filtering techniques. All the 21 authors focus on image enhancement techniques and depict that its very essential in order to get high quality in image recognition or automatic matching process, especially in noisy, wound or damaged fingerprint image.

REFERENCES

[1] Virdi, M. K. (2014). Fingerprint Matching System for Spurious Minutiae. *Journal of Basic and Applied Engineering Research*, 1(11), 50-53.

[2] Dermatoglyphics.org. (2017). *11 Basic Patterns of Fingerprint* [online] Available at: http://dermatoglyphics.org/*11 Basic Patterns of Fingerprint* / [Accessed 17 July. 2017].

[3] Karani, K. P., Aithal, P. S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),*1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[4] Krishna Prasad, K. and Aithal, P. S.(2017). A Conceptual Study on User Identification and Verification Process Using Face Recognition Techniques. International Journal of

Applied Engineering and Management Letters (IJAEML), (ISSN Applied), 1(1), 6-17. DOI:http://doi.org/10.5281/zenodo.810343.

[5] https://images.google.com/. (2017). *Google*.[online] Available at: https://images.google.com/Low level features of fingerprint [Accessed 18 July. 2017].

[6] https://images.google.com/. (2017). *Google*.[online] Available at: examples of level 2 features of fingerprint [Accessed 19 July. 2017].

[7] Sherlock, B. G., Monro, D. M., & Millard, K. (1994). Fingerprint enhancement by directional Fourier filtering. *IEE Proceedings-Vision, Image and Signal Processing*, *141*(2), 87-94.

[8] Chikkerur, S., Cartwright, A. N., & Govindaraju, V. (2007). Fingerprint enhancement using STFT analysis. *Pattern recognition*, *40*(1), 198-211.

[9] Hsieh, C. T., Lai, E., & Wang, Y. C. (2003). An effective algorithm for fingerprint image enhancement based on wavelet transform. *Pattern Recognition*, *36*(2), 303-312.

[10] Paul, A., & Lourde, R. (2006). *A Study on Image Enhancement Techniques for Fingerprint Identification*. *2006 IEEE International Conference on Video and Signal Based Surveillance*. https://doi.org/10.1109/AVSS.2006.14

[11] Ye, Z., Mohamadian, H. and Ye, Y. (2007) Information Measures for Biometric identification via 2D Discrete Wavelet Transform, Proceedings of the 3rd Annual IEEE Conference on Automation Science and Engineering Scottsdale, AZ, USA, Pp. 22- 25

[12] Farina, A., Kovacs-Vajna, Z. M., & Leone, A. (1999). Fingerprint minutiae extraction from skeletonized binary images. *Pattern recognition*, *32*(5), 877-889.

[13] Maio, D., & Maltoni, D. (1997). Direct gray-scale minutiae detection in fingerprints. *IEEE transactions on pattern analysis and machine intelligence*, *19*(1), 27-40.

[14] Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, *85*(9), 1365-1388.

[15] Gabor, D. (1946) Theory of communication, Journal of IEE, 92, 429-457.

[16] Hong, L., Jain, A.K., Pankanti, S. and Bolle, R. (1996) Fingerprint enhancement IEEE, 5, 202-207.

[17] Yang, J., Liu, L., Jiang, T., & Fan, Y. (2003). A modified Gabor filter design method for fingerprint image enhancement. *Pattern Recognition Letters*, *24*(12), 1805-1817.

[18] Greenberg, S., Aladjem, M., Kogan, D., & Dimitrov, I. (2000). Fingerprint image enhancement using filtering techniques. In *Pattern Recognition, 2000. Proceedings. 15th International Conference on* (Vol. 3, pp. 322-325). IEEE.

[19] Wu, C., Shi, Z., & Govindaraju, V. (2004). Fingerprint image enhancement method using directional median filter. In *Proc. of SPIE Vol* (Vol. 5404, p. 67).

[20] Teddy, K. and Martin, L. (2002) Fingerprint Enhancement by spectral analysis techniques, Proceedings of 31st Applied Imagery Pattern Recognition workshop, Pp 133-139.

[21] Yun, E. K., & Cho, S. B. (2006). Adaptive fingerprint image enhancement with fingerprint image quality analysis. *Image and Vision Computing*, *24*(1), 101-110.

[22] Chengpu, Y., Mei, X. and Jin, Q. (2008) An effective and robust fingerprint enhancement method, IEEE International Symposium on computational Intelligence and Design, 7, 110-113.

[23] Wang, W., Li, J., Huang, F., & Feng, H. (2008). Design and implementation of Log-Gabor filter in fingerprint image enhancement. *Pattern Recognition Letters*, *29*(3), 301–308. https://doi.org/10.1016/j.patrec.2007.10.004.

[24] Yuanyuan, Z. (2012). Fingerprint image enhancement based on elliptical shape Gabor filter. *2012 6th IEEE International Conference Intelligent Systems*, 344–348. https://doi.org/10.1109/IS.2012.6335240.

[25] Babatunde, I. G. (2012). Fingerprint Image Enhancement : Segmentation to Thinning.*(IJACSA) International Journal of Advanced Computer Science and Applications*, *3*(1), 15–24.

[26] Saatci, E., & Tavsanoglu, V. (2003). Fingerprint image enhancement using CNN filtering techniques. *International Journal of Neural Systems*, *13*, 453–460. https://doi.org/10.1142/S012906570300173X.

[27] He, Y., Tian, J., Luo, X., & Zhang, T. (2003). Image enhancement and minutiae matching in fingerprint verification. *Pattern Recognition Letters*, *24*(9–10), 1349–1360. https://doi.org/10.1016/S0167-8655(02)00376-8.

****

Chapter 3

Fingerprint Image Segmentation: A Review of State of the Art Techniques

In Automatic Fingerprint Identification System (AFIS), preprocessing of the image is a crucial process in deciding the quality and performance of the system. Preprocessing is consists many stages as Segmentation, Enhancement, Binarisation, and Thinning. In this segmentation is one of the steps of preprocessing which differentiate foreground and background region of fingerprint images. Segmentation is the separation of the fingerprint region or extraction of the presence of ridges from the background of the initial image. Segmentation is necessary because it constructs the region of interest from the input image, reduces the processing time, increases the recognition or matching process performance, and reduces the probability of false feature extraction. A 100% accurate segmentation is always very difficult, especially in the very poor quality image or partial image filled with noise such as the presence of latent. Fingerprints are made of Ridge and Valley structure and their features are classified in three levels as Level 1, Level 2, and Level 3. Level 1 Features are singular macro details like ridge pattern and ridge flows. Level 2 is ridge local features like ridge bifurcation and ridge ending or simply minutiae points or ridge orientation. Level 3 is micro details like sweat pores, incipient ridges. This paper provides an overview of the state of the art techniques of fingerprint image segmentation and contribution of other researchers on segmentation. This paper also discusses a different class of segmentation algorithms with its measuring parameters, computational complexity, advantages, limitations, and applications.

Keywords: AFIS, Ridge Orientation, Level 1, Level 2, Level 3, Segmentation, Singular points, Biometrics.

3.1 INTRODUCTION

Biometrics is any intrinsic physical or behavioral traits that can be used to identify or verify the person. The most common types of biometrics are face, speech, iris, fingerprint, gait, and signature. The fingerprint is very common and popular biometric of type behavior traits due to its universality, distinctiveness, and permanence and also many advances and new researchers are available in this field. Even though Automated Fingerprint Identification System (AFIS) is effectively able to match a test sample fingerprint image with already stored fingerprint image in the database, still partial or latent fingerprint image suffers from the low-performance rate. An essential and important step in order to obtain high quality and performance rate at all types of image is through accurate segmentation. Fingerprints are generally classified into three types as rolled, plain and latent fingerprints based on the procedure, how they are captured or collected [1]. In rolled fingerprint image is captured from one end of the finger to another end by rolling and mounting on capturing device in order to obtain complete ridge and valley details of the fingerprint. The plain fingerprint is directly captured using a fingerprint capturing device through pressing a finger tip onto a flat surface. Rolled and plain fingerprints are acquired in a sophisticated attended mode; they will be having good visual quality at the time of training and performance quality at the time of matching one to one or one to many for verification or identification purpose [2].

Usually, Latent fingerprints are collected from the crime scene and mixed with another image or components like structure noise or other fingerprints or on the surface of a wall that was inadvertently touched or handled. The algorithms work well for rolled and plain fingerprint shows significant flaws for latent image or suspect in identifying crime persons. Fingerprint segmentation is the one of the main process involved in fingerprint pre-processing and it refers to the process of dividing or separating the image into two disjoint regions as the foreground and background [3]. The foreground also called as Region of Interest (ROI) because only the region which contains ridge and valley structure is used for processing, while the background contains noisy and irrelevant content and that will be discarded in later enhancement or orientation or classification process. The performance or quality of fingerprint image is crucial and critical as it influences the precise extraction of minutiae and remarkable point or Level 2 and Level 1 features respectively, which are key points for image extraction and which will also reflect and affect the performance of AFIS. Therefore the ultimate goal of the segmentation algorithm is to reduce the noise, reduce the number of false minutiae, clearly differentiate background and foreground image and discard the background, and improve the overall performance of AFIS. Identifying the importance of segmentation process in AFIS, we are discussing in this paper researcher's contribution to this field using review of the literature.

The simple method for segmentation of the fingerprint image is based on binarisation. Initially, the input image can be any of the type like rolled, plain or latent. In next step, the image has to resize using cropping the image or any other image resizing process. The fingerprint is usually in grayscale, but very rarely it can be color (RGB) image in the case of latent or any other types of partial or fingerprint captured using mobile devices. If the image is color, it should be converted into gray scale using RGB to Gray scale converter function. In

next step, Gray scale image is converted into a Binary image using coarse binarisation process. The purpose of coarse binarisation is to remove the background or noise associated with the input image or to separate foreground from the background image. Threshold method is used in order to get an initial binary image. To remove some background from the image, any threshold method can be used. Compared to the local adaptive threshold method, global methods are parameter independent and inexpensive [4-5]. Coarse scan supports detection of the fingerprint ridge positions from the background image. After the coarse binarisation process, the existence of false background is checked and if there exists (normal case), orientation angle is calculated using any orientation method, if not (abnormal case) again refined binarisation process is activated [6]. The objective of refined binarisation is to find an optimal threshold to eliminate the background while preserving as much ridge pattern as possible. After all these processes, we get the segmented image.

In literature, a good number of papers are available for fingerprint segmentation, which can be roughly categorized under two classifications as block-wise methods and pixel-wise methods. In the block-wise method, the fingerprint images are classified into different equal sized nonoverlapping blocks and further organize blocks into foreground and background region based on the extracted block-wise features. On the other hand, pixel-wise methods emphasis on pixel and classifies the fingerprint image based on pixel-wise features of the image. The most common types of features used in segmentation algorithms are gray-level features, orientation features, ridge pattern and ridge frequency features, ridge intensity features, and frequency domain features. The effective segmentation algorithms mainly used for latent fingerprint images are TV-L1 based Adaptive Total Variation Model, TV-L2 based Directional Total Variation Model, The methods which use features of ridge orientation and ridge frequency characteristics, Methods based on ridge orientation filed combined with the statistical features of gray like mean, and variance, the three pixel features method which includes the coherence, the mean, and the variance is discussed in this paper.

3.2 EXISTING SEGMENTATION ALGORITHMS

In literature, several algorithms for fingerprint image segmentation are available with a goal to remove the background or noisy part of the finger print ridge structures. They are TV-L1 based Adaptive Total Variation Model (Zhang, Lai, & Kuo, 2012a) [7], TV-l2 based Directional Total Variation Model (Zhang, Lai, & Kuo, 2012b) [8], Method based on a combination of ridge orientation and ridge frequency characteristics using orientation tensor approach (Choi, Boaventura, Boaventura, & Jain, 2012) [9], Orientation field is combined with the statistical characteristics of the gray to form new method (Xue, J., & Li, H. 2012, July) [10], Ridge orientation Method based on Ridge Temple using correlation with a sinusoid (Short, Hsiao, Abbott, & Fox, 2011) [11], and the coherence, the mean, the variance as three pixel features method (Bazen & Gerez, 2001) [12].

3.2.1 Adaptive Total Variation based on TV-LI Model

Adaptive Total Variation Model [7] is based on TV-L1 model [1]. In TV-L1, the input image ‘f’ is decomposed into two signal layers as cartoon ‘u’, geometric and smoothly varying component of the image f, which contains both ordered noise and small scale organization, and texture ‘v’, which contains oscillatory or textured component in f, i.e. consists of latent

fingerprints and small amount of noise. The weight coefficient λ of the fidelity term is adaptively adjusted depending on the background noise. This characteristic is used in the Adaptive TV-L1 model. The decomposition can be expressed as, f= u + v, which is actually derived from the variation problem i.e. $min_u \int|\overline{\nabla}u| + \int \lambda(x)\,|u-f|$dx. Where f, u, and v are gray-scale image brightness values in R^2 are symbolized using f, u and v functions. The gradient value of u and spatial varying parameter are represented through $\overline{\nabla}u$ and $\lambda(x)$ respectively. Fidelity term and total variation of u are correspond to $|u-f|$ and $\int|\overline{\nabla}u|$ respectively. The quality of the image is directly proportional to $\lambda(x)$ value, which represents fidelity value. If fidelity decreases, image noise decreases, or smoothness increases. When there is less noise or image is more smooth more texture can be extracted in v. Fidelity with $\lambda(x)$ value, plays an important the role in the region with structured high noise, to ensure whether the region should be filtered out from texture v, or not. This algorithm delivers very reasonable result except for the latent fingerprints.

3.2.2 Directional Total Variation based on TV-L2 Model

The TV-L2 model based Directional Total Variation (DTV) model [8], decomposes image almost similar to TV-L1 model, which is more accurate and efficient in handling latent fingerprint noise detection and to separate background from a foreground image and achieves good segmentation. TV-L2 model (DTV) uses orientation vector $\vec{a}$ along with TV-LI model component, to manage the signal obtained in the texture output 'v'. The decomposition is achieved using the formula $min_u \int \overline{\nabla}u\cdot\vec{a}(x)\left|dx + \frac{\lambda}{2}\right| |f-u|^2$, which is based on variation problem. Here spatially changing orientation vector attuned to confined texture orientation, which is represented as $\vec{a}$(x). The main focus, here is to reduce the total variation of u along any direction, by tuning $\vec{a}$ to that direction and also by maintaining a total variation of u along other directions. Due to this phenomenon v not only fully captures texture along that direction but also weakens texture of other directions. This algorithm outperforms when the image contains oriented texture. Figure 3.1 depicts the effect of $\vec{a}$ on output of 'v'.

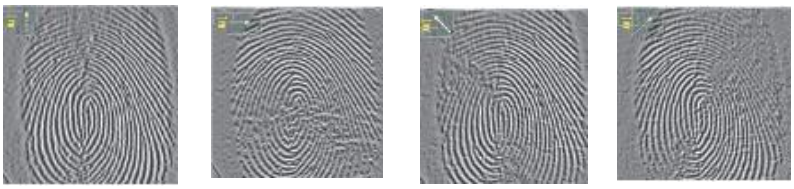


Figure 3.1: Texture output for v for $\vec{a}$ in four different directions [8]

3.2. 3. Method based on combination of Ridge Orientation and Frequency features

In [9], a fingerprint image segmentation algorithm is developed using Ridge orientation and frequency features. Extraction of a symmetric pattern of the fingerprint image and removal of structured noise is done with the aid of orientation tensor. The estimation of the confined ridge frequency of the latent or dormant fingerprint and placing of fingerprint region by considering valid frequency regions are handled by Local Fourier Analysis method. It is essential to obtain foreground or candidate fingerprint region for every orientation and frequency feature, and localization of the latent fingerprint region at intersection regions of

orientation and frequency features. The new algorithm performed well compared to manual segmentation. Figure3.2 depicts a flowchart of this method.

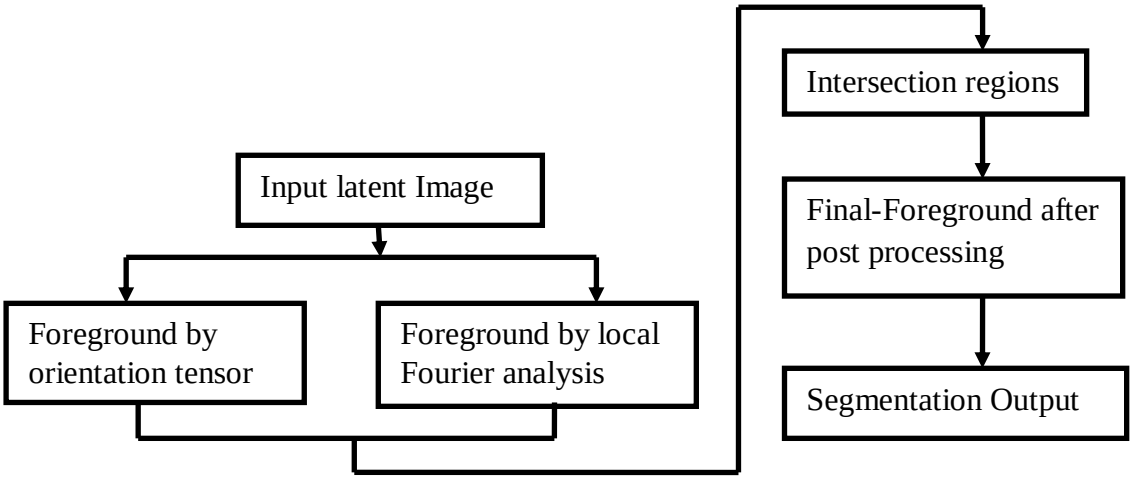


Figure 3.2: A flowchart of the method based on ridge orientation and frequency features [8]

3. 2. 4 Method based on the orientation field combined with statistical characteristics of Gray

A combined method segmentation approach for fingerprint image is proposed in [10], which is based on orientation filed and statistical characteristics of gray. Statistical concepts like mean, variance and standard deviation can be used to extract background region segmentation of large areas and small noise area's segmentation, which is driving and motivating information used in this study. Based on the orientation field information, algorithm conducts secondary segmentation in blocks to improve the overall performance. This algorithm performs well in terms of execution time but is not adequate to handle too wet or too dry image.

3.2.5 Ridge Template Correlation Method

The quote "ideal ridge surface" is used in Ridge Template Correlation Method [11], to explain idealized friction ridge grayscale image, which is initially referred by Domeniconi et al. (1998) [12] and Short et al. (2011) [13], in this method further study made on this to define the minutia region for the purpose of localization of minutiae. Actual gray scale image of the friction ridge is the source for "ideal" ridge, means ideal ridge is reconstructed from the actual grayscale image, with an assumption that image intensity values vary sinusoidal and adjusted local contrast, frequency, and direction. In this method, a "goodness of fit" score is computed to compare an observed block region to already stored ideal template. Before this, the image is divided into small blocks. The goodness of split score is also used to assign score levels to blocks, and these score levels will identify background image, based on the property that background region of the image exhibits positive correlation with the template structure. The algorithm provides reasonably good results under some certain limitations. Workflow of this algorithm is represented in Figure 3.3.

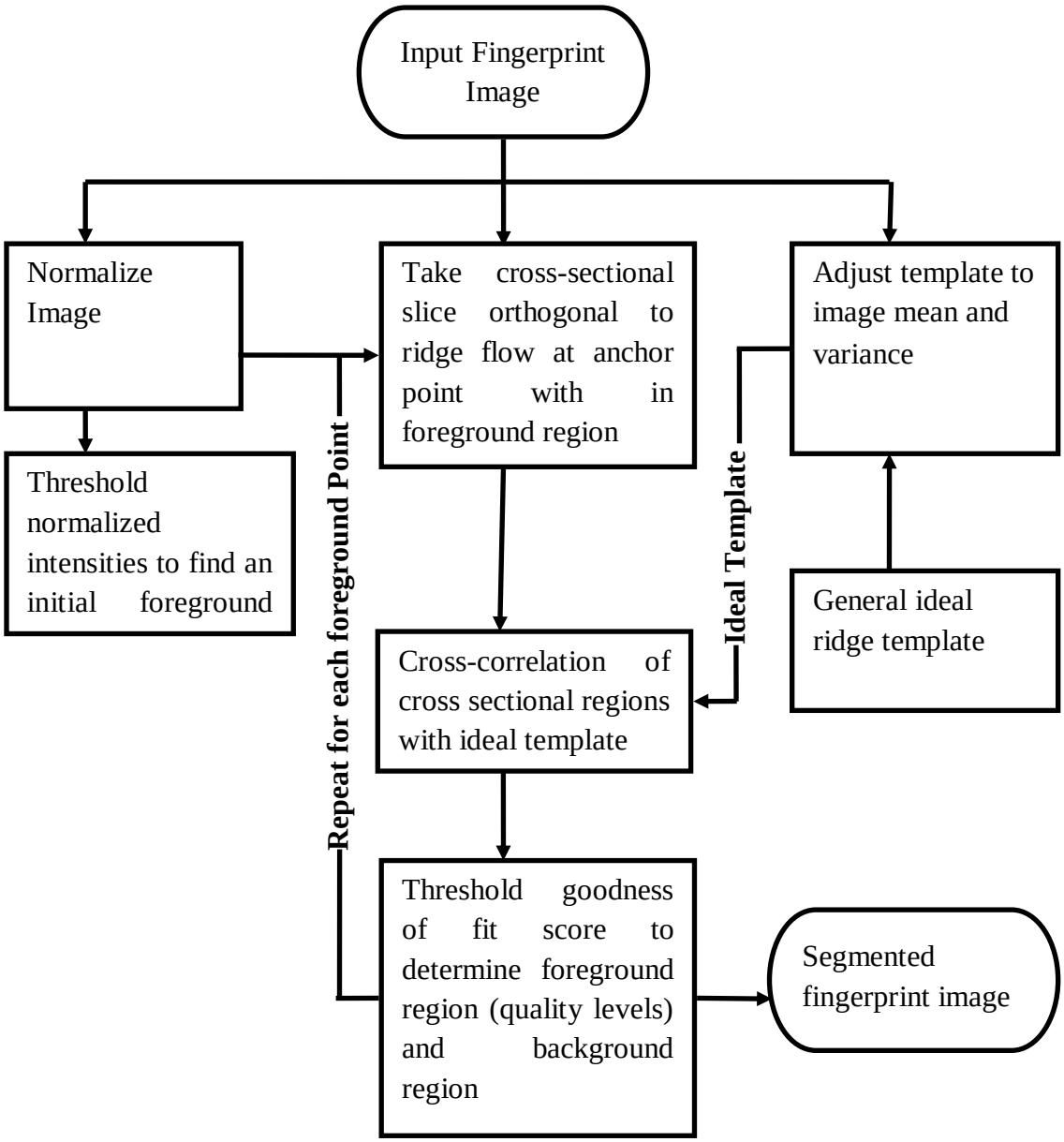


Figure 3: Workflow for Ridge Template Correlation Method [11]

3.2.6 Three Pixel Features Method

In the segmentation process, the first step is to extract the features of the pixels. The first-pixel feature out of the three features is coherence [14]. The coherence calculates how the best gradient is organized in the same direction, usually fingerprint ridge pattern contains parallel lines, and due to this reason, foreground image will be having more coherence characteristics compared to the background. In a window W around a pixel, coherence is defined as $\text{Coh}=\frac{|\sum_w(G_{s,x},G_{s,y})|}{\sum_w|(G_{s,x},G_{s,y})|}=\frac{\sqrt{(G_{xx}-G_{yy})^2+4G_{xy}^2}}{G_{xx}+G_{yy}}$

In the above equation $(G_{s,x}, G_{s,y})$ is called as squared gradient, local gradient are $G_{xx}=\sum_w G_x^2$, $G_{yy}=\sum_w G_y^2$, $G_{xy}=\sum_w G_x\, G_y$ and (G_x, G_y).

The second-pixel feature is the mean. The background will contain more mean gray value (darker gray) than the foreground image. When the intensity of the image is represented as I and the local mean of each pixel is represented as Mean = $\sum_w$I.
The third-pixel feature is the variance. In a fingerprint image, variance takes into account ridge valley structure. In the foreground, between the ridge and valley variance will be more comparable to the variance of the noise in the background. The variance of each pixel is represented as
Var = $\sum_w$(I-Mean) ^{2}.

3. 2.6.1 Classification

In order to classify to form a cluster based on supervised learning, this approach uses a linear classifier, which basically tests the linear combinations of the features, which are expressed as v= W^Tx = W_0Coh + W_1Mean + W_2Var + W_3. In this equation v is the value to be tested, w = [W_0 W_1 W_2 W_3] ^{T} represents the weight vector and x = [Coh Mean Var 1] ^{T}.

3.2.6.2 Post Processing

The ultimate purpose of the post processing is to minimize classification error or to obtain the best classifier, morphology is applied for the estimation of classification. In the process of reducing classification error first small cluster that is faulty classified to the foreground are removed. Then the small cluster that is assigned to the background due to incorrectly process is removed. This algorithm seems to be simple while adopting but becomes complex when implemented.

3.3 LITERATURE REVIEW OF SEGMENTATION

Segmentation is one of the deciders of performance in the automatic fingerprint recognition system. There is enough amount of literature with respect to image segmentation process or approach dating back over thirty years. Jain & Dubes, (1988) [15], explains the algorithm for clustering in his book, these early approaches for clustering can be used for segmentation, which acts as the basis for many new methods including boundary based segmentation such as Canny edge detection Canny, 1986 [16]. In this method, researcher defines a comprehensive set of goals for the computation of edge detection points. Adams and Bishof, (1994) [17], proposed segmentation algorithm for images, which are intensity images with certain characteristics like robust, rapid, and free of tuning parameters. This algorithm can take input as either individual pixels or regions and points these inputs to some region formed by the algorithm. The algorithms explain two methods in which input corresponds to the region, either by using manual seed or by an automated procedure. Chakraborty et al., (1996) [18], proposed a method which combines region based segmentation and boundary finding to form new method which is more robust to noise and high performance. The literature covered above is some general segmentation algorithms which will apply for any types of images.

In literature, there are many studies available, which mainly focuses on fingerprint image segmentation. Most of the segmentation algorithm does classification of the image based on either supervised learning or unsupervised learning. When a class label is not known or

unknown, means of unsupervised learning, classification is significantly and very difficult. Researchers, Mehtre, et al. (1989) [19] classified the image into blocks, which is administrative specific and the size was 16 × 16 pixels. Based on the gradient distribution, each block was classified. This method is best suited for simple fingerprint images which contain only background and foreground. Later Researchers Mehtre and Chatterjee, (1989) [20] extended this work by leaving the grayscale variance, which will usually be lower than some threshold value. Researchers Ratha et al. (1995) [21] proposed 16 × 16 blocks of classes and each one was developed based on the gray scale variance in the direction opposite to the orientation of ridges.

The authors Jain and Ratha, (1997) [22] concentrated for the detection of objects located in complex backgrounds. The given object is first applied to a bank of even-symmetric Gabor filters. The output image received from the Gabor filter is subjected to a sigmoid function transformation. The yield image of the Gabor filter is applied as an input to the clustering algorithm, which develops spatially compact clusters. Sun and Ai (1996) [23] pre-processed initially fingerprint image by converting it into a binary image with the help of dynamic threshold value (T). Moayer and Fu (1975) [24] used sampling squares, which are obtained from the subdivision of fingerprint images for the ultimate goal of feature extraction. They used dynamic threshold value (T) to convert the initial image to a binary image. In order to determine the local threshold value, researchers used neighbor pixels by group 5 × 5 pixels.

Bazen and Gerez (2000) [25] used coherence and morphology of fingerprint image with an intention to obtain a smooth image by filtering different types of noises. The same author Bazen and Gerez (2001) [14] improved their work by adding two more statistical features as the mean and variance for their previous work. Here classification is done with the aid of optimal linear classifiers, which acts as a trainer for classification. With a goal to find compact cluster and reducing, classification error for post processing morphology is applied.

Naji et al. (2002) [26] developed a segmentation algorithm, which computerized or automated the method of selecting a threshold value at the time of segmentation with the aid of histogram equalizer. Segmentation algorithm generally falls under two categories of machine learning techniques as supervised learning and unsupervised learning. Unsupervised learning uses threshold decided on detecting features to cluster the image. Supervised learning uses a simple linear classifier to classify features as a region of interest (ROI) or background and foreground. As a part of supervised methods, Alonso-Fernandez et al. (2005) [27] used a Gabor filter to filter the input image and to obtain a smooth image. The neural network can also be used in the segmentation process to reduce the noise or to enhance the image quality.

Barreto et al. (2005) [28] used a neural network to train the fingerprint image data sets using Fourier spectrum and obtained a segmentation of fingerprint images. Zhu et al. (2006) [29] also used neural network concepts in order to train the fingerprint data set, but they used the gradient of the fingerprint orientation to segment the images. Wu et al. (2007) [30] proposed a new method for segmentation; in their method, they used the strength of Harries corner function to extract the background from foreground or to extract a region of interest. In order to separate region of interest from the background image, they used corner strength measures.

Tiwari, K., & Gupta, P. (2015) [31] proposed a new method for extracting a single fingerprint image from the slap fingerprint scanner, which simultaneously scans four fingerprints of a person in a single image. While extracting the single fingerprint image the image is also required to be segmented. They used a novel technique to extract solitary (single) fingerprint image based on force field and heuristics using divide and conquer strategy and is tested in IITK-4slap-Rural and IITK-4slap-student database.

Thai, Huckemann, & Gottschlich, 2016 [32] proposed the new approach for fingerprint segmentation in three folds, firstly used factorized directional bandpass (FDB) and directional Hilbert transform originated from Butterworth bandpass (DHBB) filter combined with soft-thresholding for texture extraction. Secondly, as an evaluation benchmark with 10560 images marked manually for ground truth segmentation. Thirdly they have compared systematically factored directional filtering with other similar fingerprint segmentation approach and obtained comparatively good performance.

3.4 COMPARISON OF DIFFERENT ALGORITHMS

The main six segmentation algorithms discussed above are compared and analyzed using different parameters like Measuring Parameters, Computational complexities, Limitations, Advantages, and Applications (Nimkar & Mishra, 2004) [33].

3.4.1 Adaptive Total Variation Model Analysis [1 & 33]

Measuring Parameters: Fidelity Weight coefficient represented as , plays an important role in region with structured high noise, to ensure whether the region should be filtered out from texture v, or not. Also, coherence, mean, and variation can be used as measuring parameters.
Computational Complexity: Measuring the value of Fidelity Weight coefficient, in various region of the fingerprint. Processing the algorithm for the latent fingerprint is also computationally complex.
Limitations: The adaptive total variation model does not well suits for latent fingerprint images.
Advantages: Performance of the algorithm in terms of accuracy, execution time, and noise filtering ratio are satisfactory good except for latent fingerprint image. Edges preserve TV-L1 model.
Applications: The adaptive total variation model effectively carries fingerprint segmentation and image decompositions.

3.4.2 Directional Total Variation Model Analysis [8 & 33]

Measuring Parameters: The spatially varying orientation vector adjusted to local texture orientation is represented as (x) and also variance features are used for measuring purposes.
Computational complexities: Maintaining or keeping the spatially varying orientation vector (x) for well, aligning local ridge orientation for the fingerprint is computationally complex or difficult.
Limitations: Complex calculations are involved in latent fingerprint image processing only can be treated as limitations; otherwise there is no limitation for this approach.
Advantages: Good performance compared to adaptive total variation model and a right choice for processing latent fingerprint images.

Applications: Latent fingerprint segmentation process results in high accuracy, decomposition of the specifically oriented textures.

3.4.3 Method based on combinations of ridge orientation and frequency features Analysis [9 & 33]

Measuring Parameters: Ridge frequency or ridge density and mean value is used as measuring parameters for the algorithm based on ridge orientation and frequency features.
Computational complexities: Ridge orientation and frequency features are considered for each print separately and then their intersection is taken for localization of latent fingerprint is complex computation involved in this algorithm.
Limitations: Requires robust confidence measure for segmentation output.
Advantages: The algorithm performs well compared to manual segmentation and satisfactory results as far as visual inspection are considered.
Applications: Latent fingerprint detection and segmentation process are effectively done compared other similar type of segmentation algorithms.

3.4.4 Combination Method-Ordination features combined with statistical features of the gray analysis [10 & 33]

Measuring Parameters: Mean of the gray value and variance of the gray values are considered as measuring parameters for this combined algorithm.
Computational complexities: Mean gray value and variance calculation of each gray value is considered as complex computation.
Limitations: Algorithm is not adequate to handle too wet or too dry image.
Advantages: Compared to other similar class of segmentation algorithm this combined algorithm improves accuracy and improves execution time.
Applications: Affectively used for fingerprint segmentation process.

3.4.5 Ridge Template Correlation Analysis [11 & 33]

Measuring Parameters: Image mean and variance are considered as measuring parameters for this algorithm.
Computational complexities: The procedure used for segmentation process is lengthy and which is the complex calculation involved in this algorithm.
Limitations: When a fingerprint is large and missed minutiae are high or false foreground is high, the segmentation incorrectly labels the background as foreground and actual region of interest is missed out.
Advantages: The algorithm results in reduced average detected fingerprint area from 60.7% of the total image to 33.6%.
Applications: Effectively used for fingerprint segmentation process.

3.4.6 Three pixel features method-the coherence, the mean and the variance Analysis [12 & 33]

Measuring Parameters: The coherence, the mean, and the variance are considered as measuring parameters for this algorithm.

Computational complexities: Post processing of the segmented image is compulsory and necessary is considered to be a complex computation.
Limitations: Initially around 6.8% of the pixels are misclassified, but later post processing reduces this percentage and still there will be a small percentage of misclassified pixels.
Advantages: The results of segmentation are highly accurate with good resolution.
Applications: Affectively used for fingerprint segmentation process.

3.5 CONCLUSION

Segmentation can turn out to be exceptionally intricate in light of the fact that the limit between the area of the region of interest and the background obscures due to the noise. Different segmentation strategies are created. Be that as it may, these strategies are not totally fulfilling. For instance, if there is a background area with high noise encompassing the poor differentiation forefront of the unique fingerprint picture, these strategies will neglect to isolate Region of interest from the background area. A hearty and good segmentation strategy is required to manage lower quality noisy pictures In this paper we have discussed six types of segmentation algorithm basics, framework and each having different accuracy levels in segmenting fingerprint image. This paper also makes a brief literature review on these algorithms and research work contributed by different authors all over the world. In Section 4 also we discussed algorithm with is measuring parameters, computational complexity, advantages, limitations, and applications. The paper concludes that almost all the algorithms discussed above perform well in terms of accuracy, execution time and other important parameters, but only a few algorithms handle and process latent fingerprint images like an adaptive total variation model and directional total variation model.

REFERENCES

[1] Zhang, J., Lai, R., & Kuo, C. C. J. (2012). Latent fingerprint detection and segmentation with a directional total variation model. In Proceedings - International Conference on Image Processing, ICIP, 1145–1148. https://doi.org/10.1109/ICIP.2012.6467067.

[2] Krishna Prasad, K. and Aithal, P. S. (2017). A Conceptual Study on User Identification and Verification Process Using Face Recognition Techniques. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(1), 6-17. DOI:http://doi.org/10.5281/zenodo.810343.

[3] Krishna Prasad, K., Aithal, P. S. (2017). A Conceptual Study on Image Enhancement techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*,1(1), 63-72.DOI: 10.5281/zenodo.831678.

[4] Yu, L., Yan, G., Wang, C., Yang, W., Zan, P., & Wu, J. (2008). Advanced Intelligent Computing Theories and Applications: With Aspects of Artificial Intelligence.

[5] Vielhauer, C., Dittmann, J., Drygajlo, A., Juul, N. C., & Fairhurst, M. (Eds.). (2011). Biometrics and ID Management: COST 2101 European Workshop, BioID 2011, Brandenburg (Havel), March 8-10, 2011, Proceedings (Vol. 6583). Springer Science & Business Media.

[6] https://images.google.com/. (2017). Google.[online] Available at: https://images.google.com/ Fingerprint image segmentation using coarse binarisation [Accessed 28 July. 2017].

[7] Zhang, J., Lai, R., & Kuo, C. C. J. (2012). Latent fingerprint segmentation with adaptive total variation model. In Proceedings - 2012 5th IAPR International Conference on Biometrics, ICB 2012 (pp. 189–195). https://doi.org/10.1109/ICB.2012.6199807.

[8] Zhang, J., Lai, R., & Kuo, C. C. J. (2012). Latent fingerprint detection and segmentation with a directional total variation model. In Proceedings - International Conference on Image Processing, ICIP (pp. 1145–1148). https://doi.org/10.1109/ICIP.2012.6467067

[9] Choi, H., Boaventura, M., Boaventura, I. A. G., & Jain, A. K. (2012). Automatic segmentation of latent fingerprints. 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 303–310. https://doi.org/10.1109/BTAS.2012.6374593

[10] Xue, J., & Li, H. (2012, July). Fingerprint image segmentation based on a combined method. In Virtual Environments Human-Computer Interfaces and Measurement Systems (VECIMS), 2012 IEEE International Conference on (pp. 207-208). IEEE.

[11] Short, N. J., Hsiao, M. S., Abbott, A. L., & Fox, E. A. (2011). Latent fingerprint segmentation using ridge template correlation. 4th International Conference on Imaging for Crime Detection and Prevention 2011 (ICDP 2011), P28–P28. https://doi.org/10.1049/ic.2011.0125

[12] Domeniconi, C,. Tari, S. and Liang. P., (1998). Direct Gray Scale Ridge Reconstruction in Fingerprint Images. *International Conference on Acoustics, Speech, and Signal Processing*, 5, 2941-2944.

[13] Short, N. J., Abbott, A. L., Hsiao, M. S., & Fox, E. A. (2011). A Bayesian approach to fingerprint minutia localization and quality assessment using adaptable templates. *International Joint Conference on Biometric*s, (IJCB), pp. 1-7.

[14] Asker M. Bazen and Sabih H. Gerez. (2001). Segmentation of Fingerprint Images, Workshop on Circuits, Systems and Signal Processing, Veldhoven. The Netherlands.

[15] Jain, A. K., & Dubes, R. C. (1988). Algorithms for clustering data. Prentice-Hall, Inc.

[16] Canny, J. (1986). A computational approach to edge detection. *IEEE Transactions on pattern analysis and machine intelligence*, (6), 679-698.

[17] Adams, R., & Bischof, L. (1994). Seeded region growing. *IEEE Transactions on pattern analysis and machine intelligence*, 16(6), 641-647.

[18] Chakraborty, A., Staib, L. H., & Duncan, J. S. (1996). Deformable boundary finding in medical images by integrating gradient and region information. *IEEE Transactions on Medical Imaging*, 15(6), 859-870.

[19] Mehtre, B. M., Murthy, N. N., Kapoor, S., & Chatterjee, B. (1987). Segmentation of fingerprint images using the directional image. *Pattern Recognition*, 20(4), 429-435.

[20] Mehtre, B. M., & Chatterjee, B. (1989). Segmentation of fingerprint images—a composite method. *Pattern Recognition*, 22(4), 381-385.

[21] Ratha, N. K., Chen, S., & Jain, A. K. (1995). Adaptive flow orientation-based feature extraction in fingerprint images. *Pattern Recognition*, 28(11), 1657-1672.

[22] Jain, A. K., Ratha, N. K., & Lakshmanan, S. (1997). Object detection using Gabor filters. Pattern Recognition, 30(2), 295-309.

[23] Sun, X. and Ai, Z. (1996). Automatic feature extraction and recognition of fingerprint images, Proceeding of ICSP'96, Beijing, pp.1086-1089.

[24] Moayer, B., & Fu, K. S. (1975). A syntactic approach to fingerprint pattern recognition. Pattern Recognition, 7(1–2), 1–23. https://doi.org/10.1016/0031-3203(75)90011-4

[25] Bazen, A.M. and Gerez, S.H. (2000). Directional field computation for fingerprints based on the principal component analysis of local gradients, Proceedings of ProRISC2000, 11th Annual Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands.

[26] Naji, A.W., Ramli, A.R., Ali, R., Rahman, S.A., and Ali, M.L. (2002). A segmentation algorithm based on histogram equalizer for fingerprint classification system, Second International Conference on Electrical and Computer Engineering ICECE 2002, Dhaka, Bangladesh, pp. 390-393.

[27] Alonso-Fernandez, F., Fierrez-Aguilar, J. and Ortega-Garcia, J. (2005). An enhanced Gabor filter based segmentation algorithm for fingerprint recognition systems, In Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, pp. 239-244.

[28] Barreto, P., Marques, A.C. and Thome, A.C. (2005) A neural network fingerprint segmentation method, 5th International Conference on Hybrid Intelligent Systems P.6.

[29] Zhu, E., Yin, J., Hu, C. and Zhang, G. (2006) A systematic method for fingerprint ridge orientation estimation and image segmentation, Pattern Recognition, Vol. 39, No.8, Pp. 1452-1472.

[30] Wu C., Tulyakov S. and Govindaraju V. (2007). Robust point-based Feature Fingerprint Segmentation Algorithm, ICB (2007), Pp. 1095-1104.

[31] Tiwari, K., & Gupta, P. (2015). An efficient technique for automatic segmentation of fingerprint ROI from digital slap image. Neurocomputing, 151(P3), 1163–1170. https://doi.org/10.1016/j.neucom.2014.04.086

[32] Thai, D. H., Huckemann, S., & Gottschlich, C. (2016). Filter design and performance evaluation for fingerprint image segmentation. PLoS ONE, 11(5). https://doi.org/10.1371/journal.pone.0154160

[33] Nimkar, R., & Mishra, A. (2014). Fingerprint segmentation algorithms: A literature review. International Journal of Computer Applications, 95(5).

****

CHAPTER 4

A Novel Method to Control Dominating Gray Levels during Image Contrast Adjustment using Modified Histogram Equalization

Contrast and Brightness are two major factors, which affect the superiority of an image for easy or stainless or pleasant viewing. Overall lighting condition and darkness condition of the image collectively called as brightness, whereas differences in brightness or intensity range between the low and high-intensity value of an image are called as contrast. Histogram equalization is a very famous approach for image contrast adjustment or enhancement in image processing, but which produces sometimes washed out appearance, especially for a small region of the grayscale image. Contrast adjustment is part of the noise filtering or smoothing process, which is essential in automatic identification or recognition systems like a fingerprint or any other biometric-based recognition systems to get higher efficiency. Histogram-based equalization is simple in terms understandability and implementation, which is referred as one of the greatest advantages of this contrast adjustment method. Histogram equalization is less expensive compared to another similar type of contrast adjustment or enhancement algorithm. The novel approach planned in this paper controls dominating gray levels before applying histogram equalization process so that it performs enhancement of the image without over brightness or over darkness, which makes smaller part of the image invisible or loss of details in that portion of the image. This method outperforms histogram equalization method by enhancing the contrast with intermediate brightness or neither too bright nor too dark. In this paper, we compare different types of the grayscale image using the novel method and global histogram equalization method using MATLAB.

Keywords: Histogram equalization, Contrast enhancement, Washed out appearance, Brightness, Image processing.

4.1 INTRODUCTION

Contrast adjustment methods are extensively used for image processing to attain wider dynamic range and which is considered as preprocessing stage, especially in Automatic recognition system based on different types of images like a fingerprint, face, iris etc. The different four possible ways in which brightness and contrast can be misadjusted is shown using Figure 4.1. When brightness is too high all the pixels of the image turn into lighter, conversely when the brightness is too low all the pixels of the image turn into darker. When the intensity is a too high, lighter area of the image becomes lighter and darker area of the image becomes darker.

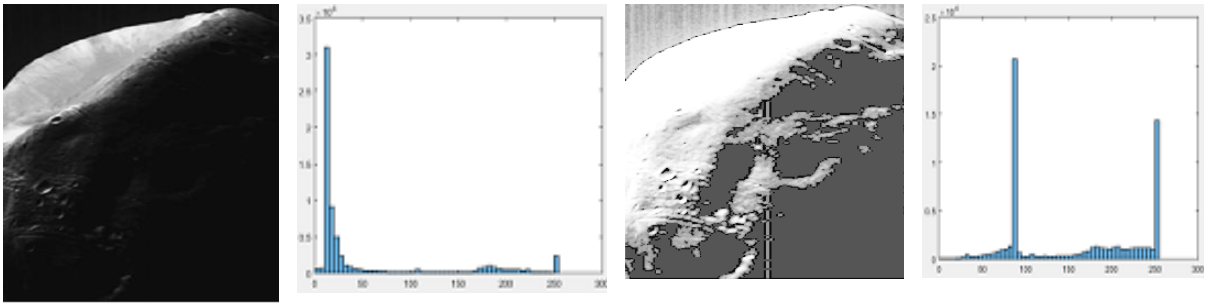
Distinct contrast enhancement methods have already been developed and advanced which make use of easy linear or non-linear gray level transformation functions in addition to complicated evaluation of special image capabilities. Amongst them, histogram equalization (HE) [1-4] is a very popular technique for contrast adjustment or enhancement of images, especially grayscale images.

(a) Brightness too high [5] (b) Brightness too low (c) Contrast too high (d) Contrast too low

Figure 4.1: Brightness and Contrast misadjusted [5]

In general, the histogram equalization distributes pixel values consistently and produces an outcome in a superior image with the linear increasing histogram. Some useful applications of HE enhancement consist of scientific image processing, speech recognition, fingerprint identification and texture synthesis, which might be typically employed with histogram adjustment [6-9].

Histogram based techniques strategies for image enhancement is in most cases primarily based on equalizing the histogram of the image and increasing the dynamic variety corresponding to the image. Histogram equalization (HE) technique has two foremost flaws which affect performance of this technique. Histogram equalization assigns one gray level into two diverse neighbor gray levels with distinctive intensities. If maximum of an image consists of a grey level, histogram equalization assign a gray level with higher intensity to that gray level and it causes a phenomenon as we referred to as it washed out. Figure 4.2 indicates this effect. Even though in histogram after washout appearance dominating bins appears, this is part of another area of the image. Compared to initial image, some parts of the initial image are washed out in the histogram equalized image.



Original Image [10] | Histogram of original image | Image after applying Histogram equalization | Histogram of image after applying HE

Figure 4.2: Washout appearance of an image after Histogram equalization [10]

In this study, a new method is proposed to overcome the domination of the gray levels, which increases the image contrast based on histogram equalization without making the loss of any details of the image. Usually, in global histogram equalization, some gray level of the image having more accumulations compared to some other gray levels which have fewer accumulations. Usually, a higher bin component dominates over lower bin points. In this new method more or fewer accumulations or frequencies are equalized by shorting the higher bins and adding an extra bin to lower bin gray levels. The contrast adjustment can be used for fingerprint image enhancement process [11-13].The remaining part of the paper is arranged as follows. Section 2 describes Review on existing work. Section 3 explains the objective the study. Section 4 describes the methodology of the proposed method. Section 5 describes the Global histogram equalization and proposed a new method using the algorithm. Section 6 presents some experimental results of using novel approach and Histogram equalization with the aid of MATLAB. Section 7 shows the snapshots of the coding of the new method used in this study through MATLAB programming. Section 8 makes concluding remarks.

4.2 RELATED RESEARCH

Different techniques of making use of histogram equalization are determined in the literature. Global histogram equalization (GHE) [1] makes use of the entire information of the input image to map into new distinct intensity levels of the image. Although this Global technique is suitable for ordinary or general enhancement, it fails to consider with the local brightness capabilities of the entered image. The gray ranges with very excessive frequencies (wide variety of occurrences) dominate over the opposite gray levels having decrease frequencies in an image. In any such situation, GHE remaps the gray levels in a way that the contrast stretching turns into confined in some dominating gray levels having large image histogram components, and it causes sizable contrast loss for other small ones.

Local histogram equalization (LHE) [1] can overcome the problem encountered in GHE. LHE uses a small window that slides on all pixel of the image sequentially and handiest the block of pixels that fall within this window are taken into consideration for HE and then gray level mapping for enhancement is carried out for the center pixel of that window. Therefore, it may make splendid use of local information also. But, LHE requires excessive computational cost and occasionally reasons over enhancement in some part of the image.

Another shortfall of this approach is that it also enhances the noises inside the input image. To overcome the problem of high computational cost one more approach is to use the non-overlapping block for HE [1]. But almost all times this method produces checkerboard effect. In literature, many types of research are centered on image or video contrast adjustment or enhancement [14-19]. Mean preserving bi-histogram equalization (MPBHE) proposed to get rid of the brightness problem issues [15, 17]. MPBHE separates the entered or captured input image or video histogram into two classifications as mean of the input before equalizing them independently. Some other variants of bi-histogram equalization are a similar area or equal area or place dualistic sub-image or picture histogram equalization (DSIHE) [20], minimum or lower mean brightness or luminance error bi-histogram equalization (MMBEBHE) [19-20]. DSIHE [7] technique uses entropy value for histogram separation. MMBEBHE [19-20] is the extension of BBHE technique that offers maximal brightness maintenance. Even though these strategies can carry out exact contrast adjustments, additionally they generate some side effects depending on the variation of gray level distribution in the histogram [21]. Recursively Separating the mean and finding histogram Equalization (RMSHE) another up gradation of BHE [19] however, it additionally is not free from drawbacks. Moreover, such strategies won't ensure desirable upgrades of all of the partitions [10]. The difference in the ranges of upgrades of various components might also create undesired artifacts in the image. There are many variations MPBHE are Recursive Separated and Weighted HE (RSWHE) [23], Multipeak HE (MPHE) [24], Brightness preserving Weight Clustering HE (BPWCHE) [25], Brightness preserving Dynamic HE (BPDHE) [26] and HE with Range Offset (HERO) [27-28].

The related research reveals that even though there are a lot of modifications for HE are proposed and implemented, still, there is scope for improvement in terms reducing noise, improving brightness, contrast adjustment and equalizing accumulations or larger bins. This paper focuses on cutting the accumulations or bins of dominating gray levels of the image and reassigning them to lower bin points of the image.

4.3 OBJECTIVE OF THE STUDY

The objectives of the study are;

- To remove the domination of the gray levels and reassign them to lower accumulation gray level with an intention to equalize more or less accumulation of all intensity levels of the image.
- To increase contrast, which exists in the image as a range of gray levels and to overcome the washout appearance occurs for small part of the image.
- To compare the new method with GHE with the aid of MATLAB coding.

4.4 METHODOLOGY

The methodology used in this research work is explained using workflow diagram using Figure 3. We use MATLAB R2015a for implementing the new approach to control dominating gray level. Initially, the image is loaded into MATLAB. The image is resized into 256 x 256 grayscale intensity image even though the image is any dimensional image like 3D or 2D with a different count of pixels in the first dimension (row) and a second dimension

(column). So intensity levels of grayscale image range between 0-255. Next, we have to find the occurrence of each gray level or frequency from zero to two fifty-five. Find the mean of accumulations or frequencies, considering all grayscale intensity levels. Next check any intensity level of the input grayscale image having individual frequency value greater than mean. If so, find the difference between frequencies of that intensity level and mean. The new value of that particular intensity level is reassigned with mean value. Next, we have to add difference value to all pixels uniformly. This is done, dividing the difference value by mean value. Find the some of the frequencies all intensity value; usually, it should be equal to a maximum number of pixels. In 256 x 256 sized image maximum number of pixels is 65536 (i.e. 256 x 256). We have altered the count above. So there is a necessity of checking sum of frequencies of intensity levels. If the sum crosses the maximum number of pixels, then we simply subtract the excess value from highest frequency or accumulation value of the intensity levels. If the sum is less than the maximum number of pixels then find the count of frequencies of all gray levels. Take the difference of sum and a total number of pixels. Divide the difference by count and distribute the value to all gray levels which are having a value less than the mean. Next, we use Global histogram equalization for finding probability density function cumulative density function and mapping function. Finally, the intensity adjusted output image is generated.

4.5 PROPOSED NOVEL APPROACH

In this section first, the usual procedure of global histogram equalization is explained (GHE). In the second phase, we explain the procedure of novel approach using a pseudo algorithm to overcome shortfalls of GHE. Suppose that an image k (x, y) consists of distinct gray levels in the range of [0, R-1]. The transformation function T (d_k) is defined as

G_k= T (d_k) = $\sum_{j=0}^{l}$ P (d_j) = $\sum_{j=0}^{l} \frac{m_i}{m}$ ---------- (4.1)

Where 0 ≤ Gk ≤ 1 where l=0, 1, 2 ...R-l. In Eq. 4.1, mi depict the count of pixels having gray level d_k, m is the maximum count of pixels in the entered image and P (d_j) correspond to Probability Density Function (PDF) of the input d_j. The cumulative density function here refereed as T (d_k). G_k, is a mapping function, which maps to dynamic range of [0, R-1] values by multiplying it with R-1.

In 256 × 256 sized gray scale images Eq. 4.1 value of G_k is $0 \leq G_k \leq 255$ where l can take distinct 256 values from zero to 255 and a maximal number of pixels are 65536 (256 × 256). G_k, is a mapping function, which maps to a dynamic range of [0, 255] values by multiplying it with 255.

GHE typically offers a good image enhancement, but sometimes ends up with some artifacts and unwanted aspect results along with the washed out look. In Eq. 4.1, larger values of m_i purpose the respective gray levels to be mapped aside from every different that guarantees precise enhancement. However, the mapping of the grey levels having smaller m_i values, are forced to be condensed in a small range that makes much less enhancement in such gray levels. Furthermore, rounding problems might also occur inside the transformation such gray levels while the output gray levels are quantized into integer values. In such cases, there is the possibility mapping a couple of input gray levels to the equal output gray level that ends in the loss of image information.

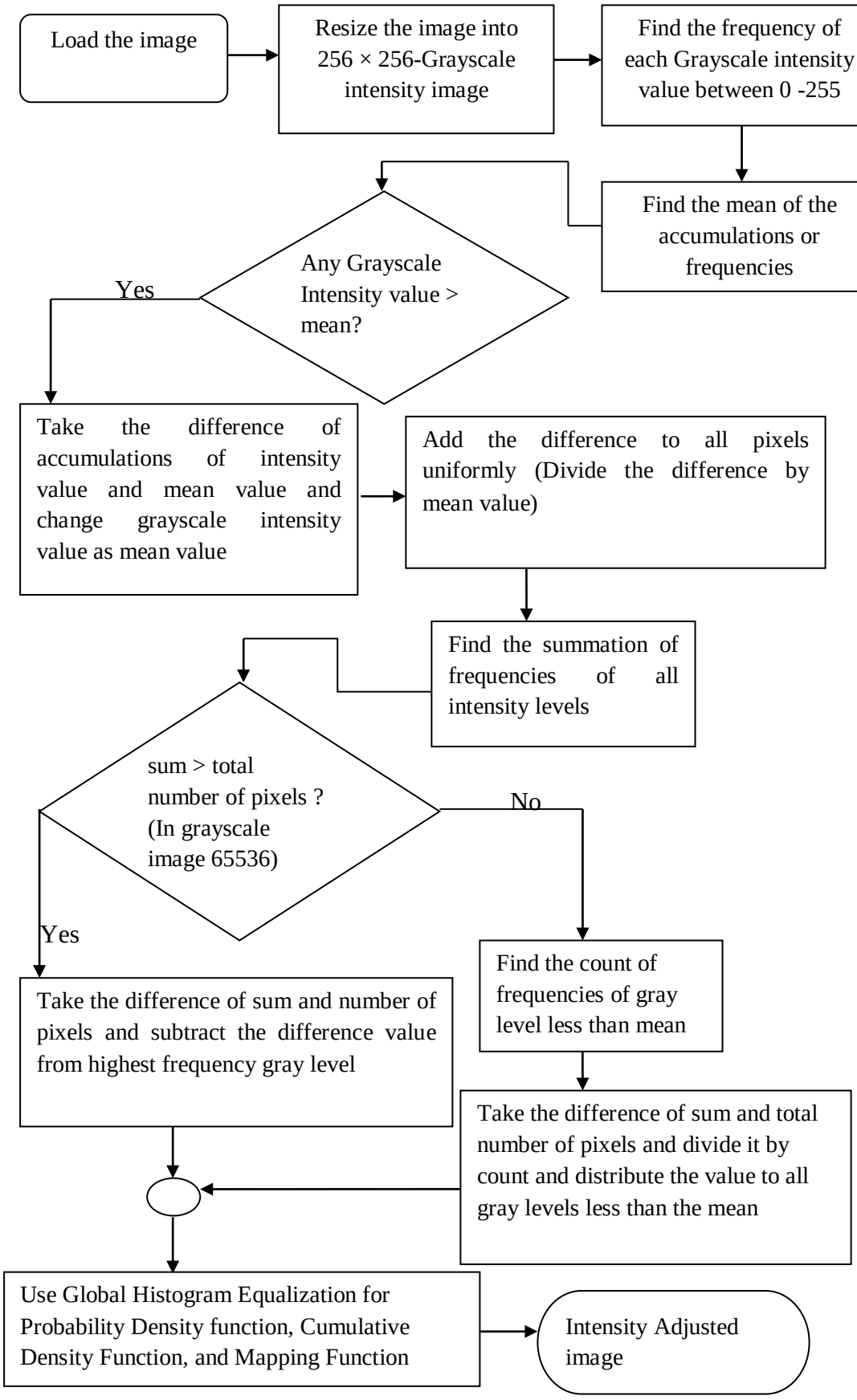


Fig. 3: Work Flow diagram of Methodology used in this study

(a) Original image [5] (b) GHE image (c) Histogram plotted for the original image

Figure 4.4: GHE of the image and histogram showing loss of information [25].

These phenomena are the main sources of the washed out appearances within the output image, which is shown in Figure 4.4.

The Figure 4.4 (c) shows the histogram of Figure 4.4 (a). The small frequencies in the rightmost point the histogram comes due to the flower image in the original image (Figure 4.4 (a)). Compare to the other high accumulations, these are very small, which might be not observed sometimes and may cause washout appearance. In this study, our main focus is to control the dominating gray levels over other small gray levels and making all gray levels more or less equal. This study also focuses on improving or adjusting the contrast of the image. Section 4.5.1 is explained with the pseudo algorithm.

4.5.1 Controlling of Dominating Gray levels

We make a modification for the Global Histogram Equalization at first step while calculating accumulations or frequencies of all gray level values. Our intention is to preserve even small part of the image. The algorithms of the approach used in this study referred as Novel Histogram Equalization (NHE) are shown below;

Step 1: Load the image of any size (input)

Step 2: Resize the image into 256 × 256 sized grayscale intensity image

Step 3: Find the frequency of the each gray level

```
for i= 1 to  row_size_of_image
    for j= 1 to column_size_of_image
        find frequency of individual pixels of i^th row and j^th column (freq [i] [j])
    end
end
```

Step 4: Find mean of frequencies (mean_freq)

Step 5**:** Find the frequency of intensity levels > mean

```
for i=1 to size_of_frequency_array
  if  freq [i] > mean_freq
```

Step 6: Find the difference value of frequency [i] and mean_freq

```
remaining_values = freq [i] - mean_freq
```

Step 7: Divide the difference value by mean

remaining_values = remaining_values / mean

Step 8: Assign the value of mean to freq[i]

freq [i] = mean

Step 9: Move from initial gray level frequency to last gray level frequency and add the remaining value to all intensity levels equally

```
for j= 1 to size_of_frequency_array
   freq [j] = freq [j] + remaining_values
end
end
end
```

Step 10: find summation of all frequencies and difference value of maximum number of pixels and sum of the frequency as sum_freq

diff= maximal number pixels (65536) – sum_freq // find difference

Step 11: if the difference greater or more than or equal to 1 (sum_freq less than maximum number of pixels) if diff > = 1

Step 12: Initialize a count for finding number of gray levels less than mean value

count = 0

Step 13: Find all intensity levels less than mean frequency and increment counter

```
for i=1 to size (freq)
   if freq[i] < mean_feq
        count++;
   end
   end
end
```

Step 14: Divide the difference by count assign this value to all gray levels frequencies whose value is less than mean value

```
diff / count
for i=1 to size (freq)
   if freq[i] < mean
      freq[i] = freq[i]+difference
   end
end
```

Step 15: if difference found in step 11 is less than 0 (sum_freq greater than maximum number of pixels)

if diff < 0

Step 16: Find the maximum frequency gray level

max_freq = max(freq)

Step 17: Locate the maximum frequency gray level and subtract the difference value from it.

```
for i=1 to size(freq)
   if freq[i] =max_freq
        freq[i] = freq[i]-diff
   end
end
```

Step 18: Follow the steps of GHE to find probability density function for each gray level
Step 19: Follow the steps of GHE to find cumulative density function for each gray level
Step 20: Follow the steps of GHE to find mapping function by rounding for each gray level obtaining by multiplying CDF with maximal intensity level or bin value
Step 21: Intensity adjusted image (output)

The NHE is mainly focused on controlling the dominating Gray levels. This algorithm takes into account the larger frequency gray level. If any gray level frequency value more than the mean value of the accumulations or frequencies, are cut-off or removed and the same value is equally distributed among all other gray levels including the same gray level, which had value more than the mean. There might be some time more than one gray level having value more than the mean value of the accumulations. The count of a total number of frequencies is always equal to the maximum count of pixels usually an image contains. In a 256 × 256 image, it will be 65536. In order to maintain this value after above operation we check sum of frequencies of all gray level and if it is less than the maximum count of pixels, then we equally assign the difference to all gray level frequencies, which is lower than the mean value. If it is more than the maximum count of pixels then we identify the maximum value of gray level frequency value and subtract the difference from it. By this way we try to keep a maximum number of frequencies is more or less or almost equal to the maximum count of pixels of the image. Because of round off calculations, there may be a small scale or very small difference in the maximum count of frequencies. We neglect these small differences. The NHE produces more range of intensity levels compare to GHE. Some of the comparisons of NHE and GHE are shown in Table 4.1.

Table 4.1: Comparison between NHE and GHE

Sr. No	**NHE**	**GHE**
1	Gray level frequencies or accumulations are more or less equal	Some Gray level count of frequencies or accumulations dominates over small gray level frequencies count.
2	Produces more range of intensity levels.	Produces less range of intensity levels.
3	The Brightness of the image is average, neither high nor less.	Some part of the image having high brightness.
4	Washout appearance is reduced maximum extent.	Washout appearance of the small part of the image is more.

4.6. EXPERIMENTAL RESULTS

The algorithm for Novel Histogram Equalization mentioned above is implemented using MATLAB 2015a. In this section, we will compare proposed NHE with GHE to know the performances of the enhancement techniques. In Figure 4.5 (a) low contrast boy image enhancement or contrast adjustment is done using Global Histogram Equalization (GHE) and

Novel Histogram Equalization (NHE). In GHE is image becomes brighter but contrast is not adjusted as much as an image obtained through NHE.

(a) Original image [5] (b) GHE image (c) NHE

Figure 4.5: Contrast adjustment outputs for a boy image (a) original image (b) GHE image (c) NHE image (using proposed method)

In Figure 4.6 (a) grayscale image of a lion is considered for testing. Initially, GHE equalization is done for initial lion image. The lion image becomes brighter but background grass is not clear in GHE. But which is clearer in NHE and also contrast is more adjusted.

Original image [5] GHE image (c) NHE

Figure 4.6: Contrast adjustment outputs for a lion image (a) original image (b) GHE image (c) NHE image (using proposed method)

The real power of the NHE method we can observe in Figure 4.7. The butterfly is sitting in a flower. The flower image in GHE has become brighter and its contrast is lost. In Figure 4.7 (c), even though flower image is not too bright it has good contrast compare to GHE image.

Original image [5] GHE image (c) NHE

Fig. 7: Contrast adjustment outputs for a butterfly with background flower image (a) original image (b) GHE image (c) NHE image (using proposed method)

4.7. SNAPSHOT OF THE CODING OF NHE USING MATLAB PROGRAMMING

Figure 4.8 shows the snap shot of the Novel Histogram equalization MATLAB coding. In this snapshot we focus mainly the code of proposed method, without giving emphasis on Global Histogram Equalization (GHE) steps.

```
global in
%Load the image of any size (input)
[fi,p]=uigetfile('\Contrast Adjustment\*','.*');
in=imread([p fi]);
% convert the input image to gray scale
in=rgb2gray(in);
%Resize the image into 256 × 256 sized gray scale intensity image
in=imresize(in,[256 256]);
normalizedImage =in;
%freq counts the occurrence of each pixel value.
freq=zeros(256,1);
%Find the frequency of the each gray level
for i=1:size(normalizedImage,1)
    for j=1:size(normalizedImage,2)
        value=normalizedImage(i,j);
        freq(value+1)=freq(value+1)+1;

    end
end
 %Find mean of frequencies
 mean1=round(mean(freq,1));
for i=1:size(freq,1)
    %Find the frequency of intensity levels > mean
     if freq(i)>mean1
     %Find the difference value of frequency  and mean of Frequency
        remaining=freq(i)-mean1;
        remain=round(remaining/mean1);
     %Assign the value of mean to freq[i]
        freq(i)=mean1;
     % Move from initial gray level frequency to last gray level frequency
     % and add the remaining value to all intensity levels equally
          for v=1:size(freq,1)
            freq(v)=freq(v)+remain;
        end
    end
end
numofpixels=size(normalizedImage,1)*size(normalizedImage,2);
s=0;
%find summation of all frequencies and difference value of maximum
%number of pixels and sum of frequency
s=numofpixels-sum(freq,1);
%if the difference greater than or equal to 1
%(sum_freq less than maximum number of pixels)
if s >=1
%Initialize a count for finding number of gray levels less than mean value
 count=0;
   for i=1:size(freq,1)
     if freq(i)< mean1
       count=count+1;
     end
   end
```

```
    ----
%Divide the difference by count assign this value to all gray levels
%frequencies whose value is less than mean value
  snew=round(s/count);
for v=1:size(freq,1)
    if freq(v)< mean1
     freq(v)=freq(v)+snew;
    end
end
end
%if difference found in step 11 is less than 0 (sum_freq greater
%than maximum number of pixels)
if s<0
  s=abs(s);
%Find the maximum frequency gray level
  t=max(freq,1);
 %Locate the maximum frequency gray level and subtract the
 %difference value from it.
  for i=1:size(freq,1)
      if t==freq(i);
       freq(i)=freq(i)-t;
      end
  end
end
```

Figure 4.8: Snapshot of MATLAB coding for Novel Histogram Equalization (NHE)

4.8 CONCLUSION

Contrast adjustment is a critical aspect or an important part of the enhancement or filtering process in image processing or recognition system. Their many variations of Global histogram equalization are mentioned in the literature. The new approach used in this study- Novel histogram equalization mainly focuses on controlling the dominating gray levels in terms of accumulations or frequencies over other small gray levels accumulations and making all gray levels more or less equal. This study also focuses on improving or adjusting the contrast of the image. This new method is computationally also simple to implement and any image processing applications easily can adopt this method. The limitation of the study is:

- In this study, the method is only implemented for a gray level image with size 256 x 256.
- The contrast adjustment is not too good but better than GHE
- Not works well with color image.
- More testing is required in order to generalize this approach.

In this study, a true attempt is made to improve the GHE method in terms of improving or adjusting the contrast of the 256 x 256 sized grayscale image.

REFERENCES

[1] Gonzalez, R. C., Woods, R. W. (2002). *Digital Image Processing*. *Education*. DOI: https://doi.org/10.1049/ep.1978.0474.

[2] Jain, A. K. (1989). *Fundamentals of Digital Image Processing*. *Portalacmorg* (Vol. 14). DOI: https://doi.org/10.1002/9780470689776.

[3] Zimmerman, J. B., Pizer, S. M., Staab, E. V., Perry, J. R., Mccartney, W., & Brenton, B. C. (1988). An Evaluation of the Effectiveness of Adaptive Histogram Equalization for Contrast Enhancement. *IEEE Transactions on Medical Imaging*, 7(4), 304–312. DOI: https://doi.org/10.1109/42.14513.

[4] Kim, Y. T. (1997). Contrast enhancement using brightness preserving bi-histogram equalization. *IEEE Transactions on Consumer Electronics*, 43(1), 1–8. DOI: https://doi.org/10.1109/30.580378.

[5] https://images.google.com/. (2017). Google. [online] Available at: https://images.google.com/ Low contrast Gray scale images [Accessed 15 September 2017].

[6] Pei, S. C., Zeng, Y. C., & Chang, C. H. (2004). Virtual restoration of ancient Chinese paintings using color contrast enhancement and Lacuna texture synthesis. *IEEE Transactions on Image Processing*, 13(3), 416–429. DOI: https://doi.org/10.1109/TIP.2003.821347.

[7] Wahab, A., Chin, S., & Tan, E. (1998). Novel approach to automated fingerprint recognition. *IEE Proceedings - Vision, Image and Signal Processing*. DOI: https://doi.org/10.1049/ip-vis:19981809.

[8] De La Torre, Á., Peinado, A. M., Segura, J. C., Pérez-Córdoba, J. L., Benítez, M. C., & Rubio, A. J. (2005). Histogram equalization of speech representation for robust speech recognition. *IEEE Transactions on Speech and Audio Processing*, 13(3), 355–366. DOI: https://doi.org/10.1109/TSA.2005.845805.

[9] Pizer, S. M. (2003). The Medical Image Display and Analysis Group at the University of North Carolina: Reminiscences and philosophy. *Medical Imaging, IEEE Transactions on*, 22(1), 2–10. DOI: https://doi.org/10.1109/TMI.2003.809707.

[10] Ziaei, A., Yeganeh, H., Faez, K., & Sargolzaei, S. (2008). A novel approach for contrast enhancement in biomedical images based on histogram equalization. In *International Conference on Computer and Communication Engineering 2008* (Vol. 1, pp. 855–858). DOI: https://doi.org/10.1109/BMEI.2008.300.

[11] Krishna Prasad, K. & Aithal, P. S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678.

[12] Krishna Prasad, K. & Aithal, P. S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608.

[13] Krishna Prasad, K. & Aithal, P. S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191.

[14] Lau, S. S. Y. (1994). Global image enhancement using local information. *Electronics Letters*, 30(2), 122–123. DOI: https://doi.org/10.1049/el:19940081.

[15] Kim, Y.-T. (1997). Quantized bi-histogram equalization. *Acoustics, Speech, and Signal Processing, 1997. ICASSP-97., 1997 IEEE International Conference on*, 4, 2797–2800 vol.4. DOI: https://doi.org/10.1109/ICASSP.1997.595370.

[16] Zhang, Y. J. (1992). Improving the accuracy of direct histogram specification. *Electronics Letters*, 28(3), 213-214.

[17] Xu, J., Zhang, Z., Xiao, X., Yang, Y., Yu, G., & Winslett, M. (2013). Differentially private histogram publication. *VLDB Journal*, 22(6), 797–822. DOI: https://doi.org/10.1007/s00778-013-0309-y.

[18] Yao, Z., Lai, Z., & Wang, C. (2017). Image Enhancement Based on Equal Area Dualistic Sub-image and Non-parametric Modified Histogram Equalization Method. In *Proceedings - 2016 9th International Symposium on Computational Intelligence and Design, ISCID 2016* (Vol. 1, pp. 447–450). https://doi.org/10.1109/ISCID.2016.1110.

[19] Chen, S. Der, & Ramli, A. R. (2003). Contrast enhancement using recursive mean-separate histogram equalization for scalable brightness preservation. *IEEE Transactions on Consumer Electronics*, 49(4), 1301–1309. DOI: https://doi.org/10.1109/TCE.2003.1261233.

[20] Chen, S. Der, & Ramli, A. R. (2003). Minimum mean brightness error bi-histogram equalization in contrast enhancement. *IEEE Transactions on Consumer Electronics*, 49(4), 1310–1319.DOI: https://doi.org/10.1109/TCE.2003.1261234.

[21] Chi-Chia, S., Shanq-Jang, R., Mon-Chau, S., & Tun-Wen, P. (2005). Dynamic contrast enhancement based on histogram specification. *Consumer Electronics, IEEE Transactions on*, 51(4), 1300–1305. DOI: https://doi.org/10.1109/TCE.2005.1561859.

[22] Abdullah-Al-Wadud, M., Kabir, M., Akber Dewan, M., & Chae, O. (2007). A Dynamic Histogram Equalization for Image Contrast Enhancement. *IEEE Transactions on Consumer Electronics*, 53(2), 593–600. DOI: https://doi.org/10.1109/TCE.2007.381734.

[23] Jagatheeswari, P., Kumar, S. S., & Rajaram, M. (2009). Contrast stretching recursively separated histogram equalization for brightness preservation and contrast enhancement. In *ACT 2009 - International Conference on Advances in Computing, Control and Telecommunication Technologies* (pp. 111–115). DOI: https://doi.org/10.1109/ACT.2009.37.

[24] Wongsritong, K., Kittayaruasiriwat, K., Cheevasuvit, F., Dejhan, K., & Somboonkaew, A. (1998, November). Contrast enhancement using multipeak histogram equalization with brightness preserving. In *Circuits and Systems, 1998. IEEE APCCAS 1998. The 1998 IEEE Asia-Pacific Conference on* (pp. 455-458). IEEE.

[25] Sengee, N., & Choi, H. K. (2008). Brightness preserving weight clustering histogram equalization. *IEEE Transactions on Consumer Electronics*, 54(3), 1329–1337. DOI: https://doi.org/10.1109/TCE.2008.4637624.

[26] Ibrahim, H., & Kong, N. S. P. (2007). Brightness preserving dynamic histogram equalization for image contrast enhancement. *IEEE Transactions on Consumer Electronics*, 53(4), 1752–1758. DOI: https://doi.org/10.1109/TCE.2007.4429280.

[27] Ibrahim, Haidi. "Histogram equalization with range offset for brightness preserved image enhancement." *International Journal of Image Processing (IJIP)* 5, no. 5 (2011): 599-609.

[28] Abdullah-Al-Wadud, M. (2012). A modified histogram equalization for contrast enhancement preserving the small parts in images. *International Journal of Computer Science and Network Security (IJCSNS)*, 12(2), 1.

******

Chapter 5

A Critical Study on Fingerprint Image Sensing and Acquisition Technology

Automatic Fingerprint Recognition System (AFIS) mainly depends on the quality of the fingerprint captured during the enrollment process, even though a lot of techniques developed in literature for fingerprint matching, all most all system is influenced or affected by the quality of acquisition method. Automated fingerprint identification system requires fingerprint images in a special format. Normally it can't receive and process the photographic image or photo taken from virtual camera or cell camera. There are many special acquisition or sensing strategies to extract the ridge-and-valley structure of finger skin or fingerprint. Traditionally, in law or regulation enforcement packages, fingerprints were especially received offline. Fingerprint acquisition can be specially classified into groups as an offline and live scan. An offline acquisition technique gets input through inked affect of the fingertip on paper and digitized with the aid of the paper with an optical scanner or video digital camera. The live acquisition is received through the sensor that is having the ability to directly digitize the sensing tip of the finger. As the fingerprint sensing, image processing, signal processing, and communication technology advance, an increasing number of new technologies in this acquisition technology are arriving at the main facet. In this paper, we discuss different types of fingerprint acquisition technologies, which involve optical, ultrasonic, capacitance, passive capacitance, and active capacitance. This paper helps to identify new fingerprint acquisition technology.

Keywords: *Fingerprint Sensing Technology, Fingerprint image, Optical fingerprint sensor, Ridge, Valley.*

5.1 INTRODUCTION

Automatic Fingerprint Identification System requires fingerprint image in particular format. Usually, it cannot accept and process the photographic image or image taken from digital camera or mobile camera. There are many special acquisition or sensing strategies to gain the ridge-and-valley structure of finger skin or fingerprint [1]. Traditionally, in regulation or law enforcement applications, fingerprints had been specially obtained offline. Fingerprint acquisition can be mainly categorized into two groups as an offline and live scan. An offline acquisition method gets input through inked affect of the fingertip on paper and digitized with the aid of the paper with an optical scanner or video digital camera. The live acquisition is obtained through the sensor that is having the ability to directly digitize the sensing tip of the finger. As the fingerprint sensing, image processing, signal processing, and communication technology advance more and more new technologies are arriving at the leading edge.

In recent times, most business and forensic programs receive live-experiment digital photographs acquired by way of directly sensing the finger surface with a fingerprint sensor based totally on optical, solid-state, ultrasonic and other imaging technology. Fingerprint sensors are available numerous sizes and styles but generally fall into two classes; region experiment (or contact) sensor and swipe sensor. With a touch sensor, the user places and holds the finger on the sensor surface and impact transferred from the pad of the final joint of finger or thumb. Touch sensors are used typically in constant systems because of their size and form [2]. Usually, touch sensors are square in shape and occupy more space and also weighs more; used in passport or immigration based applications. In swipe sensor, the user glides a finger vertically over the surface. The size and shape of the swipe sensors make it suitable for portable electronic gadgets like laptop computers and mobile phones [2-3]. However, swipe sensor technology intrinsically restricts their appropriateness for a few programs [4-9]. These sensors require customer education and practice to work consistently and they frequently fail to capture the fingerprint image. However, in each type of sensors, there are some common problems exist, like direct exposure to the surroundings, damage from mechanical results, electrostatic discharge (ESD), thermal surprise, discrimination between liveness and spoof. In this paper, we discuss different types of fingerprint acquisition technologies, which involve optical, ultrasonic, capacitance, passive capacitance, and active capacitance.

5.2 FINGERPRINT SENSING TECHNOLOGY-REVIEW

The initial types of fingerprint image have been impersonation in a fine-grained surface and later in a yellowish moldable substance called as wax. Starting from late 19th century to entire period of 20th century, the gaining or acquiring of fingerprint images were particularly carried out via ink-technique. This kind of acquisition method is referred as offline fingerprint sensing through moving in a particular direction-rolling, which remains being utilized in forensic packages and historical past assessments of applicants for highly sensitive jobs.

Later scanning instantaneously or live scanning device were developed, which makes use of technology multi-touch community based on Total Internal Reflection (FTIR), where F stands for Frustrated. The sensors carried out earlier had the disadvantage that they have been not suited for wet or dry arms and had to be wiped clean regularly to save you grease and dust from compromising the photo or image excellent.

Since last 20 years, fingerprint sensing technology has grown tremendously. Witnessing this growth as an instance Multispectral Fingerprint Imaging (MFI) has been introduced by the company Lumidigm, Inc. [10]. In contrast to traditional optical fingerprint sensors, MSI gadgets experiments the subsurface of the skin by using the usage of one-of-a-kind wavelengths of light. The fundamental idea is that distinct functions of skin motive extraordinary absorbing and scattering moves relying on the wavelength of light. Fingerprint snapshots obtained using the MSI technology appear to be of appreciably higher excellent in comparison to standard optical sensors for dry and wet palms. Multispectral fingerprint snapshots have also been shown to be beneficial for spoof detection [10].

Later, in 2006, sensing generation primarily based on the Multicamera device has been added. Those were termed as a touch less imaging and were added by means of TBS, Inc. [11]. Touchless imaging avoids direct touch among the sensor and the pores and skin and, therefore, constantly preserves the fingerprint ground reality without introducing skin deformation throughout photograph acquisition.

One of the maximum crucial traits of a digital fingerprint image is its resolution, which shows the number of dots or pixels per inch (PPI). Normally most of the fingerprint sensing device has resolution 250 to 300 (PPI) is considered to be a minimal requirement for any fingerprint feature extraction algorithm to extract minutiae details. FBI-compliant sensors have to fulfill the 500 (PPI) resolution requirements. However, a good way to capture pores in a fingerprint image, a significantly higher resolution, which is nearly of size 1,000 (PPI).
Even though it isn't yet realistic to layout solid-state sensors with the sort of high resolution due to the cost factor, optical sensors with a resolution of 1,000 (PPI) are to be had commercially. Extra excitingly, optical sensors with resolutions of 4,000-7,000 PPI have also been developed, which are most effective in capturing fingerprint image level 3 features for identification, and also helps to identify pore activities (commencing and final) for spoof detection.

Current years have visible a new high-resolution fingerprint device called P3400 [12-14]. That is a small and financially cheaper fingerprint reader brought by Zvetco inc. This device can produce 500 dpi images and is built of great aluminum. It is geared up with a 6-foot USB cable and is highly used with most biometric security access software packages.
The compact guardian consists of capabilities which include patented automatic capture capability and ideal rolling era, making it perfect for foolproof fingerprint acquisition in high-volume processing environments, consisting of visa issuance and border manipulate. The device can collect quality fingerprints at high resolution (500 dpi) in few seconds and meets worldwide requirements that observe government necessities in many nations.

The ten-print MFS-500 stay scanner is high resolution (500 and 1000 dpi) devices designed and built for optical perfection [15]. It may examine aircraft static fingerprints and can also be implemented in 3D print-pressed rolling scan. A sensor presents the very clean image and stops dry fingerprint problems. A form of fingerprint identity software is brought into the sensor to discover the fingerprint. The fingerprint captured with this scanner will have the highest identification and matching ratio, which is claimed by the manufactures.
Futronic FS80 USB2.0 fingerprint scanner uses a sophisticated CMOS sensor generation and precise optical device to supply high first-class fingerprint image. The finger is illuminated via 4 infra-purple LED's at some stage in scanning and the mild depth is robotically adjusted in step with scanning fingerprint's characteristics (wet, dry, blurred, etc.) to optimize the satisfactory of the captured fingerprint picture. it captures an undistorted uncooked fingerprint photo of 500dpi decision into the computer in 100msec. The scanner can reject fake fingers crafted from silicone rubber and play-doh. It supports fingerprint recognition, verification, authentication, and matching programs.

The sort of scanner used relies on the utility and environment where it is to be applied. in general, it is preferred to have scanners that are merchandise licensed for compliance with the FBI's included computerized fingerprint identity gadget image excellent specs. These forms encompass information concerning fingerprint image resolution, length (place), the number of pixels, geometric accuracy, gray-level quantization and gray variety, spatial frequency reaction, and signal-to-noise (SNR) ratio. The scanners licensed by way of the FBI as examined and in compliance with the FBI's subsequent technology identification (NGI) initiatives and included automatic fingerprint identification system (IAFIS). Table 5.1 List outs features of different types of fingerprint sensing technology.

Table 5.1: Various Fingerprint Sensing Technology and its Features

Sr. No	Sensing Technology	Features
1	Multispectral Fingerprint Imaging	• Ubiquitously Works for all types of users • Fast method for acquisition • Highly robust and repeatedly images can be taken
2	Touchless imaging	• Highly superior quality image • Highly invariant to fingerprint conditions • Built in accordance with user guidance • Non-intrusive capturing capacity
3	P3400	• Small in size • Most-cost effective fingerprint sensing technology • High resolution image-about 500 dpi • Highly scratch resistant
4	Ten-print MFS-500 stay scanner	• High resolution image-500 to 1000 dpi • High quality 3D image

		• Very clean image • Stops dry fingerprint problems • Good identification and matching capacity
5	Futronic FS80 USB2.0 fingerprint scanner	• Good quality image due to advanced CMOS technology • Having the capacity to reject false fingerprint from silicone rubber and play-doh • Affective in fingerprint recognition, verification, authentication, and matching programs

5.3 FINGERPRINT ACQUISITION METHODS

This section narrates different fingerprint acquisition method, which acts as an input or raw image for Automatic Fingerprint Identification System [16-18].

Optical: Optical fingerprint scanners are the oldest technique for capturing and evaluating fingerprints. This technique mainly depends on capturing an optical picture, basically a picture, and the use of algorithms to come across unique patterns on the surface, which include a ridge. Optical sensor comprises of the specialized digital camera, touch surface, a light-emitting phosphor layer, and solid state pixels. The specialized digital camera is used to acquire an image of the fingerprint ridge and valley pattern. A digital camera is located on the sensor and it captures the digital image using visible light. The touch surface is nothing but where the finger is kept, which is situated in the top layer of the sensor. Below the layer of touch surface is light emitted phosphor layer, which illuminates the surface of the finger when the finger is kept on the touch surface. The light emitted from the finger reaches to an array of solid state pixels with the aid of phosphor layer. Wound, scratch and dirty finger will cause a negative effect on the quality of the acquired image. The disadvantage of this kind of sensor is the reality that the imaging abilities are suffering from the high-quality of skin on the finger. As an instance, a dirty or marked finger is hard to image well. This sensor has a capacity of acquiring only two-dimensional images, synthetic or good quality image can be used to fool this acquisition device. Live finger detector mechanism should fuse along with this technology to attain more security.

Ultrasonic: Ultrasonic sensor works on the theory of medical ultrasonography with an intention to develop a visual image of the fingerprint. An ultrasonic sensor utilizes very high-frequency sound waves with an intention to penetrate epidermal layer of the skin. The sound waves are produced with the aid of piezoelectric transducers and also in order to measure reflected energy piezoelectric transducers are used. Image of the fingerprint can be generated by the reflected wave measurement due to reason that dermal skin layers show same features of the fingerprint. Due to this fact even though the skin is damaged and dirty it will exhibit same features of the fingerprint or which will not affect the quality of the input image [19].

Capacitance: Capacitance sensor utilizes the technology capacitance to shape fingerprint image. To generate ride and valley structure of the fingerprint capacitance sensor uses electric current. Capacitance sensor comprises a tiny array of cells with one or more semiconductor chips. Every cell includes two conductor plates with parallel plate capacitor and dermal layer and epidermal acts as a dielectric, which is a nonconductor [20].

Passive Capacitance: A passive capacitance sensor is almost similar to capacitance sensor, which forms an image of the fingerprint on the dermal layer of the skin. At every point of the array, a capacitance is measured with the help of sensor pixels. An air gap bridges the volume between the dermal layer and sensing element in valleys, which creates capacitance variance in ridge and valley structure of fingerprint. Two values are already known, which are a dielectric constant of the epidermis and area of the sensing element. Ridge and valley of the fingerprint are differentiated with the help of measured capacitance value [20].

Active Capacitance: In this type of sensor, initially before measurement of the fingerprint takes place, a voltage is applied to the skin with the help of charging cycle. Effective capacitor charges as an application of voltage. The pattern of the ridges in the dermal skin is identified with the help of electric field between finger and sensor. A reference voltage is maintained in discharge cycle in order to calculate the capacitance, by cross-comparing voltage across the dermal layer and sensing element. Later to form the image of the fingerprint the distance values are mathematically calculated. Like the ultrasonic sensor ridge pattern of the dermal layer are taken into considerations for measurement purpose. So this process overcomes the need for a clean surface and undamaged epidermal skin of the fingerprint [21-22].

5.4 COMPARISON OF OPTICAL AND NON OPTICAL SENSORS

In Table 5.2 Optical and Non optical fingerprint scanners are discussed with five parameters. These parameters are Measurements, Advantages, Benefits, Constraints, and Disadvantages.

Table 5.2: Comparison of Optical and Non optical Sensors

	Optical	Non optical
Measurements	Light	Pressure, Heat, Capacitance and Ultrasonic wave.
Advantages	Specially-strong performance, Physical or electrical durability, Excellent image	Mass production leads to low cost. Compact and low size makes it appropriate for low power applications like a mobile phone or laptop computers.
Benefits	Oldest and well-known method, Good technology support, Applications in the area of Attendance control, entry control, banking service etc.	Positive competition leads to mass production, which in turn leads to cost reduction. Similar to optical can be used for various applications.

Constraints	Difficult to build spoof free or highly secured system	Complex structure, Lack of technical knowledge leads to capture false points of a fingerprint.
Disadvantages	Reduction in size of the image is too costly, Relatively easy to compromise the security	Performance variations with respect to outer changes in temperature and dryness of a finger

5. 5 CONCLUSION

Fingerprint image sensing technology is meant for capturing fingerprint image in a particular format with various factors like image resolution, length (place), Quantity or number of pixels, Geometric accuracy, Gray-level Quantization and Gray Variety, Spatial frequency and many more, which is utilized by highly powered Automatic fingerprint recognition or identification device for Authentication purpose. As we have discussed in this paper there are many types of sensor devices mainly based Optical and Non-optical devices. In this paper, we discuss different types of fingerprint acquisition technologies, which involve optical, ultrasonic, capacitance, passive capacitance, and active capacitance. This paper helps to identify new fingerprint acquisition technology.

REFERENCES

[1] Xia, X., & O'Gorman, L. (2003). Innovations in fingerprint capture devices. *Pattern Recognition*, 36(2), 361-369.

[2] Memon, S., Sepasian, M., & Balachandran, W. (2008, December). Review of finger print sensing technologies. In *Multitopic Conference, 2008. INMIC 2008. IEEE International* (pp. 226-231). IEEE.

[3] Galy, N., Charlot, B., & Courtois, B. (2007). A full fingerprint verification system for a single-line sweep sensor. *IEEE Sensors Journal*, *7*(7), 1054-1065.

[4] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[5] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608

[6] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[7] Krishna Prasad, K. & Aithal, P.S. (2017).A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization.

International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[8] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 51-65. DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[9] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), 98-111. DOI: http://dx.doi.org/10.5281/zenodo.1067110

[10] Nixon, K. A., & Rowe, R. K. (2005, March). Multispectral fingerprint imaging for spoof detection. In *Proc. of SPIE Vol* (Vol. 5779, p. 215).

[11] Parziale, G., Diaz-Santana, E., & Hauke, R. (2006, January). The surround imagertm: A multi-camera touchless device to acquire 3d rolled-equivalent fingerprints. In *International Conference on Biometrics* (pp. 244-250). Springer, Berlin, Heidelberg.

[12] Lockie, M. (2006). Fakta stores go biometric in Denmark. *Biometric Technology Today*.

[13] Esekhaigbe, E. J. (2016). *Contributions to Biometric Recognition: Fingerprint For Identity Verification* (Doctoral dissertation, Cardiff Metropolitan University).

[14] Chao, T. H., & Cammack, J. (2007). *U.S. Patent Application No. 11/654,197*.

[15] Kaye, D. H. (2012). The Report of the Expert Working Group on Human Factors in Latent Print Analysis--Latent Print Examination and Human Factors: Improving the Practice through a Systems Approach.

[16] Kozan, N., Kotsyubinskaya, J., & Zelenchuk, G. (2017). Express Prediction of External Distinctive Features Of Person Using The Program of Dermatoglyphics For Prediction. *Eureka: Health Sciences*, (3), 26-32.

[17] Scheibert, J., Leurent, S., Prevost, A., & Debrégeas, G. (2009). The role of fingerprints in the coding of tactile information probed with a biomimetic sensor. *Science*, *323*(5920), 1503-1506.

[18] Baratelli, P. J. (2001). *U.S. Patent No. 6,325,285*. Washington, DC: U.S. Patent and Trademark Office.

[19] Meghdadi, M., & Jalilzadeh, S. (2005, October). Validity and acceptability of results in fingerprint scanners. In *Proceedings of the 7th WSEAS International Conference on Mathematical Methods and Computational Techniques In Electrical Engineering* (pp. 259-266). World Scientific and Engineering Academy and Society (WSEAS).

[20] Setlak, D. R. (2005). Advances in biometric fingerprint technology are driving rapid adoption in consumer marketplace. *Retrieved December*, *08*, 2017.

[21] Aithal, P. S. (2016). A Review on Advanced Security Solutions in Online Banking Models,

International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 421-429. DOI: http://doi.org/10.5281/zenodo.160971.

[22] Aithal, P. S. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. *International Journal of Management, IT and Engineering (IJMIE)*, 5(7), 455-464, DOI :http://doi.org/10.5281/zenodo.268875.

****

Chapter 6

A Conceptual Study on Fingerprint Thinning Process based on Edge Prediction

Biometric recognition encompasses numerous modern strategies. Among them, fingerprint reputation is taken into consideration to be the most effective approach for utmost security authentication. As industrial incentives boom, many new technologies for user identity are being advanced, each with its very own strengths and weaknesses and a potential area of interest marketplace. Fingerprint matching consists of a different process like filtering or preprocessing, binarisation, thinning or skeletonisation, postprocessing, feature extraction, and matching. Out of these fingerprint thinning or skeletonisation is one of the important processes in fingerprint identification or verification systems. Fingerprint thinning or skeletonisation is the manner or technique of lowering the thickness of every line of a fingerprint pattern or ridge pattern to just a single pixel width. After extracting the minutiae from the improved, binarised and thinned image some post-processing is carried out on this final fingerprint image to take away any spurious minutiae. The techniques on this class are of types–crossing number based and morphology-based totally. In this paper even though a new method for thinning is not proposed but a real attempt is made to explain the Edge prediction based thinning process. The Edge Prediction based Skelton formation is totally based on the conditional thinning set of rules, which is used to carry out thinning. The Edge Prediction based thinning process is explained with the help of workflow, algorithm, and flowchart.

Keywords: *Thinning, Skeletonisation, Minutiae, Crossing Number, Edge Prediction Based Skelton Formation.*

6.1 INTRODUCTION

The drastic changes in mobile and wireless based technologies and increasing number of applications and users demanded for high security concern, which leads to research on biometrics with a purpose to increase the security aspects and to minimize security threats. Even though biometric systems are not so easily vulnerable to security threats but some intelligent intruder can compromise the system using the information of biometric templates. So it's essential and necessary to develop non invertible, revocable and highly robust biometric templates [1-5].

Fingerprint thinning or skeletonisation is the manner or technique of lowering the thickness of every line of a fingerprint pattern or ridge pattern to just a single pixel width [6-7]. The necessities of a good thinning algorithm with respect to the fingerprint are

- The thinned fingerprint image received must be of single pixel width without discontinuities.
- Each ridge must be thinned to its center pixel.
- Noise and singular pixels have to be removed.
- Elimination of pixels should not cause elimination of true minutiae or after the completion of thinning method none of the pixels eliminated.

There are many techniques to be had in literature for skeletonisation or thinning process. After extracting the minutiae from the improved, binarised and thinned image a post processing is accomplished in this final fingerprint image to filter or remove any spurious minutiae.

Skeletonised technique of minutiae extraction is likewise called Skeletonisation-based minutiae extraction. Here again, pre-processing strategies are carried out to enhance or remove noise, the fingerprint image is segmented and binarised. The binarised image is then thinned using a set of rules that removes pixels from ridges until the ridges are one pixel length [8]). There are many methods available in literature for skeletonisation or thinning process [9-11]. After extracting the minutiae from the improved, binarised and thinned image some post processing is carried out on this final fingerprint image to take away any spurious minutiae. The techniques on this class are of types–crossing number based and morphology based totally.

Crossing number wide variety based, which is the most extensively used technique of minutiae extraction inside the skeletonized binary image class. This method is ideal over different methods due to its computational performance and intrinsic simplicity. In this method, a skeleton image is used in which the ridge run pattern is considered as a window with size of eight-connected. The nearby pixel of every ridge pixel in the image is scanned the usage of a 3×3 window from which the minutiae are extracted as shown in Figure 6.1. The crossing number may be used to categorize a ridge pixel as a finishing, bifurcation or non-minutiae point. As an example, a ridge pixel with a crossing-number of zero will correspond to an isolated factor and a crossing number of 4 correspond to a crossing factor.

P4 P3 P2
P5 P P1
P6 P7 P8

Figure 1: 3 × 3 Neighborhood

Jain et al., (1997) [12] have additionally performed minutiae extraction with the need of the skeleton image. Their approach entails the usage of a 3x3 window to verify the nearby area of each ridge pixel within the image. A pixel is then categorized as a ridge finishing if it has most effective one neighboring ridge pixel within the image, and categorized as a bifurcation if it has 3 neighboring ridge pixels. Therefore, it can be seen that this approach is very much like the crossing number technique. Table 6.1 shows properties of crossing number of Skeletonisation.

Table 1: Properties of crossing number of Skeletonisation

(Source: Bansal et al., 2011 [21])

Crossing number	**Property**
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Fake or false minutiae may be added to the image because of elements including noisy image, and image artifacts created by the thinning or Skeletonisation process. Subsequently, after the minutiae are extracted, it's far essential to do post-processing which will validate the minutiae. Few examples of false minutiae structures include the spur, hollow, triangle and spike systems (Xiao & Raafat, 1991). It could be seen that the spur shape generates false ridge endings; whereas both the hollow and triangle systems generate false bifurcations. The spike structure creates a fake bifurcation and a fake ridge finishing point.

The majority of the proposed work for image post processing-processing after thinning, in the literature [13-15] are based on a series of structural policies used to discard spurious minutiae. For example, a ridge ending factor that is linked to a bifurcation point, and is below a sure or convinced threshold distance is removed. But, alternatively, then using a unique set of heuristics every time to do away with a unique kind of fake minutia, some processes include the validation of different varieties of minutiae right into a single algorithm. They verified the validity of each minutiae point by way of scanning the skeleton image and analyzing the local neighborhood across the minutiae. The algorithm is then able to cancel out fake or false minutiae primarily based on the configuration of the ridge pixels connected to the minutiae point.

Amengual et al., (1997) [16] considered low-level features or minutiae points in order to extract features of the fingerprint image. For the description and retrieval of minutiae, they used already available varieties of minutiae extraction method or techniques by modifying a little bit. Farina et al., (1999) [17] proposed set of algorithms for minutiae extraction from the fingerprint image.

Gnanasivam & Muttan (2010) [18] proposed preprocessing techniques for filtering and noise removal of the image before extracting features from the image. The preprocessing is done to acquire the vertical orientated fingerprint image followed through the center point of fingerprint pattern detection-core point and region of interest choice. Then characteristics extraction is performed in the extracted area of concern image.

Leung et al., (1991) [19] proposed a neural network primarily based approach to minutiae extraction where preprocessing strategies are first carried out to clean or remove the noises and then binary ridge pattern is thinned or skeletonised. Before applying neural network approach skeleton is ready for feature extraction. In a later stage, a multilayer perceptron concept of three layers is trained to extract the minutiae from the skeletonised image of the fingerprint.

The morphology-based minutiae extraction strategies are based on mathematical morphology (Humbe et al., 2007; Bansal et al., 2010) [20-21] in which the image is pre-processed with an intention to reduce the overhead of post-processing filtering. The image is pre-processed with morphological operators to do away with spurs, bridges and so on (Bansal et al., 2010) [21]. After which the authentic minutiae are extracted through the morphological hit or miss rework to extract original minutiae. The morphological operators are forming operators which permit the manipulation of shapes for identity and also the composition of objects and item capabilities. Morphological operators are essentially shaping operators and their composition permits the natural manipulation of shapes for the identity and the composition of objects and object-capabilities [22-26]. The approach develops structuring factors for exceptional forms of minutiae found in a fingerprint image to be utilized by the HMT to extract legitimate minutiae. Ridge endings are those pixels in an image which have only one nearby point in a 3x3 neighbourly located pixels or points.
In this paper Edge Prediction based Skeleton formation method is discussed with its workflow, algorithm. The algorithm is analyzed using FVC ongoing 2002 datasets.

6.2 EDGE PREDICTION BASED SKELTON FORMATION

The Edge Prediction based Skelton formation is totally based on the conditional thinning set of rules (You & Wang, 2003) [27], which are used to carry out thinning. Mark the target point 1, the background as zero. The main idea is here to use, eight-neighbourhood and there may be at least one background pixel or point, defined as a boundary point. This method considers segmented image, $I_{segment}$ as input for this process.
The output from this method is skeletonised or thinned image, denoted as $I_{skeleton}$. Initially the size of the $I_{segment}$ is calculated. In this method 3 × 3 frame is moved across every pixel of the image. If $I_{segment}$ (i, j) =1, then it signifies that particular pixel is not part of the

image's foreground, it's just background pixel. Where i, and j represents index of row and column dimension of the image. Image is traced in row and column order from second row and column to till the second last row and column. If $I_{segment}$ (i, j) =1, then for each pixel, including that pixel, a 3 × 3 frame is created based on following equations. The frame image is referred as temp. $temp = I_{segment}\big((i-1:i+1),(j-1:j+1)\big)$

In above assignment statement, i and j represents row and column position of the $I_{segment}$ image. The shape of the frame for $I_{segment}$ (2, 2), image matrix is as follows. The actual pixel position is (2, 2), which is surrounded by 8 pixels in different eight directions. The central pixel is surrounded by a ring shape starting from (1, 1) , (1, 2), (1, 3), (2, 3), (3, 3), (3, 2), (3, 1), (2, 1), and (1, 1). The central pixel is checked with all eight neighbouring pixels. The image type is logical so it contains either zero or one as its intensity values. One represents background of the fingerprint image and zero represents foreground of the image. Figure 6.2 shows 3 x 3 frame used in Edge Prediction based Skelton formation.

(1, 1)	(1, 2)	(1, 3)
(2, 1)	(2, 2)	(2, 3)
(3, 1)	(3, 2)	(3, 3)

Figure 6.2: Example of 3 x 3 frame used in Edge Prediction based Skelton formation

Next we find values of these eight positions and store that values in a variable called, RE_{temp}. Generally Ring structure for any pixel position is created as follows,

Trace from first column of the temporary variable to column size value-1 for following two statements

$RE_{temp}(i) = temp(1,i)$ \\RE_{temp}→Ring Extracted for temp Matrix

$RE_{temp}\left(\left(C_{temp}-1\right)+\left(R_{temp}-1\right)+i\right) = temp(R_{temp}, C_{temp}+1-i)$ \\$C_{temp}$→column size, variable i, is index of column.

Trace from first row of the temporary variable to row size value-1 for following two statements.

$RE_{temp}\left(C_{temp}+i\right) = temp\left(1, C_{temp}\right)$

$RE_{temp}\left(\left(C_{temp}-1\right)+\left(R_{temp}-1\right)+i\right) = temp(R_{temp}+1-i, C_{temp})$ \\$R_{temp}$→Row size of temporary variable, variable i, is index of Row.

Assign the temporary variable first element value to Ring Extracted for temp Matrix's last position (RE_{temp}), which is usually becomes (9, 9) position in 3 × 3 frame. This assignment statement is shown below.

$$RE_{temp}\left(\left(C_{temp}-1\right)+\left(R_{temp}-1\right)+\left(C_{temp}-1\right)+\left(R_{temp}-1\right)+1\right) = temp(1,1)$$

Consider For example, central pixel position as (2, 2). The pixels positions of the RE_{temp} matrix are assigned as shown in Table 6.2.

Table 6.2: Example of Edge Vector used in Edge Prediction based Skelton formation

Sr. No	Edge Vector ($\boldsymbol{RE_{temp}}$)	Temporary Image formed from $\boldsymbol{I_{segment}}$ (temp)
1	RE_{temp} (1)	temp (1, 1)
2	RE_{temp} (5)	temp (3, 3)
3	RE_{temp} (2)	temp (1, 2)
4	RE_{temp} (6)	temp (3, 2)
5	RE_{temp} (3)	temp (1, 3)
6	RE_{temp} (7)	temp (3, 1)
7	RE_{temp} (4)	temp (2, 3)
8	RE_{temp} (8)	temp (2, 1)
9	RE_{temp} (9)	temp (1, 1)

Next, we find the NP corresponds to total number of points which is having logical value 1 or which contains background part of the fingerprint segmented image. Simply, NP is Temporary Variable to save the result of that corresponding calculation. NP can be obtained using following equation.

$$N_p = \frac{\left(\sum RE_{temp}\right)^2 - (RE_{temp}(1))^2}{\left(\sum RE_{temp}\right) + RE_{temp}(1)} \quad \text{---------- (Eq. 6.1)}$$

The RE_{temp} matrix is reshaped as 1 × 9 logical matrix. Next we find total number of terminating point around the central pixel. We consider a variable T_p, corresponds to terminating point. Last position of RE_{temp} matrix contains value of first position itself. So we trace and find only eight neighbourhood pixel position values and at a time we consider contiguous two pixel position starting from first position. If first pixel position contains zero and next succeeding pixel contains one then it is marked as T_p. This is shown in following statement,

if $(RE_{temp}(p) = 0)$ & $(RE_{temp}(p+1) = 1)$ $T_p = T_p + 1$

Here p can take any value from 1 to 8. When RE_{temp} contains NP > =2 and NP<=6 and TP=1 and $(RE_{temp}(2) * RE_{temp}(4) * RE_{temp}(6) = 0)$ and $(RE_{temp}(4) * RE_{temp}(6) * RE_{temp}(8) = 0)$, we have to store the current central pixel row and column position or index value to one temporary matrix denoted as F1 with two columns and n number of rows. Where n represents total number of central pixels which is having value 1 or which is a part of background pixels of the segmented image.

We trace eight neighbourhood pixel position values starting from 1 position to 8 through P. The statement can be expresses as

if (N_p >=2) & (N_p <=6) & (T_p ==1) & $\left(RE_{temp}(2) * RE_{temp}(4) * RE_{temp}(6) == 0\right)$ & $\left(RE_{temp}(4) * RE_{temp}(6) * RE_{temp}(8) == 0\right)$ (Eq. 2)

F1 (F+1, 1) = i and F1 (F+1, 2) = j where F is a temporary variable with initial value as 0. Increment the value of F as F= F+1.

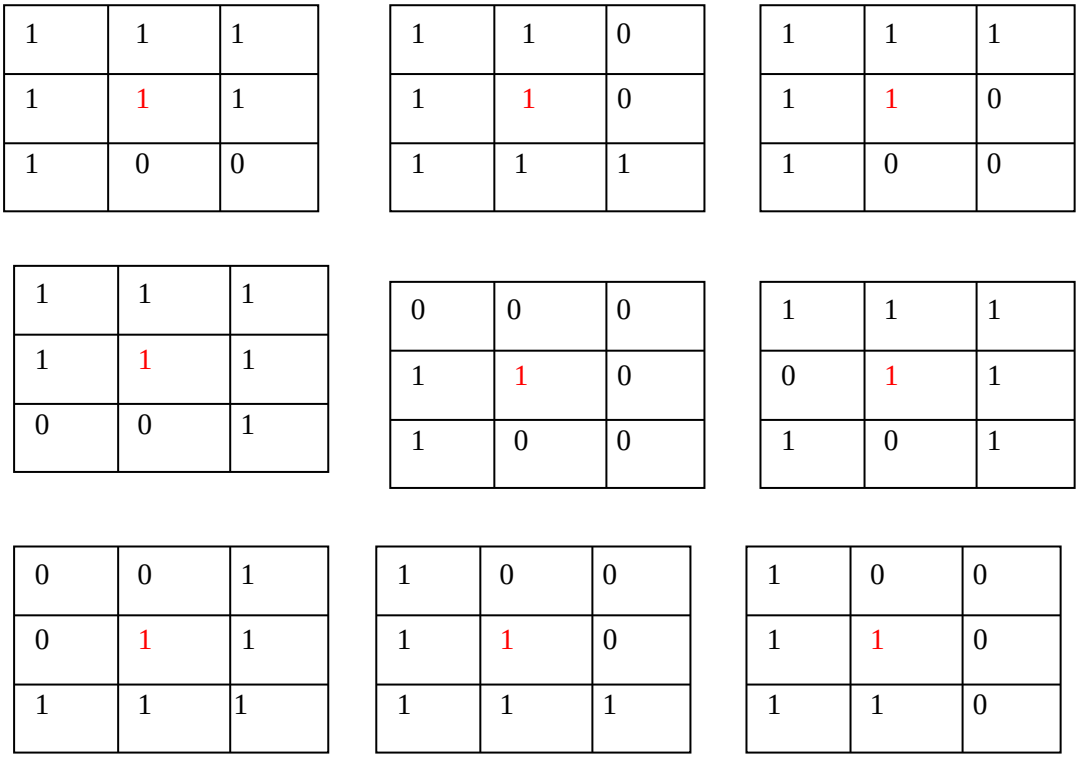


Figure 6.3: Examples of few different possibilities where thinning function is repeated

Figure 6.3 shows examples of different possibilities where temporary matrix F1 is initialized with position of central pixel position. In general words, near by pixel of the central pixel, which contains foreground pixel has to be thinned. Usually red color represents central pixel. All the central pixel positions are stored in temporary matrix F1, if it satisfies the Eq. 2. The F1 matrix corresponding to $I_{segment}$ image is reassigned with value 0, which is shown below.

$$I_{segment}\big(F1(i,1), F1(i,2)\big) = 0$$

The above statement is repeated from first row position of F1 to till last row position with fixed column size as 2. Next we create another temporary variable N_{F2} and initialize it with value zero. Next we repeat same process starting from, if $I_{segment}$ (i, j) =1 to $I_{segment}\big(F2(i,1), F2(i,2)\big) = 0$. Until condition (F > 0 or $N_{F2} > 0$) fails, repeat all above steps of for $I_{segment}$.

6.3 EDGE PREDICTION BASED SKELETON FORMATION ALGORITHM

Input: Segmented Image, $I_{segment}$

Output: Skeletonised Image, $I_{skeleton}$

Step-1: [R C]=size($I_{segment}$) \\ R→Row Size of skeleton Image; C→Column Size of skeleton Image and assign F=0; \\ F→Temporary variable

Step-2: for i=2 to R-1

Step-3: for j=2 to C-1

Step-4: if $I_{segment}(i,j) = 1$

Step-5: $temp = I_{segment}\big((i-1:i+1),(j-1:j+1)\big)$;

Step-6: for i=1 to $C_{temp} - 1$

Step-7: $RE_{temp}(i) = temp(1, i)$ \\$RE_{temp}$→Ring Extracted for temp Matrix

Step-8: $RE_{temp}\left(\left(C_{temp} - 1\right) + \left(R_{temp} - 1\right) + i\right) = temp(R_{temp}, C_{temp} + 1 - i)$; end step-6 for

Step-9: for i=1 to $R_{temp} - 1$ \\R_{temp}→Row size of temporary variable

Step-10:$RE_{temp}\left(C_{temp} + i\right) = temp\left(1, C_{temp}\right)$

\\C_{temp}→Column Size of temporary variable

Step-11: $RE_{temp}\left(\left(C_{temp} - 1\right) + \left(R_{temp} - 1\right) + i\right) = temp(R_{temp} + 1 - i, C_{temp})$;

Step-12: end step-9 for loop

Step-13: $RE_{temp}\left((C_{temp} - 1) + \left(R_{temp} - 1\right) + (C_{temp} - 1) + \left(R_{temp} - 1\right) + 1\right) = temp(1,1)$

Step-14: $N_p = \frac{\left(\sum RE_{temp}\right)^2 - (RE_{temp}(1))^2}{\left(\sum RE_{temp}\right) + RE_{temp}(1)}$

\\N_p→ Temporary Variable to save the result of that corresponding calculation

Step-14a: for p=1 to size(RE_{temp}, 2)-1

Step-14b: if ($RE_{temp}(p) = 0$) & ($RE_{temp}(p + 1) = 1$)

Step-14c: $T_p = T_p + 1$; end if end for loop

Step-15: for p=1 to size(RE_{temp}, 2)-1

Step-16: if (N_p>=2) & (N_p<=6) & (T_p==1) &$\left(RE_{temp}(2) * RE_{temp}(4) * RE_{temp}(6) == 0\right)$&$\left(RE_{temp}(4) * RE_{temp}(6) * RE_{temp}(8) == 0\right)$

Step-17: F1(F+1,:)=[i j];

Step-18: F=F+1; end if

Step-19: end if loop in step-4; end for loop in step-2

Step-20: if (F>0)

Step-21: for i=1 to size(F1,1)

Step-22: $I_{segment}\left(F1(i,1), F1(i,2)\right) = 0$;

Step-23: end for loop end if loop

Step-24: $N_{F2} = 0$

\\ N_{F2}→Temporary Variable which will change for every iteration of for loop on step-25

Step-25: for i=2 to $R_{segment} - 1$

Step-26: for j=2 to $C_{segment} - 1$

Step-27: if ($I_{segment}(i, j) = 1$)

Step-28: $temp = I_{segment}((i - 1{:}\, i + 1), (j - 1{:}\, j + 1))$

Step-29: for i=1 to $C_{temp} - 1$

Step-30: $RE_{temp}(i) = temp(1, i)$

Step-31: $RE_{temp}\left(\left(C_{temp} - 1\right) + \left(R_{temp} - 1\right) + i\right) = temp(R_{temp}, C_{temp} + 1 - i)$; end step-29 for

Step-32: for i=1 to $R_{temp} - 1$

Step-33:$RE_{temp}\left(C_{temp} + i\right) = temp\left(1, C_{temp}\right)$

Step-34: $RE_{temp}\left(\left(C_{temp}-1\right)+\left(R_{temp}-1\right)+i\right)=temp(R_{temp}+1-i,C_{temp})$;

Step-35: end step-32 for loop

Step-36: $N_p=\frac{\left(\sum RE_{temp}\right)^2-(RE_{temp}(1))^2}{\left(\sum RE_{temp}\right)+RE_{temp}(1)}$

\\N_p→ Temporary Variable to save the result of that corresponding calculation

Step-36a: for p=1 to size(RE_{temp}, 2)-1

Step-36b: if ($RE_{temp}(p)=0$) & ($RE_{temp}(p+1)=1$)

Step-36c: $T_p=T_p+1$;

Step-37: end if end for loop

Step-38: if (N_p>=2) & (N_p<=6) & (T_p==1) &$\left(RE_{temp}(2)*RE_{temp}(4)*RE_{temp}(6)==0\right)$&$\left(RE_{temp}(4)*RE_{temp}(6)*RE_{temp}(8)==0\right)$

Step-38a: F2($N_{F2}+1$,:)=[i j];

Step-39: $N_{F2}=N_{F2}+1$

Step-40: end step-38 if; end step-27 if; end step-25 for loop

Step-41: if $N_{F2}>0$

Step-42: for i=1 to R_{F2}

Step-43: $I_{segment}\left(F2(i,1),F2(i,2)\right)=0$;

Step-44: end for loop; end if statement

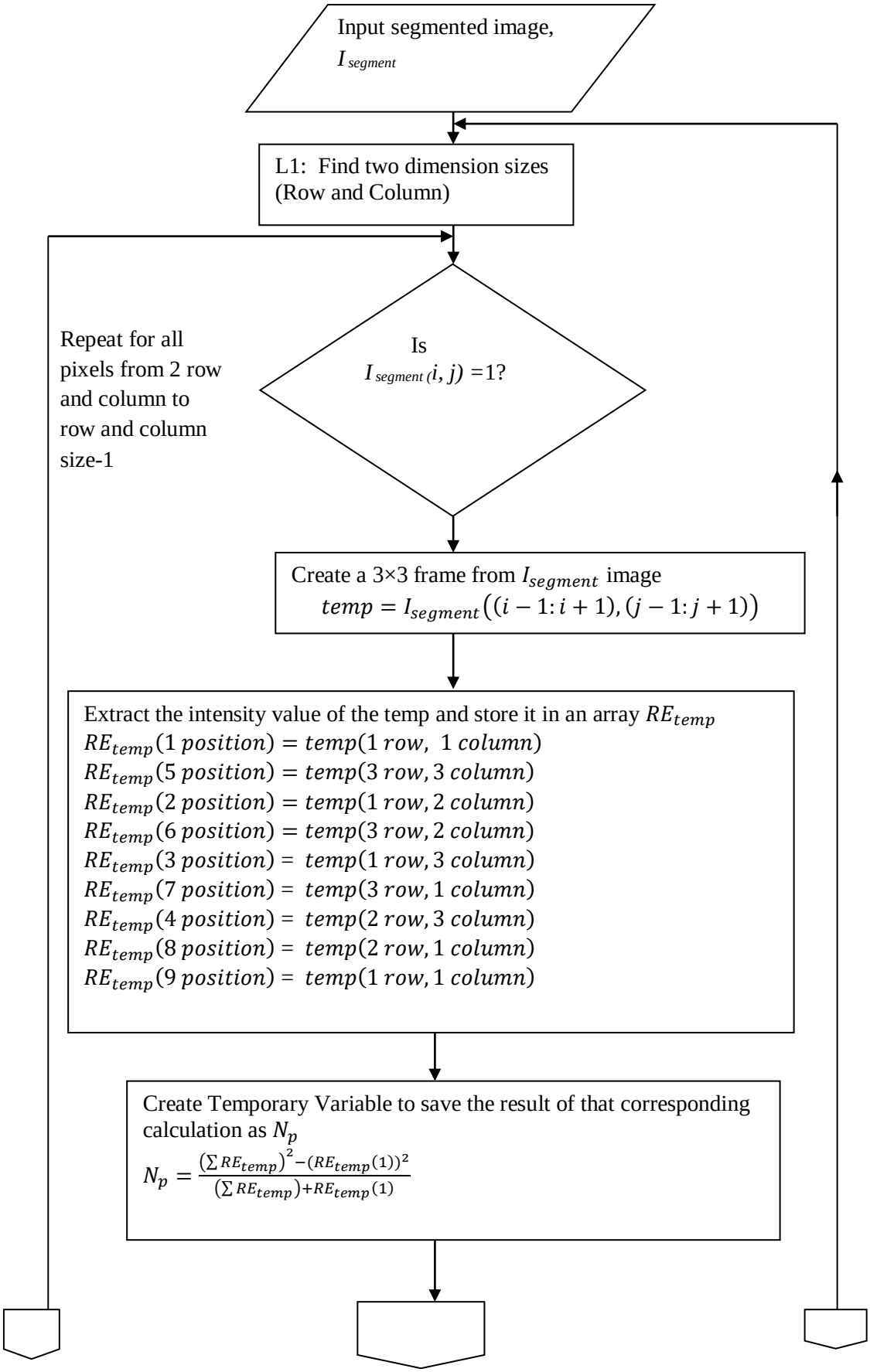
Step-45: if (F>0 or $N_{F2}>0$)

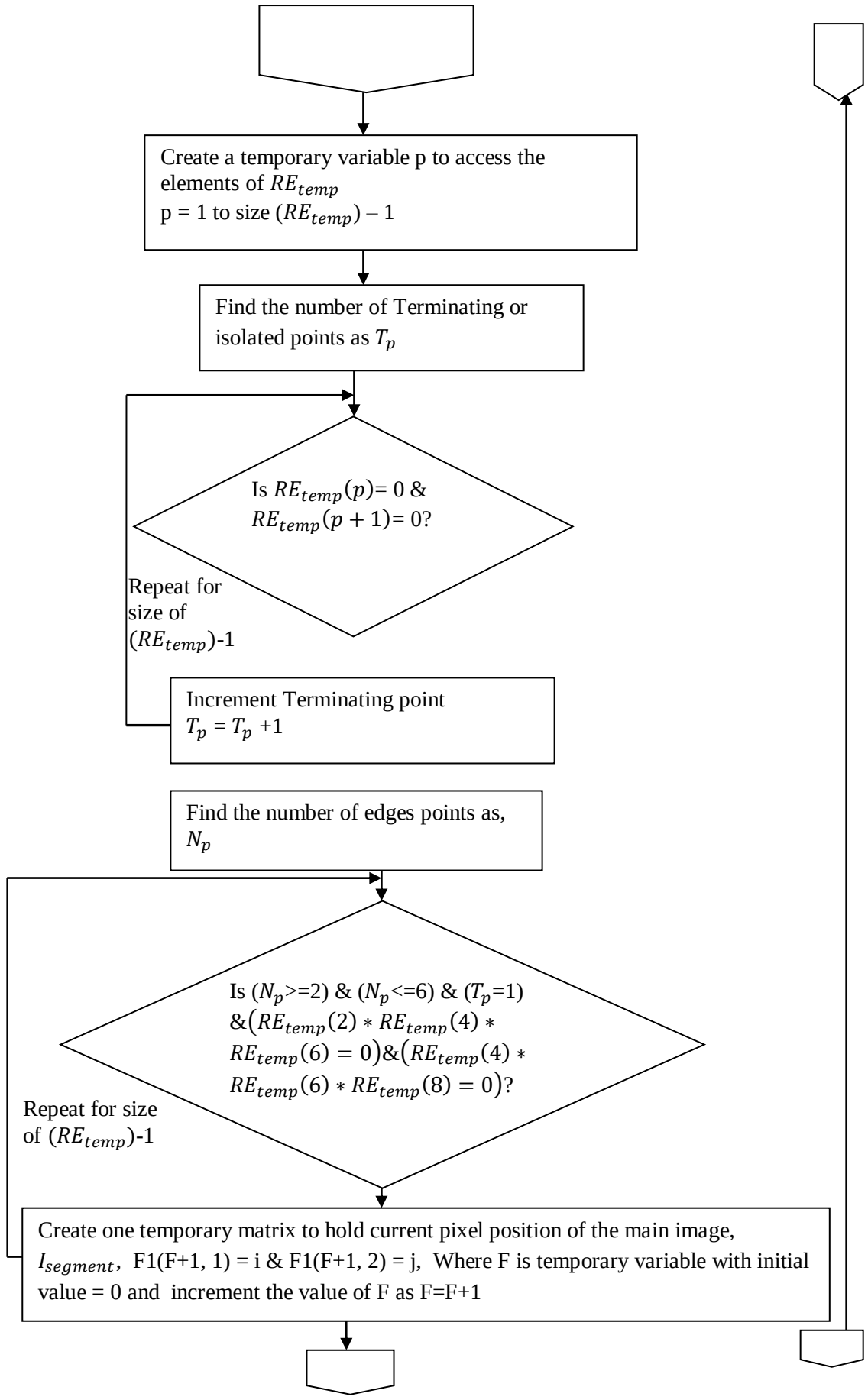
Step-46: $I_{skeleton}=repeat\ all\ the\ steps\ for\ I_{segment}$; end if

6.4 FLOWCHART FOR EDGE PREDICTION BASED SKELETON FORMATION ALGORITHM

This proposed algorithm for skeleton Formation is explained using flowchart. The input for this algorithm is segmented grayscale fingerprint image which is represented as $I_{segment}$. The final output is segmented image denoted as $I_{skeleton}$. The different workflows of the proposed algorithm are listed out below. The flow chart of this algorithm is shown in Figure 6.4.

- Check each pixel of the segmented image for background part of the image
- Create a 3×3 frame from $I_{segment}$ by keeping each pixel at centre and surrounded by 8 pixels starting from second row and second column to till last row and column-1.
- Create a ring of nine pixels (8+starting pixels) and extract ring values.
- Find the number of edges from the extracted ring for each central pixel.
- Find the count of terminating points of the ridge by simply counting the edge number (Edge number should be 0 or 1 for terminating point)
- Reduce the width of the foreground image, by making central pixel value zero.


Input segmented image, $I_{segment}$
L1: Find two dimension sizes (Row and Column)
Repeat for all pixels from 2 row and column to row and column size-1
Is $I_{segment}(i, j)$ =1?
Create a 3×3 frame from $I_{segment}$ image
$temp = I_{segment}\big((i-1:i+1),(j-1:j+1)\big)$
Extract the intensity value of the temp and store it in an array RE_{temp}
$RE_{temp}(1\ position) = temp(1\ row,\ 1\ column)$
$RE_{temp}(5\ position) = temp(3\ row, 3\ column)$
$RE_{temp}(2\ position) = temp(1\ row, 2\ column)$
$RE_{temp}(6\ position) = temp(3\ row, 2\ column)$
$RE_{temp}(3\ position) = temp(1\ row, 3\ column)$
$RE_{temp}(7\ position) = temp(3\ row, 1\ column)$
$RE_{temp}(4\ position) = temp(2\ row, 3\ column)$
$RE_{temp}(8\ position) = temp(2\ row, 1\ column)$
$RE_{temp}(9\ position) = temp(1\ row, 1\ column)$
Create Temporary Variable to save the result of that corresponding calculation as N_p
$N_p = \frac{\left(\sum RE_{temp}\right)^2 - (RE_{temp}(1))^2}{\left(\sum RE_{temp}\right) + RE_{temp}(1)}$


Create a temporary variable p to access the elements of RE_{temp}
p = 1 to size $(RE_{temp}) - 1$
Find the number of Terminating or isolated points as T_p
Is $RE_{temp}(p)$= 0 & $RE_{temp}(p+1)$= 0?
Repeat for size of (RE_{temp})-1
Increment Terminating point $T_p = T_p + 1$
Find the number of edges points as, N_p
Is (N_p>=2) & (N_p<=6) & (T_p=1) &$\left(RE_{temp}(2) * RE_{temp}(4) * RE_{temp}(6) = 0\right)$&$\left(RE_{temp}(4) * RE_{temp}(6) * RE_{temp}(8) = 0\right)$?
Repeat for size of (RE_{temp})-1
Create one temporary matrix to hold current pixel position of the main image, $I_{segment}$, F1(F+1, 1) = i & F1(F+1, 2) = j, Where F is temporary variable with initial value = 0 and increment the value of F as F=F+1

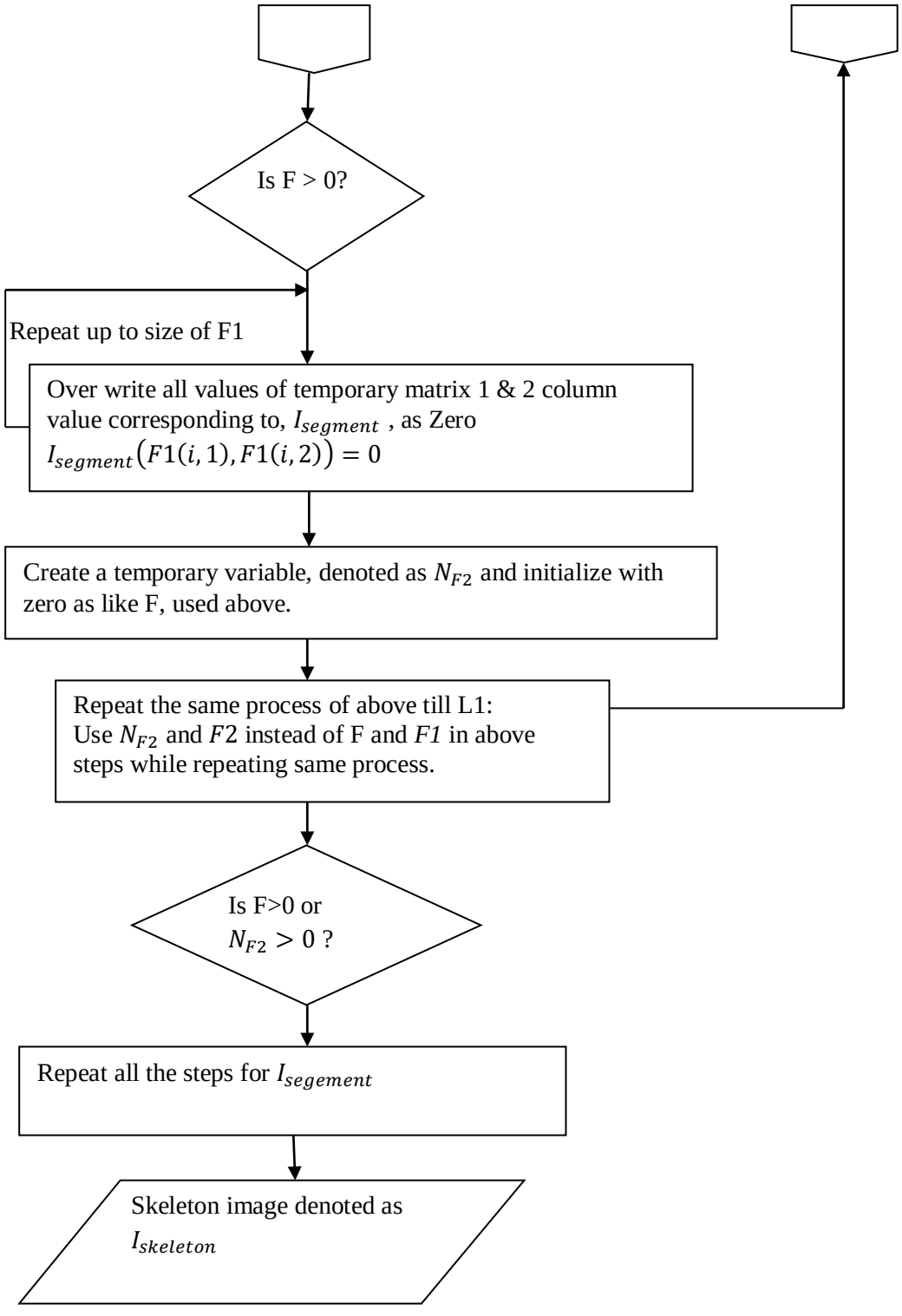


Figure 6.4: Flow chart for Edge Prediction based skeleton Formation Algorithm

Analysis of Edge Prediction based skeleton formation Algorithm

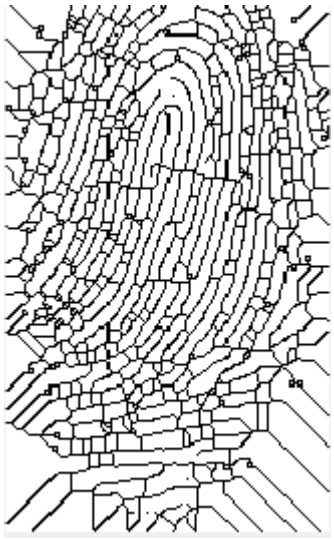
The Edge Prediction based Skeleton formation algorithm is analysed by considering FVC ongoing 2002 datasets. Figure 5 shows segmented image and skeleton image for sample image 101_1.tif.

In figure 6.5, 101_1.tif is a sample fingerprint image taken from FVC ongoing 2002 DB1_B dataset, which is of size 388 × 374 pixels. This image is initially converted into 256 × 256, before filtering process. After segmentation this image is again resized into 256 × 148. The figure 5 (a) represents this segmented image, and 5 (b) represents, its skeleton image. The skeleton image size is again resized into 254 × 146. Same way, in figure 5, 101_5.tif is a sample fingerprint image taken from FVC ongoing 2002 DB1_B dataset, which is of size 388 × 374 pixels. This image is initially converted into 256 × 256, before filtering process. After segmentation this image is again resized into 256 × 148. The figure 5 (c), represents this segmented image, and 3.19 (d) represents, its skeleton image. The skeleton image size is again resized into 254 × 156.

Segmented image-101_1.tif

Skeleton image of (a)

Segmented image-105_1.tif



Skeleton image of (c)

Figure 6.5: Example of Edge prediction based skeleton Formation

6.5 CONCLUSION

Biometrics innovation has ended up being a precise and proficient response to the security issue. Biometrics are a developing field of research as of late and has been dedicated to the distinguishing proof or authentication of people utilizing one or multiple inherent physical or behavioral characteristics.

Thinning is a special process that consecutively wears away the foreground pixels and finally produces lines that are almost one-pixel. The first and foremost condition for thinning is input image should be a binary image and produces output as a binary image. Thinning is a final prior step to minutiae extraction in automatic fingerprint recognition system. Thinning is not achieved in a single step but it achieved through an iterative process. The connectivity of ridges and bifurcation can be reproduced from the thinning, means it preserves the basic structure of the image without affecting its original structure.

After extracting the minutiae from the thinned image a few post processing is carried to cast off any spurious minutiae and final features of fingerprint image is obtained. The strategies on this elegance are of types–crossing number based and morphology based.
However, techniques based totally on thinning are sometime sensitive to noise and the skeleton shape does no longer conform to intuitive expectation. Non skeletonised feature extraction uses a binary image based totally technique. The principle problem within the minutiae extraction technique the use of thinning processes comes from the reality that minutiae within the skeleton image do not usually correspond to true minutiae inside the fingerprint image. In fact, quite a few spurious minutiae are determined because of undesired spikes, breaks, and holes. Consequently, put up processing is usually followed to keep away from spurious minutiae, which are based on each statistical and structural fact after characteristic or feature detection.

The main idea in Edge Prediction based skeleton formation to use, eight-neighbourhood and there may be at least one background pixel or point, defined as boundary point.
This method considers segmented image, $I_{segment}$ as input for this process. The output from this method is skeletonised or thinned image, denoted as $I_{skeleton}$. Initially the size of the $I_{segment}$ is calculated. This method is well known method for fingerprint thinning process and also effectively used for preprocessing skeleton in order to get better matching at the time of testing fingerprint phase..

REFERENCES

[1] K., Krishna Prasad, Aithal, P. S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[2] K., Krishna Prasad, Aithal, P. S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608

[3] K., Krishna Prasad, Aithal, P. S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[4] K., Krishna Prasad, Aithal, P. S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[5] K., Krishna Prasad, Aithal, P. S. (2017). Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 51-65. DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[6] Hastings, E. (1992). A survey of thinning methodologies. *Pattern analysis and Machine Intelligence, IEEE Transactions*, 4(9), 869-885.

[7] Lam, H. K., Hou, Z., Yau, W. Y., Chen, T. P., & Li, J. (2008, December). A systematic topological method for fingerprint singular point detection. In *Control, Automation, Robotics and Vision, 2008. ICARCV 2008. 10th International Conference on* (pp. 967-972). IEEE.

[8] Espinosa-Duro, V. (2002). Mathematical Morphology approaches for fingerprint Thinning. In *Security Technology, 2002. Proceedings. 36th Annual 2002 International Carnahan Conference on* (pp. 43-45). IEEE.

[9] Ahmed, M., & Ward, R. (2002). A rotation invariant rule-based thinning algorithm for character recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(12), 1672-1678.

[10] Patil, P. M., Suralkar, S. R., & Sheikh, F. B. (2005, November). Rotation invariant thinning algorithm to detect ridge bifurcations for fingerprint identification. In *Tools with Artificial Intelligence, 2005. ICTAI 05. 17th IEEE International Conference on* (pp. 8-pp). IEEE.

[11] X. You, B. Fang, V. Y. Y. Tang, and J. Huang, " Multiscale approach for thinning ridges of fingerprint", in Proc. Second Iberian Conference on Pattern Recognition and Image Analysis, volume LNCS 3523, 2005, pp. 505–512.

[12] Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9), 1365-1388.

[13] Xiao, Q., & Raafat, H. (1991). Fingerprint image postprocessing: a combined statistical and structural approach. *Pattern Recognition*, 24(10), 985-992.

[14] Zhao, F., & Tang, X. (2007). Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. *Pattern Recognition*, 40(4), 1270-1281.

[15] Akram, M. U., Tariq, A., Khan, S. A., & Nasir, S. (2008). Fingerprint image: pre-and post-processing. *International Journal of Biometrics*, 1(1), 63-80.

[16] Amengual, J. C., Juan, A., Pérez, J. C., Prat, F., Sáez, S., & Vilar, J. M. (1997). Real-time minutiae extraction in fingerprint images.

[17] Farina, A., Kovacs-Vajna, Z. M., & Leone, A. (1999). Fingerprint minutiae extraction from skeletonized binary images. *Pattern recognition*, 32(5), 877-889.

[18] Gnanasivam, P., & Muttan, S. (2010). An efficient algorithm for fingerprint preprocessing and feature extraction. *Procedia Computer Science*, *2*, 133-142.

[19] W. F. Leung, S. H. Leung, W. H. Lau, A. Luk, "Fingerprint Recognition using Neural Networks", in Proc. IEEE Workshop on Neural Networks for Signal Processing, 1991, pp. 226-235.

[20] Humbe, V., Gornale, S. S., Manza, R., & Kale, K. V. (2007). Mathematical morphology approach for genuine fingerprint feature extraction. *International Journal of Computer Science and Security*, 1(2), 45-51.

[21] Bansal, R., Sehgal, P., & Bedi, P. (2010). Effective morphological extraction of true fingerprint minutiae based on the hit or miss transform. *International Journal of Biometrics and Bioinformatics (IJBB)*, 4(2), 71.

[22] Maio, D., & Maltoni, D. (1997). Direct gray-scale minutiae detection in fingerprints. *IEEE transactions on pattern analysis and machine intelligence*, *19*(1), 27-40.

[23] Maio, D., & Maltoni, D. (1998, August). Neural network based minutiae filtering in fingerprints. In *Pattern Recognition, 1998. Proceedings. Fourteenth International Conference on* (Vol. 2, pp. 1654-1658). IEEE.

[24] Jiang, X., Yau, W. Y., & Ser, W. (2001). Detecting the fingerprint minutiae by adaptive tracing the gray-level ridge. *Pattern recognition*, 34(5), 999-1013.

[25] Liu, J., Huang, Z., & Chan, K. L. (2000, September). Direct minutiae extraction from gray-level fingerprint image by relationship examination. In *Image Processing, 2000. Proceedings. 2000 International Conference on* (Vol. 2, pp. 427-430). IEEE.

[26] Nilsson, K., & Bigun, J. (2001). Using linear symmetry features as a pre-processing step for fingerprint images. In *Audio-and Video-Based Biometric Person Authentication* (pp. 247-252). Springer Berlin/Heidelberg.

[27]Wang, Y. G., & Carey, V. (2003). Working correlation structure misspecification, estimation and covariate design: implications for generalised estimating equations performance. *Biometrika*, 90(1), 29-41.

Chapter 7

Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images

One of the huge methods in Automated Fingerprint Identification System (AFIS) is the segment or separation of the fingerprint. The process of decomposing an image into exclusive components is referred as segmentation. Fingerprint segmentation is the one of the predominant process involved in fingerprint pre-processing and it refers to the method of dividing or separating the image into disjoint areas as the foreground and the background region. The foreground also called as Region of Interest (ROI) due to the fact only the region which contains ridge and valley structure is used for processing, whilst the background carries noisy and irrelevant content material and so that it will be discarded in later enhancement or orientation or classification method. The challenge proper right here is to decide which a part of the image belongs to the foreground, retrieved as an input from the fingerprint sensor device or from benchmark datasets and which part belongs to the background. A 100% correct segmentation is continually very tough, specifically inside the very poor quality image or partial image together with the presence of latent. In this paper, we discuss a modified clipped based segmentation algorithm by adopting threshold value and canny edge detection techniques. We segment the background image is x and y dimensions or in other words left the edge, right edge, top edge and bottom edge of the image. For the purpose of analyzing the algorithm FVC ongoing 2002 benchmark dataset is considered. The entire algorithm is implemented using MATLAB 2015a. The algorithm is able to find affectively ROI of the fingerprint image or separates the foreground region from the background area of the fingerprint image very effectively. In high configuration system proposed algorithm achieves execution time of 1.75 seconds.

Keywords: Segmentation, Two Dimensional Clipping, Canny Edge Detection, Image Enhancement, Region of Interest (ROI).

7.1 INTRODUCTION

Biometrics is an intrinsic bodily or behavioral characteristic that may be used to discover or verify the person. The most commonplace types of biometrics are face, speech, iris, fingerprint, gait, and signature. The fingerprint is very not unusual and popular biometric of type traits due to its universality, distinctiveness, and permanence and additionally, many advances and new researchers are to be had on this discipline. Despite the fact that AFIS is capable of recognizing a fingerprint image sample with already saved fingerprint image within the database, nevertheless, partial or latent fingerprint image suffers from the low-overall performance rate. A critical and crucial step with a purpose to obtain high first-class and overall performance at all sorts of the image is through correct segmentation. Fingerprints are generally labeled into three kinds as rolled, plain and latent fingerprints primarily based on the system, how they may be captured or accumulated [1]. In rolled fingerprint image is captured from one end of the finger to another end by rolling and mounting on capturing device in order to obtain complete ridge and valley details of the fingerprint. The plain fingerprint is directly captured using a fingerprint capturing device through pressing a fingertip onto a flat surface. Rolled and plain fingerprints are acquired in a sophisticated attended mode; they will be having good visual quality at the time of training and performance quality at the time of matching one to one or one to many for verification or identification purpose [2-5].

The emphasis is on ROI-segmentation is to accurately extract the ROI, which is real ridge details, which directly influences the performance of feature extraction and matching process. The example of ROI is shown below in Figure 7.1

(a) Original Image (b) ROI of the image (a)

Figure 7.1: Example of ROI

Usually, Latent fingerprints are collected from the crime scene and mixed with another image or components like structure noise or other fingerprints or on the surface of a wall that was inadvertently touched or handled. The algorithms work well for rolled and plain fingerprint shows significant flaws for latent image or suspect in identifying crime persons. Fingerprint segmentation is the one of the main process involved in fingerprint pre-processing and it

refers to the process of dividing or separating the image into two disjoint regions as the foreground and background.

The simple method for segmentation of the fingerprint image is based on binarisation. Initially, the input image can be any of the type like rolled, plain or latent. In next step, the image has to resize using cropping the image or any other image resizing process. The fingerprint is usually in grayscale, but very rarely it can be color (RGB) image in the case of latent or any other types of partial or fingerprint captured using mobile devices. If the image is color, it should be converted into grayscale using RGB to Grayscale converter function. In next step, the Grayscale image is converted into a Binary image using coarse binarisation process. The purpose of coarse binarisation is to remove the background or noise associated with the input image or to separate foreground from the background image. Threshold method is used in order to get an initial binary image. To remove some background from the image, any threshold method can be used. Compared to the local adaptive threshold method, global methods are parameter independent and inexpensive [6-7]. Coarse scan supports detection of the fingerprint ridge positions from the background image. After the coarse binarisation process, the existence of false background is checked and if there exists (normal case), orientation angle is calculated using any orientation method, if not (abnormal case) again refined binarisation process is activated. The objective of refined binarisation is to find an optimal threshold to eliminate the background while preserving as much ridge pattern as possible. After all these processes, we get the segmented image.

In literature, a good number of papers are available for fingerprint segmentation, which can be roughly categorized under two classifications as block-wise methods and pixel-wise methods. In the block-wise method, the fingerprint images are classified into different equal sized nonoverlapping blocks and further organize blocks into a foreground region and background region based on the extracted features. On the other hand, pixel-wise methods emphasis on pixel and classifies the fingerprint image based on pixel-wise features of the image. In this paper, we discuss a modified clipping based segmentation algorithm which clips white spaces or background image as left, right, top and bottom boundary. We discuss and analyze algorithm based on grayscale fingerprint image considered from FVC ongoing 2002 datasets.

7.2 LITERATURE REVIEW OF SEGMENTATION

Segmentation or dividing is one of the deciders of performance in the automatic fingerprint recognition system. There is enough amount of literature with respect to image segmentation process or approach dating back over thirty years. Jain & Dubes, (1988) [8], explains the algorithm for clustering in his book, these early approaches for clustering can be used for segmentation, which acts as the basis for many new methods including boundary based segmentation such as Canny edge detection Canny, 1986 [9]. In this method, researcher defines a comprehensive set of goals for the computation of edge detection points. Adams and Bishof, (1994) [10], proposed segmentation algorithm for images, which are intensity images with certain characteristics like robust, rapid, and free of tuning parameters. This algorithm can take input as either individual pixels or regions and points these inputs to some region formed by the algorithm. The algorithms explain two methods in which input

corresponds to the region, either by using manual seed or by an automated procedure. Chakraborty et al., (1996) [11], proposed a method which combines region based segmentation and boundary finding to form new method which is more robust to noise and high performance. The literature covered above is some general segmentation algorithms which will apply for any types of images.

In literature, there are many studies available, which mainly focuses on fingerprint image segmentation. Most of the segmentation algorithm does classification of the image based on either supervised learning or unsupervised learning. When a class label is not known or unknown, means of unsupervised learning, classification is significantly and very difficult. Researchers, Mehtre, et al. (1989) [12] classified the image into blocks, which is administrative specific and the size was 16 × 16 pixels. Based on the gradient distribution, each block was classified. This method is best suited for simple fingerprint images which contain only background and foreground. Later Researchers Mehtre and Chatterjee, (1989) [13] extended this work by leaving the grayscale variance, which will usually be lower than some threshold value. Researchers Ratha et al. (1995) [14] proposed 16 × 16 blocks of classes and each one was developed based on the gray scale variance in the direction opposite to the orientation of ridges.

The authors Jain and Ratha, (1997) [15] concentrated for the detection of objects located in complex backgrounds. The given object is first applied to a bank of even-symmetric Gabor filters. The output image received from the Gabor filter is subjected to a sigmoid function transformation. The yield image of the Gabor filter is applied as an input to the clustering algorithm, which develops spatially compact clusters. Sun and Ai (1996) [16] pre-processed initially fingerprint image by converting it into a binary image with the help of dynamic threshold value (T). Moayer and Fu (1975) [17] used sampling squares, which are obtained from the subdivision of fingerprint images for the ultimate goal of feature extraction. They used dynamic threshold value (T) to convert the initial image to a binary image. In order to determine the local threshold value, researchers used neighbor pixels by group 5 × 5 pixels.
Bazen and Gerez (2000) [18] used coherence and morphology of fingerprint image with an intention to obtain a smooth image by filtering different types of noises. The same author Bazen and Gerez (2001) [19] improved their work by adding two more statistical features as the mean and variance for their previous work. Here classification is done with the aid of optimal linear classifiers, which acts as a trainer for classification. With a goal to find compact cluster and reducing, classification error for post processing morphology is applied.
Naji et al. (2002) [20] developed a segmentation algorithm, which computerized or automated the method of selecting a threshold value at the time of segmentation with the aid of histogram equalizer. Segmentation algorithm generally falls under two categories of machine learning techniques as supervised learning and unsupervised learning. Unsupervised learning uses threshold decided on detecting features to cluster the image. Supervised learning uses a simple linear classifier to classify features as a region of interest (ROI) or background and foreground. As a part of supervised methods, Alonso-Fernandez et al. (2005) [21] used a Gabor filter to filter the input image and to obtain a smooth image. The neural

network can also be used in the segmentation process to reduce the noise or to enhance the image quality.

Barreto et al. (2005) [22] used a neural network to train the fingerprint image data sets using Fourier spectrum and obtained a segmentation of fingerprint images. Zhu et al. (2006) [23] also used neural network concepts in order to train the fingerprint data set, but they used the gradient of the fingerprint orientation to segment the images. Wu et al. (2007) [24] proposed a new method for segmentation; in their method, they used the strength of Harries corner function to extract the background from foreground or to extract a region of interest. In order to separate region of interest from the background image, they used corner strength measures.

Tiwari, K., & Gupta, P. (2015) [25] proposed a new method for extracting a single fingerprint image from the slap fingerprint scanner, which simultaneously scans four fingerprints of a person in a single image. While extracting the single fingerprint image the image is also required to be segmented. They used a novel technique to extract solitary (single) fingerprint image based on force field and heuristics using divide and conquer strategy and is tested in IITK-4slap-Rural and IITK-4slap-student database.

Thai, Huckemann, & Gottschlich, 2016 [26] proposed the new approach for fingerprint segmentation in three folds, firstly used factorized directional bandpass (FDB) and directional Hilbert transform originated from Butterworth bandpass (DHBB) filter combined with soft-thresholding for texture extraction. Secondly, as an evaluation benchmark with 10560 images marked manually for ground truth segmentation. Thirdly they have compared systematically factored directional filtering with other similar fingerprint segmentation approach and obtained comparatively good performance.

7.3 TWO DIMENSIONAL CLIPPING BASED SEGMENTATION-DESCRIPTION

This algorithm considers binary fingerprint image, which is referred as I_{binary}. Initially to find the edges of the I_{binary} image efficiently canny edge detection method is used. Canny edge detection finds the edges of the image through different processes, which includes, smoothing, locating gradients, non-maximum suppression, double thresholding, and edge tracking by using hysteresis. Smoothing of the image is done with the help of convolution, which blurs the image to get rid of the noise. Canny edge detection uses double thresholding in order to find edges of the image. The result of the canny edge detection method is stored as I_{canny}. Next, the edge detected image, I_{canny} is converted into the-low resolution image by converting 256 × 256 sized grayscale images to 128 × 128 sized grayscale image.

$$I_{LRE} = I_{binary}(i \times 2, j \times 2)$$

The low-resolution image is represented as I_{LRE}. In the next phase I_{LRE} image is padded with zeros using pad array and usually for simplicity in this method we use pad array size is eight and is referred as P. For $I_{LRE,}$ eight zeros are added to row and column respectively, and it enhanced to 144 × 144 sized grayscale images, which is denoted as I_{Parray}.

The, I_{Parray} is clipped into 15×15 sized image and processed. The clipped image is stored in temp1. The entire 225 pixels of temp1 are reshaped as 1×225 matrix and denoted as temp2. The covariance of the matrix of the image, temp2 is calculated and if it is less than the threshold then the pixel of the I_{binary} (256 × 256 sizes) image is considered as not a part of ROI or foreground. Covariance of a matrix is calculated by considering row as observations and columns as random variables. Every pixel of the I_{binary} image is traced like this and marked as either foreground or background of the image based on covariance value. If it is greater than the threshold value then the pixel is considered to be foreground, means which is a real part of the fingerprint image. Each time when padarray is considered, this takes into account one pixel out of 128×128 low-resolution image and two pixels out of 256 ×128 sized image.

As the algorithm name suggests two-dimensional clipping, we discard maximum background part of the image by checking whether all the pixels of the each column intensity value sum become 256. If the column sum is 256 means all the pixels of that particular column contains intensity value 1. This signifies that this column contains background of the image. If any one column intensity value sum leads to value less than 256, which signifies that the particular column contains part of the foreground or ROI of the image. Then we skip the iteration and count considering starting of the column pixel for output of the segmented image from just previous to that column number. The same process we repeat from the last column to the first column in reverse direction and stop moving backward until we get a column number sum of intensity value less than 256 for the purpose of finding last column number, which contains at least one pixel of foreground pixel. This means that from the last column to till this position image contains only background part of the image. The above-mentioned method repeated for rows also. So that it eliminates background or white blank area in left edge, right edge, top edge and bottom edge regions.

7.4 TWO DIMENSIONAL CLIPPING BASED SEGMENTATION-ALGORITHM

Input: binary image, I_{binary}
Output: Segmented Image, $I_{segment}$
Step-1: Read I_{binary} image
Step-2: Apply canny edge formation to the I_{binary} and store it in a variable I_{canny}
Step-3: for i=1 to floor(R/2)
Step-4: for j=1 to floor (C/2)
Step-5: $I_{LRE} = I_{binary}(i \times 2, j \times 2)$; end for loop; I_{LRE}→Low Resolution Edge Image
Step-6: $[R_{LRE}, C_{LRE}] = size(I_{LRE})$
Step-7: P=floor (max (15, 15)/2+1);
Step-8:$I_{Parray} = \text{padarray}(I_{LRE}, [P\ P])$
Step-9: for i=P+1 to R_{LRE}+P
Step-10: for j=P+1 to C_{LRE}+P

Step-11: temp1= $I_{Parray}(\left(i - floor\left(\frac{15}{2}\right) : i + floor\left(\frac{15}{2}\right)\right), \left(j - floor\left(\frac{15}{2}\right) : j + floor\left(\frac{15}{2}\right)\right))$

Step-12: temp2=reshape (temp1, 1, 225)

Step-13: $V_1 = covariance(temp2)$

Step-14: if $V_1 < T$ \\ T→Threshold value=0.101

Step-15: $I_{binary}\big((i-P)*2-2+1 : (i-P)*2, (j-P)*2-2+1 : (i-P)*2\big) = 1$

Step-16: end if; end for;

Step-17: $N_R = ColumnSize\ of\ I_{binary}$

Step-18: for i=1 to N_R

Step-19: $C_{sum} = \sum I_{binary}(:, i)$

Step-20: Check if $C_{sum} = N_R$

Step-21: $\text{Position}_1 = i$; end if

Step-22: for i=1 to N_R

Step-23: $C_{sum} = \sum I_{binary}(:, N_R + 1 - i)$

Step-24: Check if $C_{sum} = N_R$

Step-25: $\text{Position}_2 = \frac{({N_R}^2 - i^2)}{N_R + i}$; end if; end step-22 for

Step-26: $N_C = RowSize\ of\ I_{binary}$

Step-27: for i=1 to N_R

Step-28: $R_{sum} = \sum I_{binary}(:, i)$

Step-29: Check if $R_{sum} = N_C$

Step-30: $\text{Position}_3 = i$; end if

Step-31: for i=1 to N_C

Step-32: $R_{sum} = \sum I_{binary}(N_C + 1 - i, :)$

Step-33: Check if $R_{sum} = N_C$

Step-34: $\text{Position}_4 = \frac{({N_C}^2 - i^2)}{N_C + i}$; end if; end step-27 for

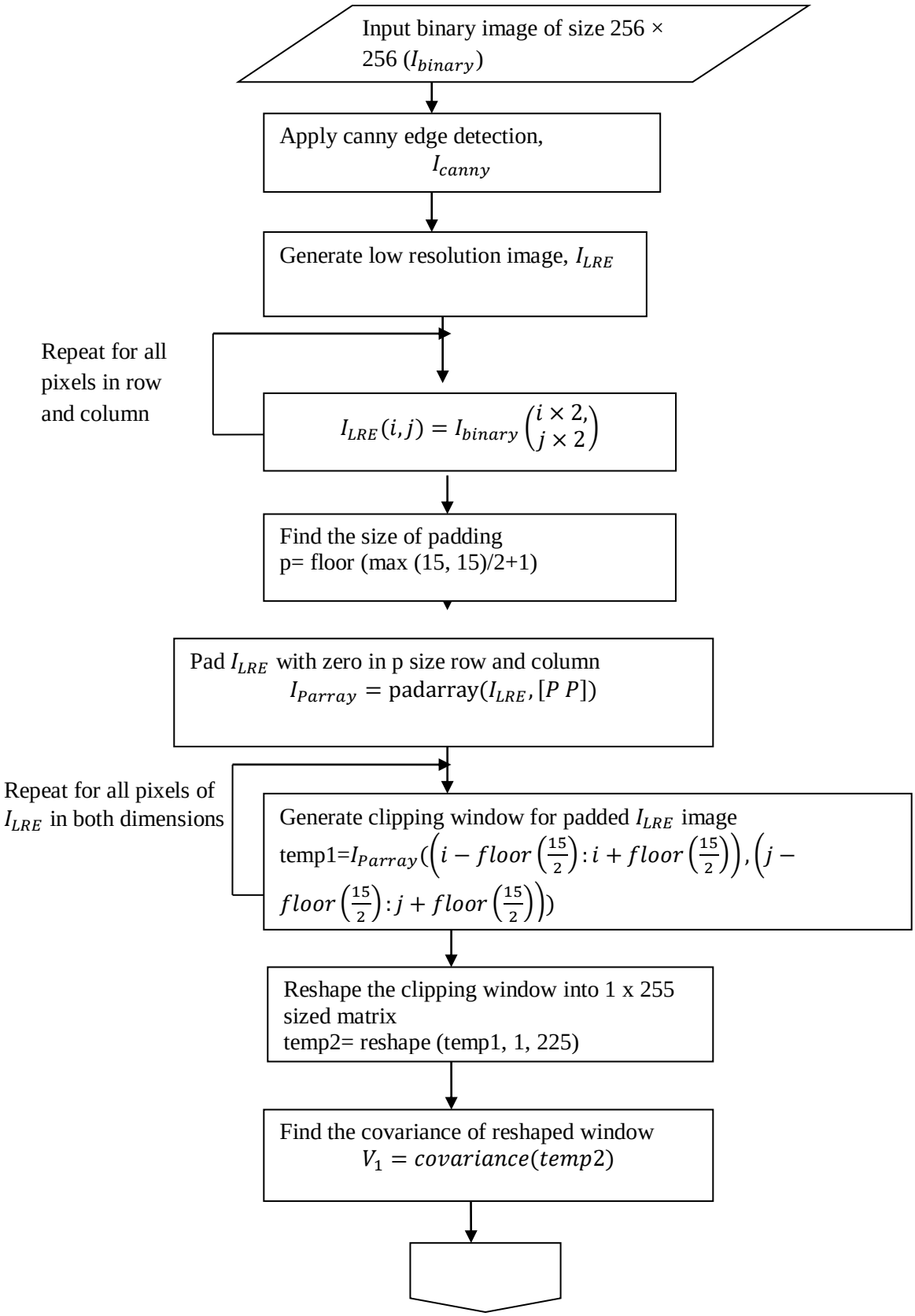
Step-35: $I_{segment} = I_{binary}(\text{Position}_3 to\ \text{Position}_4 :, \text{Position}_1 to\ \text{Position}_2)$

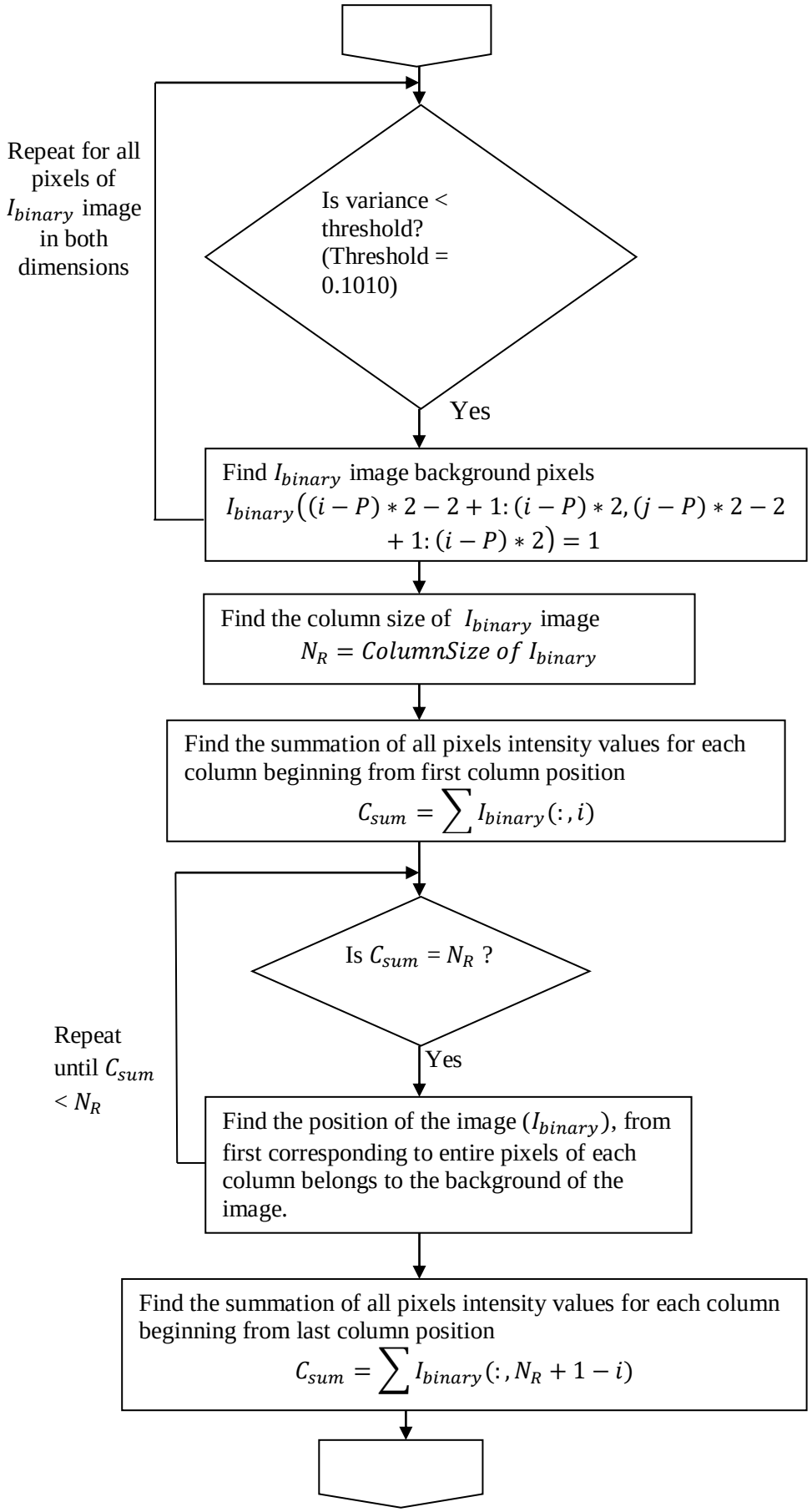
7.5. FLOWCHART OF TWO DIMENSIONAL CLIPPING BASED SEGMENTATION

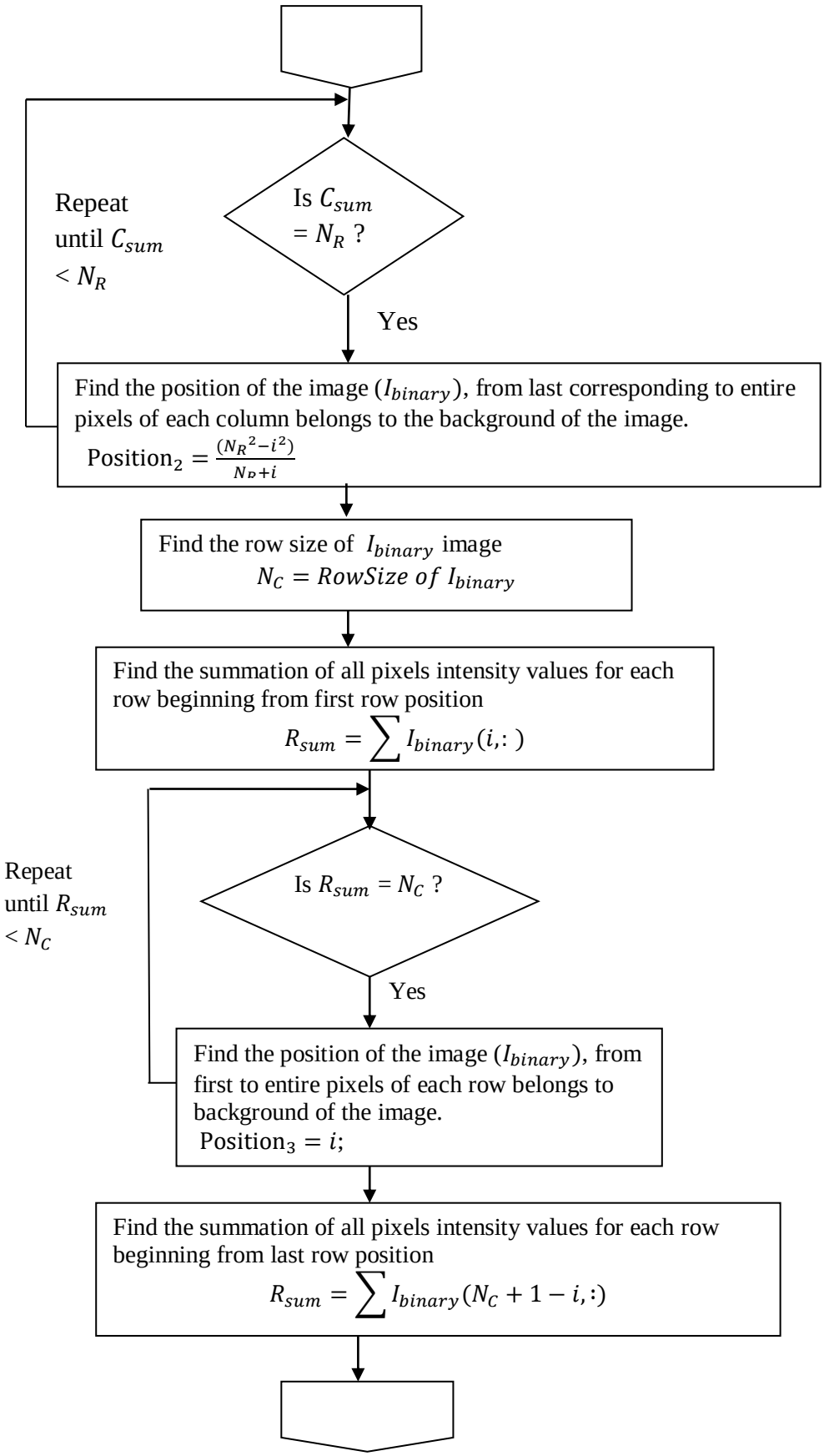
This proposed algorithm for segmentation is explained using a flowchart in figure 7.2. The input for this algorithm is a binary image of size 256 × 256 which is represented as I_{binary}. The final output is segmented image denoted as, $I_{segment}$. The different workflows of the proposed algorithm are listed out below.

- Find the edge of the image using canny edge detection method. Generate the low-resolution image from the 256 × 256 sized grayscale image
- Find the size of the padding. Pad the low-resolution image with zero along row and column directions.
- Generate the clipping window of size 15×15 for the low-resolution padded image.
- Reshape the clipping widow as 1 × 256 size window

- Find covariance of the matrix of the image for each element of the input image through the padded image. If covariance is less than the threshold treat it as background image otherwise treat it as the foreground image.
- Discard the each column of the image if it completely contains the intensity value 1 from both left and right directions of the image. Discard the each row of the image if it completely contains the intensity value 1 from both top and bottom directions of the image.


Input binary image of size 256 × 256 (I_{binary})
Apply canny edge detection, I_{canny}
Generate low resolution image, I_{LRE}
Repeat for all pixels in row and column
$I_{LRE}(i,j) = I_{binary}\begin{pmatrix} i \times 2, \\ j \times 2 \end{pmatrix}$
Find the size of padding
p= floor (max (15, 15)/2+1)
Pad I_{LRE} with zero in p size row and column
$I_{Parray} = \text{padarray}(I_{LRE}, [P\ P])$
Repeat for all pixels of I_{LRE} in both dimensions
Generate clipping window for padded I_{LRE} image
temp1=$I_{Parray}(\left(i - floor\left(\frac{15}{2}\right) : i + floor\left(\frac{15}{2}\right)\right), \left(j - floor\left(\frac{15}{2}\right) : j + floor\left(\frac{15}{2}\right)\right))$
Reshape the clipping window into 1 x 255 sized matrix
temp2= reshape (temp1, 1, 225)
Find the covariance of reshaped window
$V_1 = covariance(temp2)$


Repeat for all pixels of I_{binary} image in both dimensions
Is variance < threshold? (Threshold = 0.1010)
Yes
Find I_{binary} image background pixels
$I_{binary}\big((i-P)*2-2+1:(i-P)*2,(j-P)*2-2+1:(i-P)*2\big)=1$
Find the column size of I_{binary} image
$N_R = ColumnSize\ of\ I_{binary}$
Find the summation of all pixels intensity values for each column beginning from first column position
$C_{sum} = \sum I_{binary}(:,i)$
Is C_{sum} = N_R ?
Repeat until C_{sum} < N_R
Yes
Find the position of the image (I_{binary}), from first corresponding to entire pixels of each column belongs to the background of the image.
Find the summation of all pixels intensity values for each column beginning from last column position
$C_{sum} = \sum I_{binary}(:,N_R+1-i)$


Repeat until $C_{sum} < N_R$
Is $C_{sum} = N_R$?
Yes
Find the position of the image (I_{binary}), from last corresponding to entire pixels of each column belongs to the background of the image.
$\text{Position}_2 = \frac{(N_R{}^2 - i^2)}{N_R + i}$
Find the row size of I_{binary} image
$N_C = RowSize\ of\ I_{binary}$
Find the summation of all pixels intensity values for each row beginning from first row position
$R_{sum} = \sum I_{binary}(i,:)$
Repeat until $R_{sum} < N_C$
Is $R_{sum} = N_C$?
Yes
Find the position of the image (I_{binary}), from first to entire pixels of each row belongs to background of the image.
$\text{Position}_3 = i;$
Find the summation of all pixels intensity values for each row beginning from last row position
$R_{sum} = \sum I_{binary}(N_C + 1 - i,:)$

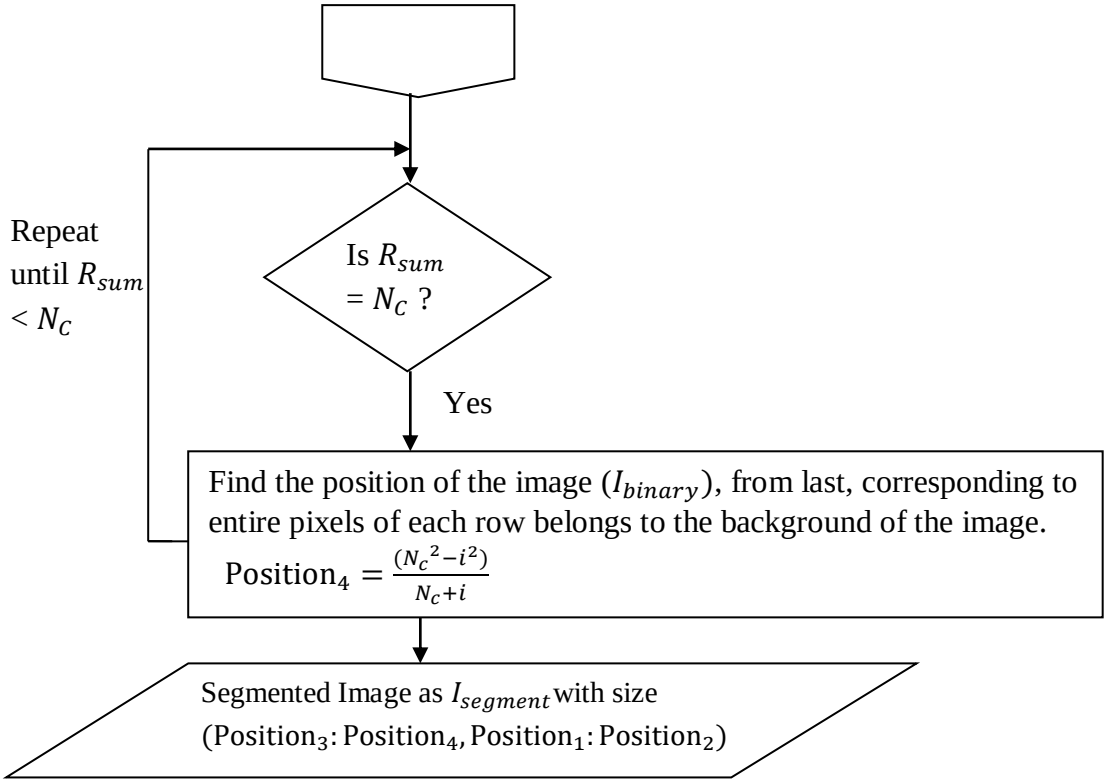
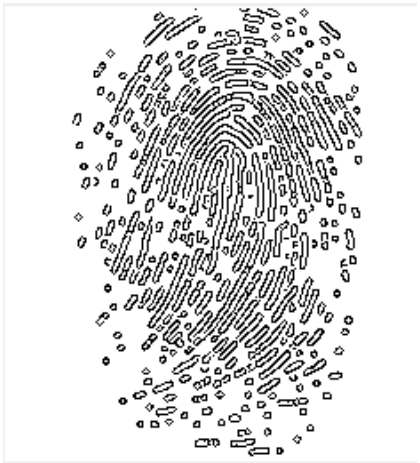


Figure 7.2: Flowchart of Two dimensional clipping based segmentation algorithm

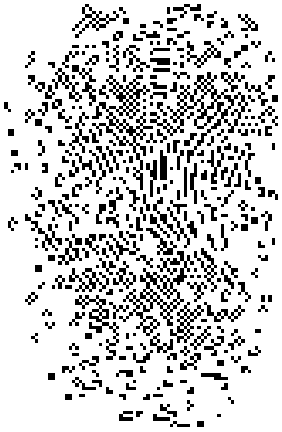
7.6 ANALYSIS OF THE TWO DIMENSIONAL CLIPPING BASED SEGMENTATION

The two dimensional clipping based Segmentation is analyzed by considering FVC ongoing 2002 DB1_B datasets. A sample fingerprint image named as 102_1.tif from FVC ongoing 2002 dataset is considered in Figure 7.3. The algorithm is implemented using MATLAB programming version 2015a.

(a) Original image



(b) Canny edge image



(c) Low Resolution Image

(d) Segmented image without clipping

(e) Segmented image by clipping left, right, top and bottom border

Figure 7.3: Examples of Two dimensional Clipping based segmentation algorithm different phase's results

Table 7.1, shows edges obtained using canny edge detection method. Total numbers of edges are considered in terms of a total number of pixels.

Table 7.1: Total number of edges identified through canny edge detection

Sr. No	Image name	Total number of Edges identified using canny edge Detection
1	101_1.tif	8774
2	102_1.tif	8302
3	103_5.tif	10023
4	104_4.tif	10402
5	105_8.tif	7354
6	101_6.tif	10921
7	103_2.tif	10136

Figure 7.4 shows input image, and results of segmentation process using two dimensional clipping based segmentation for different sample images of FVC ongoing DB1_B datasets. While seeing the two images we don't find any differences. But if we observe carefully after segmentation left and right part of the filtered image is clipped, which corresponds to background pixels.

(a) Input image (b) Segmented image

Figure 7.4: Examples of input and segmented image using proposed methods

Table 7.2 shows the total number of pixels before the segmentation and after segmentation. If the numbers of pixels are reduced, this improves the execution performance or speed in following stages of automatic fingerprint identification systems like minutiae formation, feature extraction, and matching.

Table 7.2: Comparison of total number of pixels before and after segmentation

Sr. No	Image name	Size of the image before segmentation	Size of the image after segmentation	Total number of pixels before segmentation	Total number of pixels after segmentation
1	101_1.tif	256 × 256	230 × 148	65536	34040
2	102_1.tif	256 × 256	251 × 149	65536	37399
3	103_5.tif	256 × 256	228 × 183	65536	41724
4	104_4.tif	256 × 256	222× 193	65536	42846
5	105_8.tif	256 × 256	236 × 153	65536	36108
6	101_6.tif	256 × 256	213 × 180	65536	38340
7	103_2.tif	256 × 256	256 × 150	65536	38400

Table 7.3 shows the execution time of two dimensional clipping based segmentation algorithm.

Execution time is calculated based on duration or time between input and output. Execution time is calculated on two different configuration laptops. One is referred as System-I and other is System-II.

The configuration of System-I and System-II are given in Table 7.4.

Table 7.3: Execution time for different sample images using two dimensional clipping based segmentation

Sr. No	Image name	Execution Time in Seconds Using System-I	Mean Execution time using System-I	Execution Time in Seconds Using System-II	Mean Execution time using System-II
1	101_1.tif	4.019798	3.960607	1.741521	1.754737
2	102_1.tif	4.011555		1.815977	
3	103_5.tif	3.931000		1.712644	
4	104_4.tif	3.946413		1.669623	
5	105_8.tif	3.933841		1.742137	
6	101_6.tif	3.866910		1.676781	
7	103_2.tif	4.014733		1.924482	

Table 7.4: Configuration of System-I and Sytem-2 used for finding Execution Time

Sr. No.	Parameters	System-I	System-II
1	Model	Compaq 435	TravelMate 5742
2	Processor	AMD E-350 processor 1.60 GHz	Intel (R) Core (TM) i3 CPU, M 370 @ 2.40 GHz
3	Installed Memory	3 GB (2 GB usable)	6 GB (5.68 GB usable)
4	System Type	32-bit operating System	64-bit operating System
5	Operating System	Windows 7 Starter	Windows 7 Professional
6	Software	MATLAB 2015a 32-bit	MATLAB 2015a 32-bit

Execution time for the two dimensional clipping based segmentation algorithm in System-I is almost near to 4 seconds and in System-II is 1.75 seconds. So it can be proved that execution time is depending on the configuration of the system. If the system is high configured system in terms of processor, memory etc. The algorithm executes faster than the system which is having less configuration.

7.7 CONCLUSION

An essential and important step in order to obtain high quality and performance rate at all types of image is through accurate segmentation. Fingerprint segmentation is the one of the main process involved in fingerprint pre-processing and it refers to the process of dividing or separating the image into two disjoint regions as the foreground and background.

The Two dimensional clipping based segmentation algorithm affectively clips the background region of the fingerprint in all four permissible boundaries, left edge, right edge, top edge and bottom edge. The use of canny edge detection method improves the

identification of the edges effectively. The proposed algorithm has good execution time in high configured systems. The proposed algorithm has following characteristics.

- Usage of canny edge detection techniques finds all edges of the image efficiently.
- Having the ability to generate the low resolution image from the 256 × 256 sized grayscale image
- Pads the low resolution image with zero along row and column directions.
- Generate the clipping window of size 15×15 for low resolution padded image.
- Reshape the clipping widow as 1 × 256 size window
- Find covariance of the matrix of the image for each element of the input image through the padded image.
- If covariance is less than the threshold treats it as background image otherwise treat it as the foreground image.
- Discards each column of the image, if it completely, contains the intensity value 1 from both left and right directions of the image.
- Discards each row of the image, if it completely, contains the intensity value 1 from both top and bottom directions of the image.

REFERENCES

[1] Zhang, J., Lai, R., & Kuo, C. C. J. (2012). Latent fingerprint detection and segmentation with a directional total variation model. In Proceedings - International Conference on Image Processing, ICIP, 1145–1148. DOI: https://doi.org/10.1109/ICIP.2012.6467067

[2] Krishna Prasad, K. & Aithal, P. S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[3] Krishna Prasad, K. & Aithal, P. S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608

[4] Krishna Prasad, K. & Aithal, P. S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[5] Krishna Prasad, K. & Aithal, P. S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[6] Wang, Q. P., Du, J. X., & Zhai, C. M. (2010). Advanced Intelligent Computing Theories and Applications. With Aspects of Artificial Intelligence. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics),* 6216(February 2016), 240–246. DOI: https://doi.org/10.1007/978-3-642-14932-0

[7] Vielhauer, C., Dittmann, J., Drygajlo, A., Juul, N. C., & Fairhurst, M. (Eds.). (2011). Biometrics and ID Management: COST 2101 European Workshop, BioID 2011, Brandenburg (Havel), March 8-10, 2011, Proceedings (Vol. 6583). Springer Science & Business Media.

[8] Jain, A. K., & Dubes, R. C. (1988). Algorithms for clustering data. Prentice-Hall, Inc.

[9] Canny, J. (1986). A computational approach to edge detection. IEEE Transactions on pattern analysis and machine intelligence, (6), 679-698.

[10] Adams, R., & Bischof, L. (1994). Seeded region growing. IEEE Transactions on pattern analysis and machine intelligence, 16(6), 641-647.

[11] Chakraborty, A., Staib, L. H., & Duncan, J. S. (1996). Deformable boundary finding in medical images by integrating gradient and region information. IEEE Transactions on Medical Imaging, 15(6), 859-870.

[12] Mehtre, B. M., Murthy, N. N., Kapoor, S., & Chatterjee, B. (1987). Segmentation of fingerprint images using the directional image. Pattern Recognition, 20(4), 429-435.

[13] Mehtre, B. M., & Chatterjee, B. (1989). Segmentation of fingerprint images—a composite method. Pattern Recognition, 22(4), 381-385.

[14] Ratha, N. K., Chen, S., & Jain, A. K. (1995). Adaptive flow orientation-based feature extraction in fingerprint images. Pattern Recognition, 28(11), 1657-1672.

[15] Jain, A. K., Ratha, N. K., & Lakshmanan, S. (1997). Object detection using Gabor filters. Pattern Recognition, 30(2), 295-309.

[16] Sun, X. and Ai, Z. (1996) Automatic feature extraction and recognition of fingerprint images, Proceeding of ICSP'96, Beijing, Pp.1086-1089.

[17] Moayer, B., & Fu, K. S. (1975). A syntactic approach to fingerprint pattern recognition. Pattern Recognition, 7(1–2), 1–23. DOI: https://doi.org/10.1016/0031-3203(75)90011-4

[18] Bazen, A.M. and Gerez, S.H. (2000) Directional field computation for fingerprints based on the principal component analysis of local gradients, Proceedings of ProRISC2000, 11th Annual Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands.

[19] Asker M. Bazen and Sabih H. Gerez. 2001. Segmentation of Fingerprint Images, Workshop on Circuits, Systems and Signal Processing, Veldhoven. The Netherlands.

[20] Naji, A.W., Ramli, A.R., Ali, R., Rahman, S.A., and Ali, M.L. (2002) A segmentation algorithm based on histogram equalizer for fingerprint classification system, Second International Conference on Electrical and Computer Engineering ICECE 2002, Dhaka, Bangladesh, pp. 390-393.

[21] Alonso-Fernandez, F., Fierrez-Aguilar, J. and Ortega-Garcia, J. (2005) An enhanced Gabor filter based segmentation algorithm for fingerprint recognition systems, In Proceedings of the 4th International Symposium on Image and Signal Processing and Analysis, Pp. 239-244.

[22] Barreto, P., Marques, A.C. and Thome, A.C. (2005) A neural network fingerprint segmentation method, 5th International Conference on Hybrid Intelligent Systems P.6.

[23] Zhu, E., Yin, J., Hu, C. and Zhang, G. (2006) A systematic method for fingerprint ridge orientation estimation and image segmentation, Pattern Recognition, Vol. 39, No.8, Pp. 1452-1472.

[24] Wu C., Tulyakov S. and Govindaraju V. (2007). Robust point-based Feature Fingerprint Segmentation Algorithm, ICB (2007), Pp. 1095-1104

[25] Tiwari, K., & Gupta, P. (2015). An efficient technique for automatic segmentation of fingerprint ROI from digital slap image. Neurocomputing, 151(P3), 1163–1170. https://doi.org/10.1016/j.n eucom.2014.04.086

[26] Thai, D. H., Huckemann, S., & Gottschlich, C. (2016). Filter design and performance evaluation for fingerprint image segmentation. PLoS ONE, 11(5). DOI: https://doi.org/10.1371/j ournal.pone.0154160

****

Chapter 8
A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User

Biometrics innovation has ended up being a precise and proficient response to the security issue. Biometrics is a developing field of research as of late and has been dedicated to the distinguishing proof or authentication of people utilizing one or multiple inherent physical or behavioral characteristics. The unique fingerprint traits of a man are exceptionally exact and are special to a person. Authentication frameworks in light of unique fingerprints have demonstrated to create low false acceptance rate and false rejection rate, alongside other favorable circumstances like simple and easy usage strategy. But the modern study reveals that fingerprint is not so secured like secured passwords which consist of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at the door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. In this paper, we discuss fingerprint image Hash code generation based on the Euclidean distance calculated on the binary image. Euclidean distance on a binary image is the distance from every pixel to the nearest neighbor pixel which is having bit value one. Hashcode alone not sufficient for Verification or Authentication purpose, but can work along with Multifactor security model or it is half secured. To implement Hash code generation we use MATLAB2015a. This study shows how fingerprints Hash code uniquely identifies a user or acts as index-key or identity-key.

Keywords: *Fingerprint Image, Fingerprint Hashcode, Authentication, Multifactor Authentication Model, Euclidean Distance.*

8.1 INTRODUCTION

Biometrics is an investigation of checking and setting up the identity of an individual through physiological components or behavioral qualities. Even though biometric technologies differ in complexities, capacities and performance parameters, still all offer a few regular components like biometric sensor module, feature extractor module, a matching module, decision-making module and system database. Fingerprint biometric has been utilized in numerous areas together with entrance management and door-lock programs, smart cards, vehicle ignition control framework and fingerprint controlled access control system. Automatic Fingerprint Identification System (AFIS) consists of different steps like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [1-6]. The distinctiveness of fingerprint is added forward by using ridge patterns and it has been proved that the information in small regions of friction ridges is in no way repeated. These friction ridges broaden in a human system all through the fetus level itself Fingerprint sensors or acquisition devices uses different types of sensors to take input or to get fingerprint image into the system [7].

Commonly, all the profitable biometric systems shield the stored templates by using encrypting those using general cryptographic techniques. Either a public key cryptosystem like RSA (RSA laboratories, 1999) or a symmetric key cipher like AES (Advanced Encryption Standard, 2001) is usually used for template encryption.

One of the important challenges in biometric identification or verification system is keeping the biometric data or template safe and secure. A hash function is usually transformed functions, which converts or transform data or features from one form to another. Always transform function should be a one-way function or another way it should not be invertible [8].

A number of template protection strategies like fuzzy commitment [9], fuzzy vault [9], protecting functions [10] and distributed supply coding [11] can be considered as the key binding biometric cryptosystem. Different schemes for securing biometric templates along with those positioned forth in [12-15] also fall under this class.

In this study, we calculate Euclidean distance for a binary fingerprint image, which is a straight line distance from a pixel with value zero to the pixel with value non-zero, which is one in a binary image using Euclidean norm. The Euclidean distance is calculated for all the pixels of the binary fingerprint image. The two points k and l in two-dimensional Euclidean spaces and k with the coordinates (k1, k2), l with the coordinates (l1, l2). The line segment with the endpoints of k and l will form the hypotenuse of a right-angled triangle. The space among factors k and l is defined as the square root of the sum of the squares of the differences among the corresponding coordinates of the points. In a two-dimensional Euclidean geometry Euclidean distance between two points k = (kx, ky) and l = (lx, ly) is given as follows;

$$d(k, l) = \sqrt{(lx - kx)^2 + (ly - ky)^2}$$

For example consider a 3×3 sized matrix with values as follows

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The Euclidean distance for each point is calculated as follows

$$\begin{bmatrix} 1.4142 & 1.0000 & 1.4142 \\ 1.0000 & 0 & 1.0000 \\ 1.4142 & 1.0000 & 1.4142 \end{bmatrix}$$

The most natural or common matrix for finding distance matrix in the binary image is Euclidean distance [16-18]. Due to the lack of efficient algorithms in the field of Euclidean distance led to the development of many types of research in this field in order to define, elaborate and also to use some other methods to find the distance using other methods like the city block, chessboard or chamfer [18-20]. The Euclidean distance transform is global operation and the calculation of Euclidean distance is most common and simple operation and amount of calculation required is always directly proportional to the size of the entire image because this is calculated for every pixel.

Fingerprints are a half-secret if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan. Fingerprints are left at the car, door or anyplace where every person goes and places his finger [21]].

Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security mechanisms like password or OTP in order to enhance security. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or reader [22-24].

This paper has sections. Section-1 explains about introductory information of fingerprint and Euclidean distance, and template protection. Section-2, explain about objective and methodology of the study. Section-3 explains about Algorithm of Hash code generation, Section-4 depicts a flowchart of Hash code generation. Section-5 explains Results and Discussions. Section-6 concludes the paper.

8.2 OBJECTIVES AND METHODOLOGY

There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause difference in Hash code. So this research does not concentrate on developing fingerprint hash code which is translation and rotation invariant. Fingerprint alone not gives full security, in order to improve the security of the system fingerprint acts one factor along with OTP, password, or any other biometric psychological or behavioral traits. The main objectives of this study are given below.

- To Study a Fingerprint Hash code generation using Euclidean distance value calculated for each pixel of the binary image.

- To verify the uniqueness of fingerprint Hash code using FVC ongoing 2002 benchmark dataset.

Figure 8.1 explains the methodology used in this research work.

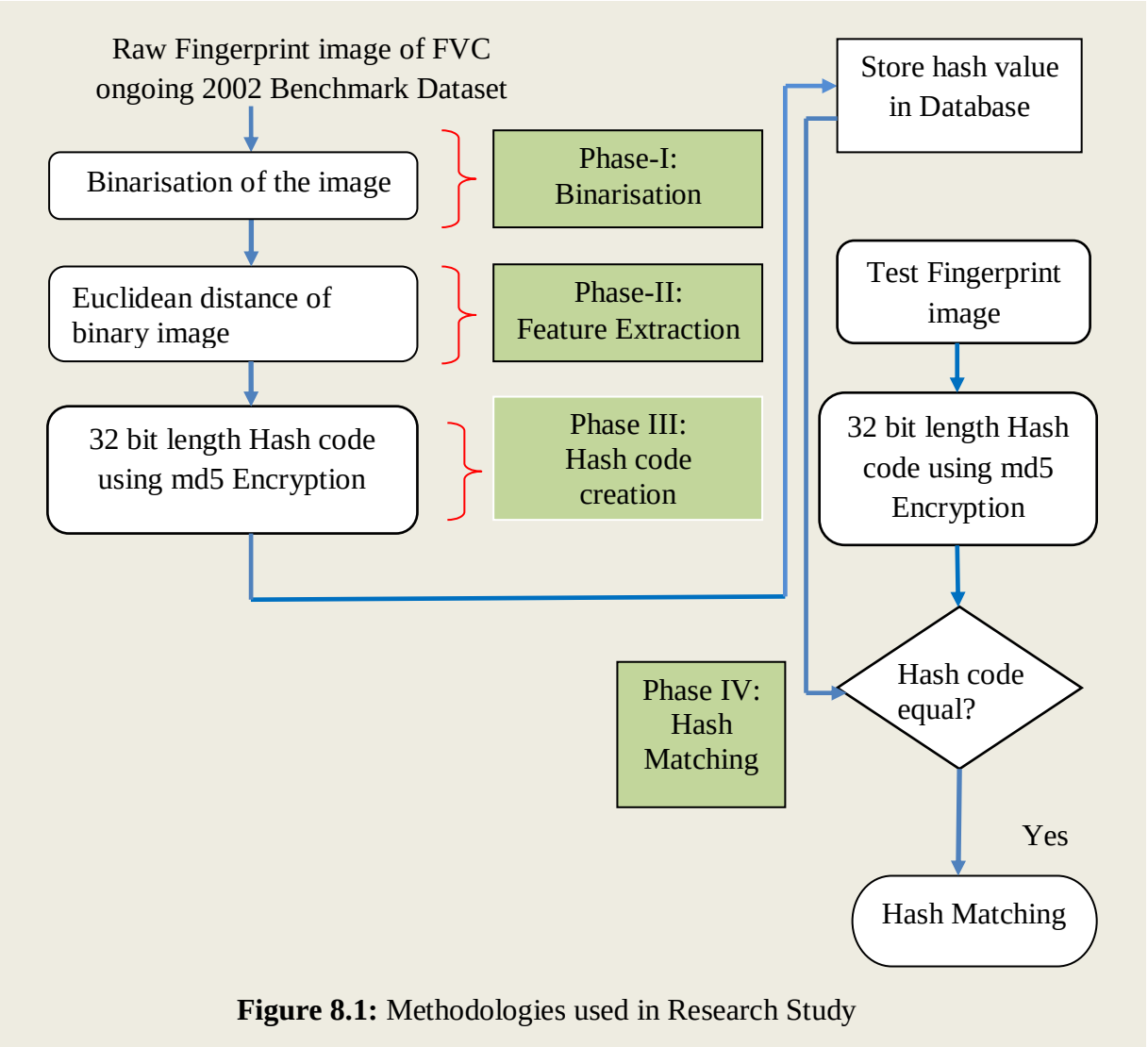


Figure 8.1: Methodologies used in Research Study

Here initially FVC ongoing 2002 benchmark dataset is considered for testing the hash code. The benchmark dataset image is binarised and Euclidean distance of the image is calculated for each pixel. The distinct values of the Euclidean distance matrices values are considered and 32-bit length hash code is generated. Distinct Euclidean distance value summation, mean value and standard deviation values are considered for generating Hash code.

8.3 ALGORITHM OF HASHCODE GENERATION USING EUCLIDEAN DISTANCE

This section explains step by step procedure to develop Hashcode by making use of Euclidean distance matrix on a binary fingerprint image. The steps of the algorithm are explained below. The algorithm also shows the pseudo code.

Step 1: Input Grayscale fingerprint image

read (input_image)

Step 2: Convert input image into 256 × 256 sized two-dimensional image

resized_image = image_resize (input_image, [256, 256])

Step 3: Convert 256 × 256 sized grayscale image into binary image

binary_image = convert_to_binary(resized_image)

Step 4: Find the Euclidean distance of the image

euclidean_image = Euclidean_distance(binary_image)

Step 5: Find the distinct value of the Euclidean distance

distinct_eucllidean_value = distinct_value(euclidean_image)

Step 6: Find the distinct value summation

For i=1 to size(distinct_eucllidean_value)

euclidean_sum = distinct_eucllidean_value (i)

end for

Step 7: Find the mean of the distinct Euclidean value

euclidean_mean = mean(distinct_eucllidean_value)

Step 8: Find the standard deviation of the distinct Euclidean value

std_deviation = standard_deviation(distinct_eucllidean_value)

Step 9: Combine the value of Step-6, Step-7, and Step-8

combine_value = combine(euclidean_sum, euclidean_mean, std_deviation)

Step 10: Pass the value of Step-9 as parameter for MD5 Hash function

hash_value = MD5_DataHash(combine_value)

8.4 FLOWCHART OF HASHCODE GENERATION USING EUCLIDEAN DISTANCE

The above algorithm is explained using flowchart in Figure 8.2. The different process or work flow are listed below. With an intension to make the MD5 Hashcode more robust and to get the advantage of salting Euclidean distance sum, mean, and standard deviation are combined and passed to the MD5 algorithm.

- Converting input image to 256 × 256 sized grayscale image.
- Converting to binary image. Finding Euclidean distance.
- Finding distinct value of the Euclidean distance.
- Finding the sum of the distinct Euclidean distance.
- Finding the mean of the distinct Euclidean distance.
- Finding the standard deviation of the distinct Euclidean distance.
- Generating MD5 Hashcode using combined sum, mean, and standard deviation of distinct Euclidean distance value.

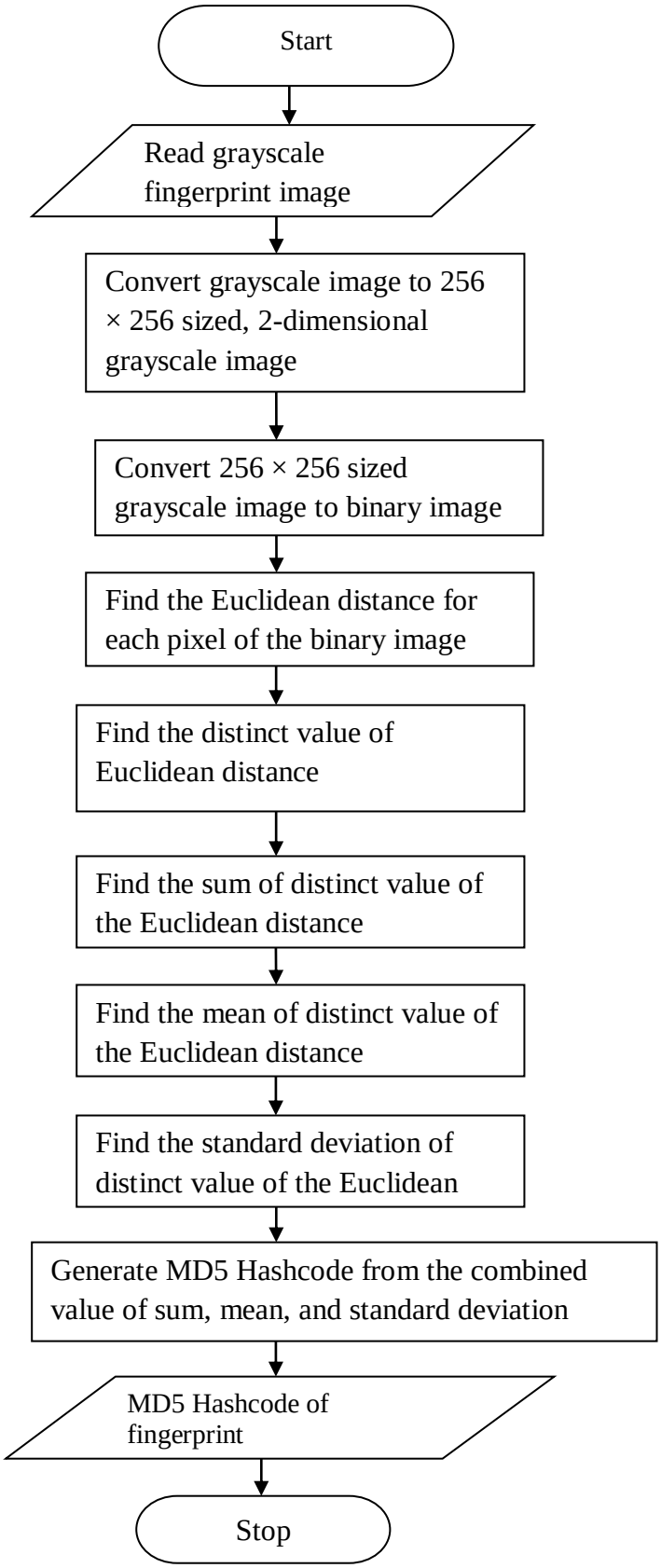


Figure 8.2: Flowchart of Hash code generation using Euclidean Distance

The process of the MD5 algorithm is disused below.
Input: Extracted Features
Output: Hash Code
Step-1: Attach the padded bits
Step-2: Append the length of the initial input to the result of the previous step-1
Step-3: Initialize MD buffer as A, B, C, D.
A four-word buffer (A, B, C, D) was used to evaluate the message digest. Here each of A, B, C, D is a 32- bit register
Step-4: Process message in 16-word blocks
Step-5: Finally, we get the 32-bit Hashcode as output

8.5 RESULTS AND DISCUSSIONS

In this study, WampServer is used to create a database. This database table contains two fields as id and Hashcode. The Hashcode generation using Euclidean distance is implemented using MATLAB2015a. The configuration of the system used to implement this study is given in Table 8.1.

Table 8.1: Configuration of System used for finding Execution Time

Sr. No.	Parameters	System Details
1	Model	Compaq 435
2	Processor	AMD E-350 processor 1.60 GHz
3	Installed Memory	3 GB (2 GB usable)
4	System Type	32-bit Operating System
5	Operating System	Windows 7 Starter
6	Software	MATLAB 2015a 32-bit

The execution time for different randomly selected images of FVC ongoing 2002 dataset is shown in Table 8.2.

Table 8.2: Execution time of the training phase

Method Name	Image name	Execution Time (in seconds)	Average
Method-1	101_1	0.507921	0.144420
	101_5	0.245508	
	102_2	0.146157	
	103_3	0.108258	
	104_4	0.102478	
	104_7	0.056262	
	104_8	0.068901	
	105_8	0.080591	
	106_6	0.114282	

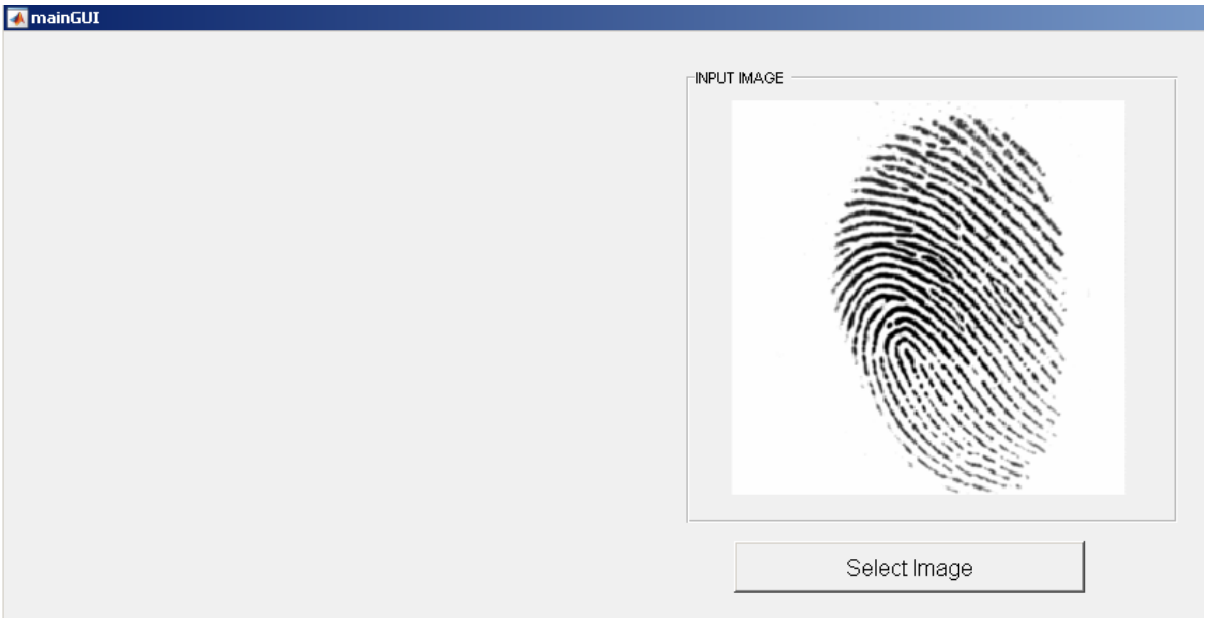
109_3	0.117105
109_8	0.109788
110_3	0.104671
110_8	0.115539

The average execution time of the fingerprint Hashcode generation using Euclidean distance is very good and it is approximately 0.144420. Here we only consider the training phase. The testing phase includes around 0.44 seconds more than training phase. If the configuration of the system increases definitely execution time also increases. Table 8.3 shows the Hashcode generated based on an MD5 algorithm using Euclidean distance.

Table 8.3: Hash code generated using Euclidean distance

Serial No.	**Hashcode**
1	e06c186b309ba7351d716b519d7c73b2
2	6e621fa2509d451735cc3a6371ddb5bc
3	58700de96bb19d7fae96279f37e2f134
4	63fd88581c026148ff47df64ccb1d070
5	1dae3325e72f45e183431fb2bbd79377
6	2ce72a2f2b342594c2333f607b8da5f5
7	52fee94aa0ae0bacd8450613997f181d
8	d9d9fa4f656ce9f56cc09aaf4633a588
9	5c3035d3ae414d8ebf7bf117de58c21c
10	911cd7041e72ae334477ef593b217666
11	1d00b55914c7559b8cab2569c9a035a3
12	5fb8835210967067ce0612ae341222ce
13	375eaf11d2909e267ea8e37012895d0b

The screenshots of the grayscale fingerprint image capture is shown using Figure 3.



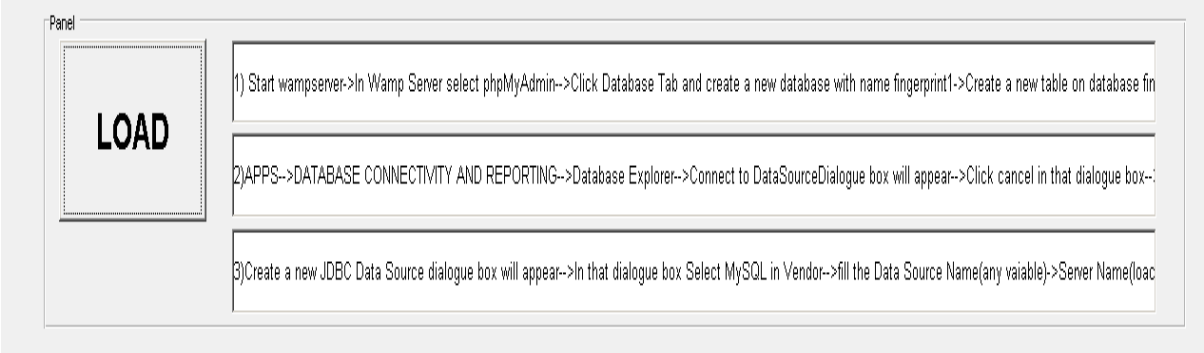
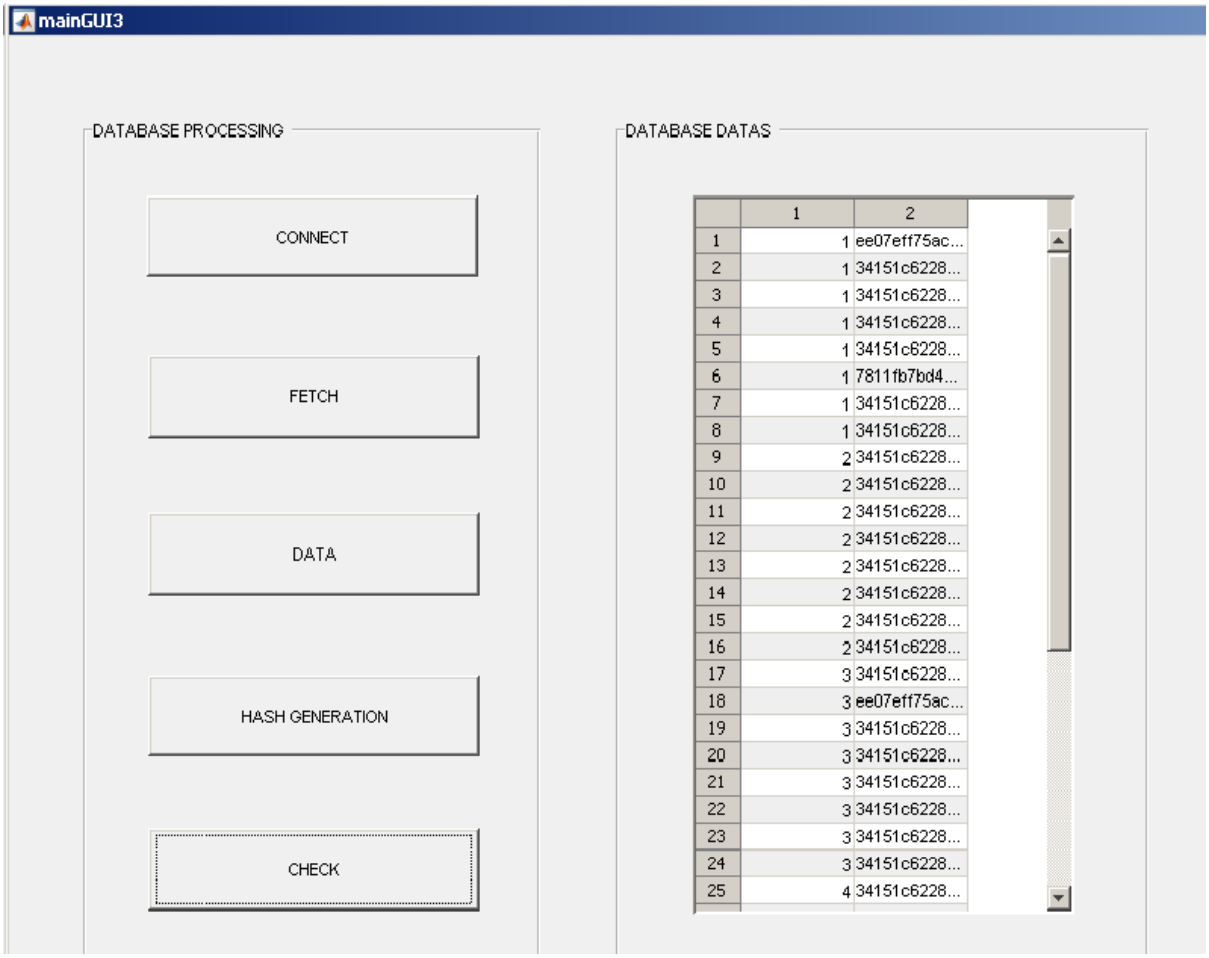


Figure 8.3: Screenshots of Fingerprint image capture

The screenshot or Figure 8.3 contains two push buttons. One push button is used to select grayscale fingerprint image. Another one gives instruction to create WampServer and to connect this from MATLAB2015a. The screenshots of Database processing and status is shown using Figure 8.4.



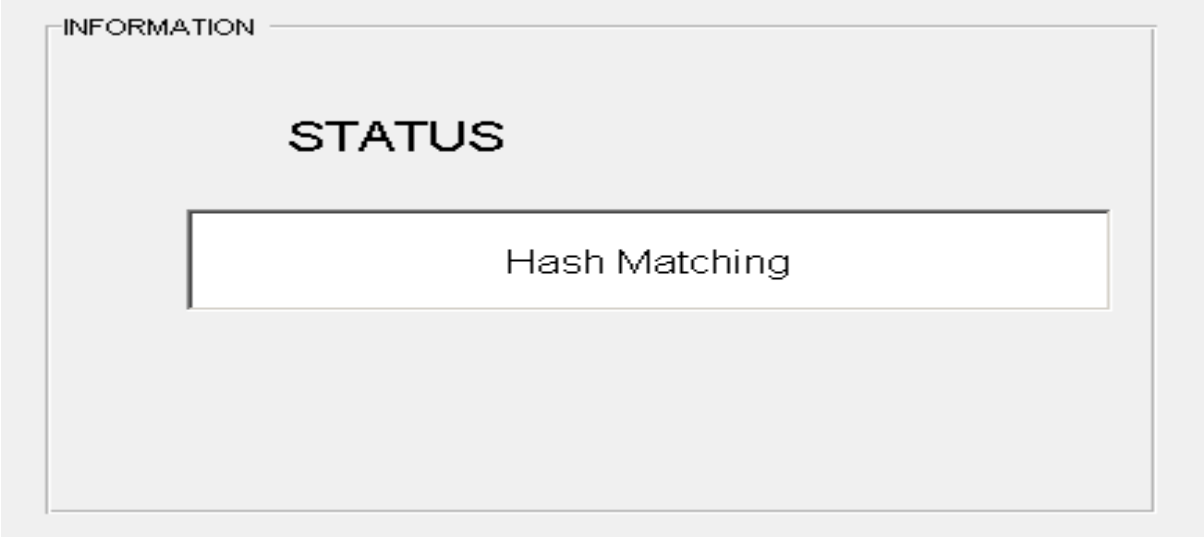


Figure 8.4: Screenshots of Database processing and Status

The data processing control of Figure 8.4 consists of five push buttons as Connect, Fetch, Data, Hash Generation, and Check. Connect button is used to connect to the database, Fetch button is used to fetch records from the database, Data button is used to show data in tables, hash generation is used to generate Hashcode for sample input fingerprint, and Check is used to check sample input Fingerprint image is matching or not matching with already stored hash code.

Advantages of Hash value produced using Euclidean distance

- Hash code produced using Euclidean distance matrices are noninvertible
- Hash code takes very small amount of memory
- Hash code Hides original information of fingerprint image from the intruder
- The execution time of Hash code generation using Euclidean distance is very good.
- It is unique for each fingerprint of the same person means ten fingerprints will be having ten different Hash codes.

Benefits of Hash value produced using Euclidean distance

- Hash code is used as identity-key or index-key for unique identification purpose of a user.
- Easily we can append salting in order to make the Hash code more robust.
- Fingerprint Hash code is a transformed function, which does not reveal original minutiae details.
- Fingerprint Hash code consumes very less time for training phase.
- Unlike another fingerprint matching, this study does not use scoring level. It uses only binary value either matching or not matching.

Constraints of Hash value produced using Euclidean distance

- Small changes in fingerprint hash code make large differences.
- Fingerprint generation using Euclidean distance are translation and rotation variant which is not having much scope when the fingerprint is used for identification purpose rather than security purpose.

Disadvantages of Hash value produced using Euclidean distance

- Fingerprint hash code cannot be solely used for security or authentication purpose.
- If fingerprint image of same finger input is taken through any type of solid and robust sensors in consecutive two intervals, still fingerprint hash code generates different hash code.
- Even though developed fingerprint Hash code is invariant to translation and rotation, if the user presses hardly into one reader or sensor, or swipe the finger in a different orientation, or a cut in the finger, for a successive two capture, produces different Hash code.

8.6 CONCLUSION

Even though fingerprints are most common and easily usable and many research contribution available areas of biometrics, which is having some flaws like which left by a human being at many places like door, wall, on the car and many more places are easily mimicked by fraud or intruder. The fingerprint does not get matched when the finger has some cut or wound and sensors are not able to recognize in some weather conditions like winter season. The fingerprint is effective as identity or index key and not as a full security feature. It works well with multifactor biometrics authentication as one major factor.

In this paper, we developed a Hash code based on an MD5 Hash function by making use of Euclidean distance of binary fingerprint image. This Hashcode can be effectively used as Index-key or identity-key. This method shows considerably better execution time. This method also gives 100% accurate matching as far as input fingerprint image is once captured and stored static digital fingerprint image. If we capture through sensor each time this gives different Hash code. So this method is not suitable for solely security purpose.

REFERENCES

[1] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[2] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608

[3] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[4] Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[5] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 51-65.

DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[6] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 98-111.

DOI: http://dx.doi.org/10.5281/zenodo.1067110

[7] Krishna Prasad, K. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE),* 1(2), 86-92. DOI: http://dx.doi.org/

[8] Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.

[9] Juels, A. (2002). M. Sudan 'A fuzzy vault scheme'. In *Proceedings of the 2002 IEEE International Symposium on Information Theory* (Vol. 408).

[10] Tuyls, P., Akkermans, A. H., Kevenaar, T. A., Schrijen, G. J., Bazen, A. M., & Veldhuis, R. N. (2005, July). Practical biometric authentication with template protection. In *AVBPA* (Vol. 3546, pp. 436-446).

[11] Holst, J. C., & Draper, D. A. (1999). *U.S. Patent No. 5,999,039*. Washington, DC: U.S. Patent and Trademark Office.

[12] Davida, G. I., Frankel, Y., Matt, B., & Peralta, R. (1999). On the relation of error correction and cryptography to an online biometric based identification scheme. In *Workshop on coding and cryptography*.

[13] Hao, F, Anderson, R & Daugman, J 2006, _Combining Crypto with Biometrics Effectively', IEEE Transactions on Computers, vol. 55, pp. 1081-1088.

[14] Kelkboom, E. J., Gökberk, B., Kevenaar, T. A., Akkermans, A. H., & van der Veen, M. (2007, August). "3D face": biometric template protection for 3D face recognition. In *International Conference on Biometrics* (pp. 566-573). Springer, Berlin, Heidelberg.

[15] Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005). PalmHashing: a novel approach for cancelable biometrics. *Information processing letters*, *93*(1), 1-5.

[16] Das, P. P., Chakrabarti, P. P., & Chatterji, B. N. (1987). Distance functions in digital geometry. *Information Sciences*, *42*(2), 113-136.

[17] Yamada, H. (1984). Complete Euclidean distance transformation by parallel operation. In *Proc. of 7th Int. Conf. on Pattern Recognition, Montreal* (Vol. 1, pp. 69-71).

[18] Borgefors, G. (1986). Distance transformations in digital images. *Computer vision, graphics, and image processing*, *34*(3), 344-371.

[19] Danielsson, P. E. (1980). Euclidean distance mapping. *Computer Graphics and image processing*, *14*(3), 227-248.

[20] Yamashita, M., & Ibaraki, T. (1986). Distances defined by neighborhood sequences. *Pattern Recognition*, *19*(3), 237-246.

[21]https://hackaday.com/2015/11/10/your-unhashable-fingerprints-secure-nothing/, Last Accesses Date: 05-12-2017.

[22]https://security.stackexchange.com/questions/42384/is-there-any-way-to-cryptographically-hash-a-human-thumbprint, Last Accesses Date: 05-12-2017.

[23] Aithal, P. S. (2016). A Review on Advanced Security Solutions in Online Banking Models, International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 421-429. DOI : http://doi.org/10.5281/zenodo.160971.

[24] Aithal, P. S. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. *International Journal of Management, IT and Engineering (IJMIE)*, 5(7), 455-464, DOI : http://doi.org/10.5281/zenodo.268875.

Chapter 9
An Alternative Approach to Fingerprint Hash Code Generation based on Modified Filtering Techniques

Fingerprint unique Hash code and template protection are the new technologies in biometric identification and verification system. Fingerprint hashing is the new technique which combines biometrics and cryptography. The modern study reveals that fingerprint is not so secured like secured passwords which consist of alphanumeric characters, number and special characters. Fingerprint Hash code acts as a key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. In this paper, a fingerprint Hash code is generated using a novel Contrast Adjustment algorithm, modified segmentation algorithm, and Gabor filtering. The Hash code is generated from the extracted features of the grayscale fingerprint image using MD5 Algorithm. Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. This study makes use of fingerprint Hash code as a unique key for human identification purpose.

Keywords-*Fingerprint Hash code, Gabor Filtering, Contrast Adjustment algorithm, Segmentation, MD5 Algorithm.*

9. 1 INTRODUCTION

Automatic Fingerprint Identification System (AFIS) contain the use of automatically and reliably enhance the image, reduce the noise and extract the minutiae features from the biometric images of the fingerprint. The performance of a minutiae extraction principle relies heavily on the pleasant quality of the input biometric image. The automatic fingerprint identification system consists of preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment as its different stages or subprocess [1-9].

Contrast adjustment methods are extensively used for image processing to attain wider dynamic range and which is considered as preprocessing stage, especially in Automatic recognition system based on different types of images like a fingerprint, face, iris etc. When brightness is too high all the pixels of the image turn into lighter, conversely when the brightness is too low all the pixels of the image turn into darker. When the intensity is a too high, lighter area of the image becomes lighter and darker area of the image becomes An essential and important step in order to obtain high quality and performance rate at all types of image is through accurate segmentation. Fingerprint segmentation is the one of the main process involved in fingerprint pre-processing and it refers to the process of dividing or separating the image into two disjoint regions as the foreground and background. The foreground also called as Region of Interest (ROI) because only the region which contains ridge and valley structure is used for processing, while the background contains noisy and irrelevant content and that will be discarded in later enhancement or orientation or classification process.

Some of the most common types of segmentation algorithms are, TV-L1 based Adaptive Total Variation Model [11], TV-l2 based Directional Total Variation Model [12], Method based on a combination of ridge orientation and ridge frequency characteristics using orientation tensor approach [13], Orientation field is combined with the statistical characteristics of the gray to form new method [14], Ridge orientation Method based on Ridge Temple using correlation with a sinusoid [15], and the coherence, the mean, the variance as three pixel features methods.

One of the important challenges in biometric identification or verification system is keeping the biometric data or template safe and secure. A Hash function is usually transformed functions, which converts or transform data or features from one form to another. Always transform function should be the one-way function or another way it should not be invertible. Symmetric Hash functions for biometric fingerprints are some hash function, which is independent of the order in which input is presented to the system or invariant to translation and rotation [16]. In literature, few methods are already proposed by different researchers for building cancellable biometric template. In this regard, there are mainly two techniques, out of which one is error correcting code and another one is noninvertible transformation.

In this paper initially τ- Tuning Based Filtering Algorithm is used to improve grayscale fingerprint image contrast. The later image is converted into binary image and image is segmented based on Surfeit clipping based segmentation algorithm. From the segmented

binary image, fingerprint features are extracted using Gabor filtering techniques, using angular and frequency variations. Finally, these features are converted into Hash code using the MD5 hash algorithm. To implement this algorithm MATLAB2015a is used by considering input from FVC ongoing 2002 benchmark dataset. The remaining part of the paper is organized as follows. Section 2 describes relative to research on the contrast adjustment, segmentation, and Gabor Filtering. Section 3 describes Research objective and Methodology. Section 4 describes the tuning based Contrast Adjustment algorithm. Section 5 describes Surfeit Based segmentation algorithm. Section 6 describes features extraction using Gabor filter. Section 7 describes Results and Discussion. Section 8 concludes the paper.

9.2 RELATED RESEARCH

Equalization through Histogram (HE) is a very famous approach for image contrast adjustment or enhancement in image processing. In general, the histogram equalization distributes pixel values consistently and produces an outcome in a superior image with the linear increasing histogram. Some useful applications of HE enhancement consist of scientific image processing, speech recognition, fingerprint identification and texture synthesis, which might be typically employed with histogram adjustment [17-20].

Different techniques of making use of histogram equalization are determined in the literature. Global histogram equalization or GHE (Gonzalez & Woods, 2002) [21] makes use of the entire information of the input image to map into new distinct intensity levels of the image. Although this Global technique is suitable for ordinary or general enhancement, it fails to consider with the local brightness capabilities of the entered image. The gray ranges with very excessive frequencies (wide variety of occurrences) dominate over the opposite gray levels having decrease frequencies in an image. In any such situation, GHE remaps the gray levels in a way that the contrast stretching turns into confined in some dominating gray levels having large image histogram components, and it causes sizable contrast loss for other small ones.

Local histogram equalization (LHE) can overcome the problem encountered in GHE (Gonzalez & Woods, 2002) [21]. LHE uses a small window that slides on all pixel of the image sequentially and handiest the block of pixels that fall within this window are taken into consideration for HE and then gray level mapping for enhancement is carried out for the center pixel of that window. Therefore, it may make splendid use of local information also. But, LHE requires excessive computational cost and occasionally reasons over enhancement in some part of the image. Another shortfall of this approach is that it also enhances the noises inside the input image. To overcome the problem of high computational cost one more approach is to use the non-overlapping block for HE (Gonzalez & Woods, 2002; K. Krishna Prasad & Aithal P. S., 2017) [21 & 1]. But almost all times this method produces checkerboard effect.

In literature, there are many studies available, which mainly focuses on fingerprint image segmentation. Researchers, Mehtre, B. M., & Chatterjee, B. (1989) classified the image into blocks, which is administrative specific and the size was 16 × 16 pixels. Based on the gradient distribution, each block was classified. This method is best suited for simple fingerprint images which contain only background and foreground. Later Researchers Mehtre

and Chatterjee (1989) [22] extended this work by leaving the grayscale variance, which will usually be lower than some threshold value. Researchers Ratha, N. K., Chen, S., & Jain, A. K. (1995) [23] proposed 16 × 16 blocks of classes and each one was developed based on the gray scale variance in the direction opposite to the orientation of ridges.

The authors Jain, Ratha, & Lakshmanan (1997) [24] concentrated for the detection of objects located in complex backgrounds. The given object is first applied to a bank of even-symmetric Gabor filters. The output image received from the Gabor filter is subjected to a sigmoid function transformation. The yield image of the Gabor filter is applied as an input to the clustering algorithm, which develops spatially compact clusters. Sun and Ai (1996) [25] pre-processed initially fingerprint image by converting it into a binary image with the help of dynamic threshold value (T). Moayer and Fu (1975) [26] used sampling squares, which are obtained from the subdivision of fingerprint images for the ultimate goal of feature extraction. They used dynamic threshold value (T) to convert the initial image to a binary image. In order to determine the local threshold value, researchers used neighbor pixels by group 5 × 5 pixels.

Naji, Ramli, Ali, R., Rahman, and Ali, M.L. (2002) [27] developed a segmentation algorithm, which computerized or automated the method of selecting a threshold value at the time of segmentation with the aid of histogram equalizer. Segmentation algorithm generally falls under two categories of machine learning techniques as supervised learning and unsupervised learning. Unsupervised learning uses threshold decided on detecting features to cluster the image. Supervised learning uses a simple linear classifier to classify features as a region of interest (ROI) or background and foreground. As a part of supervised methods, Alonso-Fernandez, Fierrez-Aguilar, & Ortega-Garcia, (2005) [28], used a Gabor filter to filter the input image and to obtain a smooth image. The neural network can also be used in the segmentation process to reduce the noise or to enhance the image quality.

9.3 RESEARCH OBJECTIVE AND METHODOLOGY

The most of the research work in fingerprint identification system fails to provide template protection with main characteristics like revocability, diversity, non-invertible, and permanence. Most of the fingerprint identification algorithms or techniques are not able to match or recognize partial fingerprints. These two are the motivation for this study. The research gap identified in this study is listed below.

- When fingerprints are easily mimicable, what is the use of developing Hash code Translation and Rotation or orientation change invariant?
- Is it possible to compare and match fingerprint with only one Hash code stored in the database?
- Is there any possibility of using a fingerprint as identity-key or index-key with the aid of Hash code, without capturing through sensors every time, by considering the image captured at the beginning or onetime only (using a static image of the fingerprint)?

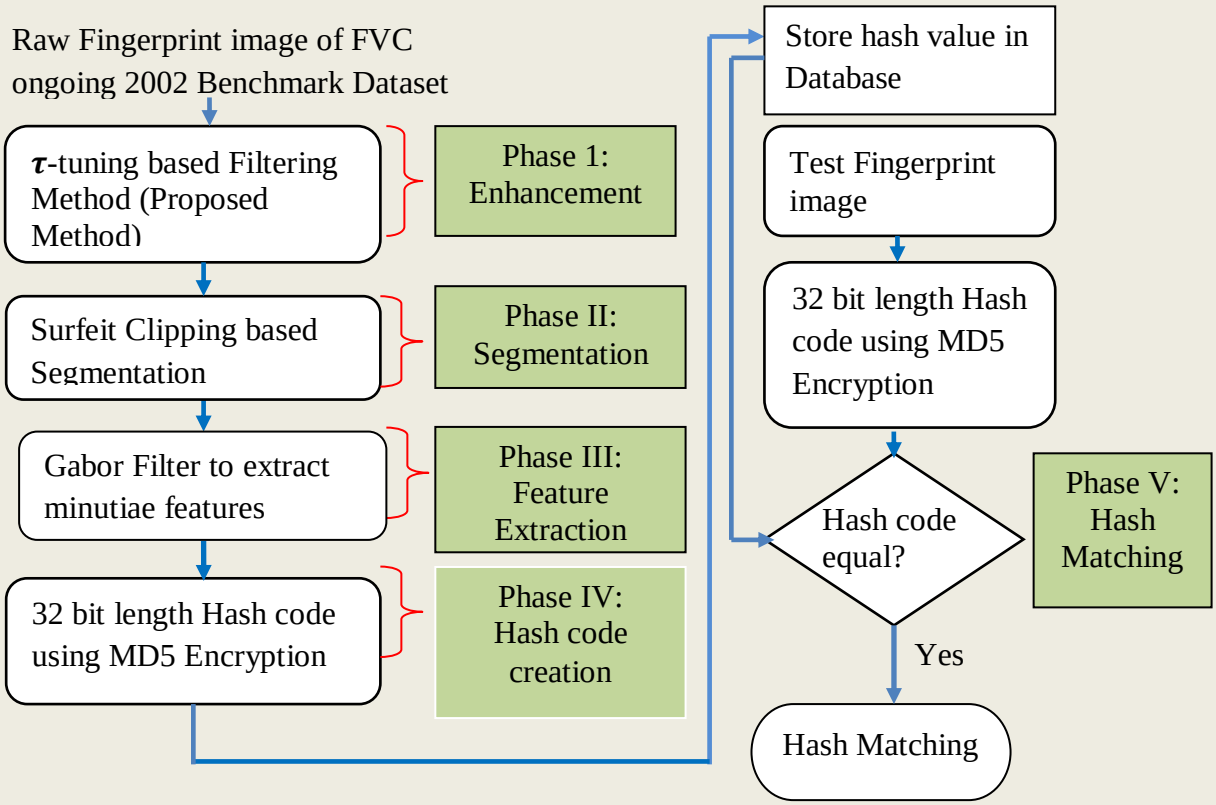


Figure 9.1: Proposed Methodologies

The main objective of the research is given below.

- To Study a Fingerprint Hash code based on MD5 Hash Algorithm, using Gabor filter which includes modified filtering techniques, Contrast adjustment filtering, and Segmentation.

Here two-dimensional 64 × 64 sized Gabor Filter is used to extract features directly from segmented image without performing thinning process. The proposed work is implemented using MATLAB2015a. FVC ongoing 2002 benchmark dataset are used for training and test purpose. The methodology used in this study is shown in Figure 9.1.

9.4 TUNING BASED CONTRAST ADJUSTMENT ALGORITHM

The input for this algorithm is row image referred as I, and final output will be I_{filter}. Initially maximum intensity value of the image is found. We consider here 256 × 256 sized grayscale image. If the input fingerprint image is greater than this size then it will be converted into 256 × 256 sized grayscale image. The maximum intensity value in a 256 × 256 sized grayscale image is 255. The range of values is 0 to 255, which means that minimum value is 0 and maximum value is 255. Maximum intensity value of the image is represented as max (I). Each pixel intensity value is compared with max (I).

If pixel value is equal to max (I), then that pixel is assigned to ρ_{max}. The ρ_{max} is individual count of maximum intensity value. The total count of ρ_{max} is represented using lower case delta symbol δ_{max} and is calculated as follows [10].

$$\delta_{max} = \frac{\sum \rho_{max}}{R \times C} \quad \text{..... (9.1)}$$

In Eq. (9.1) R, and C, are total number of rows and columns respectively. $\sum \rho_{max}$, indicates all pixels, whose intensity value is equal to maximum intensity value of the grayscale fingerprint image (I). Next minimum intensity values of the grayscale image are found and are referred as min (I). If pixel value is equal to min (I), then that pixel is assigned to ρ_{min}. The ρ_{min} is individual count of minimum intensity value of the image. The total count of ρ_{min} is represented using lower case delta symbol δ_{min} and is calculated as follows.

$$\delta_{min} = \frac{\sum \rho_{min}}{R \times C} \quad \text{----------(9.2)}$$

As like Eq. (9.1) in Eq. (9.2), R, and C, is total number of rows and columns respectively. $\sum \rho_{min}$, indicates all pixels, whose intensity value is equal to intensity value of the grayscale fingerprint image (I).

Each row of the intensity matrix of the image is considered as a window and is represented as δ_w, which is expressed as

$$\delta_w = \delta_{max}\left(\frac{\delta(l) - \delta_{min}}{\delta_{max} - \delta_{min}}\right)^{\epsilon} \quad \text{---------- (9.3)}$$

In Eq. (9.3) ϵ value is 0.5, which is a constant. $\delta(l)$ is low or minimum value of each row. The difference value of $\delta(l) - \delta_{min}$ is divided by $\delta_{max} - \delta_{min}$. The quotient is multiplied by δ_{max}.

∂_w which is almost equal to Histogram equalization, cumulative density function, of window l is represented using 'tho' or partial derivative symbol and is defined as

$$\partial_w = \sum_{l=0}^{l_{max}} \frac{\delta_w(l)}{\sum \delta_w} \quad \text{----------(9.4)}$$

In Eq. (9.4) $\sum \delta_w$ represents summation value of all window l or summation of δ_w. $\sum \delta_w$ is calculated as follows

$$\sum \delta_w = \sum_{l=0}^{l_{max}} \delta_w(l) \quad \text{..... (9.5)}$$

The final output of this proposed algorithm (I_{filter}) is obtained using following equation

$$I_{filter} = \left(l_{max} \times \left(\frac{I(i,j)}{l_{max}}\right)\right)^{\tau} \quad (9.6)$$

In Eq.(9.6), tau (τ) is an important value, which filters or maps input pixel intensity value to new intensity value in the output image and is defined as

$$\tau = round(1 - \max((\partial_w(:))) \quad (9.7)$$

The Eq. (9.7) is rounded to 6 decimal points to get higher precision or accuracy.

The output of the robust tuning based algorithm (proposed method), I_{filter} is converted from grayscale 256 × 256 uint8 to double type for the purpose of grayscale image adjustment. The 256 × 256 double image consists of only two intensity values as 0 and 1. 0 represents dark and 1 represents bright or 0 dark black and 1 bright white. Here in image enhancement we focus more on Robust τ- Tuning Based Filtering Algorithm and in concluding part of the enhancement we just convert the output of this phase to just double type with an ultimate goal to achieve grayscale image adjustment.

A. Tuning Based Filtering Algorithm [10]

Input: Raw Image; I

Output: Filtered Output Image,I_{filter}

Step-1: for i=1 to R \\ R→ Row size of input image

Step-2: for j=1 to C \\ C→ Column size of input image

Step-3: if I(i,j)= =max(I)

Step-4:$\rho_{max} = I(i,j)$; end if;end for

Step-5: $\delta_{max} = \frac{\sum \rho_{max}}{R \times C}$

Step-6: for i=1 to R \\ R→ Row size of input image

Step-7: for j=1 to C \\ C→ Column size of input

\\ image

Step-8: if I(i,j) = = min(I)

Step-9:$\rho_{min} = I(i,j)$; end if;end for

Step-10: $\delta_{min} = \frac{\sum \rho_{min}}{R \times C}$

Step-11: $\delta_w = \delta_{max}(\frac{\delta(l)-\delta_{min}}{\delta_{max}-\delta_{min}})^{\epsilon}$ \\ ϵ→Constant; $\epsilon = 0.2$

Step-12: $\partial_w = \sum_{l=0}^{l_{max}} \frac{\delta_w(l)}{\sum \delta_w}$

Step-13: $\sum \delta_w = \sum_{l=0}^{l_{max}} \delta_w(l)$

Step-14: $\tau = round(1 - \max((\partial_w(:)))$ \\round to 6 decimal

\\points

Step-15: $I_{filter} = (l_{max} \times (\frac{I(i,j)}{l_{max}}))^{\tau}$

9.5 SURFEIT BASED SEGMENTATION ALGORITHM

This algorithm considers Enhanced fingerprint image and produces a good quality segmented image. Let $I_{enhanced}$ be the enhanced image using robust τ-tuning based filtering method. The enhanced image is converted to binary image and stored as I_{binary}. Initially to find the edges of the I_{binary} image efficiently canny edge detection method is used. Canny edge detection finds the edges of the image through different processes, which includes, smoothing, locating gradients, non-maximum suppression, double thresholding, and edge tracking by using hysteresis. Smoothing of the image is done with the help of convolution, which blurs the image to get rid of noise. Canny edge detection uses double thresholding in order to find edges of the image. The result of the canny edge detection method is stored as I_{canny}. Next, the edge detected image, I_{canny} is converted into low resolution image by converting 256 × 256 sized grayscale image to 128 × 128 sized grayscale image.

$$I_{LRE} = I_{binary}(i \times 2, j \times 2)$$

The low resolution image is represented as I_{LRE}. In the next phase I_{LRE} image is padded with zeros using pad array and usually for simplicity in this method we use pad array size is eight and is referred as P. For $I_{LRE,}$ eight zeros are added in row and column respectively, and it enhanced to 144 × 144 sized grayscale image, which is denoted as I_{Parray}.

The I_{Parray} is clipped into 15×15 sized image and processed. The clipped image is stored in temp1. The entire 225 pixels of temp1 are reshaped as 1×225 matrix and denoted as temp2. The covariance of the matrix of the image, temp2 is calculated and if it is less than the threshold then the pixel of the I_{binary} (256 × 256 size) image is considered as not a part of ROI or foreground. Covariance of a matrix is calculated by considering row as observations and columns as random variables. Every pixel of the I_{binary} image is traced like this and marked as either foreground or background of the image based on covariance value. If it is greater than the threshold value then the pixel is considered to be foreground, means which is real part of the fingerprint image. Each time when padarray is considered, this takes into account one pixel out of 128×128 low resolution image and two pixels out of 256 ×128 sized image.

As the algorithm name suggests surfeit, means maximum, we discard maximum background part of the image by checking whether all the pixels of the each column intensity value sum becomes 256. If the column sum is 256 means all the pixels of that particular column contains intensity value 1. This signifies that this column contains background of the image. If any one column intensity value sum leads to value less than 256, which signifies that the particular column contains part of the foreground or ROI of the image. Then we skip the iteration and count considering starting of the column pixel for output of the segmented image from just previous to that column number. Same process we repeat from the last column to first column in reverse direction and stop moving backward until we get a column number sum of intensity value less than 256 for the purpose of finding last column number, which contains at least one pixel of foreground pixel. This means that from the last column to till this position image contains only background part of the image. The above-mentioned

method repeated for rows also. So that it eliminates background or white blank area in left edge, right edge, top edge and bottom edge regions.

Surfeit Clipping based Segmentation Algorithm [6]

Input: binary image, I_{binary}

Output: Segmented Image, $I_{segment}$

Input: binary image, I_{binary}

Output: Segmented Image, $I_{segment}$

Step-1: Read I_{binary} image

Step-2: Apply canny edge formation to the I_{binary} and store it in a variable I_{canny}

Step-3: for i=1 to floor(R/2)

Step-4: for j=1 to floor (C/2)

Step-5: $I_{LRE} = I_{binary}(i \times 2, j \times 2)$; end for loop; I_{LRE}→Low Resolution Edge Image

Step-6: $[R_{LRE}, C_{LRE}] = size(I_{LRE})$

Step-7: P=floor (max (15, 15)/2+1);

Step-8:$I_{Parray} = \text{padarray}(I_{LRE}, [P\ P])$

Step-9: for i=P+1 to R_{LRE}+P

Step-10: for j=P+1 to C_{LRE}+P

Step-11: temp1= $I_{Parray}(\left(i - floor\left(\frac{15}{2}\right) : i + floor\left(\frac{15}{2}\right)\right), \left(j - floor\left(\frac{15}{2}\right) : j + floor\left(\frac{15}{2}\right)\right))$

Step-12: temp2=reshape (temp1, 1, 225)

Step-13: $V_1 = covariance(temp2)$

Step-14: if $V_1 < T$ \\ T→Threshold value=0.101

Step-15: $I_{binary}\big((i-P) * 2 - 2 + 1 : (i-P) * 2, (j-P) * 2 - 2 + 1 : (i-P) * 2\big) = 1$

Step-16: end if; end for;

Step-17: $N_R = ColumnSize\ of\ I_{binary}$

Step-18: for i=1 to N_R

Step-19: $C_{sum} = \sum I_{binary}(:, i)$

Step-20: Check if $C_{sum} = N_R$

Step-21: $\text{Position}_1 = i$; end if

Step-22: for i=1 to N_R

Step-23: $C_{sum} = \sum I_{binary}(:, N_R + 1 - i)$

Step-24: Check if $C_{sum} = N_R$

Step-25: $\text{Position}_2 = \frac{({N_R}^2 - i^2)}{N_R + i}$; end if; end step-22 for

Step-26: $N_C = RowSize\ of\ I_{binary}$

Step-27: for i=1 to N_R

Step-28: $R_{sum} = \sum I_{binary}(:, i)$

Step-29: Check if $R_{sum} = N_C$

Step-30: $\text{Position}_3 = i$; end if

Step-31: for i=1 to N_C

Step-32: $R_{sum} = \sum I_{binary}(N_C + 1 - i, :)$

Step-33: Check if $R_{sum} = N_C$

Step-34: $\text{Position}_4 = \frac{({N_C}^2 - i^2)}{N_C + i}$; end if; end step-27 for

Step-35:$I_{segment} = I_{binary}(\text{Position}_3 to\ \text{Position}_4 :, \text{Position}_1 to\ \text{Position}_2)$

9.6 FEATURE EXTRACTION USING GABOR FILTER

After segmentation, we extract the features. This is mentioned in this study as Methodology. In this study first we convert the $I_{segment}$ image to double intensity image. Four floating point numbers are created using following statement

f=[1/3.2,1/3.4,1/3.6,1/3.8]*2*pi

Next gray thresh value of the Grayimage is calculated. Gray thresh is a threshold value between 0 and 1, and which always return a fraction value between 0 and 1. The above this value is treated as 1 and below this value is treated as 0, while converting Grayimage to binary image. In the binary image, I_{binary} the value 1 is considered as background of the image and 0 is foreground or ROI of the fingerprint image. All the pixels, which are having value 1 is extracted using index position which is having value 0 in, I_{binary} image. The starting and ending positions of the pixel which is having value 0 is calculated using imin, jmin, imax, and jmax respectively. i and j represents row and column of the I_{binary} image. These variables are used to extract ROI of the image from the I_{binary} image. To extract minutiae details here 64 × 64 sized Gabor filter is used with 4 different frequencies. The equation for Gabor filter is given by

G (i, j) = exp(-.5*((xPrime/Sx)^2+

Prime/Sy)^2))*cos(2*pi*f(1,fre)*xPrime) ----------(9.8)

In Eq. (9.8) xPrime = x * cos(theta) + y * sin(theta), yPrime = y * cos(theta) - x * sin(theta), theta=(pi*i)/8, i, can take value from 1 to 4.

Then convolution of the image p1 and imaginary part of G is found. p1 is a 64 × 64 sized double image obtained from I_{binary}. Again the convolution of the image p1 and Real part of G is also found, these two are stored in variables Imgabout and Regabout. Finally mean, standard deviation, and variance mean of Regabout is calculated. The above entire process is repeated for 4 different values of f. Total 12 real values are obtained and which is given as an input for hash function.

Algorithm for extracting features directly from segmented image

Input: Segmented image, $I_{segment}$

Output: Extracted features

1. Convert segmented image to double type

   I_{double} = double ($I_{segment}$)

2. Initialize three constants Sx and Sy with value 3 and L with value 4.

Sx=3, Sy=3, L=4

3. Initialize frequency for Gabor filter

   f= [1/3.2, 1/3.4, 1/3.6, 1/3.8] * 2 * pi // [where pi = 22/7]

4. Initialize a matrix p1 for Gabor filter as p1 with initialize value 1 with size

   64 × 64, as, $p1_{64\times64} = 1$

5. Find a grey thresh (threshold value) for I_{double}

   level = graythresh (I_{double})

6. Convert double image to binary image using graythresh value

   I_{binary} = binary_image (I_{double}, level)

7. [i, j] = find (zero index position of I_{binary} in row and column matrix)

8. Find the minimum and maximum position value for i and j.

   imin = min(i), imax = max(i), jmin = min(j), jmax = max(j)

9. Create a new binary image, $I_{binary1}$ which contains only value zero from I_{binary}

10. Initialize a constant variable rate

    rate = 64/max (size($I_{binary1}$))

11. Resize the $I_{binary1}$ as

    Resize $I_{binary1}$ (i × rate, j × rate) // where i and j are row and column dimension

12. Find the new size of I_{binary}

    [i, j] = size ($I_{binary1}$)

13. Round off the value of i, and j

    i1 = round ((64-i) / 2)

    j1 = round ((64-j) / 2)

14. Reassign the value of p1

    p1 = (i1 + 1 to i1 + i, j1 + 1 to j1 + j)

15. Convert p1 to double from binary

    p1= double(p1)

16. **for each** i (from 1 to 4) **do**

    Initialize the theta value as theta = (pi × i) / 8;

    for x= round to nearest integer value (-Sx) to round to nearest integer value (Sx)

    for y= round to nearest integer value (-Sy) to round to nearest integer value (Sy)

```
        Rotate with respect to theta
        xPrime = x * cos(theta) + y * sin(theta)
        yPrime = y * cos(theta) - x * sin(theta)
        Use Gabor filter by varying frequency and angle
        G(x, y) = exp(-((xPrime/Sx)^2+(yPrime/Sy)^2))*cos(2*pi
                        *f(1,fre)*xPrime)   // ^ represents power
      end for
    end for
  Do convolution of P1 and imaginary part of G from central part
    Imgabout = conv2 (p1, double (imag (G)), 'same') // 'same' does the
                                                //convolution from the central part
    Do convolution of P1 and real part of G from central part
      Regabout = conv2 (p1, double (real (G)), 'same') // 'same' does the
                                                //convolution from the central part
    Find the mean of  Imgabout and Regabout
     imfea1(i) = mean (Imgabout)
     imfea2(i) = mean (Regabout)
     Find Standard Deviation of  Imgabout and Regabout
      stfea1(i) = standard_deviation (Imgabout)
      srfea2(i) = standard_deviation (Regabout)
    Find the mean of variance of  Regabout
     medfea2(i)=mean(var(Regabout))
  End for
  End for
features = [ imfea2, srfea2, medfea2]
```

9.7 RESULTS AND DISCUSSIONS

Extracting features directly from segmented image based on Gabour filter uses four different values for frequency and theta, which is shown in Table 4.3. These four frequencies and Angle value helps to generate a matrix of size, 7 × 7 containing total 49 real values due to Gabor filtering process. Each row of the Table 9.1 results in 3 positive or negative real numbers due to mean, standard deviation, and mean of variance calculations. Before calculating these three statistical calculation convolutions process was conducted on Gabor filter matrix of size 64 × 64 (p1) and real part of the imaginary number of Gabor value (G).

Table 9.1: Frequency and Theta value used in Gabor Filter to extract features

Sr. No	Frequency value	Angle (theta) value
1	1.9635	0.3927
2	1.8480	0.7854
3	1.7453	0.1781
4	1.6535	1.5708

With the aid of Gabor filter process, each fingerprint image produces total of twelve (12) double precision values. These large double precision values ensure that each fingerprint sample produces different hash values through MD5 Hash functions.

Table 9.2 shows the trainhash1 table values for the benchmark dataset FVC ongoing 2002 DB1_B, dataset image 101_1 to 101_8 using Gabor filtering. Each user will be having 8 fingerprint images.

Table 9.2: Hash values for image DB1_B 101.Tif

id	**Hash**
1	d579254fa5831c03e60e18729fbc710b
1	27024ce2cdd3dbdfa8d689adb7abc36c
1	23a8d9d5cb9b4eb62dab62bb4a67e30c
1	51398c3f65804111d281ba3e9f62e084
1	3db3a5b0777e10d97b49851c4e71fe49
1	d7d4a52858c98fb16e37d9613242ca36
1	d2901a0ae4e697d2ca2b9122e7bd2a1e
1	9f164d2dfaa2dff871208789d9056098

Figure 9.2 shows output of the tuning based contrast adjustment algorithm. In τ- Tuning Based Filtering Algorithm, dark pixels are highest dark and bright pixels are either highest or near to high bright values. This algorithm is best suited for grayscale fingerprint image, especially 256 × 256 sized. As like histogram equalization one of the pixel intensity values dominates over other. So this algorithm is not best for natural image because it may cause wash out appearance. But this is very good and robust for grayscale fingerprint image. In fingerprint image usually black colour represents ridges and white color represents valley. The dominating intensity value usually falls in upper boundary region of intensity range, which makes the image brighter

The Surfeit clipping based segmentation is analyzed by considering FVC ongoing 2002 DB1_B datasets. A sample fingerprint image named as 102_1.tif from FVC ongoing 2002 dataset is considered in Figure 9.2.

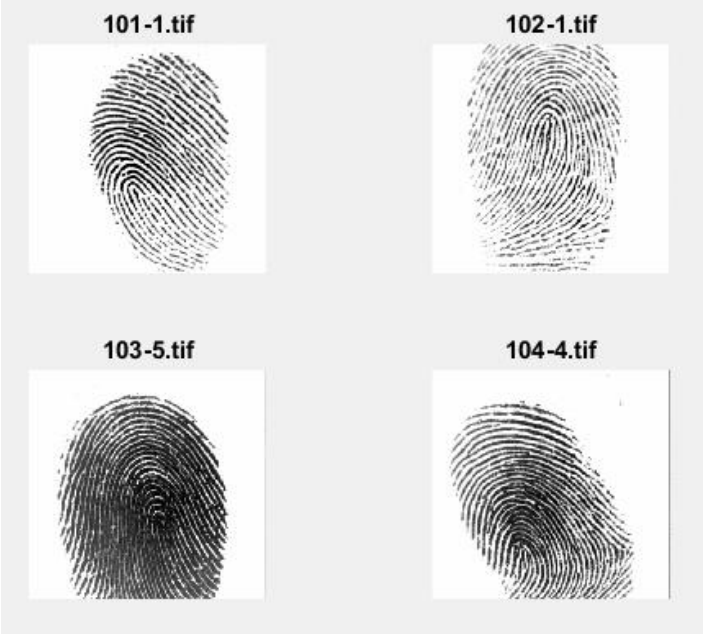


Figure 9.2: Sample original fingerprint images of FVC ongoing 2002 DB1_B dataset

The speed refers the time taken by the system to enroll as well as authenticate or reject. In technology term this can be referred as Elapsed time or time utilized by the new algorithm or model in to enroll and match. Elapsed time is calculated on following configuration system, and which are given in Table 9.3.

Table 9.3: Configuration of System for finding Elapsed Time

Sr. No.	Parameters	System Configuration
1	Model	Compaq 435
2	Processor	AMD E-350 processor 1.60 GHz
3	Installed Memory	3 GB (2 GB usable)
4	System Type	32-bit operating System
5	Operating System	Windows 7 Starter
6	Software	MATLAB 2015a 32-bit

Table 9.4 shows execution time of the training phase for Hash generation using Gabor filter. Gabor filter is used to extract features from the segmented image. Execution time of the testing phase is same for all four methods, which are about 0.6 seconds and 0.44 seconds more than training phase.

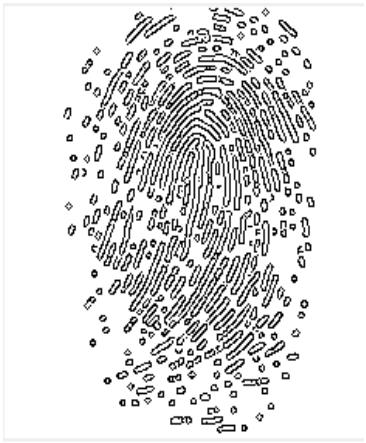
Table 9.4: Elapsed Time of the Training Phase

Method Name	Image name	Execution Tine (in seconds) using System-I	Average
Method-2	101_1	9.433374	6.783357
	101_5	5.912853	
	102_2	5.997807	
	103_3	5.789369	

9.8 CONCLUSION

In this research study, a new approach for fingerprint Hashcode generation developed based on MD5 Algorithm, which makes use of Tuning based Contrast Adjustment Algorithm and Surfeit based segmentation algorithm (Modified algorithm). The generated Hash code is rotation and translation variant and can be used as an identity or index key and also can be used along with multifactor Authentication model as one factor out of multiple factors like password or OTP. Figure 9.3 shows outputs of different phases of Surfeit based Segmentation Algorithm.

(a) Original image



(b) Canny edge image

(c) Low Resolution Image

(d) Segmented image with margins

(e) Segmented image by clipping left right top and bottom border

Figure 9.3: Outputs of different phases of Surfeit based Segmentation Algorithm

REFERENCES

[1] Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[2] Krishna Prasad, K. & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE),* 1(2), 86-92. DOI: http://dx.doi.org/

[3] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72.
DOI: http://dx.doi.org/10.5281/zenodo.831678

[4] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19.
DOI: http://dx.doi.org/10.5281/zenodo.835608

[5] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[6] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 51-65.
DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[7] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 98-111.

DOI: http://dx.doi.org/10.5281/zenodo.1067110
[8] Krishna Prasad, K. & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 116-126.
DOI : http://doi.org/10.5281/zenodo.1133545
[9] K. Krishna Prasad & P. S. Aithal (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP, International Journal of Advanced Trends in Engineering and Technology, 3(1), 1-11.
[10] K.Krishna Prasad & P.S. Aithal (2018). A Novel Tuning Based Contrast Adjustment Algorithm for Grayscale Fingerprint Image.
In press.
[11] Zhang, J., Lai, R., & Kuo, C. C. J. (2012). Latent fingerprint detection and segmentation with a directional total variation model. In Proceedings - International Conference on Image Processing, ICIP (pp. 1145–1148).
[12] Zhang, J., Lai, R., & Kuo, C. C. J. (2012). Latent fingerprint segmentation with adaptive total variation model. In Proceedings - 2012 5th IAPR International Conference on Biometrics, ICB 2012 (pp. 189–195).
[13] Choi, H., Boaventura, M., Boaventura, I. A. G., & Jain, A. K. (2012). Automatic segmentation of latent fingerprints. 2012 IEEE Fifth International Conference on Biometrics: Theory, Applications, and Systems (BTAS), 303–310.
[14] Xue, J., & Li, H. (2012, July). Fingerprint image segmentation based on a combined method. In Virtual Environments Human-Computer Interfaces and Measurement Systems (VECIMS), 2012 IEEE International Conference on (pp. 207-208). IEEE.
[15] Short, N. J., Hsiao, M. S., Abbott, A. L., & Fox, E. A. (2011). Latent fingerprint segmentation using ridge template correlation. 4th International Conference on Imaging for Crime Detection and Prevention 2011 (ICDP 2011), P28–P28.

[16] Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.

[17] Wahab, A., Chin, S., & Tan, E. (1998). Novel approach to automated fingerprint recognition. *IEE Proceedings - Vision, Image and Signal Processing*. DOI: https://doi.org/10.1049/ip-vis:19981809.
[18] Pizer, S. M. (2003). The Medical Image Display and Analysis Group at the University of North Carolina: Reminiscences and philosophy. *Medical Imaging, IEEE Transactions on*, 22(1), 2–10. DOI: https://doi.org/10.1109/TMI.2003.809707.
[19] Pei, S. C., Zeng, Y. C., & Chang, C. H. (2004). Virtual restoration of ancient Chinese paintings using color contrast enhancement and Lacuna texture synthesis. *IEEE Transactions on Image Processing*, 13(3), 416–429. DOI: https://doi.org/10.1109/TIP.2003.821347
[20] De La Torre, Á., Peinado, A. M., Segura, J. C., Pérez-Córdoba, J. L., Benítez, M. C., & Rubio, A. J. (2005). Histogram equalization of speech representation for robust speech recognition. *IEEE Transactions on Speech and Audio Processing*, 13(3), 355–366. DOI: https://doi.org/10.1109/TSA.2005.845805.

[21] Gonzalez, R. C., Woods, R. W. (2002). *Digital Image Processing*. *Education*. DOI: https://doi.org/10.1049/ep.1978.0474.

[22] Mehtre, B. M., & Chatterjee, B. (1989). Segmentation of fingerprint images-a composite method. Pattern Recognition, 22(4), 381-385.

[23] Ratha, N. K., Chen, S., & Jain, A. K. (1995). Adaptive flow orientation-based feature extraction in fingerprint images. *Pattern Recognition*, *28*(11), 1657-1672.

[24] Jain, A. K., Ratha, N. K., & Lakshmanan, S. (1997). Object detection using Gabor filters. *Pattern recognition*, *30*(2), 295-309.

[25] Sun, X. and Ai, Z. (1996) Automatic feature extraction and recognition of fingerprint images, Proceeding of ICSP'96, Beijing, Pp.1086-1089.

[26] Moayer, B., & Fu, K. S. (1975). A syntactic approach to fingerprint pattern recognition. Pattern Recognition, 7(1–2), 1–23. https://doi.org/10.1016/0031-3203(75)90011-4.

[27] Naji, A.W., Ramli, A.R., Ali, R., Rahman, S.A., and Ali, M.L. (2002). A segmentation algorithm based on histogram equalizer for fingerprint classification system, Second International Conference on Electrical and Computer Engineering ICECE 2002, Dhaka, Bangladesh, Pp. 390-393.

[28] Alonso-Fernandez, F., Fierrez-Aguilar, J., & Ortega-Garcia, J. (2005, September). An enhanced gabor filter-based segmentation algorithm for fingerprint recognition systems. In *Image and Signal Processing and Analysis, 2005. ISPA 2005. Proceedings of the 4th International Symposium on* (pp. 239-244). IEEE.

Chapter 10

A Novel Tuning Based Contrast Adjustment Algorithm for Grayscale Fingerprint Image

In Filtering contrast, brightness and normalization of the image are performed with an ultimate goal to remove or reduce the noise to a maximum extent. Contrast and Brightness are two major factors, which affect the superiority of an image for easy or stainless or pleasant viewing. Equalization through Histogram (HE) is a very famous approach for image contrast adjustment or enhancement in image processing. In general, the histogram equalization distributes pixel values consistently and produces an outcome in a superior image with the linear increasing histogram. Contrast adjustment is the part of image preprocessing and specifically filtering noise. In this paper, the new algorithm is discussed for a Grayscale Fingerprint image. The algorithm tunes pixel intensity value to a higher intensity value based on a constant value τ. In this paper, we compare the new algorithm with Histogram Equalization and try to find its advantages and disadvantages. This method is effectively used in Fingerprint Identification/verification purpose as an alternative for image filtering. The algorithm is implemented using MATLAB2015a. The rate of growth of the time is in the order of quadratic form ($O(n^2)$).

Keywords: *Contrast Adjustment, Fingerprint recognition, Grayscale Image, Histogram Equalization, Image filtering, MATLAB2015a.*

10.1 INTRODUCTION

Contrast adjustment methods are extensively used for image processing to attain wider dynamic range and which is considered as preprocessing stage, especially in Automatic recognition system based on different types of images like a fingerprint, face, iris etc. When brightness is too high all the pixels of the image turn into lighter, conversely when the brightness is too low all the pixels of the image turn into darker. When the intensity is a too high, lighter area of the image becomes lighter and darker area of the image becomes darker [1].

Automatic Fingerprint Identification System (AFIS) consists of different steps like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [2-9]. The distinctiveness of fingerprint is added forward by using ridge patterns and it has been proved that the information in small regions of friction ridges is in no way repeated.

Distinct contrast enhancement methods have already been developed and advanced which make use of easy linear or non-linear gray level transformation functions in addition to complicated evaluation of special image capabilities. Amongst them, histogram equalization (HE) [10-13] is a very popular technique for contrast adjustment or enhancement of images, especially grayscale images. Contrast adjustment or filtering algorithms are extensively used in medical clinical image enhancement for the diagnostic purpose [14]. Global histogram equalization (GHE) [10] makes use of the entire information of the input image to map into new distinct intensity levels of the image. Although this Global technique is suitable for ordinary or general enhancement, it fails to consider with the local brightness capabilities of the entered image. The gray ranges with very excessive frequencies (wide variety of occurrences) dominate over the opposite gray levels having decrease frequencies in an image. In any such situation, GHE remaps the gray levels in a way that the contrast stretching turns into confined in some dominating gray levels having large image histogram components, and it causes sizable contrast loss for other small ones.

Fingerprint recognition is one of the interesting and complex image processing problems, which requires a constant and continuous contribution to new research from the research community especially in filtering and image enhancement process [4].

Local histogram equalization (LHE) [10] can overcome the problem encountered in GHE. LHE uses a small window that slides on all pixel of the image sequentially and handiest the block of pixels that fall within this window are taken into consideration for HE and then gray level mapping for enhancement is carried out for the center pixel of that window. Therefore, it may make splendid use of local information also. But, LHE requires excessive computational cost and occasionally reasons over enhancement in some part of the image. Another shortfall of this approach is that it also enhances the noises inside the input image. To overcome the problem of high computational cost one more approach is to use the non-overlapping block for HE [10]. But almost all times this method produces checkerboard effect.

In this paper, a new algorithm for contrast adjustment is proposed, which is based on a constant valueτ. The algorithm enhances the pixel intensity range to higher intensity range and which is in between 245to 255, for a 256 × 256 sized grayscale image. The remaining part of the paper is organized as follows. Section 2 describes relative to research on the contrast adjustment algorithm. Section 3 describes the objective of the research. Section 4 describes the τ-tuning based algorithm. Section 5 describes flowchart of the new algorithm. Section 6 makes an analysis of the algorithm using time complexity and also compares with histogram equalization. Section 7 concludes the paper.

10. 2 RELATED RESEARCH

In literature, many types of research are centered on image or video contrast adjustment or enhancement [15-20]. Mean preserving bi-histogram equalization (MPBHE) proposed to get rid of the brightness problem issues [16, 18]. MPBHE separates the entered or captured input image or video histogram into two classifications as mean of the input before equalizing them independently. Some other variants of bi-histogram equalization are a similar area or equal area or place dualistic sub-image or picture histogram equalization (DSIHE) [21], minimum or lower mean brightness or luminance error bi-histogram equalization (MMBEBHE) [20-21]. DSIHE technique uses entropy value for histogram separation. MMBEBHE [20-21] is the extension of BBHE technique that offers maximal brightness maintenance. Even though these strategies can carry out exact contrast adjustments, additionally they generate some side effects depending on the variation of gray level distribution in the histogram [22]. Recursively Separating the mean and finding histogram Equalization (RMSHE) another up gradation of BHE [20] however, it additionally is not free from drawbacks. Moreover, such strategies won't ensure desirable upgrades of all of the partitions. The difference in the ranges of upgrades of various components might also create undesired artifacts in the image. There are many variations MPBHE are Recursive Separated and Weighted HE (RSWHE) [24], Multipeak HE (MPHE) [25], Brightness preserving Weight Clustering HE (BPWCHE) [26], Brightness preserving Dynamic HE (BPDHE) [27] and HE with Range Offset (HERO) [28-29].

In Global Histogram Equalization, Suppose that an image k (x, y) consists of distinct gray levels in the range of [0, R-1]. The transformation function T (dk) is defined as

G_k= T (d_k) = $\sum_{j=0}^{l}$ P (d_j) = $\sum_{j=0}^{l} \frac{m_i}{m}$

Where 0 ≤ Gk ≤ 1 where l=0, 1, 2 ...R-l. In above equation, mi depict the count of pixels having gray level dk, m is the maximum count of pixels in the entered image and P (dj) correspond to Probability Density Function (PDF) of the input dj. The cumulative density function here refereed as T (dk). Gk, is a mapping function, which maps to dynamic range of [0, R-1] values by multiplying it with R-1.

In 256 × 256 sized gray scale images the above equation value of Gk is 0 ≤ Gk ≤ 255 where l can take distinct 256 values from zero to 255 and a maximal number of pixels are 65536 (256 × 256). Gk, is a mapping function, which maps to a dynamic range of [0, 255] values by multiplying it with 255. GHE typically offers a good image enhancement, but sometimes

ends up with some artifacts and unwanted aspect results along with the washed out look. The larger values of mi purpose the respective gray levels to be mapped aside from every different that guarantees precise enhancement.

10.3 OBJECTIVE OF THE STUDY

The objectives of the study are;

- To propose a new τ -tuning based contrast filtering algorithm for grayscale fingerprint image, with an intension to maximize intensity value.
- To compare the new method with GHE with the aid of MATLAB coding.
- To find out time complexity of the new algorithm

10.4 TUNING BASED CONTRAST FILTERING ALGORITHM

The input for this algorithm is row image referred as I, and final output will be I_{filter}. Initially maximum intensity value of the image is found. We consider here 256 × 256 sized grayscale image. If the input fingerprint image is greater than this size then it will be converted into 256 × 256 sized grayscale image. The maximum intensity value in a 256 × 256 sized grayscale image is 255. The range of values is 0 to 255, which means that minimum value is 0 and maximum value is 255. Maximum intensity value of the image is represented as max (I). Each pixel intensity value is compared with max (I). If pixel value is equal to max (I), then that pixel is assigned to ρ_{max}. The ρ_{max} is individual count of maximum intensity value. The total count of ρ_{max} is represented using lower case delta symbol δ_{max} and is calculated as follows.

$$\delta_{max} = \frac{\sum \rho_{max}}{R \times C} \quad \text{---------- (10.1)}$$

In Eq. (10.1) R, and C, are total number of rows and columns respectively. $\sum \rho_{max}$, indicates all pixels, whose intensity value is equal to maximum intensity value of the grayscale fingerprint image (I). Next minimum intensity values of the grayscale image are found and are referred as min (I). If pixel value is equal to min (I), then that pixel is assigned to ρ_{min}. The ρ_{min} is individual count of minimum intensity value of the image. The total count of ρ_{min} is represented using lower case delta symbol δ_{min} and is calculated as follows.

$$\delta_{min} = \frac{\sum \rho_{min}}{R \times C} \quad \text{---------- (10. 2)}$$

As like Eq. (10.2), R, and C, is total number of rows and columns respectively. $\sum \rho_{min}$, indicates all pixels, whose intensity value is equal to intensity value of the grayscale fingerprint image (I).

Each row of the intensity matrix of the image is considered as a window and is represented as δ_w, which is expressed as

$$\delta_w = \delta_{max}\left(\frac{\delta(l)-\delta_{min}}{\delta_{max}-\delta_{min}}\right)^{\epsilon} \quad \text{---------- (10.3)}$$

Where ϵ value is 0.5, which is a constant. $\delta(l)$ is low or minimum value of each row. The difference value of $\delta(l) - \delta_{min}$ is divided by $\delta_{max} - \delta_{min}$. The quotient is multiplied by δ_{max}.

∂_w which is almost equal to Histogram equalization, cumulative density function, of window l is represented using 'tho' or partial derivative symbol and is defined as

$\partial_w = \sum_{l=0}^{l_{max}} \frac{\delta_w(l)}{\sum \delta_w}$ ---------- (10.4)

Where $\sum \delta_w$ represents summation value of all window l or summation of δ_w. $\sum \delta_w$ is calculated as follows

$\sum \delta_w = \sum_{l=0}^{l_{max}} \delta_w(l)$ (10. 5)

The final output of this proposed algorithm (I_{filter}) is obtained using following equation

$$I_{filter} = (l_{max} \times (\frac{I(i,j)}{l_{max}}))^{\tau} \quad (10.6)$$

In Eq. (10.6), (τ) is an important value, which filters or maps input pixel intensity value to new intensity value in the output image and is defined as

$$\tau = round(1 - \max((\partial_w(:))) \quad (10.7)$$

The Eq. (10.7) is rounded to 6 decimal points to get higher precision or accuracy.

The output of the robust tuning based algorithm (proposed method), I_{filter} is converted from grayscale 256 × 256 uint8 to double type for the purpose of grayscale image adjustment. The 256 × 256 double image consists of only two intensity values as 0 and 1. 0 represents dark and 1 represents bright or 0 dark black and 1 bright white. Here in image enhancement we focus more on τ- Tuning Based Filtering Algorithm.

Proposed filtering algorithm

Input: Raw Image; I

Output: Filtered Output Image,I_{filter}

Step-1: for i=1 to R \\ R→ Row size of input image

Step-2: for j=1 to C \\ C→ Column size of input image

Step-3: if I(i,j)= =max(I)

Step-4:$\rho_{max} = I(i,j)$; end if;end for

Step-5: $\delta_{max} = \frac{\sum \rho_{max}}{R \times C}$

Step-6: for i=1 to R \\ R→ Row size of input image

Step-7: for j=1 to C \\ C→ Column size of input image

Step-8: if I(i,j) = = min(I)

Step-9:$\rho_{min} = I(i,j)$; end if; end for

Step-10: $\delta_{min} = \frac{\sum \rho_{min}}{R \times C}$

Step-11: $\delta_w = \delta_{max}(\frac{\delta(l) - \delta_{min}}{\delta_{max} - \delta_{min}})^{\epsilon}$ \\ ϵ→Constant; $\epsilon = 0.2$

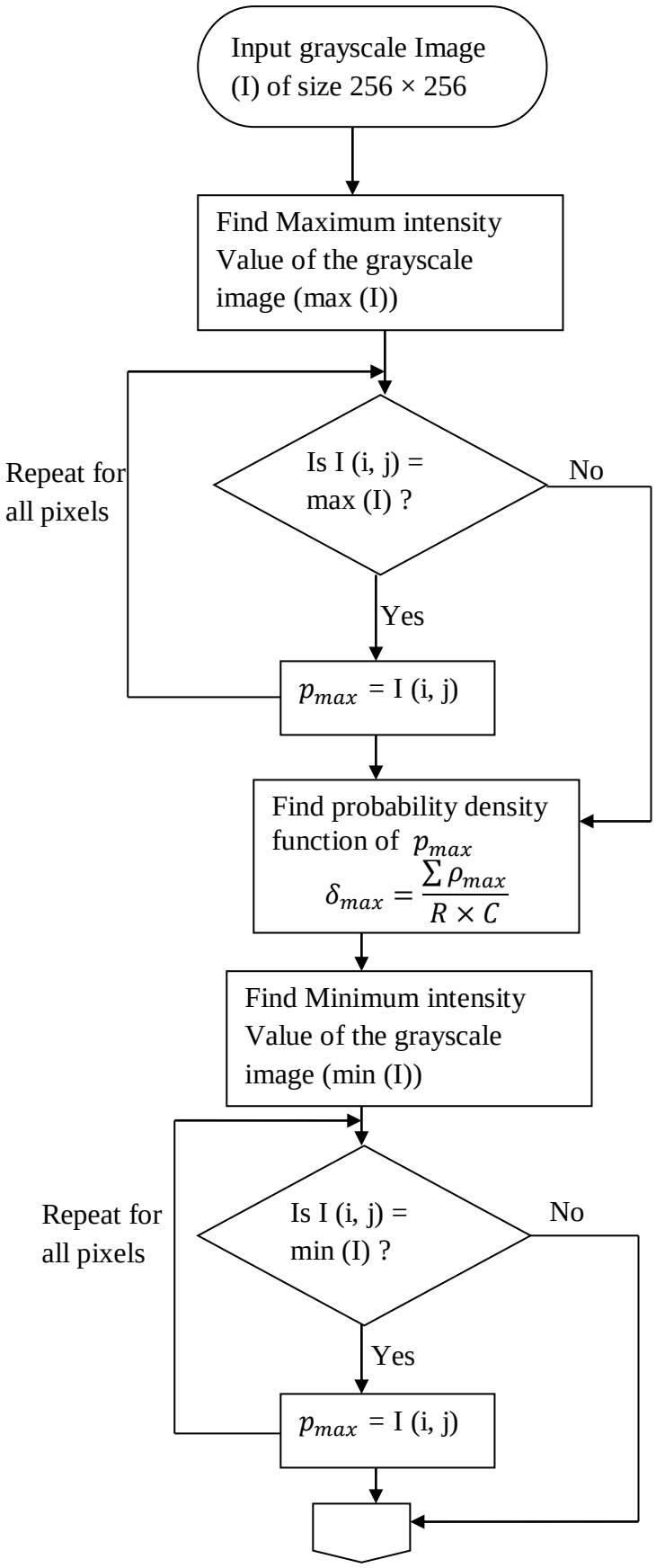
Step-12: $\partial_w = \sum_{l=0}^{l_{max}} \frac{\delta_w(l)}{\sum \delta_w}$

Step-13: $\sum \delta_w = \sum_{l=0}^{l_{max}} \delta_w(l)$

Step-14: $\tau = round(1 - \max((\partial_w(:)))$ //round to 6 decimal points

Step-15: $I_{filter} = (l_{max} \times (\frac{I(i,j)}{l_{max}}))^{\tau}$

10.5 FLOWCHART FOR PROPOSED ALGORITHM



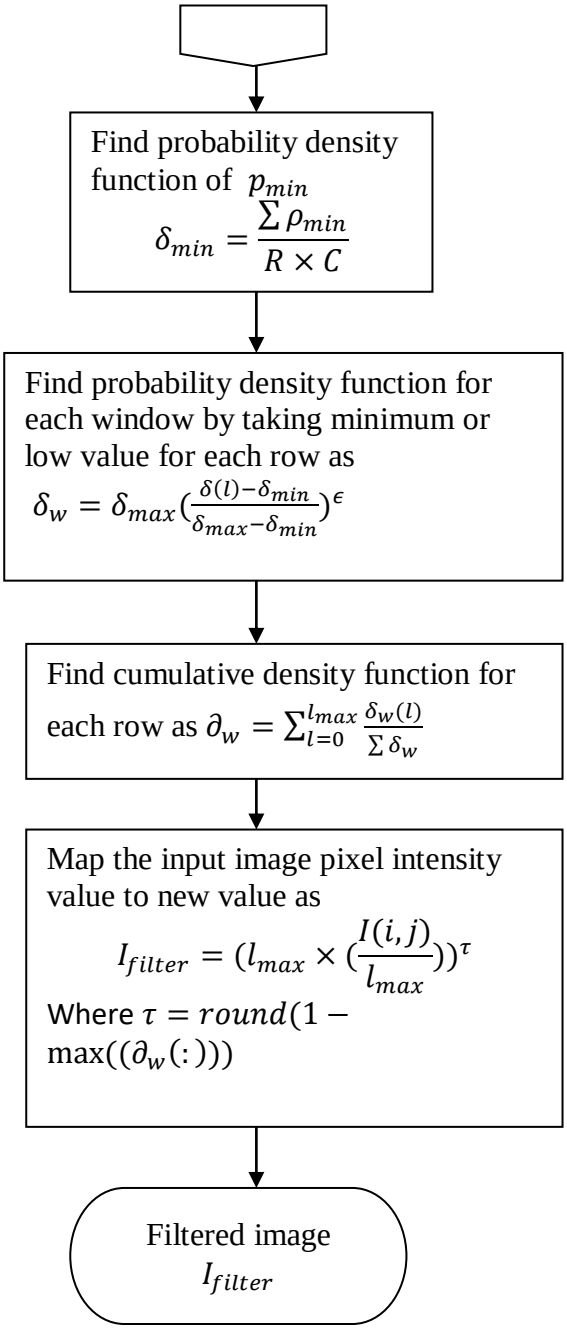


Figure 10.1: Flowchart of proposed filtering algorithm

The above algorithm is explained using flowchart as shown in Figure 10.1. The input for this algorithm is row grayscale fingerprint image of size 256 × 256 which is represented as I. The final output is filtered image is I_{filter}. The different workflows of the proposed algorithm are listed out below.

- Find maximum intensity value of the grayscale input image
- Find maximum intensity value pixels total count in the grayscale image
- Find probability density function of maximum intensity value
- Find minimum intensity value of the grayscale input image

- Find minimum intensity value pixels total count in the grayscale image
- Find probability density function of minimum intensity value
- Locate minimum value for each row
- Locate probability density function for each row
- Find cumulative density function for each row
- Find the value of τ
- Map the intensity value of the input pixels to new intensity value in the output image.
- Generate filtered image

10.6 ANALYSIS AND RESULTS

In order to analyze the algorithm Benchmark fingerprint dataset is considered from FVC ongoing 2002 DB1_B (Maltoni et al., 2009) [30]. The table 1 shows the range of grayscale intensity values for the few of FVC 2002 DB1_B datasets before using the proposed filtering algorithm and after applying filtering algorithm. The table also shows range of grayscale intensity values using Histogram equalization. In this benchmark dataset each user's different eight fingerprints are considered for training or testing purposes.

From the Table 10.1 it is clear that proposed method having less intensity range compared to Histogram equalization. In Robust τ- Tuning Based Filtering Algorithm, dark pixels are highest dark and bright pixels are either highest or near to high bright values. This algorithm is best suited for grayscale fingerprint image, especially 256 × 256 sized. Figure10.2 shows output of filtered image (I_{filter}). Table 2 shows the number of occurrence of each grayscale intensity value for the proposed algorithm, for the same image considered in Table 10.1. As like histogram equalization one of the pixel intensity values dominates over other. So this algorithm is not best for natural image because it may cause wash out appearance. But this is very good and robust for grayscale fingerprint image. In fingerprint image usually black colour represents ridges and white color represents valley.

Table 10.1: Range of intensity values in 256 × 256 sized grayscale fingerprint image

Fingerprint Image Name	**Range of Intensity values before applying proposed filtering algorithm**	**Range of Intensity values after applying proposed filtering algorithm**	**Range of Intensity values using Histogram Equalization**
101_1.tif	0 to 255 (256 values)	0, 250, 252 (3 values)	0, 4, 8, 12, 16, 20, 24, 28,32, 36, 40, 45,49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 162, 255 (24 values)

102_1.tif	0 to 255 (256 values)	0, 249, 250, 251, 252 (5 values)	0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 39, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 162, 255 (24 values)
103_5.tif	0 to 255 (256 values)	0, 249, 250, 251, 252 (5 values)	0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101,105,109, 113, 117, 121, 125, 130, 134, 138, 194, 255 (37 values)
104_4.tif	0 to 255 (256 values)	0, 249, 250, 251, 252, 253 (6 values)	0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 49, 53, 57, 61, 65, 69, 73, 77, 81, 85, 89, 93, 97, 101, 105, 109, 178, 255 (30 values)
105_8.tif	0 to 255 (256 values)	0, 246, 247, 248, 249, 250, 251, 252, 253 (9 values)	0, 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 45, 49, 53, 57, 61, 65, 69, 73, 150, 255 (21 values)

Table 10.2: Intensity and frequency count of the fingerprint image for the proposed filtering algorithm

Fingerprint Image Name	**Intensity value and frequency count of the fingerprint image for the proposed algorithm**	
101_1.tif	0	8084
	250	57196
	252	256
102_1.tif	0	5300
	249	43808
	250	14954
	251	1222
	252	252
103_5.tif	0	25855
	249	23914
	250	14237
	251	1020
	252	510
104_4.tif	0	14152
	249	34515

	250	15333
	251	1024
	252	256
	253	256
105_8.tif	0	3053
	246	245
	247	252
	248	756
	249	41592
	250	15006
	251	3165
	252	1228
	253	239

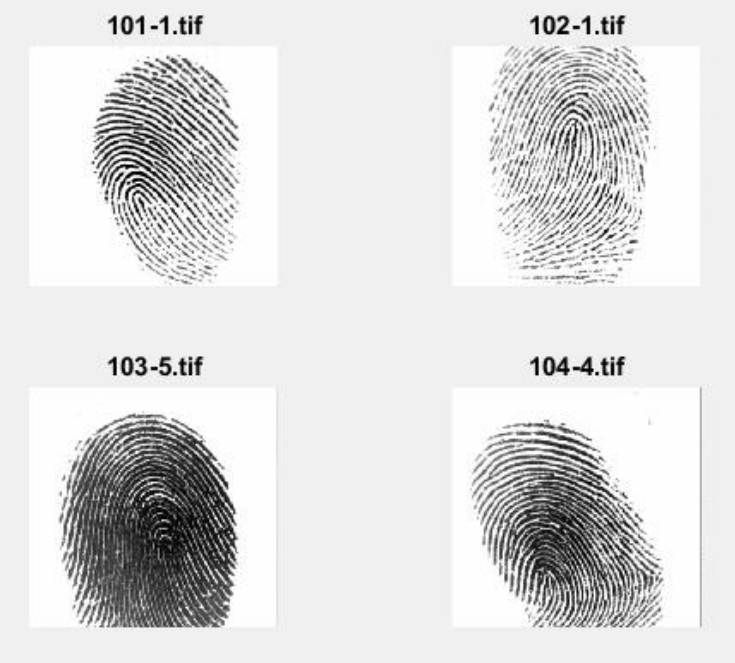


Figure 10.2: Sample original fingerprint images of FVC ongoing 2002 DB1_B dataset

In Table 10.2, we can note that the dominating intensity values usually fall in the upper boundary region of intensity range, which makes the image brighter. Figure 10.2 shows some sample images of FVC ongoing 2002 DB1_B benchmark datasets with labels as 101_1.tif, 102_1.tif, 103_5.tif, and 104_4.tif.

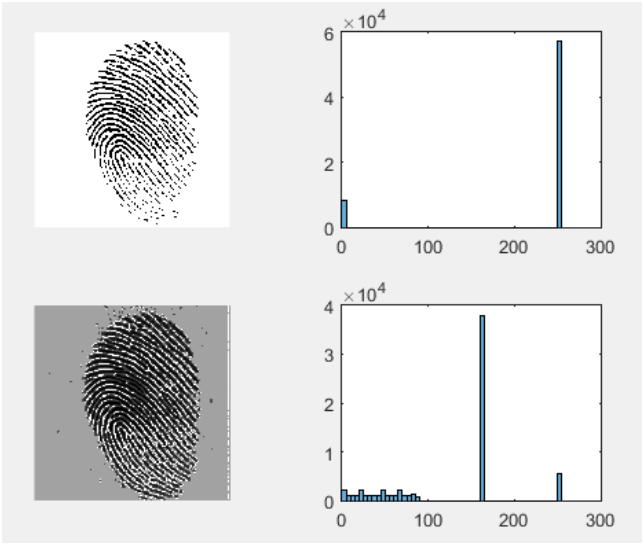


Figure 10.3: '101_1.tif'-Sample fingerprint image of FVC ongoing 2002 DB1_B after filtering process. (Top left: Filtered image using proposed method, Top Right: Histogram of top left, Bottom right: Filtered image using Histogram Equalization, Bottom right: Histogram of bottom left)

Time complexity Analysis of the Algorithm

In this research study, the new algorithm is analyzed for time complexity using hypothetical Model Machine. Some characteristics of the Hypothetical machine are given below.

- Single processor machine
- 32-bit architecture
- Sequential Execution
- Arithmetic and logical operation takes 1 unit of time
- Assignment statement takes 1 unit of time
- Function return takes 1 unit of time

In order to calculate the time complexity of the algorithm, the entire algorithm is divided into different fragments, time complexity for them is calculated first and later all this fragments time complexity is added in order to get overall time complexity of the algorithm. The different fragments time complexity is shown in Table 10.3.

Table 10.3: Time complexity of different fragments of Tuning based contrast adjustment algorithm

Sr. No	**The fragments of new algorithm**	**Time complexity**
1	Finding the Maximum and minimum intensity of the input image and probability density value of min and max intensity	$6n^2+10$
2	Finding the lowest intensity value (local minimum) in each row and then finding a total number of local minimum and	$3n^2+ 11n + 1$

	probability density value of local or row minimum.	
3	Finding cumulative density function of local minimum	3n+3
4	Map the input image pixel intensity value to higher intensity range.	$13n^2+ n + 1$
5	Overall	$22n^2+ 15n+15$

$f(n) = 22n^2+ 15n+15$
$g(n) = n^2$
$f(n) = O(g(n))$
$f(n) \leq cg(n)$, $c > 0, n_0 \geq 1$
$22n^2+ 15n+15= cn^2$ where $c=23, n \geq 16$
So the rate of growth of the time for new algorithm is $O(n^2)$. [Big (Oh) of n^2].
The Rate of growth of time for Histogram equalization is also $O(n^2)$.

10.7 CONCLUSION

The Contrast adjustment filtering is essential in fingerprint image preprocessing stage. Contrast and Brightness are two major factors, which improves the persistence of vision. The novel tuning based contrast adjustment algorithm enhances the intensity range to very higher value compared to histogram equalization. The new algorithm and histogram equalization algorithm utilizes same time complexity of O (n2) for very large input. The new algorithm also decreases the washout appearance of the image. We have represented time complexity using the hypothetical model machine. In this paper, we have proposed theory of the new algorithm and also tested using FVC ongoing 2002 dataset with aid of MATLAB2015a

REFERENCES

[1] Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653
[2] Krishna Prasad, K. & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE),* 1(2), 86-92. DOI: http://dx.doi.org/
[3] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72.
DOI: http://dx.doi.org/10.5281/zenodo.831678
[4] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19.
DOI: http://dx.doi.org/10.5281/zenodo.835608
[5] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[6] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 51-65.
DOI: http://dx.doi.org/10.5281/zenodo.1037627.
[7] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 98-111.
DOI: http://dx.doi.org/10.5281/zenodo.1067110
[8] Krishna Prasad, K. & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), 116-126.
DOI : http://doi.org/10.5281/zenodo.1133545
[9] K. Krishna Prasad & P. S. Aithal (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP, International Journal of Advanced Trends in Engineering and Technology, 3(1), 1-11.
[10] Gonzalez, R. C., Woods, R. W. (2002). *Digital Image Processing*. *Education*. DOI: https://doi.org/10.1049/ep.1978.0474.
[11] Jain, A. K. (1989). *Fundamentals of Digital Image Processing*. *Portalacmorg* (Vol. 14). DOI: https://doi.org/10.1002/9780470689776.
[12] Zimmerman, J. B., Pizer, S. M., Staab, E. V., Perry, J. R., Mccartney, W., & Brenton, B. C. (1988). An Evaluation of the Effectiveness of Adaptive Histogram Equalization for Contrast Enhancement. *IEEE Transactions on Medical Imaging*, 7(4), 304–312. DOI: https://doi.org/10.1109/42.14513.
[13] Kim, Y. T. (1997). Contrast enhancement using brightness preserving bi-histogram equalization. *IEEE Transactions on Consumer Electronics*, 43(1), 1–8.
DOI: https://doi.org/10.1109/30.580378
[14] Daniel, E., & Anitha, J. (2016). Optimum wavelet based masking for the contrast enhancement of medical images using enhanced cuckoo search algorithm. *Computers in biology and medicine*, *71*, 149-155.
[15] Lau, S. S. Y. (1994). Global image enhancement using local information. *Electronics Letters*, 30(2), 122–123. DOI: https://doi.org/10.1049/el:19940081.
[16] Kim, Y.-T. (1997). Quantized bi-histogram equalization. *Acoustics, Speech, and Signal Processing, 1997. ICASSP-97., 1997 IEEE International Conference on*, 4, 2797–2800 vol.4. DOI: https://doi.org/10.1109/ICASSP.1997.595370.
[17] Zhang, Y. J. (1992). Improving the accuracy of direct histogram specification. *Electronics Letters*, 28(3), 213-214.
[18] Xu, J., Zhang, Z., Xiao, X., Yang, Y., Yu, G., & Winslett, M. (2013). Differentially private histogram publication. *VLDB Journal*, 22(6), 797–822. DOI: https://doi.org/10.1007/s00778-013-0309-y.
[19] Yao, Z., Lai, Z., & Wang, C. (2017). Image Enhancement Based on Equal Area Dualistic Sub-image and Non-parametric Modified Histogram Equalization Method. In *Proceedings - 2016 9th International Symposium on Computational Intelligence and Design, ISCID 2016* (Vol. 1, pp. 447–450).
https://doi.org/10.1109/ISCID.2016.1110.
[20] Chen, S. Der, & Ramli, A. R. (2003). Contrast enhancement using recursive mean-separate histogram equalization for scalable brightness preservation. *IEEE Transactions on Consumer Electronics*, 49(4), 1301–1309.
DOI: https://doi.org/10.1109/TCE.2003.1261233.

[21] Chen, S. Der, & Ramli, A. R. (2003). Minimum mean brightness error bi-histogram equalization in contrast enhancement. *IEEE Transactions on Consumer Electronics*, 49(4), 1310–1319.DOI: https://doi.org/10.1109/TCE.2003.1261234.
[22] Chi-Chia, S., Shanq-Jang, R., Mon-Chau, S., & Tun-Wen, P. (2005). Dynamic contrast enhancement based on histogram specification. *Consumer Electronics, IEEE Transactions on*, 51(4), 1300–1305. DOI: https://doi.org/10.1109/TCE.2005.1561859.
[23] Abdullah-Al-Wadud, M., Kabir, M., Akber Dewan, M., & Chae, O. (2007). A Dynamic Histogram Equalization for Image Contrast Enhancement. *IEEE Transactions on Consumer Electronics*, 53(2), 593–600. DOI: https://doi.org/10.1109/TCE.2007.381734.
[24] Jagatheeswari, P., Kumar, S. S., & Rajaram, M. (2009). Contrast stretching recursively separated histogram equalization for brightness preservation and contrast enhancement. In *ACT 2009 - International Conference on Advances in Computing, Control and Telecommunication Technologies* (pp. 111–115). DOI: https://doi.org/10.1109/ACT.2009.37.
[25] Wongsritong, K., Kittayaruasiriwat, K., Cheevasuvit, F., Dejhan, K., & Somboonkaew, A. (1998, November). Contrast enhancement using multipeak histogram equalization with brightness preserving. In *Circuits and Systems, 1998. IEEE APCCAS 1998. The 1998 IEEE Asia-Pacific Conference on* (pp. 455-458). IEEE.
[26] Sengee, N., & Choi, H. K. (2008). Brightness preserving weight clustering histogram equalization. *IEEE Transactions on Consumer Electronics*, 54(3), 1329–1337.
DOI: https://doi.org/10.1109/TCE.2008.4637624.
[27] Ibrahim, H., & Kong, N. S. P. (2007). Brightness preserving dynamic histogram equalization for image contrast enhancement. *IEEE Transactions on Consumer Electronics*, 53(4), 1752–1758. DOI: https://doi.org/10.1109/TCE.2007.4429280.
[28] Ibrahim, Haidi. "Histogram equalization with range offset for brightness preserved image enhancement." *International Journal of Image Processing (IJIP)* 5, no. 5 (2011): 599-609.
[29] Abdullah-Al-Wadud, M. (2012). A modified histogram equalization for contrast enhancement preserving the small parts in images. *International Journal of Computer Science and Network Security (IJCSNS)*, 12(2), 1.
[30] Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.

Chapter 11
A Study on Multifactor Authentication Model using Fingerprint Hash Code, Password and OTP

By definition, Authentication is using one or multiple mechanisms to show that you are who you claim to be. As soon as the identity of the human or machine is demonstrated, then human or machine is authorized to grant some services. The modern research study reveals that fingerprint is not so secured like secured a password which consists of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at the door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. Using some modern technology with copper and graphite spray it's easy to mimic fingerprint image. Fingerprints are a half-secret if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan. Fingerprints are left at car, door or anyplace where every person goes and places his finger. Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. In this paper, a novel method for Authentication is proposed by making use of Fingerprint Hash Code, Password, and OTP. In this study, we make use of Euclidean Distance to generate fingerprint Hash Code. Fingerprint Hash code is generated using MD5 Hash Function. The Model is implemented using MATLAB2015a. This paper also analyzes novel Authentication model used in this study with the aid of ABCD analysis.

Keywords: *Authentication, Fingerprint Hash Code, MD5 Hash Function, OTP, Euclidean Distance, Multifactor Authentication Model*.

11.1 INTRODUCTION

Authentication is a process of identifying the registered or already known user to provide some services and to protect user information from an intruder. Three worldwide referred authentication process are Token supported authentication, Biometric supported authentication, and Knowledge supported authentication [1-2]. Token supported authentication makes use of key cards, bank cards, and smart cards. Token supported authentication system sometimes uses knowledge supported techniques to improve security. Biometric supported authentication strategies, together with fingerprints, iris scan and facial reputation aren't yet extensively adopted. The essential flaws of this technique are that such systems can be costly, and the identification process may be slow and regularly unreliable. However, this form of technique presents the highest level of protection. Knowledge supported authentication is most commonly and widely used authentication technique and encompass both text-based and image-based passwords. The image-based techniques can be further subdivided into two classes: recognition-primarily based and recall based graphical techniques. The use of recognition based strategies, a person is provided with a set of images and the user is authenticated through recognizing and identifying the images, which is registered at the time of registration process. In recall based techniques it's essential that user has to reproduce something like a pattern, which is created or drawn at the time of registration process.

Automatic Fingerprint Identification System (AFIS) consists of different techniques like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [3-10]. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or readers. There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause difference in Hash code [11]. Based on the different Methods of Fingerprint Hash code generation, it reveals that fingerprint hash code does not suit exclusively for authentication or security purpose. But it uniquely identifies an individual person or human being through a Hash code key.

In this study, we calculate Euclidean distance for a binary fingerprint image, which is a straight line distance from a pixel with value zero to the pixel with value non-zero, which is one in a binary image using Euclidean norm [10]. The Euclidean distance is calculated for all the pixels of the binary fingerprint image. The two points, k and l in two-dimensional Euclidean spaces and k with the coordinates (k1, k2), l with the coordinates (l1, l2). The line segment with the endpoints of k and l will form the hypotenuse of a right-angled triangle. The space among factors k and l is defined as the square root of the sum of the squares of the differences among the corresponding coordinates of the points. In a two-dimensional Euclidean geometry Euclidean distance between two points k = (kx, ky) and l = (lx, ly) is given as follows [10].

$$d(k, l) = \sqrt{(lx - kx)^2 + (ly - ky)^2}$$

For example consider a 3×3 sized matrix with values as follows [10].

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

The Euclidean distance for each point is calculated as follows [10].

$$\begin{bmatrix} 1.4142 & 1.0000 & 1.4142 \\ 1.0000 & 0 & 1.0000 \\ 1.4142 & 1.0000 & 1.4142 \end{bmatrix}$$

The most natural or common matrix for finding distance matrix in the binary image is Euclidean distance [12-14]. Due to the lack of efficient algorithms in the field of Euclidean distance led to the development of many types of research in this field in order to define, elaborate and also to use some other methods to find the distance using other methods like the city block, chessboard or chamfer [14-16]. The Euclidean distance transform is global operation and the calculation of Euclidean distance is most common and simple operation and amount of calculation required is always directly proportional to the size of the entire image because this is calculated for every pixel.

This paper has nine sections. Section 1 describes introductory theory related to fingerprint, Hash code and Euclidean distance matrices. Section 2 explains about brief literature review of Multifactor Authentication Model developed by many researchers. This also covers brief theoretical aspects Biometrics, Password, One Time Password (OTP) and Token. Section 3 narrates Objective and methodologies of fingerprint Hash code generation using Euclidean distance. Section 4 describes algorithm of Fingerprint Hash code generation using Euclidean distance. This section also lists workflow of Fingerprint Hash code generation and MD5 Hash function procedure. Section 5 explains the Multifactor Authentication Model using Fingerprint Hash code along with dataflow diagram. Section 6 depicts how One Time Password can be generated. This section explains the OTP generation concept using algorithm. Section 7 explains Results and Discussions of Multifactor Authentication Model. Section 8 makes analysis of Multifactor Authentication Model used in this study using ABCD analysis. Section 9 concludes the paper.

11.2. RELATED STUDY

Usually, in the literature, there is three universally recognized or accepted method of authentication, which is already known (for example password) or what is known, what you possess (For example token or ATM card), what you are throughout a lifetime or lifelong (For example Biometrics). Brainard et al., (2006) [17] proposed, one of the modern types of authentication is through somebody user knows, which is mainly based on the concept of confirmation. If more than one factor are used for authentication, which gives more security and is referred as Two-factor authentication. Two-factor authentication can be by combining any of the two factors which is mentioned above like password and One Time Password (OTP) or Password and Biometrics. Usually ATM makes use of two factor authentication model as ATM and Personal Identification Number (PIN).

Passwords alone are recognized to be one of the simplest goals of hackers. Therefore, most companies are looking for greater rigid strategies to defend or secure their clients and users.

Biometrics are regarded to be very secure and are used in special organizations, however, they are not frequently used in online transactions or ATM, due to high cost required for hardware. As an alternative, banks and corporations are making use of tokens as a mean of two-factor authentication.
A security token is used for the purpose of authentication and to provide some services to the user and is usually physical device and sometimes also referred as the cryptographic token. Token usually comes in two forms which are software token and hardware token. Hardware tokens are small gadgets which are small and may be easily portable. Some of those tokens having hash or cryptographic keys or biometric data, at the same time as others display a PIN that changes with time. At any precise time a consumer or user desires to log-in, i.e. authenticate, he makes use of the PIN displayed at the token further to his regular account password. Software program tokens are programs that run on computers and offer a PIN that also changes with time. Such programs put in force a One Time Password (OTP).
OTP algorithms are very important in employing security of the underlying system because unauthorized user or intruder cannot able to guess or find the next password in the sequence. The collection must be random to the most feasible extent, unpredictable, and irreversible. Elements that can be utilized in OTP generation consist of names, time, seed, random numbers etc.

Bemmel, V., & Mian, S. (2009) US patent states that a biometric identification method is used at a point of sale counter with a system and a method is provided for authorizing payment through customer mobile phone [18]. Aloul, F. et al., (2009) [19] explains that two-factor authorization gives more security for mobile-based financial transactions other than usual username and password, by utilization biometric identification mechanism. They develop One Time Password (OTP) which is valid for the only short duration of time which is generated based on IMEI number, IMSI number, username, hour, pin, minute etc and can be effectively used for online banking, ATM or mobile banking services. Jakobsson, M. et al., (2009) [20], introduced a new concept implicit authentication which is based on some actions carried out by the mobile user. They developed a model to implement implicit authentication and their preliminary investigation found that the approach is meaningful for usability or security purposes.

Angulo, J., & Wästlund, E. (2011) studied a lock pattern dynamics as a secure and user-friendly two-factor authentication method for giving security to user mobile phone's private and secret information. They modeled this on the Android mobile phone based on user lock pattern and used Random Forest machine learning classifier and achieved an average Equal Error Rate (EER) of approximately 10.39% [21]. Delac, K., & Grgic, M. (2004, June) [22] surveyed different biometric recognition methods and found that unimodal biometrics more vulnerable to attacks compare to multimodal biometrics. Biometric recognition system provides a consistent personal identification schema either to confirm or decide the distinctiveness of a person, which can be effectively used on any computer or mobile systems. Seo, H. et al., (2012) [23] proposes a very special method of biometrics for intelligent mobile devices for which existing physical and behavioral biometrics are

unsuitable, by analyzing users input patterns. They found using an empirical method that the new method identifies the user with 100% efficiency.

De Marsico, et al., (2014) [24] suggested a new method of biometrics for mobile engagement, using face and iris recognition, multimodal biometrics referred as "FIRME" which is specially designed and embedded in mobile devices using the Android operating system. Both design and implementation of face and iris are considered as a separate module, whose flow of work separate and finally two modules are fused. They claim that this multimodal authentication can be effectively used to find the identity of the user. Kumar, D., & Ryu, Y. (2009) [25] surveyed biometric payment system used for various kinds of payment systems, in contrast to username and password no need of remembering anything. They also suggest in their study that when more and more customer uses the biometric system, cost of biometric reader will decrease and even small business firms also can use biometric systems.

Yoo, J. H. et al., (2007, December) [26] describes the design of an embedded biometric system that authenticates the person by using face-fingerprint or iris-fingerprint multimodal biometrics technology which is a new system compared to an existing embedded system that time. The existing embedded system had problems like low computational resource and memory space. They implemented the system and also found execution time and also found the equal error rate for face, iris, and fingerprint as 1.50%, 1.68%, and 4.53% respectively. Xi, K., & Hu, J. (2009, June) [27] proposed a new fingerprint fuzzy vault based on multiple or composite features which are effective, reliable, distortion tolerant and registration free. They modeled and tested their results on the public database and found that the new schema can improve verification performance considerably.

11.3 OBJECTIVE OF THE STUDY

Literature review reveals that there are already many studies are made on Multifactor Authentication Model. But this study focuses on Multifactor authentication model by making use of Fingerprint Hash code, Password, and OTP. Fingerprint alone not gives full security, in order to improve the security of the system fingerprint acts one factor along with OTP, password, or any other biometric psychological or behavioral traits. The main objectives of this study are given below.

- To propose an alternative approach for User Authentication using Multifactor, which includes, Fingerprint Hash code, Password and time synchronized One Time Password (OTP).
- To analyze the new model using ABCD analysis

Figure 11.1 explains the methodology used in this research work to generate Fingerprint Hash code. Here initially FVC ongoing 2002 benchmark dataset is considered for testing the hash code. The benchmark dataset image is binarised and Euclidean distance of the image is calculated for each pixel. The distinct values of the Euclidean distance matrices values are considered and 32-bit length hash code is generated. Distinct Euclidean distance value

summation, mean value and standard deviation values are considered for generating Hash code.

11.4 ALGORITHM OF HASHCODE GENERATION USING EUCLIDEAN DISTANCE

This section explains step by step procedure to develop Hashcode by making use of Euclidean distance matrix on a binary fingerprint image. The steps of the algorithm are explained below. The algorithm also shows the pseudo code [10].

Step 1: Input Grayscale fingerprint image
read (input_image)
Step 2: Convert input image into 256 × 256 sized two-dimensional image
resized_image = image_resize (input_image, [256, 256])
Step 3: Convert 256 × 256 sized grayscale image into binary image
binary_image = convert_to_binary(resized_image)
Step 4: Perform One's complement of the binary_image
Binary_image = One's complement(binary_image)
Step 5: Find the Euclidean distance of the image
euclidean_image = Euclidean_distance(binary_image)
Step 6: Find the distinct value of the Euclidean distance
distinct_eucllidean_value = distinct_value(euclidean_image)
Step 7: Find the distinct value summation
For i=1 to size(distinct_eucllidean_value)
euclidean_sum = distinct_eucllidean_value (i)
end for
Step 8: Find the mean of the distinct Euclidean value
euclidean_mean = mean(distinct_eucllidean_value)
Step 9: Find the standard deviation of the distinct Euclidean value
std_deviation = standard_deviation(distinct_eucllidean_value)
Step 10: Combine the value of Step-7, Step-8, and Step-9
combine_value = combine(euclidean_sum, euclidean_mean, std_deviation)
Step 11: Pass the value of Step-10 as parameter for MD5 Hash function
hash_value = MD5_DataHash(combine_value)

The different process or work flow are listed below. With an intension to make the MD5 Hashcode more robust and to get the advantage of salting Euclidean distance sum, mean, and standard deviation are combined and passed to the MD5 algorithm [10].

- Converting input image to 256 × 256 sized grayscale image
- Converting to binary image
- Finding ones complement of binary image
- Finding Euclidean distance
- Finding distinct value of the Euclidean distance
- Finding the sum of the distinct Euclidean distance
- Finding the mean of the distinct Euclidean distance

- Finding the standard deviation of the distinct Euclidean distance

Generating MD5 Hashcode using combined sum, mean, and standard deviation of distinct Euclidean distance value

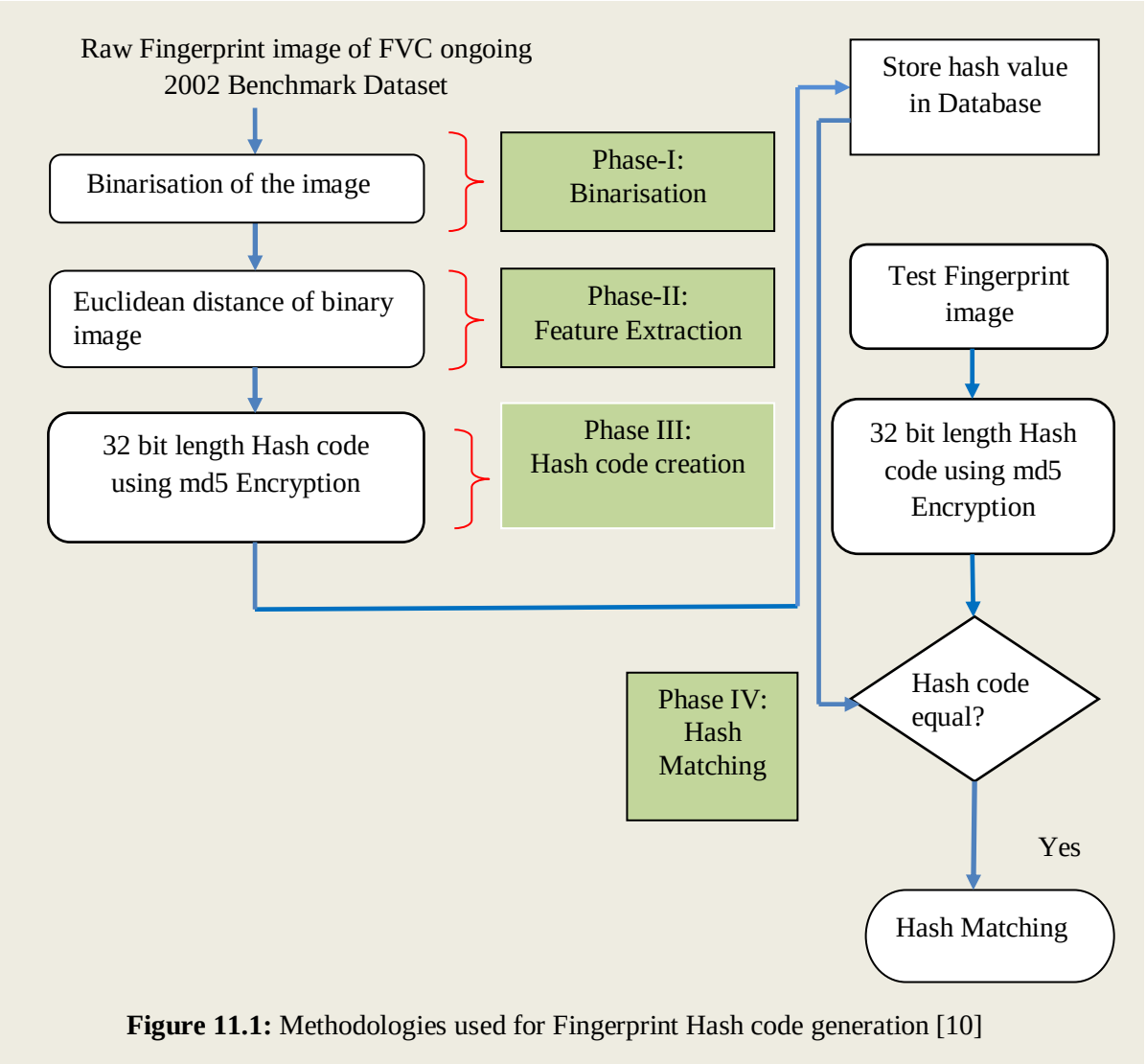


Figure 11.1: Methodologies used for Fingerprint Hash code generation [10]

The process of the MD5 algorithm is disused below.
Input: Extracted Features
Output: Hash Code
Step-1: Attach the padded bits
Step-2: Append the length of the initial input to the result of the previous step-1
Step-3: Initialize MD buffer as A, B, C, D.
A four-word buffer (A, B, C, D) was used to evaluate the message digest. Here each of A, B, C, D is a 32- bit register
Step-4: Process message in 16-word blocks
Step-5: Finally, we get the 32-bit Hashcode as output

11.5 MULTIFACTOR AUTHENTICATION MODEL USING FINGERPRINT HASH CODE, OTP, AND PASSWORD

Figure 11.2 shows Dataflow Diagram of Multifactor Authentication model used in this study. Initially on the client side using an interface user loads fingerprint image into the system. First, using Euclidean distance fingerprint image features are extracted, which is explained in Section 3 and 4. These features are encrypted and sent to the server. As soon as these features arrive at a server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered mobile phone user. Client system prompts a message to enter OTP, which is received to the registered mobile phone of the user. The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side. If OTP is verified, server requests for the password, the user enters the password through a client-side interface and entered password reaches to the server. The server verifies the user entered a password with the already stored password in its database. Since database password is stored in encrypted format. The password which is stored in the database in encrypted form and finger user-id hash code is encrypted one again to enhance security.

So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match them user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Password, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered an unauthorized user. If OTP not matches then the user is blocked from further steps in the authentication process. In this research study, this is not implemented as server and client in different machines. The model of this approach is implemented on the same machine using MATLAB 2015a.

11.6 ONE TIME PASSWORD GENERATOR

In this research work, One Time Password Generator is responsible for generating OTP. This is a function located on the server. In this study, Time synchronized OTP is generated by combining some features. The time for which OTP is valid is administrative specific, for simplicity we consider in this work as 2 minutes. The algorithm for generating OTP is explained below.

Algorithm:

Step-1: Generate the Hash code for input fingerprint using MD5 Hash Function.
Step-2: Extract system Date and Time.
Step-3: Extract seconds separately.
Step-4: Consider only integer part of the seconds.
Step-5: A 4 × 4 sized matrices of the random number is generated.
Step-6: Date and Time are converted into string data type.
Step-7: Random matrix is concatenated with Date and Time string.
Step-8: Hash code of the input fingerprint image is concatenated with result of Step-7.
Step-9: Hash code is generated for combined string obtained from Step-8.

Step-10: A random number is generated between1 to 32.
Step-11: If the random number is in between 1 to 8 (including both) then extracts first 8 characters of the Hash code of size 32 characters generated in Step-8.

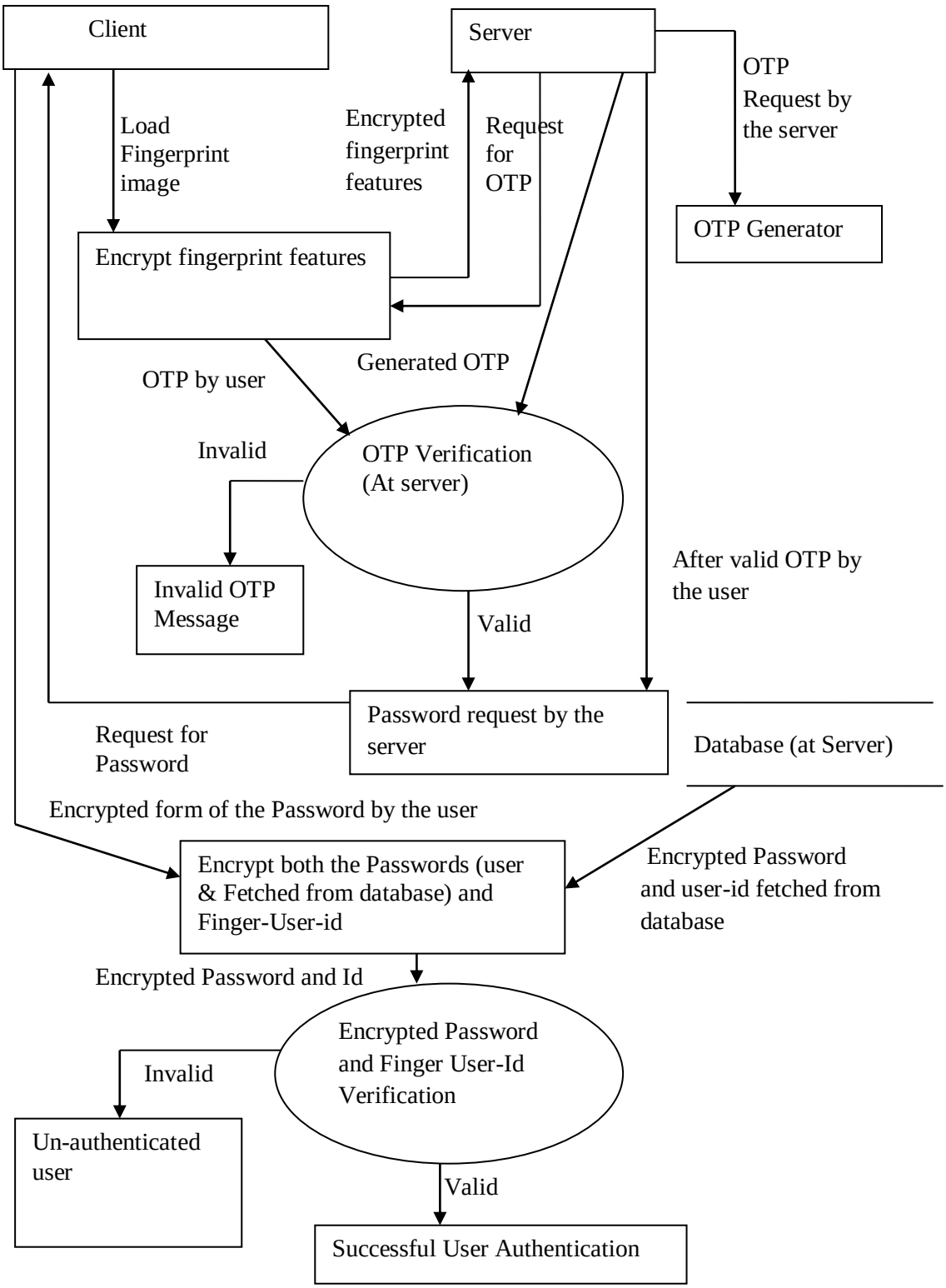


Figure 11.2: Dataflow Diagram of Proposed Multifactor Authentication

Step-12: If the random number is in between 9 to 16 (including both) then extract next 8 characters (from position 9 to 16) of the Hash code of size 32 characters generated in Step-8.
Step-13: If the random number is in between 17 to 24 (including both) then extract next 8 characters (from position 17 to 24) of the Hash code of size 32 characters generated in Step-8.
Step 14: If the random number is in between 24 to 32 (including both) then extract next 8 characters from position 24 to 32) of the Hash code of size 32 characters generated in Step-8.

11.7 RESULTS AND DISCUSSIONS

In this research work, Multifactor Authentication model is not implemented as a client-server concept, but its model is implemented using MATLAB2015a. In order to extract the features of the fingerprint image, Gabor filtering is utilized. Figure 11.3 shows screenshots of fingerprint feature extraction by utilizing segmentation process. This is treated as a client-side process. In client-side user fingerprint image is loaded into the system.

Figure 11.3: Screenshots of fingerprint feature extraction using segmentation Process (Client-side processing)

Initially, an image is segmented and foreground region of the image is extracted from background region. Next fingerprint features are extracted. These features are converted into some double precision number using Gabor filtering. These values are encrypted and sent to the server for generating Hash code. Server-side processing includes Hash generation, OTP generation, OTP verification, Password Verification, and Fingerprint Hash verification. As soon as server receives fingerprint features in encrypted form, the server decrypts it and generates Hash code. This Hash code is used to generate OTP along with some other details. Figure 11.4 shows input dialog box for OTP.

As soon as Client receives the OTP, the user enters OTP through client interface and it is passed to the server back for verification, If OTP matches, server prompts a password for a client, and the user enters the password. Figure 11.5 shows the password message.

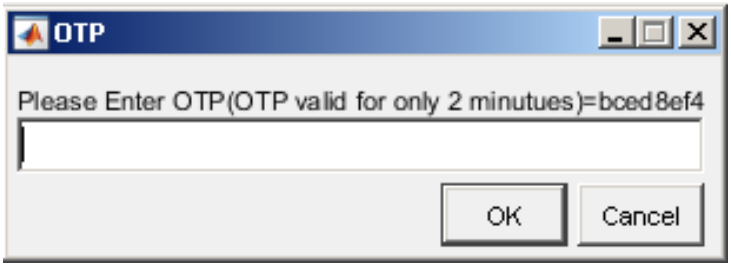


Figure 11.4: Screenshots of OTP with 2-Minutes of lifespan

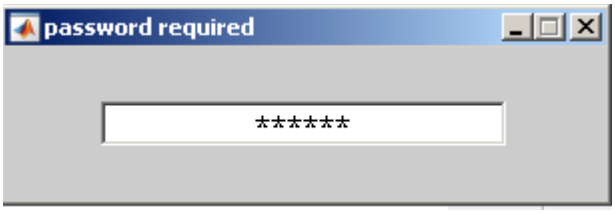


Figure 11.5: Screenshots of Password

Once user entered password reaches the server, the server verifies the password with database and if verification becomes a successful user is authenticated. Figure 11.6 shows the status of authentication.

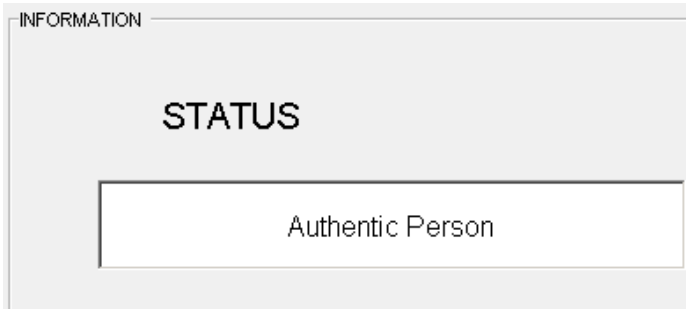


Figure 11.6: Screenshots of Status used in Multifactor Authentication Model

Table 11.1 shows screenshots of database values. Id represents the Hash value of the user fingerprint and hash column represents password. In the database, table password is stored in cryptographic Hash function. In the worst case, if an intruder hacks the database, he/she cannot understand password, because which is already stored in the Hash form in the database.

Table 11.1: Fingerprint-id and Password (hash) stored in Database

Id	hash
6b0cb74f5f8773667bf633a232b7ed12	63e7c5b52f995c466de97c7e1b13c45a
a0e5550770d0b6f72ca7f0afc1d0509a	46aa16250c809e993ccde5d5cababe12
2b4e687bf015532ba5ec6a0403d90935	2bc98e659d9627bca74ef482a953af5d
f1a14a44898a2eb2272aa76fe4ed8295	176f93ff4c5bb289decdfc2d9f8297a2
3b5a17d8092dbf0b23f71c2031dc2161	6ee1bca71a01ebba0f63fd076402f14f
4fbfe255d3610c804092653f9b4f61f6	5c98d6ca3f5d51048c98112cab8cb3b6
a542a749b79cfd482c4a45f4912f49ff	a843da9c81b63495736d1af10435227b
b8454d515e6f0a8893a5c97019e303ab	e2e638ac139b6da754e0a0e0533e65d7
c44837ccf2bf4903057c8b1678963fd5	1191e3745ad3aa05f405015cb4b88974
27f649b4d979e9b13ee5c412ab0d05a3	ebdd5c0b31050a546260fd849093f11d

11.8 ABCD ANALYSIS OF MULTIFACTOR AUTHENTICATION MODEL

Multifactor Authentication Model used in this research work can be analyzed using its predicted Advantages, Benefits, Constraints, and Disadvantages [28-30].

Advantages

- Fingerprint Hash code used in Multifactor Authentication model acts as identity-key or index-key to uniquely identify individual persons.
- Fingerprint Hash code, combined with Password and OTP makes authentication process robust or highly secure.
- The fingerprint image is hashed through the double folded layer and salted enough.
- The modern study reveals that fingerprint images are not secret, not revocable but in this model, because fingerprint Hash code is used as index-key, securing of the fingerprint image is not essential.
- Changes in finger depending on weather condition or a cut or wound in finger does not affect the system performance in this model.
- Security details database table consist of only two fields as Fingerprint Hash-id and double folded encrypted password.
- The user Registered Mobile number is stored separately in another table. Fingerprint hash-id can be used to identify the user mobile number stored in the registration table.

Benefits

- Multifactor Authentication Model can be effectively implemented in Internet banking and Mobile banking.
- This model does not require any fingerprint sensor device to capture user fingerprints. It uses a static image of the fingerprint.
- Cost and memory utilization is less compared to similar biometric fingerprint recognition systems
- Multifactor authentication model is effectively implemented in smartphones compared to any other platforms because smartphone already will be having one level of security through pattern lock or using password lock.

- In the worst case, if an intruder gets fingerprint image, it just acts as an identifier and not as security information. So intruder cannot break the system only with the fingerprint image.
- Even though fingerprint image cannot use solely in the authentication process, it can be protected in systems like laptop or desktop computer using login password.
- No need of remembering the User-id and Fingerprint Hash code just acts like email-id means even if public or intruder gets it, he/she cannot break the system.

Constraints

- The user should remember the password and should not leak, or reveal to anyone, or write it on anywhere to protect it from the intruder or hacker.
- A password should be mixed with the number, alphanumeric characters or letters, Lower case and upper case letters, and special characters and the user should remember this.
- Lower mobile network coverage makes a denial to the system because of not getting the OTP in time.

Disadvantages

- Biometric Fingerprint is less emphasized in verification or authentication process in Multifactor Authentication model.
- User cannot be verified or authenticated without remembering anything, at least password information user should carry along with him/her secretly
- Multifactor Authentication Model used in this study is not suitable for a system which does not utilize a mobile phone and computer like a biometric attendance system.
- Multifactor Authentication Model used in this study requires client-server architecture and not helpful for a standalone system.

11.9 CONCLUSION

Authentication frameworks in light of multiple factors fingerprints have demonstrated to create low false acceptance rate and false rejection rate, alongside other favorable circumstances like simple and easy usage strategy. At the same time fingerprints are the half-secret if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan.

In this paper, we have discussed fingerprint Hash code generation using Euclidean distance. Fingerprint Hash code used in Multifactor Authentication model acts as identity-key or index-key to uniquely identify individual persons. Fingerprint Hash code, combined with Password and OTP makes authentication process robust or highly secure. The fingerprint image is hashed through the double folded layer and salted enough. Multifactor Authentication Model used in this study is not suitable for a system which does not utilize a

mobile phone and computer like a biometric attendance system. Multifactor Authentication Model used in this study requires client-server architecture and not helpful for the standalone system.

REFERENCES

[1] Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image Authentication. *Journal of Computer Science and Information Technology*, *7*, 195-206.

[2] M'raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). *Hotp: An hmac-based one-time password algorithm* (No. RFC 4226).

[3] Krishna Prasad, K. & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE),* 1(2), 86-92. DOI: http://dx.doi.org/

[4] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[5] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19.

DOI: http://dx.doi.org/10.5281/zenodo.835608

[6] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[7] Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[8] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 51-65.

DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[9] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 98-111.

DOI: http://dx.doi.org/10.5281/zenodo.1067110

[10] Krishna Prasad, K. & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 116-126.

DOI : http://doi.org/10.5281/zenodo.1133545

[11] Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.

[12] Das, P. P., Chakrabarti, P. P., & Chatterji, B. N. (1987). Distance functions in digital geometry. *Information Sciences*, *42*(2), 113-136.

[13] Yamada, H. (1984). Complete Euclidean distance transformation by parallel operation. In *Proc. of 7th Int. Conf. on Pattern Recognition, Montreal* (Vol. 1, pp. 69-71).

[14] Borgefors, G. (1986). Distance transformations in digital images. *Computer vision, graphics, and image processing*, *34*(3), 344-371.

[15] Danielsson, P. E. (1980). Euclidean distance mapping. *Computer Graphics and image processing*, *14*(3), 227-248.

[16] Yamashita, M., & Ibaraki, T. (1986). Distances defined by neighborhood sequences. *Pattern Recognition*, *19*(3), 237-246.

[17] Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., & Yung, M. (2006, October). Fourth-factor authentication: somebody you know. In Proceedings of the 13th ACM conference on Computer and communications security (pp. 168-178). ACM.

[18] Bemmel, V., & Mian, S. (2009). U.S. Patent No. 7,512,567. Washington, DC: U.S. Patent and Trademark Office.

[19] Aloul, F. A., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In AICCSA (pp. 641-644).

[20] Jakobsson, M., Shi, E., Golle, P., & Chow, R. (2009, August). Implicit authentication for mobile devices. In Proceedings of the 4th USENIX conference on Hot topics in security (pp. 9-9). USENIX Association.

[21] Angulo, J., & Wästlund, E. (2011, September). Exploring touch-screen biometrics for user identification on smart phones. In IFIP PrimeLife International Summer School on Privacy and Identity Management for Life (pp. 130-143). Springer Berlin Heidelberg.

[22] Delac, K., & Grgic, M. (2004, June). A survey of biometric recognition methods. In Electronics in Marine, 2004. Proceedings Elmar 2004. 46th International Symposium (pp. 184-193). IEEE.

[23] Seo, H., Kim, E., & Kim, H. K. (2012). A novel biometric identification based on a users input pattern analysis for intelligent mobile devices. International Journal of Advanced Robotic Systems, 9, 1-10.

[24] De Marsico, M., Galdi, C., Nappi, M., & Riccio, D. (2014). FIRME: face and iris recognition for mobile engagement. Image and Vision Computing, 32(12), 1161-1172.

[25] Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. *International Journal of advanced science and Technology*, 4, 25-38.

[26] Yoo, J. H., Ko, J. G., Chung, Y. S., Jung, S. U., Kim, K. H., Moon, K. Y., & Chung, K. (2007, December). Design of embedded multimodal biometric systems. In Signal-Image Technologies and Internet-Based System, 2007. SITIS'07. Third International IEEE Conference on (pp. 1058-1062). IEEE.

[27] Xi, K., & Hu, J. (2009, June). Biometric mobile template protection: a composite feature based fingerprint fuzzy vault. In 2009 IEEE International Conference on Communications (pp. 1-5). IEEE.

[28] Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy.

[29] Aithal, P. S. (2016). Study on ABCD analysis technique for business models, business strategies, operating concepts & business systems

[30] Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2016). ABCD analysis of Stage Model in Higher Education.

Chapter 12
A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain code

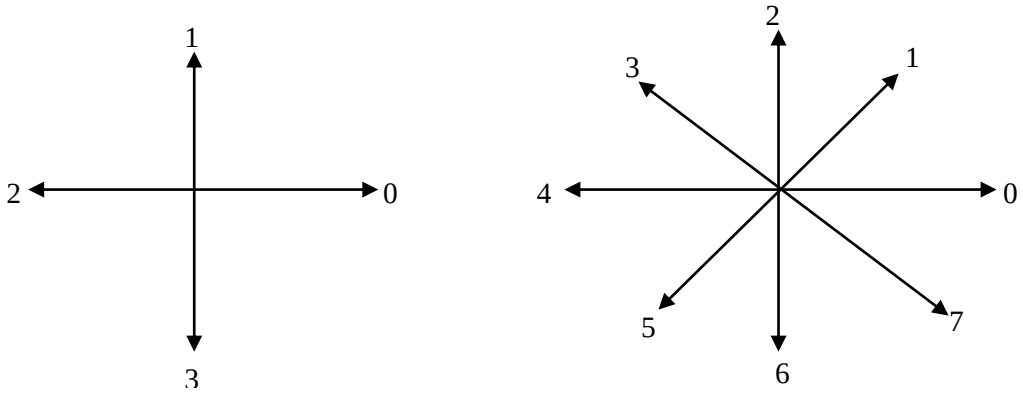
The drastic changes in mobile and wireless based technologies and increasing number of applications and users demanded high-security concern, which leads to research on biometrics with a purpose to increase the security aspects and to minimize security threats. The current global mindset toward terrorism has influenced people and their governments to take some special actions and be extra proactive in protection or security problems. Fingerprint image and identification technology have been in life for hundreds of years. Archaeologists have exposed proof suggesting that interest in fingerprints dates to prehistory. But the modern study reveals that fingerprint is not so secured like secured passwords which consist of alphanumeric characters, number and special characters. Fingerprints are left at crime places, on materials or at the door which is usually class of latent fingerprints. We cannot keep fingerprint as secure like rigid passwords. In this paper, we discuss fingerprint image Hash code generation based on the MD5 Algorithm and Freeman Chain code calculated on the binary image. Freeman chain code extracts all possible boundaries for an image and which gives starting x and y positions as x0 and y0. Hashcode alone not sufficient for Verification or Authentication purpose, but can work along with Multifactor security model or it is half secured. To implement Hash code generation we use MATLAB2015a. This study shows how fingerprints Hash code uniquely identifies a user or acts as index-key or identity-key.

Keywords: Fingerprint Image, Fingerprint Hashcode, Authentication, Multifactor Authentication Model, Freeman Chain Code, MD5 Algorithm.

12.1. INTRODUCTION

Biometrics is an investigation of checking and setting up the identity of an individual through physiological components or behavioral qualities. Despite the fact that biometric methods have been effectively connected in a vast number of true applications, outlining a decent and robust biometric system is still a testing issue. The four fundamental factors that expansion the many-sided quality furthermore, challenges of system configuration are accuracy, scalability, security, and protection [1-2]. Automatic Fingerprint Identification System (AFIS) consists of different steps like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [3-9]. The distinctiveness of fingerprint is added forward by using ridge patterns and it has been proved that the information in small regions of friction ridges is in no way repeated. These friction ridges broaden in a human system all through the fetus level itself Fingerprint sensors or acquisition devices uses different types of sensors to take input or to get fingerprint image into the system [10].

Freeman chain code is used to symbolize a boundary by means of a connected series of straight line segments of specific length and path in the predefined direction [11]. Typically this illustration is based on 4 or 8 connectivity of the segments [12]. The direction of each segment is coded or represented by the usage of a numbering format or scheme. A boundary code fashioned as a sequence of such directional numbers is called a Freeman chain code. The chain code of a boundary relies upon at the place to begin. Running with code numbers gives a unified way to research or analyze the form of the boundary. Chain code follows the contour in a counter-clockwise manner and keeps tune of the directions as we go from one contour pixel to the following. Figure 12.1 (a) and 12.1 (b) represents, 4-connected and 8-connected neighbour of Freeman Chain code respectively.



(a) (b)

Figure 12.1: Neighbour Directions of Freeman Chain code

The main drawback of 4-connectivity is that we lose the diagonal factors or pixels wherein those pixels are very useful in most of the image processing programs. So, in order to overcome the drawback of 4-connectivity here, we use 8-connectivity. In 8-connected neighbour, every code is taken into considerations. In 8-connected neighbour, the angular direction is in multiples of 450, that we have to pass or move from one contour pixel to the

next. If we take into account Figure 12.2, we can calculate freeman chain code for 4-connectivity as follows.

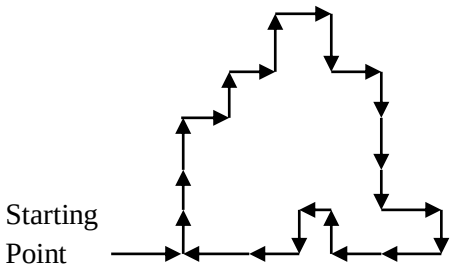


Figure 12.2: Freeman Chain code example for 4-connected

Freeman Chain code for Figure 12.2 is 1110101030333032212322. The first difference of Freeman Chain code for Figure 12.2 is 1003131331300133031130. The first difference of Freeman Chain coding for 4-connected neighbour is explained using Figure 12.3. The first difference value is calculated by counting a number of separating directions in an anti-clockwise direction from the starting point to ending point.

In this study, we make use of the MD5 Hash algorithm in order to generate Hash code. The process of the MD5 algorithm is disused below.

Input: Extracted Features

Output: Hash Code

Step-1: Attach the padded bits

Step-2: Append the length of the initial input to the result of the previous step-1

Step-3: Initialize MD buffer as A, B, C, D.

A four-word buffer (A, B, C, D) was used to evaluate the message digest. Here each of A, B, C, D is a 32- bit register

Step-4: Process message in 16-word blocks

Step-5: Finally, we get the 32-bit Hashcode as output

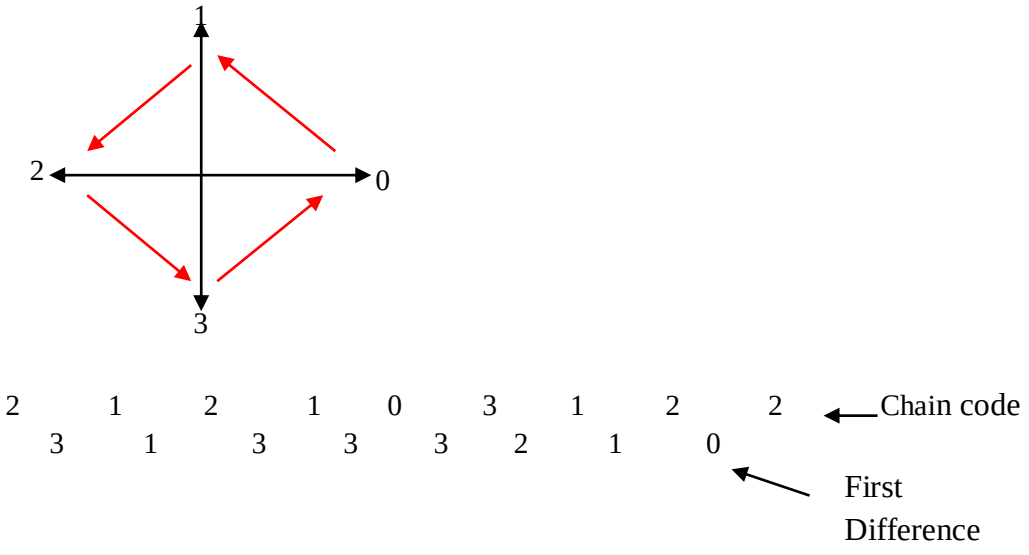


Figure12. 3: Freeman Chain code first Difference calculation-

In 8-connectivity neighbour, we have code from 0 to 7. Consider a binary point as shown below.

0010
0100
0011

The Freeman Chain code first checks for non zero points, in a binary number which is 1. So in the first row starting from left 3 bit is 1. Next bit is 1 from this point three-bit position, which is in the 2nd row. Next non zero value is five-bit position from the second non-zero bit, which is in the third row. Next non zero bit is very next bit and which is also in the third row. If you observe 8 connected neighbour the direction from the first non zero bit to second is in the direction 5. From second non zero bit to third in the direction of 7. From third non zero bit to fourth in the direction of 0. So the 8- Commonly, all the profitable biometric systems shield the stored templates by using encrypting those using general cryptographic techniques. Either a public key cryptosystem like RSA (RSA laboratories, 1999) or a symmetric key cipher like AES (Advanced Encryption Standard, 2001) is usually used for template encryption. One of the important challenges in biometric identification or verification system is keeping the biometric data or template safe and secure. A hash function is usually transformed functions, which converts or transform data or features from one form to another. Always transform function should be a one-way function or another way it should not be invertible [10]. A number of template protection strategies like fuzzy commitment [13], fuzzy vault [13], protecting functions [14] and distributed supply coding [15] can be considered as the key binding biometric cryptosystem. Different schemes for securing biometric templates along with those positioned forth in [16-19] also fall under this class.

MD5 algorithm becomes robust and harder to decrypt for an intruder if we use salting process. Salting is adding extra strings to input arguments of the MD5 hash function. We use Freeman chain coding to extract features from the fingerprint image.

Fingerprints are half-secret, if passwords are leaked or hacked, it easily revocable using another password. But in a biometric security system, which uses only biometric features, is not easy to change fingerprint key or fingerprint are static biometric, which never change much throughout the lifespan. Fingerprints are left at the car, door or anyplace where every person goes and places his finger [20]]. Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security mechanisms like password or OTP in order to enhance security. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or reader [21-26].

This paper has six sections. Section-1 explains about introductory information of fingerprint and Freeman Chain coding, template protection and basic details of MD5 Hash function. Section-2, explains about objectives and methodology of the study. Section-3 explains about Algorithm of Hash code generation, Section-4 depicts a flowchart of Hash code generation. Section-5 explains Results and Discussions. Section-6 concludes the paper.

2. OBJECTIVES AND METHODOLOGY

There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause a difference in Hash code. So this research does not concentrate on developing fingerprint hash code which is translation and rotation invariant. Fingerprint alone not gives full security, in order to improve the security of the system fingerprint acts one factor along with OTP, password, or any other biometric psychological or behavioral traits. The main objectives of this study are given below.

To Study a Fingerprint Hash code generation using Freeman Chain coding boundary starting x and y value, chain code value and the first difference value of the binary image. To verify the uniqueness of fingerprint Hash code using FVC ongoing 2002 benchmark dataset. Figure 4 explains the methodology used in this research work. Here initially FVC ongoing 2002 benchmark dataset is considered for testing the hash code. The benchmark dataset image is binarised and Freeman Chain code of the image is calculated for each pixel. Before calculating Freeman Chain code it finds boundary starting x and y value. Also, the first difference value of the chain code is calculated. The entire there parameters are considered and 32-bit length hash code is generated. Distinct Euclidean distance value summation, mean value and standard deviation values are considered for generating Hash code.

After converting fingerprint image to binary image we have to take one's complement of the binary image. So that all minutiae points will be represented using binary bit 1. Find all exterior, interior, parent and child boundary of the fingerprint binary image. Boundary_pixel_cell array returns all the pixel positions involved in a boundary. This function returns an array of boundary pixel values. Each element of the array is a matrix of size n × 2 dimensions. Where n represents a number of rows involved in forming boundary points and column are always 2, which represents x and y value of each point. Each boundary matrix is passed as an argument for Freeman Chain coding function.

Freeman Chain code function returns starting x and y position of the boundary, Freeman Chain code, the First difference value of the Freeman Chain code. Initially, if more than one argument is sent to Freeman Chain code function, then it returns an error message that too many arguments. Freeman Chain code Function then checks whether an argument matrix column value is 2. This means that each point should have two values corresponding to x and y pixel positions values respectively. If not this will return an error message that input dimension mismatched. Next, it checks for open contour or open boundary. If the first and last point of the boundary value is same then it is considered an open contour. In this case, Freeman Chain code boundary stating x and y value will be equal to first point pixel value. Both Freeman Chain code and First difference value will be zero.

If the first and last point of the boundary is not same, then find the difference x and y value, by subtracting the first point from the second point. Find difference for all the points which makes the boundary pixels. The transition from current pixel to the next pixel is computed from the connectivity diagram shown in figure 12.1 (b) and as shown in Table 12.1.

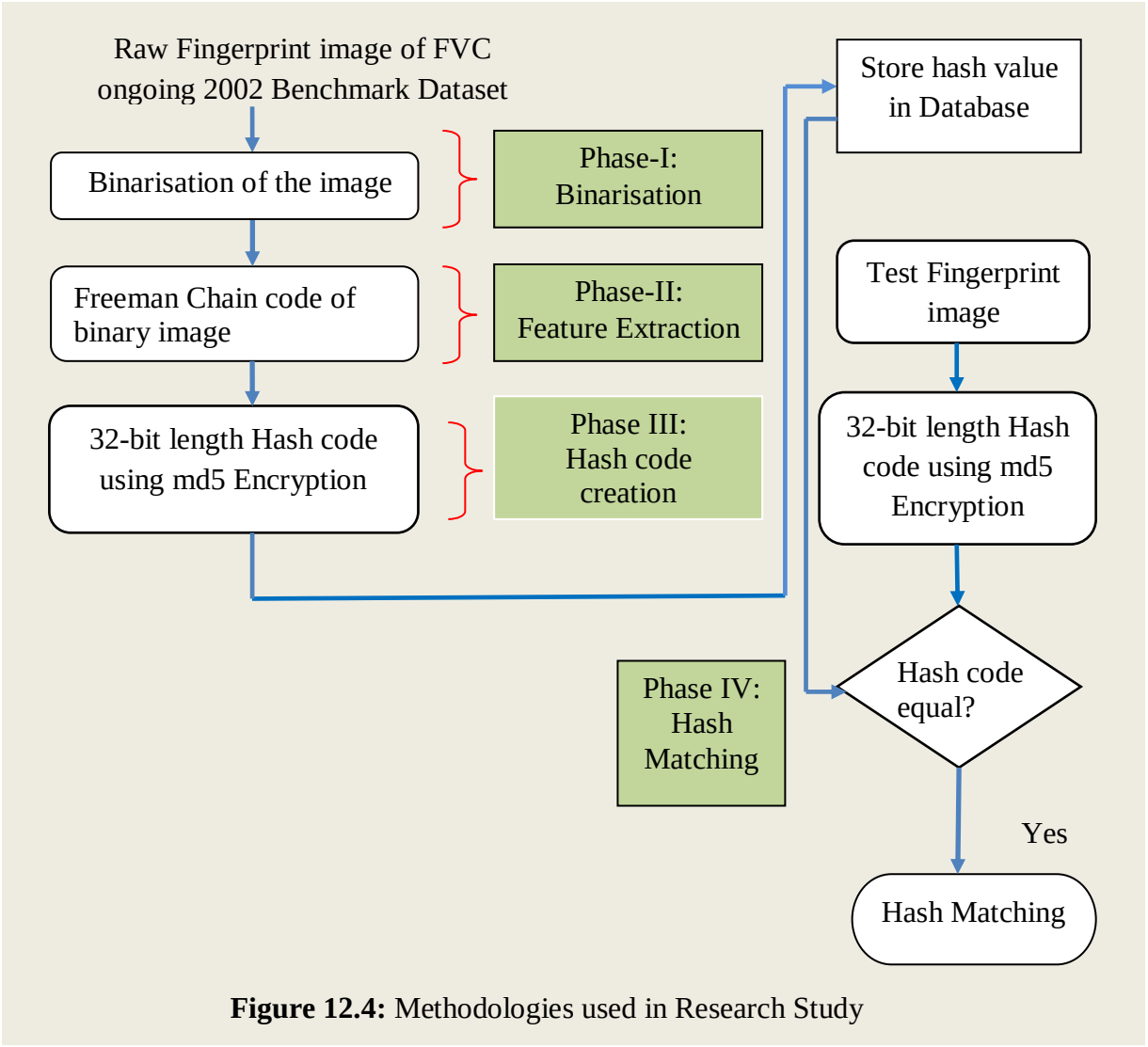


Figure 12.4: Methodologies used in Research Study

Table 12.1: Transition table of Freeman Chain code

Row difference	Column Difference	Direction
0	+1	2
0	- 1	6
- 1	+1	3
- 1	- 1	5
+1	+1	1
+1	-1	7
-1	0	4
+1	0	0

Setting up mapping mechanisms between pixel value differences in 8-connectivity directions is controlled by the following statement

idx([1 2 3 5 7 9 10 11]) = [5 4 3 6 2 7 0 1]

idx corresponds index value of code value and unique value is obtained by doing a simple calculation as follows

diffB_map = 4*row_diff + col_diff + 6

here diffB_map variable corresponds to each point pixel value difference that is involved in forming boundary pixels. These diffB_map values indexed into direction map using below statement and which produces chain code value.

chain_code_value = idx(diffB_map)

Finally, first difference value of chain code is obtained, by the following procedure

Step-1: Subtract each chain code value from Chain code end value

Step-2: Add number 8 to Step-1

Step 3: Take Modulus value of step-2 and 8 i.e. mod (Step-2, 8)

12.3 ALGORITHM OF HASHCODE GENERATION USING FREEMAN CHAIN CODE

This section explains step by step procedure to develop Hashcode by making use of Freeman Chain code on a binary fingerprint image. The steps of the algorithm are explained below. The algorithm also shows the pseudo code.

Step 1: Input Grayscale fingerprint image
read (input_image)

Step 2: Convert input image into 256 × 256 sized two-dimensional image
resized_image = image_resize (input_image, [256, 256])

Step 3: Convert 256 × 256 sized grayscale image into binary image
binary_image = convert_to_binary(resized_image)

Step 4: Perform One's complement of the binary_image
Binary_image = One's complement(binary_image)

Step 5: Find the Exterior boundaries of the binary image and boundaries of holes inside this Exterior boundary
boundary_pixel_array = boundary_pixel(binary_image)

Step 5: Find the row length of boundary_pixel_array
m = length (boundary_pixel_array) [where m is row length]

Step 6: Find Freeman Chain code for each element of the boundary_pixel_array
For i=1 to m
freeman_chain_code= freeman_chain_code (i)
end for

Step 7: Obtain Row and column coordinates for the starting pixel of the boundary from Step- 6.
start_idx = freeman_chain_code. start_idx

Step 8: Obtain Freeman Chain code value for each boundary from Step-6
chain_code = freeman_chain_code. chain_code

Step 9: Obtain Freeman Chain code first difference value for each boundary from Step-6
firstdiff = freeman_chain_code. firstdiff

Step 10: Compute summation of Step-7, Step-8, and Step-9

Step 11: Divide all 3 values of Step-10 by m.

Step 12: Pass the value of Step-11 as parameter for MD5 Hash function
hash_value = MD5_DataHash(combine_value)

12.4 FLOWCHART OF HASHCODE GENERATION USING FREEMAN CHAIN CODE

The above algorithm is explained using a flowchart.

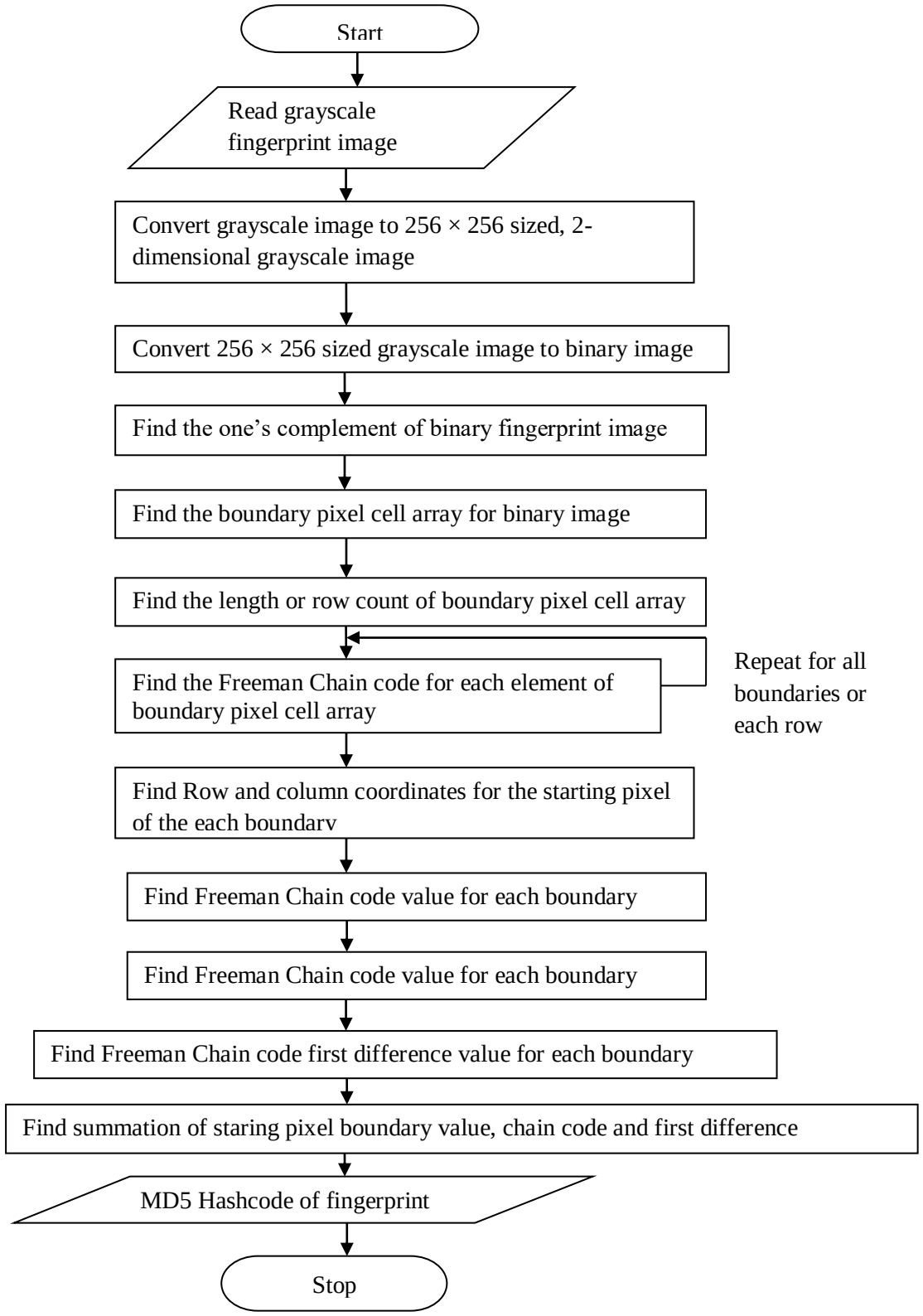


Figure 12.5: Flowchart of Hash code generation using Freeman Chain code

The different process or workflow is listed below. With an intention to make the MD5 Hashcode more robust and to get the advantage of salting Freeman Chain code summation of boundary starting x and y position, Chain code value and first difference value are divided by a total number of boundary value and all values are combined as a string and passed to the MD5 algorithm. Figure 12.5 shows a flowchart of this. Converting input image to 256 × 256 sized grayscale image

- Converting to binary image
- Taking one's complement of each pixel of binary image
- Finding Freeman Chain code function
- Obtaining Row and column coordinates for the starting pixel of the each boundary
- Obtaining Freeman Chain code value for each boundary
- Obtaining Freeman Chain code first difference value for each boundary
- Generating a strong salting string for MD5 hash function-argument

12.5 RESULTS AND DISCUSSIONS

In this study, WampServer is used to create a database. This database table contains two fields as id and Hashcode. The Hashcode generation using Freeman Chain code is implemented using MATLAB2015a. The configuration of the system used to implement this study is given in Table 12.2.

Table 12.2: Configuration of System used for finding Execution Time

Sr. No.	Parameters	System Details
1	Model	Compaq 435
2	Processor	AMD E-350 processor 1.60 GHz
3	Installed Memory	3 GB (2 GB usable)
4	System Type	32-bit Operating System
5	Operating System	Windows 7 Starter
6	Software	MATLAB 2015a 32-bit

The execution time for different randomly selected images of FVC ongoing 2002 dataset is shown in Table 12.3. The average execution time of the fingerprint Hashcode generation using Freeman Chain code is very good and it is approximately on an average is 1.672678. Here we only consider the training phase. The testing phase includes around 0.44 seconds more than training phase. If the configuration of the system increases definitely execution time also increases. Table12.4 shows the Hashcode generated based on an MD5 algorithm using Freeman Chain code.

Table12. 3: Execution time of the training phase

Method Name	Image name	Execution Time (in seconds)	Average
Method-1	101_1	4.243991	1.672678
	101_5	2.343854	
	102_2	1.488027	
	103_3	1.447657	
	104_4	1.917586	
	104_7	1.280134	
	104_8	1.374160	
	105_8	0.775691	
	106_6	1.387195	
	109_3	1.275428	
	109_8	1.457092	
	110_3	1.343319	
	110_8	1.410684	

Table12.4: Hash code generated using Freeman Chain code

Serial No.	**Hashcode**
1	81981d7bd4cce1582d8b2b7504c26a50
2	76fc72bb5650bfb491117c933449936a
3	87ab0b35e67e28775f467e9b6e988fae
4	dcf4b2aac0a2819fc410fffbd4114105
5	a0dcdb0c511d48f4b8e9e8d80addc006
6	902db2784067d125c5c2d28120974428
7	ff1f7f440d3e81b119f38f764fb9af6f
8	c64a8793be56e573f95ff0b454864fb1
9	e71511ffd44da8a76b11fdb6f3f1b68f
10	8e9fc502886a69e39c0f6e773e470b33
11	9faf0422c4e5563331322e90937a99c4
12	f60da0277c5656560ac81d12ddd4c397
13	231f87480e44ee88f4a79932560833a8

The screenshots of the grayscale fingerprint image capture is shown using Figure 12.6. The screenshot or Figure 12.6 contains two push buttons. One push button is used to select grayscale fingerprint image. Another one gives instruction to create WampServer and to connect this from MATLAB2015a. Here we use static one time captured an image of FVC ongoing 2002 benchmark dataset. The screenshots of Database processing and status is shown using Figure 12.7.

The data processing control of figure 7 consists of five push buttons as Connect, Fetch, Data, Hash Generation, and Check. Connect button is used to connect to the database, Fetch button is used to fetch records from the database, Data button is used to show data in tables, hash generation is used to generate Hashcode for sample input fingerprint, and Check is used to

check sample input Fingerprint image is matching or not matching with already stored hash code.

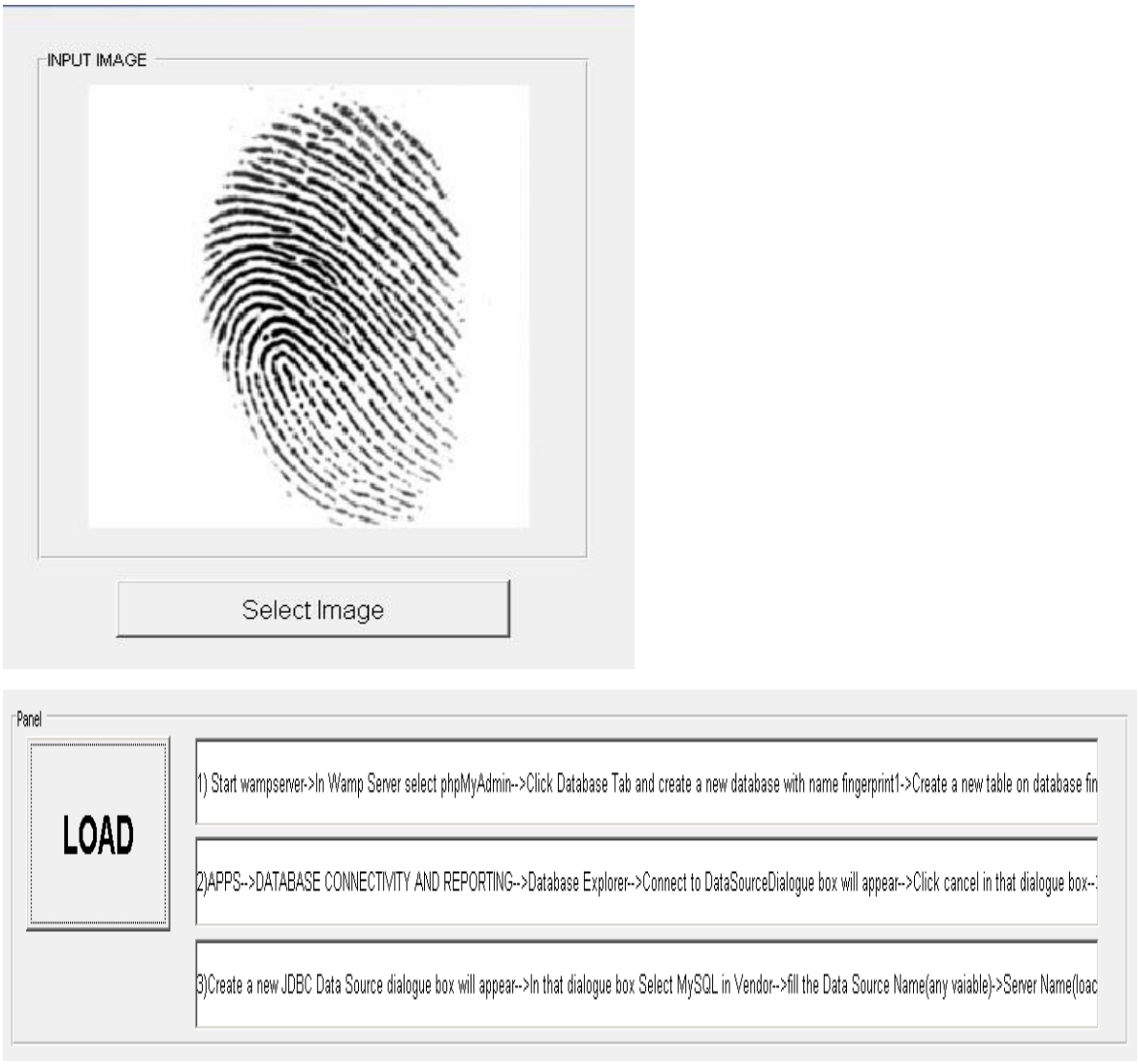


Figure 12.6: Screenshots of Fingerprint image capture

Advantages of Hash value produced using Euclidean distance

- Hash code produced using Freeman Chain code is noninvertible
- Hash code takes very small amount of memory
- Hash code Hides original information of fingerprint image from the intruder
- The execution time of Hash code generation using Freeman Chain code is very good.
- It is unique for each fingerprint of the same person means ten fingerprints will be having ten different Hash codes.

Benefits of Hash value produced using Euclidean distance

- Hash code is used as identity-key or index-key for unique identification purpose of a user.
- Easily we can append salting in order to make the Hash code more robust.
- Fingerprint Hash code is a transformed function, which does not reveal original minutiae details.

- Fingerprint Hash code consumes very less time for training phase.
- Unlike another fingerprint matching, this study does not use scoring level. It uses only binary value either matching or not matching.
- This can be used for security or authentication purpose if the user takes some security measures to protect static one time captured fingerprint image like folder locking.

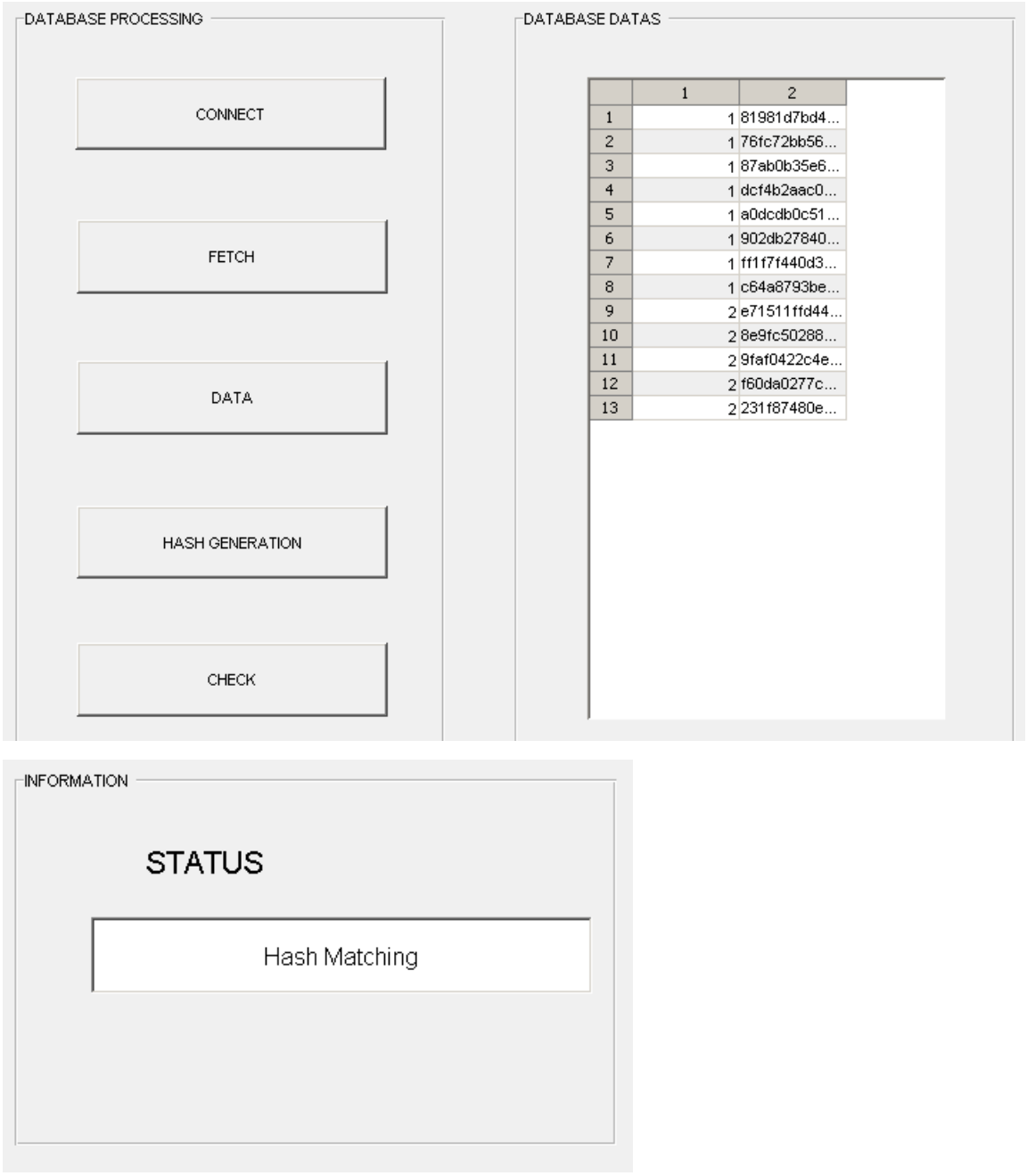


Figure 12.7: Screenshots of Database processing and Status

Constraints of Hash value produced using Euclidean distance

- Small changes in fingerprint hash code make large differences.
- Fingerprint generations using Freeman Chain code are translation and rotation variant which is not having much scope when the fingerprint is used for identification purpose rather than security purpose.

Disadvantages of Hash value produced using Euclidean distance

- Fingerprint hash code cannot be solely used for security or authentication purpose.
- If fingerprint image of same finger input is taken through any type of solid and robust sensors in consecutive two intervals, still fingerprint hash code generates different hash code.
- Even though developed fingerprint Hash code is invariant to translation and rotation, if the user presses hardly into one reader or sensor, or swipe the finger in a different orientation, or a cut in the finger, for a successive two capture, produces different Hash code.

12.6 CONCLUSION

Fingerprint hashing is the new technique which combines biometrics and cryptography. The goal is to perform identification based on fingerprint simultaneously hiding or keeping the fingerprint information secretly or noninvertible way. Even though fingerprint is compromised intruder should not get original features of the fingerprint image. Fingerprint image having some drawbacks like which left by a human being at many places like door, wall, on the car and many more places are easily mimicked by fraud or intruder. The fingerprint does not get matched when the finger has some cut or wound and sensors are not able to recognize in some weather conditions like winter season. The fingerprint is effective as identity or index key and not as a full security feature. It works well with multifactor biometrics authentication as one major factor.

In this paper, we developed a Hash code based on an MD5 Hash function by making use of Freeman Chain code for a binary fingerprint image. This Hashcode can be effectively used as Index-key or identity-key. This method shows considerably better execution time. This method also gives 100% accurate matching as far as input fingerprint image is once captured and stored static digital fingerprint image. If we capture through sensor each time this gives different Hash code. So this method is not suitable for solely security purpose unless and until the user takes some security measure to protect static fingerprint image.

REFERENCES

[1]Nandakumar, K., Jain, A. K., & Nagar, A. (2008). Biometric template security. *Eurasip Journal on Advances in Signal Processing, 2008*. https://doi.org/10.1155/2008/579416

[2]Nandakumar, K., & Jain, A. K. (2004, December). Local Correlation-based Fingerprint Matching. In *ICVGIP* (pp. 503-508).

[3] Krishna Prasad, K. & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[4] Krishna Prasad, K. & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 8-19.
DOI: http://dx.doi.org/10.5281/zenodo.835608

[5] Krishna Prasad, K. & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191
[6] Krishna Prasad, K. & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653
[7] Krishna Prasad, K. & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 51-65.
DOI: http://dx.doi.org/10.5281/zenodo.1037627.
[8] Krishna Prasad, K. & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 98-111.
DOI: http://dx.doi.org/10.5281/zenodo.1067110
[9] Krishna Prasad, K. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 86-92. DOI: http://dx.doi.org/
[10] Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.
[11] Gonzalez, R. C., & Woods, R. E. (1992). Digital image processing.
[12] Bernard, M., Fromont, E., Habrard, A., & Sebban, M. (2012, June). Handwritten digit recognition using edit distance-based KNN. In *Teaching Machine Learning Workshop*.
[13] Juels, A. (2002). M. Sudan 'A fuzzy vault scheme'. In *Proceedings of the 2002 IEEE International Symposium on Information Theory* (Vol. 408).
[14] Tuyls, P., Akkermans, A. H., Kevenaar, T. A., Schrijen, G. J., Bazen, A. M., & Veldhuis, R. N. (2005, July). Practical biometric authentication with template protection. In *AVBPA* (Vol. 3546, pp. 436-446).
[15] Holst, J. C., & Draper, D. A. (1999). *U.S. Patent No. 5,999,039*. Washington, DC: U.S. Patent and Trademark Office.
[16] Davida, G. I., Frankel, Y., Matt, B., & Peralta, R. (1999). On the relation of error correction and cryptography to an online biometric based identification scheme. In *Workshop on coding and cryptography*.
[17] Hao, F, Anderson, R & Daugman, J 2006, Combining Crypto with Biometrics Effectively', IEEE Transactions on Computers, vol. 55, pp. 1081-1088.
[18] Kelkboom, E. J., Gökberk, B., Kevenaar, T. A., Akkermans, A. H., & van der Veen, M. (2007, August). "3D face": biometric template protection for 3D face recognition. In *International Conference on Biometrics* (pp. 566-573). Springer, Berlin, Heidelberg.
[19] Connie, T., Teoh, A., Goh, M., & Ngo, D. (2005). PalmHashing: a novel approach for cancelable biometrics. *Information processing letters*, *93*(1), 1-5.
[20]https://hackaday.com/2015/11/10/your-unhashable-fingerprints-secure-nothing/, Last Accesses Date: 05-12-2017.

[21]https://security.stackexchange.com/questions/42384/is-there-any-way-to-cryptographically-hash-a-human-thumbprint, Last Accesses Date: 05-12-2017.
[22] Chikkerur, S. S. (2005). *Online fingerprint verification system* (p. 2005). State University of New York at Buffalo.
[23] Bhuyan, M. H., Saharia, S., & Bhattacharyya, D. K. (2012). An effective method for fingerprint classification. *arXiv preprint arXiv:1211.4658*.
[24] Meng, X. P., Wu, Z. G., & Zhao, Y. L. (2009). Algorithm of fingerprint identification based on fingerprint texture structure [J]. *Computer Engineering and Design*, *13*, 031.
[25] Aithal, P. S. (2016). A Review on Advanced Security Solutions in Online Banking Models. *International Journal of Scientific Research and Modern Education (IJSRME),* 1(1), 421-429. DOI: http://doi.org/10.5281/zenodo.160971.
[26] Aithal, P. S. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. *International Journal of Management, IT and Engineering (IJMIE),* 5(7), 455-464. DOI : http://doi.org/10.5281/zenodo.268875.

****

Chapter 13
A Study on Pre and Post Processing of Fingerprint Thinned Image to Remove Spurious Minutiae from Minutiae Table

In Fingerprint recognition, after the initial preprocessing, the feature is extracted from the Fingerprint thinned image. Extraction of crucial and beneficial capabilities or features of interest from a fingerprint image is an essential venture during recognition. Feature extraction algorithms pick handiest or only applicable features important for enhancing the performance of matching and recognition rate and outcomes with the feature vector. The feature extraction algorithms or techniques require only relevant features like minutiae details and do not require any background details or domain-specific details. They need to be smooth or easy to compute with a purpose to gain a viable or practicable technique for a huge image series. Minutiae details or fingerprint ridge ending or bifurcation details using skeletonized or thinning approach is a very popular method for feature extraction. The preprocessed thinned image is further post-processed to remove some false minutiae from minutiae table and which is generated through crossing number theory. One more purpose of post-processing is to reduce the number of minutiae points by removing false minutiae structures like spurs, ride breaks, short ridge, holes or islands, bridges, and ladders. In this paper w × w window neighborhood is considered for each minutia in Minutiae Table. Minutiae Table contains Ridge ending or bifurcation code as 1 or 3 with its location details means x and y position in two columns and the sum of these details as its fourth column. These Minutiae tables are used for generating Fingerprint Hash code, which can be used as index-or identity key in order to uniquely identify an individual person or as one factor in Multifactor Authentication Model.

Keywords: Post Processing, Thinning, Ridge Ending, Ridge Bifurcation, Minutiae Table.

13.1 INTRODUCTION

Automatic Fingerprint Identification System (AFIS) consists of numerous techniques and process before matching and identification, which are Contrast Adjustment or Image Enhancement, Image Segmentation, Skeletonization or Thinning, Preprocessing the thinned image, Orientation, Post processing, and Minutiae Extraction [1-12]. Minutiae details or fingerprint ridge ending or bifurcation details using skeletonized or thinning approach is a very popular method for feature extraction. Initially, the fingerprint image is preprocessed and the last stage of preprocessing is thinning. The preprocessing is usually consists of series of a process like filtering, image enhancement, binarization, segmentation and thinning. The binarized image after segmentation is then thinned using a set of policies that eliminate pixels from ridges till the ridges are one-pixel period or length [13]. There are numerous strategies available in the literature for Skeletonization or thinning method [14-16]. After extracting the minutiae from the thinned image a few post-processing is carried to cast off any spurious minutiae and final features of the fingerprint image are obtained. The strategies on this elegance are of types–crossing number based and morphology-based.

However, techniques based totally on thinning are sometimes sensitive to noise and the skeleton shape does no longer conform to intuitive expectation. Nonskeletonized feature extraction uses a binary image based totally technique. The principle problem within the minutiae extraction technique the use of thinning processes comes from the reality that minutiae within the skeleton image do not usually correspond to true minutiae inside the fingerprint image. In fact, quite a few spurious minutiae are determined because of undesired spikes, breaks, and holes. Consequently, put up processing is usually followed to keep away from spurious minutiae, which are based on each statistical and structural fact after characteristic or feature detection. After skeleton formation or on thinned image some preprocessing operation is done in order to remove spurious minutiae or ridge patterns. One of the morphological operations called erosion. The morphological establishing operation is blended with the morphological erosion and the dilation operations. Where in erosion operation is implemented to shrink or thin an object and dilation operation is utilized to make bigger or thicken an object. In a Skeletonised, fingerprint image, white regions encompass background and some styles of noises. For obtaining an amazing and easier skeleton or minutiae features the provided set of rules adapts the morphological erosion operation to delete the white areas occupied via noise or to identify non-minutiae points.

In this research, we use either skeletonized or thinned image minutiae feature extraction based on crossing number theory. In order to implement pre and post-processing algorithm, we use MATLAB2015a. The remaining part of the paper is organized as follows. Section 2 describes Preprocessing of Thinned Fingerprint Image with its theory and algorithm. Section 3 explains about Feature extraction. Section 4 describes Minutiae Table. Section 5 describes postprocessing. Section 6 explains the application of Minutiae Table. Section 7 concludes the paper.

13.2. Preprocessing of thinned fingerprint image

Fingerprint image can be identified or recognized with or without the use of skeletonized or thinned process. But fingerprint thinning is one of the most generally used pre-processing techniques before feature extraction. After skeleton formation or on thinned image some preprocessing operation is done in order to remove spurious minutiae or ridge patterns. The morphological establishing operation is blended with the morphological erosion and the dilation operations. An eight connected pixel mask is moved across the thinned image in order to remove white spaces or non-minutiae points. The 8-connected pixel mask is also called window. The window size is 3 × 3. The eight windows are obtained by keeping each pixel of the thinned image in a central position with value 1. If the 8-connected pixel mask with respect to this central position contains any edge means similar value (i.e. 1) in any one of the eight directions then central pixel is deleted. The 8 windows or pixel masks are shown below in Figure 13.1.

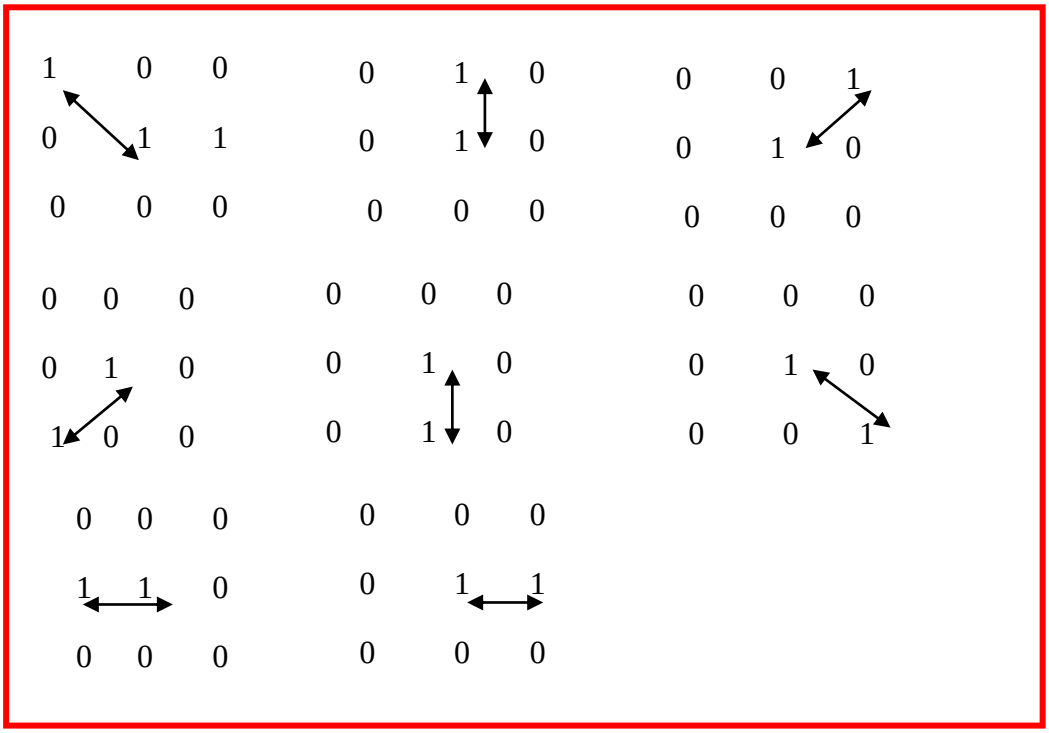


Figure 13.1: Eight windows of size 3 × 3 (pixel mask) used in skeleton preprocessing

The eight-pixel masks are in eight directions, North-West, South-West, South, North, South, South-East, West, and East from central pixel. The preprocessing function is called twice with an intention to remove more non-minutiae points or simply to improve the efficiency. Here erosion is thinned the white spaces or non-minutiae points. The result of the first window is taken as input for the second window and so on till the last or 8th window.

Algorithm for Preprocessing of Thinned image

This algorithm considers thinned image, $I_{skeleton}$ as input image and $I_{preprocessed}$ as output image.

1. Initialize 8 windows which are shown below

$temp_1 = erosion(I_{skeleton}, W_1)$ \\ w1= [1 0 0; 0 1 0; 0 0 0]
$temp_2 = erosion(temp_1, W_2)$ \\ w2= [0 1 0; 0 1 0; 0 0 0]
$temp_3 = erosion(temp_2, W_3)$ \\ w3= [0 0 1; 0 1 0; 0 0 0]
$temp_4 = erosion(temp_3, W_4)$ \\ w4= [0 0 0; 0 1 0; 1 0 0]
$temp_5 = erosion(temp_4, W_5)$ \\ w5= [0 0 0; 0 1 0; 0 1 0]
$temp_6 = erosion(temp_5, W_6)$ \\ w6= [0 0 0; 0 1 0; 0 0 1]
$temp_7 = erosion(temp_6, W_7)$ \\ w7= [0 0 0; 1 1 0; 0 0 0]
$I_{erosion} = erosion(temp_7, W_8)$ \\ w8= [0 0 0; 0 1 1; 0 0 0]
\\ $I_{erosion}$→Erosion Applied image

2. Find the size of Erosion Applied image as $[R_{erosion} C_{erosion}] = size(I_{erosion})$
3. **for each pixel** of the $I_{erosion}$ image except first and last pixel do
   Check for $I_{erosion}$ image pixel value, **if** $I_{erosion} = 1$
   Assign to a temporary images of 3 × 3 size, as
   $temp1 = I_{erosion}(i-1:i+1, j-1:j+1)$
   temp2=[temp1(1,1);temp1(1,2);temp(1,3);temp(2,1),
   temp(2,2),temp(2,3);temp(3,1);temp(3,2);temp(3,3);]
   Initialize a counter as, counter=0;
   for each pixel of temporary image **do**
   Check, **if** (temp2 (1, k) = temp1 (1, k))
   Increment counter, counter = counter +1
   end if
   end for
   Check, if (counter = 9)
   $I_{preprocessed1}$ (i, j) = 0 or $I_{preprocessed2}$ (i, j) =0
   end if **end for**

2.1 Workflow and Flowchart for Preprocessing of Thinned image

The above algorithm for Preprocessing of Thinned image is explained using workflow and flowchart. The input for this algorithm is skeletonized, represented as, $I_{skeleton}$. The final output is preprocessed image denoted as, $I_{preprocessed}$. The Workflow and Flowchart of the preprocessing of the thinned image are shown in Figure 13.2 and Figure 13.3 respectively.

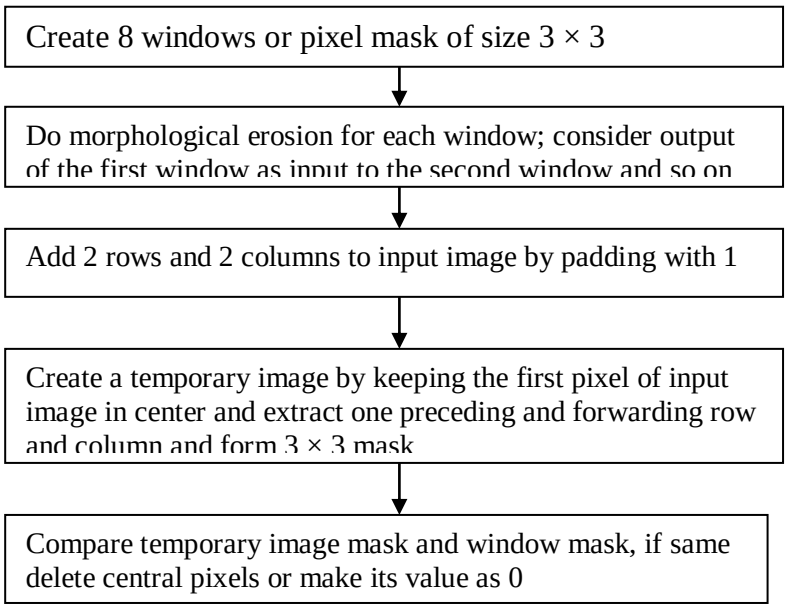


Figure 13.2: Workflow of the preprocessing of thinned image

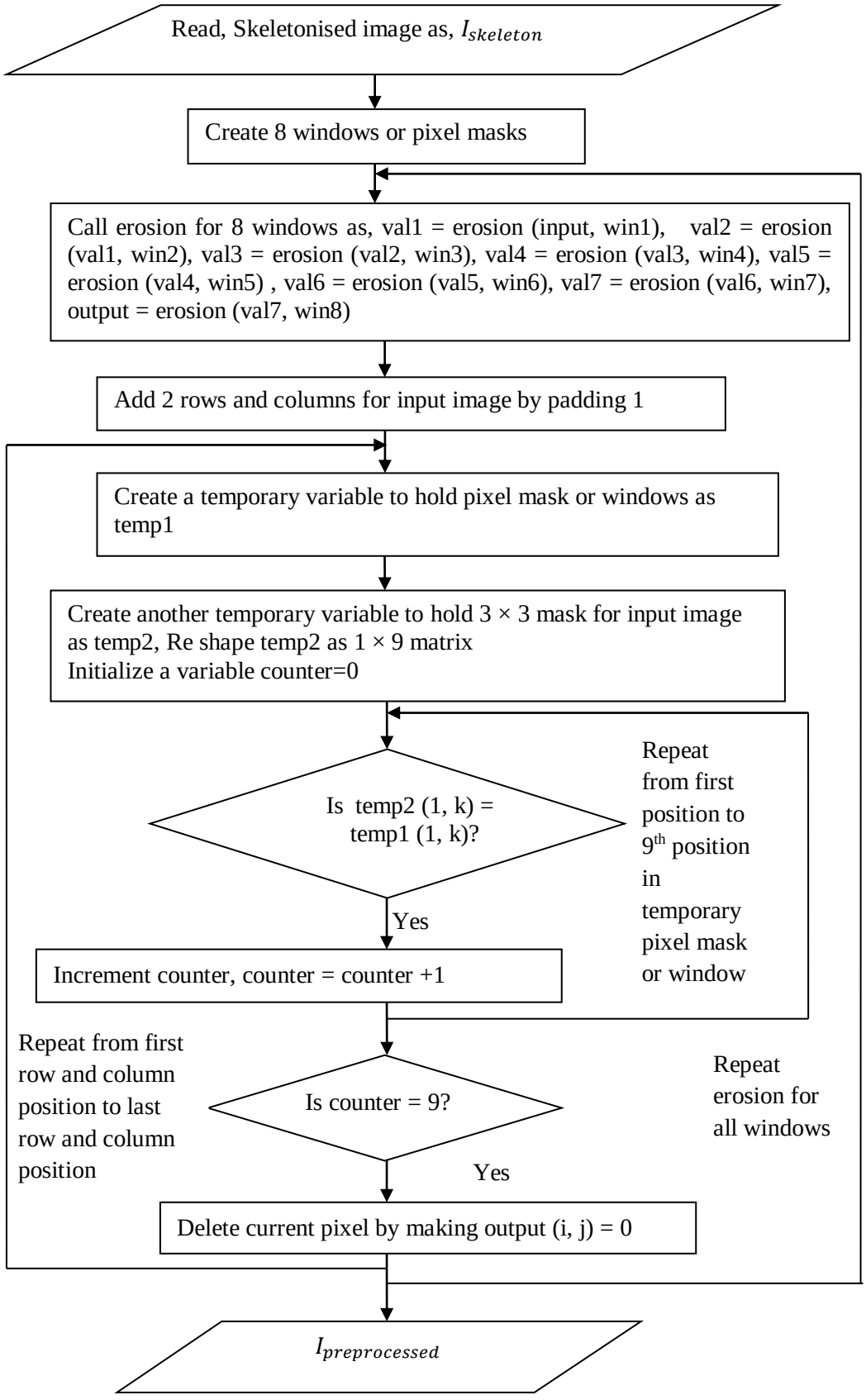


Figure 13.3: Flow chart of preprocessing state of Thinned image

Analysis of Preprocessing of Thinned image

Preprocessing for the thinned image is performed with an ultimate intention remove white spaces or non-minutiae points. Minutiae include ridge ending and ridge bifurcation, crossing, and isolated pixel and many more. But we concentrate only on ridge ending and bifurcation. Preprocessing removes white edges in all 8 directions.

The Table 13.1 shows thinned image pixel position removed for a 101_1.tif image taken from FVC ongoing DB1_B dataset. The datasets used for this study is from Fingerprint Verification Competition (FVC) ongoing 2002 benchmark datasets DB1_B, DB2_B, DB3_B, and DB4_B. Each dataset consists of 10 different fingerprint images and 8 impressions for each fingerprint labeled from 1 to 8. These datasets consist, a total of 3520 (880×4) fingerprints, but out of which only 40 fingerprints are available as a free resource for research testing purposes under the name of four datasets as DB1_B, DB2_B, DB3_B, and DB4_B. These datasets consist of image sizes of 388 pixels by 374 pixels (142 Kpixels) with resolution of 500 dpi, 296 pixels by 560 pixels (162 Kpixels) with resolution of 569 dpi, 300 pixels by 300 pixels (88 Kpixels) with resolution of 500 dpi, and 288 pixels by 384 pixels (108 Kpixels) with resolution of about 500 dpi for DB1_B, DB2_B, DB3_B, and DB4_B respectively. First two datasets are captured through optical sensor and DB3 and DB4 are captured through a capacitive sensor and SFinGe v2.51 sensor respectively. We use only DB1_B dataset for algorithm test purpose.

Table 13.1: Thinned image pixel position removed during preprocessing

Sr. No	Pixel Position of Input image	Window Value	Window Name	Function call name
1	(101, 46)	[[100]; [010]; [000]]	window1	preprocessing
2	(118, 103)	[[000]; [010]; [001]]	window6	preprocessing
3	(85, 45)	[[000]; [110]; [000]]	window7	preprocessing
4	(102, 09)	[[000]; [011]; [000]]	window8	preprocessing

In Table 1, column name, ‘Function call name' values preprocessing1and preprocessing 2 indicates, preprocessing function called during first and second call respectively. We call preprocessing with an intention to improve the efficiency of filtering process and thereby enhanced the efficiency of the matching process based on extracted features. The time complexity of pre-processing is Big-Oh (n^2).

13.3 FEATURE EXTRACTION

The individuality characteristic of the fingerprint is determined by the local ridge characteristics known as minutiae, which can be one of the most important standards utilized in fingerprint identification systems [17-18]. There are more than one hundred fifty minutiae characteristics are diagnosed in literature. These local ridge characteristics aren't similarly distributed. Minutiae are labeled in two sorts primarily based on minutiae factors as ridge ending and bifurcation. We concentrate only ridge ending and bifurcation. From a preprocessed thinned image, we can able to classify pixel positions into one of the possible 8-connected neighbors. A ridge pixel is called an isolated pixel if it does not contain any 8 connected neighbors. The ending is referred based on 8-connected neighbor having value 1. When 8-connected neighbor having value 3, then it's referred as bifurcation. If 8-connected neighbor having value exactly 4 then that is called as crossing.

The minutiae extraction processed defined in [19], used a 3 × 3-pixel mask to find or search ridge ending and ridge bifurcations. This method caused some problems or flaws due to the ridge ending repository at borders and spurious bifurcation or false minutiae inside the fingerprint. To remove these false minutiae, a series of rules are used [20]. In this regard, usually, fingerprints are less corrupt. In this all the fingerprint ridge patterns located at the border of the image are referred as invalid, this is due to the fact that, while capturing fingerprint image through sensors or any other capturing device only finite or countable number of points are only in contact. In this research, we make use of crossing number based theory to extract minutiae details-ridge ending and bifurcations.

Crossing Number

The preprocessed, thinned fingerprint image's ridge pixel usually contains only single pixel with value 1 or 0. Consider that (x, y) denote a pixel on a thinned ridge, and, p0, p1..... p8, denotes its 8 neighborhood pixels. Because the number of minutiae detected is more, the possibility of correct result increases. The concept of the crossing number (CN) is initially used by Kasaei et al., (1997) [21], for the purpose of extracting the minutiae from thinned or skeleton image. The nearby pixel of every ridge pixel in the image has scanned the usage of a 3×3 window from which the minutiae are extracted as shown in Figure 4. The crossing number may be used to categorize a ridge pixel as a finishing, bifurcation or non-minutiae point. As an example, a ridge pixel with a crossing-number of zero will correspond to an isolated factor and a crossing number of 4 correspond to a crossing factor. The Rutovitz's, crossing number for a ridge pixel is given in (1).

$$CN_p = \frac{1}{2}\sum_{i=1}^{8}|p_i - p_{i+1}| \quad \text{---------- (13.1)}$$

In Eq. (13.1) pi is a pixel value in the neighborhood of pixel p which is a central pixel with pi value is 1 or 0 and also, p1= p9. The crossing number CN_p at a point p is expressed as half of the cumulative total between pairs of adjacent pixels belonging to the eight-neighborhood of p and is shown in Figure13.4.

P1	P2	P3
P8	P	P4
P7	P6	P5

Figure 13.4: Neighborhood of crossing number based feature extraction for 3 × 3 size

Minutiae Extraction Algorithm based on Crossing Number

In this study, minutiae are extracted from the preprocessed-thinned image using the crossing number theory. This algorithm takes $I_{preprocessed}$ as input and produces output in the form of Minutiae table. The algorithm for feature extraction is as follows.

1. Find the row and column size of $I_{preprocessed2}$ and assign to m and n
2. Declare a variable to hold number of neighborhood as, count=0
3. **for each** pixel of $I_{preprocessed2}$ except first and last pixel, **do**

Check, **if** $I_{preprocessed2}$(i, j) = 1

Create a temporary image of size 3 × 3 neighborhood

tempimg = $I_{preprocessed2}$ (i-1 to i+1 , j-1 to j+1)

Reshape temping and assign to temping1 as

tempimg1 = [tempimg(1,1) ; tempimg(1,2) ; tempimg(1,3) ; tempimg(2,3) ; tempimg(3,3) ; tempimg(3,2) ; tempimg(3,1) ; tempimg(2,1) ; tempimg(1,1)]

Declare a variable to hold crossing number count and initialize with value 0

$$N_c = 0$$

repeat for 8-connected neighbor

$$N_c = N_c + |temp1(k) - temp1(k+1)|$$

end for

Divide value of N_c by 2, $N_c = 0.5 * N_c$

Check, if ($N_c = 1$) or ($N_c = 3$)

Increment the count as count = count+1

Assign to M_{table} as, $M_{table}(Count, :) = [i, j, N_c, (i + j + N_c)]$

\\M_{table}→ Minutiae Table

end if

end for

Workflow and Flowchart for Minutiae extraction based on crossing number

The above algorithm for Minutiae extraction based on crossing number is explained using a flowchart. The input for this algorithm is preprocessed thinned image, $I_{preprocessed}$. The final output is Minutiae Table, represented as, M_{table}. The flowchart of the crossing number based minutiae extraction is shown using Figure 13.5. The workflow of this is shown in Figure 13.6.

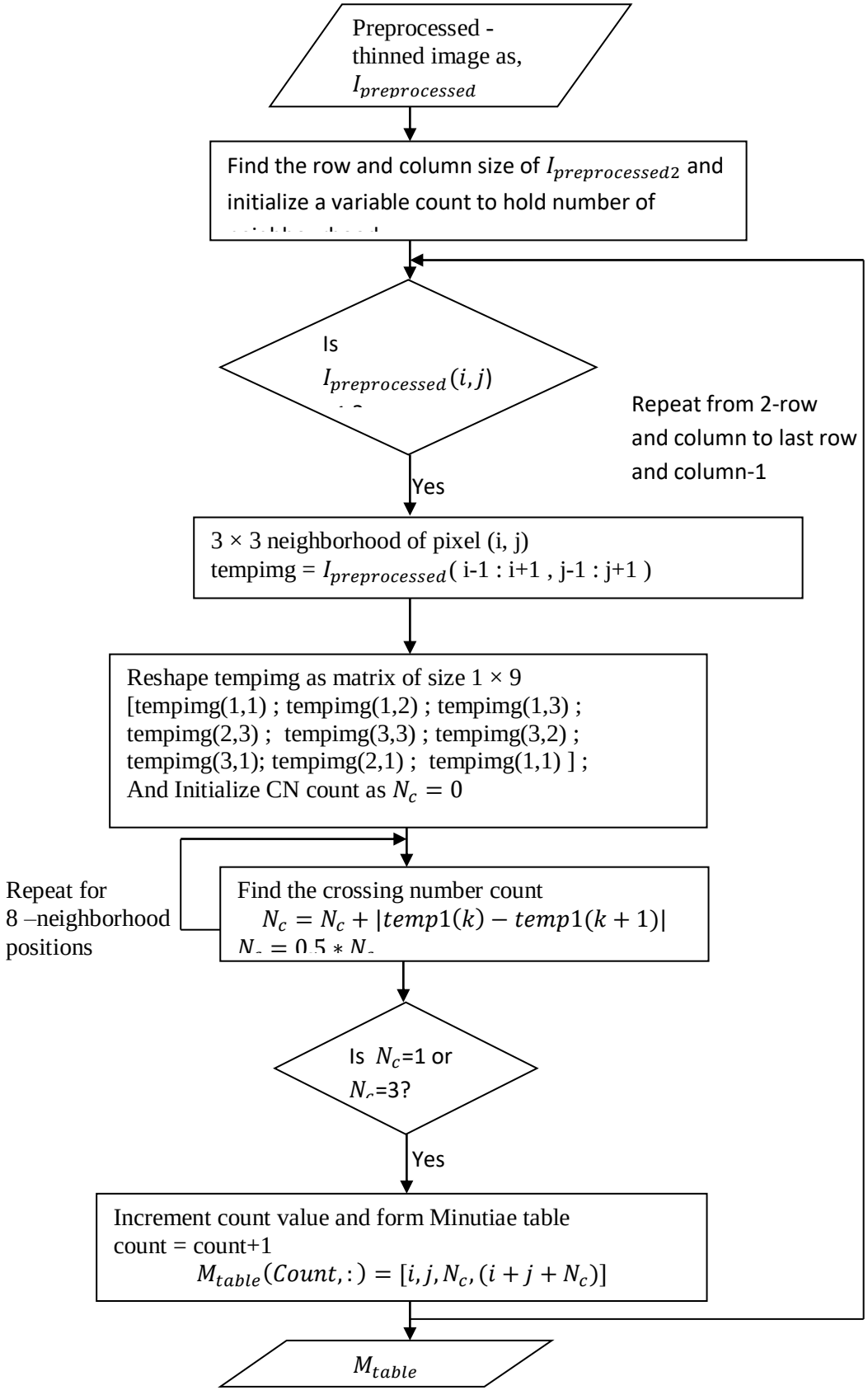


Figure 13.5: Flow chart of the Minutiae extraction based on crossing number

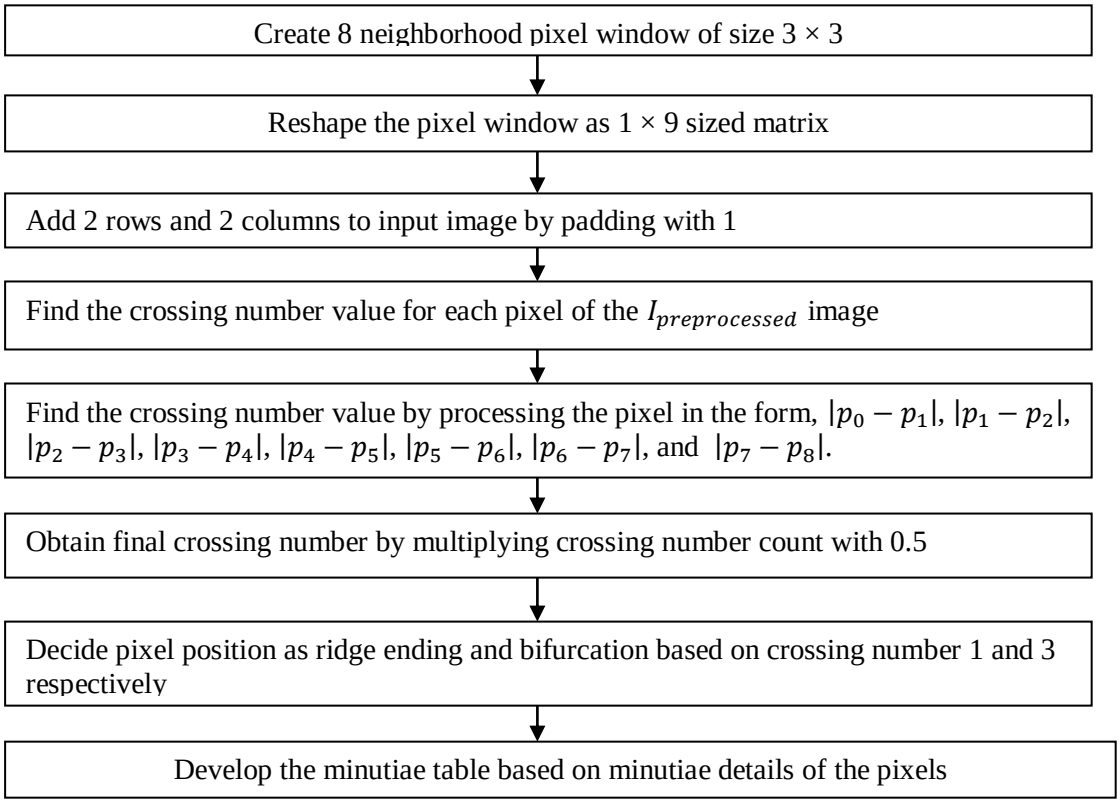


Figure 13.6: Workflow of the minutiae extraction using crossing number theory

13.4 MINUTIAE TABLE

After extracting the features from, $I_{preprocessed}$ image minutiae details are stored in Minutiae Table. This Minutiae Table contains five columns. The first column contains a serial number. The second column contains minutiae x position, third column minutiae y position and fourth ridge ending or bifurcation as code 1 or 3 and the fifth column contains the sum of a second, third and fourth column. The structure of Minutiae table is shown in Table 13.2.

Table 13.2: Structure of M_{table}

Sr. No	**Minutiae pixel 'x' position**	**Minutiae pixel 'x' position**	**Crossing number**	**Sum of 2nd, 3rd and 4th column**
1	5	86	3	94
2	15	76	3	94
3	17	106	3	126
4	18	85	3	106
5	21	49	3	73

6	21	83	3	107
7	25	57	3	85
8	25	61	3	89
9	25	99	3	127
10	46	105	1	152

This table only shows a sample value for four columns of M_{table}. Actually, an image may consist of hundreds of minutiae pixels. But in this table, only first 10 minutiae pixel details are shown.

13.5 POST PROCESSING- PROCESSING MINUTIAE TABLE

After applying fingerprint image preprocessing on raw fingerprint, which include filtering, enhancement, binarisation, and segmentation thinned image or skeleton is formed. Further skeleton or thinned image is preprocessed to remove white areas occupied by the noise. Again preprocessed thinned image is further post processed to remove some false minutiae from minutiae table and which is generated through crossing number theory. One greater reason of post processing is to reduce wide variety of minutiae points by disposing of false minutiae structures [22]. The post processing algorithm used in this study is based on [23], here w × w window neighbourhood is considered for each minutiae in minutiae table. The size of the w is calculated on the basis of following statement

w = 2d + 1, where d is considered as local ridge distance.

In this study we consider d as 1 unit. So w = 2×1+1 = 3. Average ridge distance in each region or from every pixel is usually referred as local ridge distance and it is an integer value due to round off calculation. The fingerprint image minutiae ridge ending and bifurcation is first analyzed from thinned image and in this study which is thinned preprocessed image.

The minutiae extracted through crossing number based theory may include some spurious minutiae structure, which should be eliminated to maximum extent or full with the aid of post processing the preprocessed thinned image. If 3×3 window is considered, then m along the branch of the window in all 8-directions and test whether any other ending in terms of pixel value 0→1 is not found then consider that pixel as true ridge.

Post processing Algorithm-Description

The post-processing algorithm takes three arguments as Skeleton image after preprocessing, $I_{preprocessed}$, Minutiae table, M_{table}, and window size represented as param in our study. The output of this algorithm is final Minutiae table represented as final_M_{table}. Initially, some variables are declared and initialized with some values as follows. This algorithm is explained based on window size 3 × 3.

window = param / 2

If window variable value is not an integer then round-off it. For example in this study param value is 3 means, after round off window value will be 1. Create two matrixes, Rw and Clmn, of size 3 × 1 for holding indices of nonzero elements in the matrix.

Rw = zeros (3, 1), Clmn = zeros (3, 1)

Add two rows and columns for the $I_{preprocessed}$ image by padding value 0. Next, find the total number of values or rows in M_{table}. Use a variable, count, to hold index position for final_M_{table} maxval = size (M_{table}), count =0

I_1=$I_{preprocessed}$ after padding 2 row and 2 column with value 0

Move along the minutiae table, M_{table} from 1 row or position to last row or position. Use a variable part1 of size 3 × 3 to hold pixel values of the I_1 image, corresponding to M_{table} minutiae pixel position.

part1= I_1(M_{table} (ith row) to M_{table} (ith row) + 2, M_{table} (ith column) to M_{table} (ith column) + 2) Here i, represents M_{table} index from first position to till last position.

Because we have padded 2 row and 2 column on both sides of the I_1 the minutiae pixel position occupies central position of the window. All those pixel positions which is having value 1 around the neighborhood of central pixel are referred as connected with the candidate or central pixel.

Initially part1 is multiplied by -2 so that in the window all elements which are having value 1 become, -2. Next we initialize central or candidate pixel with value -1.

partI = -2 * partI ;

partI (Window+1 , Window+1) = -1 ; // Here window value is 1 because the param value is 3. The window size is 3 × 3. So it refers in this context, candidate pixel with value, PartI (2, 2). Next again another variable is created as temppart1 with size w × w with initial value zero.

temppart1 = w × w sized matrix with initial value 0.

This temppart1 will be copied with a value of part1 and candidate pixel will be assigned with value zero.

Next find the number of connected braches of candidate pixel by identifying non-zero window element pixel position and store it on Rw and Clmn as mentioned above.

[Rw, Clmn] = find (non-zero index position of temppart1 in row and column matrix)

The above statement simply returns no of connected branches of candidate minutiae pixel.

Next, we check whether candidate pixel is minutiae ending or bifurcation. If M_{table} 3, column value 1 means its ridge ending, and 3 means ridge bifurcation, which is based on crossing number based theory.

If there exists, only one edge out of the all edges of the windows of candidate pixel, with the transition as, 0→1 and count=1, then it's considered as true ridge ending.

If the candidate pixel is ridge bifurcation then check for transition 0→1, 1→2, and 2→3, then and the count is 1 for each transition then its valid ridge bifurcation, while evaluating all edges of the candidate minutiae pixel.

Post Processing of Minutiae Table- Algorithm

Input: $I_{preprocessed2}$, M_{table}
Output: final_M_{table}
Parameters: $I_{preprocessed2}$, M_{table}, Window size (param)

1. Initialize a variable window as, window = round (param / 2) //take integer value
2. Declare a variable Rw and Clmn to holds indices of nonzero elements in the matrix, Rw(3,1) with initial value 0, Clmn (3,1) with initial value 0
3. Initialize a new image as I_1=$I_{preprocessed2}$ after padding 2 row and 2 column with value 0
4. Find the size of M_{table} as, size(M_{table}) // M_{table}-Minutiae Table
5. Initialize a variable Count to hold total number of rows of M_{table} , Count = 0
6. **for all** values of M_{table} **do**

Extract w × w sized window from I_1
Initialize a temporary variable part1 as
part1= I_1(M_{table} (ith row) to M_{table} (ith row) + 2, M_{table} (ith column) to M_{table} (ith column) + 2)
Multiply part1 by -2, Part1 = -2 * Part1
Initialize part1 candidate pixel value as -1, part1 (window+1 , window+1) = -1
Create a temporary variable as temppart1 with size w × w with initial value zero to hold window value and copy part1 to temppartI
temppart1 (param , param) dimension with value 0.
tempPart1(Window to Window+2 , Window to Window+2) = part1(Window to Window+2 , Window to Window+2)
Initialize temppart candidate pixel value to zero.
temppart1 (Window+1 , Window+1) = 0 ;
find (non-zero index position of temppart1 in row and column matrix) and assign to Rw and Clmn
Check **if** candidate pixel is ridge ending or bifurcation, if it is 1 then ridge ending, if, 3 then ridge bifurcation
if (Table(i, 3)= =1)
Create a window Test with value zero of size w× w
Test (param, param) with value 0
Find the maximum value of non-zero index position of Rw or simply Size of Rw as, Max= size (Rw)
Traverse from first position of Rw to Max or last position
for each value of Rw **do**
Check the connected branch of Part1 with candidate minutiae pixel or simply check for value, -2.
if (PartI(Rw(z) , Clmn(z)) = = -2)
Reassign Test window with value 1 Test(Rw(z) , Clmn(z)) = 1 ;
end if
end for
Check whether candidate pixel has only one connected edge or border by calling extract_ring method
borders = extract_ring (Test)

Initialize a variable to hold count for ridge ending to ensure that it has only one connected edge

T01 = 0

Traverse from first position of the border to last position minus one

for each value of border-1 **do** //all the w × w size-1 borders

Check, **if** (Borders(p)= =0) & (Borders(p+1)= 1))

increment count T01 → T01 = T01 + 1

end if

end for

Ensure that T01 has only one connected edge

Check, **if** (T01 = = 1)

Increment final_M_{table} index by one

Count = Count + 1 ;

Load candidate minutiae pixel in final_M_{table}

final_M_{table} (Count, 1) = M_{table} (i , 1) // row index of candidate pixel

final_M_{table} (Count, 2) = M_{table} (i , 2) //column index of candidate pixel

final_M_{table} (Count, 3) = M_{table} (i , 3) //type of ridge (ending or bifurcation)

final_M_{table} (Count, 4) = M_{table} (i , 4) //sum of row, column, and type of ridge

end if

else part of candidate ridge type, means bifurcation

check that candidate minutiae pixel has at least three connected branches

if size(Rw(1))>=3 && size(Clmn(1))>=3

Name first 3 connected branch with candidate minutiae pixel as 1, 2, and 3 edges or branches (Minimum 3 branches are required if its bifurcation)

Part1(Rw(1) , Clmn(1)) = 1

Part1 (Rw(2) , Clmn(2)) = 2

Part1 (Rw(3) , Clmn(3)) = 3

Assign Part1 to temporary variable Test1

Test1 = Part1

Check whether candidate pixel has three connected edge or border by calling for all three marked edges

Borders = extract_ring (Test1)

Initialize a variable to hold count for ridge bifurcation to ensure that it has exactly three connected ridges means 6 points while traversing along all connected points

T01 = 0

Traverse from first position of the border to last position minus one for marked edge-1, edge-2 and edge-3

for each value of border-1 **do** //all the w × w size-1 borders

if (Borders(p)=0) & (Borders(p+1) =1) (Borders(p) =0) & (Borders(p+1)=2) (Borders(p) =0) & (Borders(p+1) =3))

increment count T01 → T01 = T01 + 1

end if

end for

Ensure that T01 has only three connected edge

if (T01 = = 3)

Increment final_M_{table} index by one

count = count + 1
Load candidate minutiae pixel in final_M_{table}
final_M_{table} (Count, 1) = M_{table} (i , 1) // row index of //candidate pixel
final_M_{table} (Count, 2) = M_{table} (i , 2) //column index of //candidate pixel
final_M_{table} (Count, 3) = M_{table} (i , 3) //type of ridge (ending //or bifurcation)
final_M_{table} (Count, 4) = M_{table} (i , 4) //sum of row, column, //and type of ridge

else part of if (T01 = = 3)

if size(Rw(1))<3 && size(Clmn(1))<3
continue with next iteration
end if
end if
end for

Post Processing of Minutiae Table- Workflow and Flowchart

The workflow and flowchart of Postprocessing of Minutiae Table are shown in Figure 13.7 and Figure 13.8.

Analysis of Post processing Minutiae Table

Post processing of minutiae is used to eliminate false minutiae structures occurred due to spurs, ride breaks, short ridge, holes or islands, bridges, and ladders. The postprocessing Minutiae Table algorithm stores minutiae table pixels on Final minutiae table if it is only valid ending or bifurcation, after verifying against all spurious minutiae. The process of elimination or deletions of spurious minutiae are explained below [24-25].

Table 13.3 shows total number of ridge ending and ridge bifurcation pixels identified before and after post processing operation for sample images of FVC ongoing 2002 DB1_B benchmark dataset. From the Table 3, it is understood that post processing operation drastically reduces total number of pixels in final Minutiae Table. The total number of ridge bifurcation and ending pixel is depending on the structure of thinned fingerprint image. The time complexity of post processing minutiae table is Big-Oh (n).

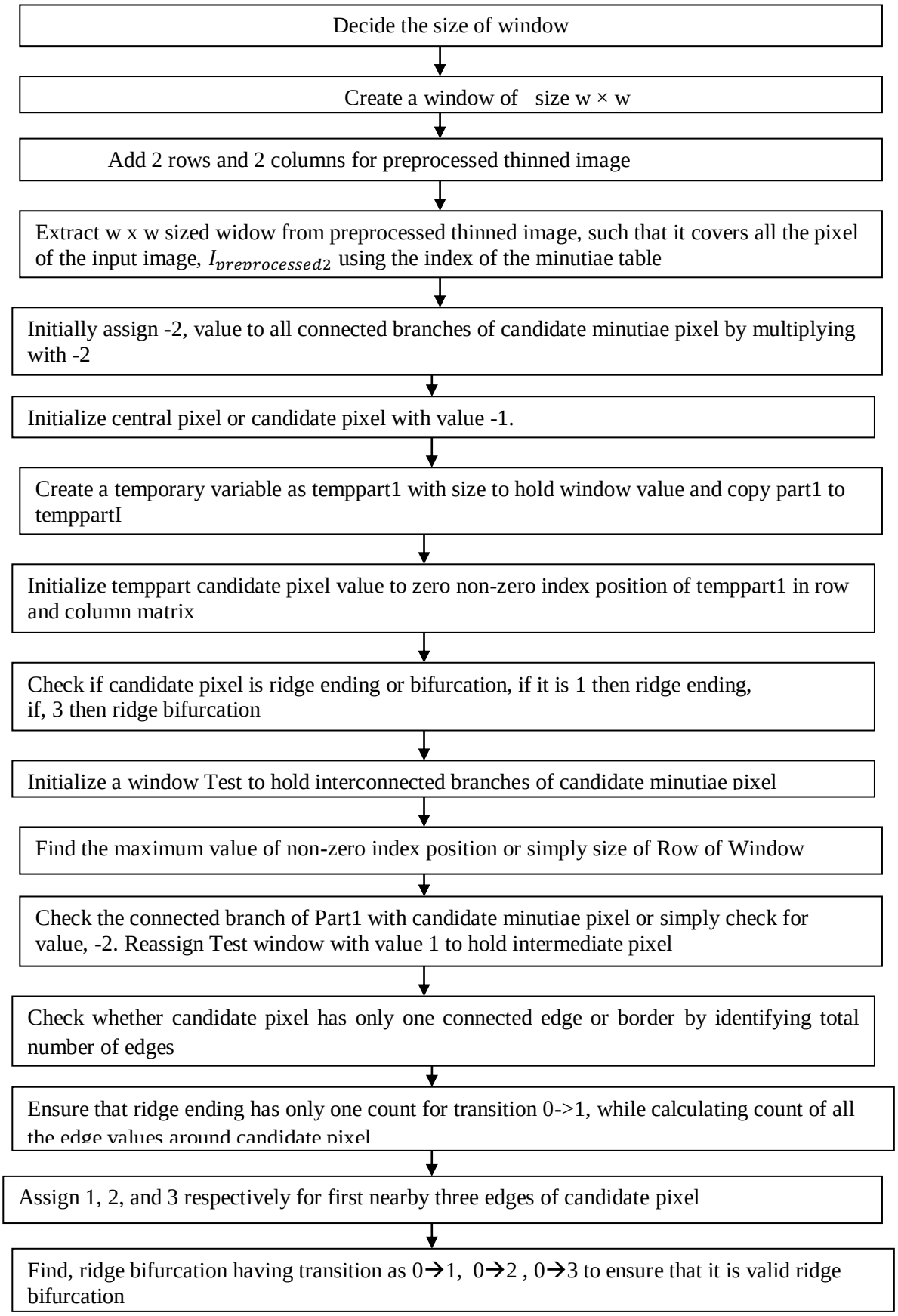
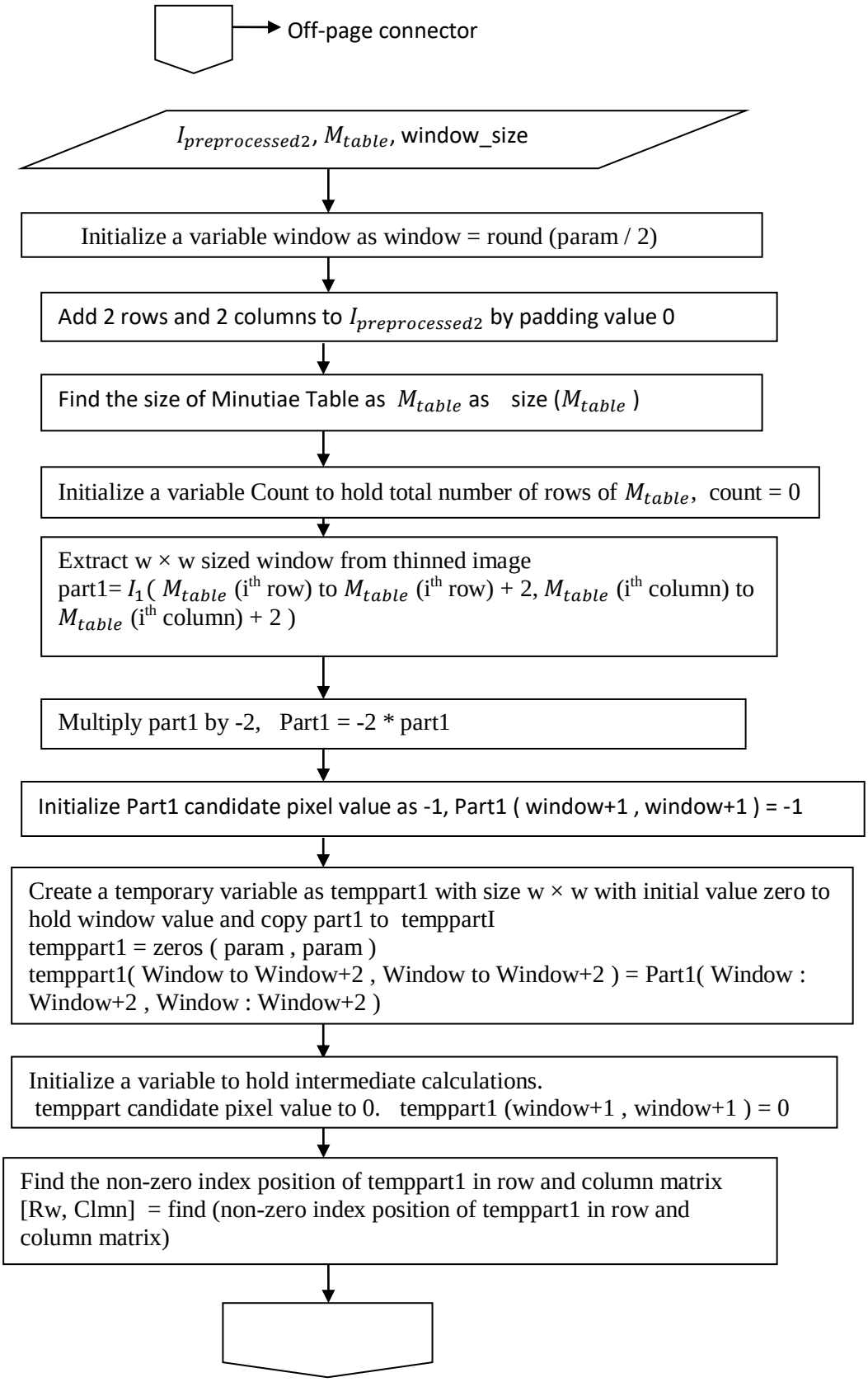
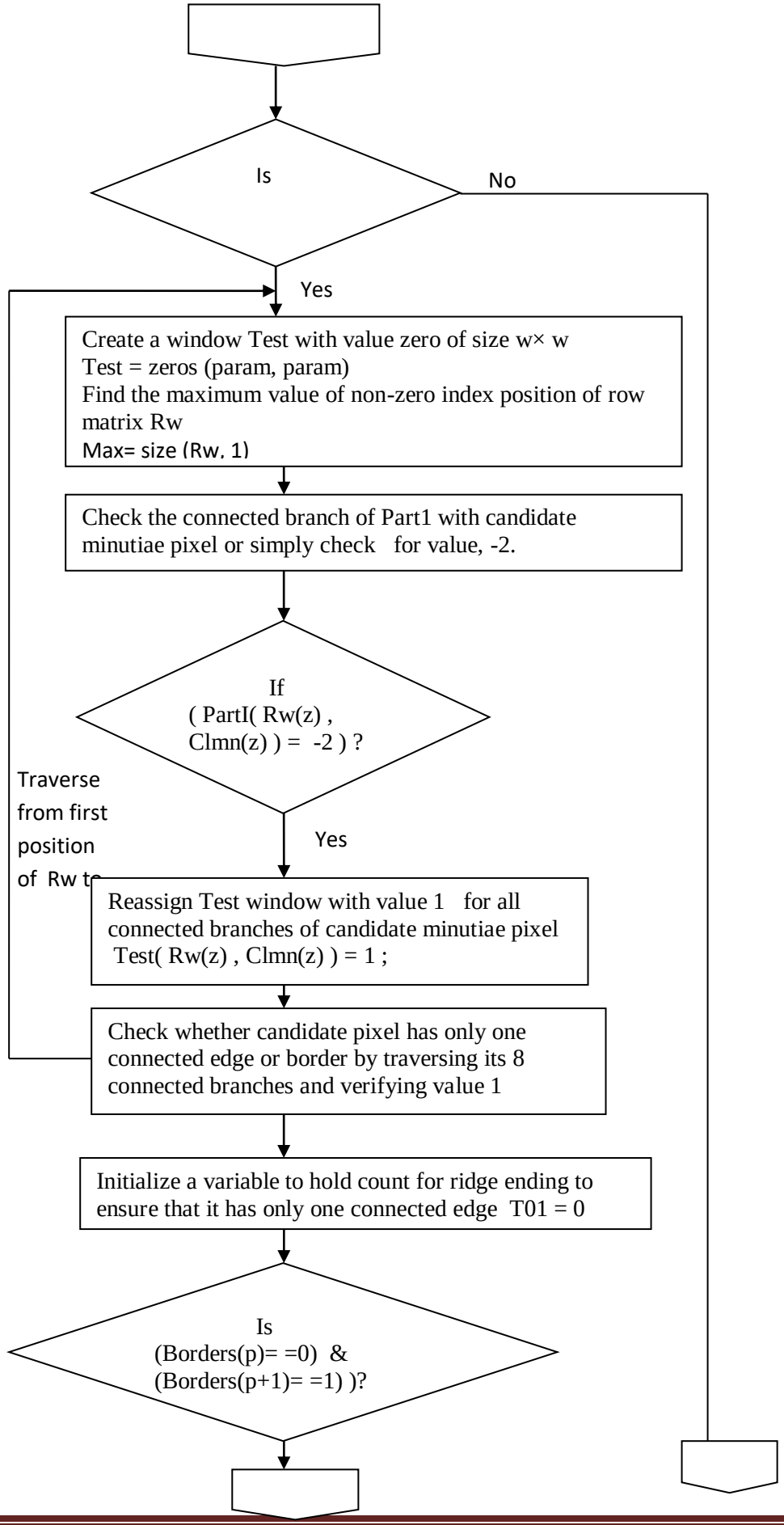
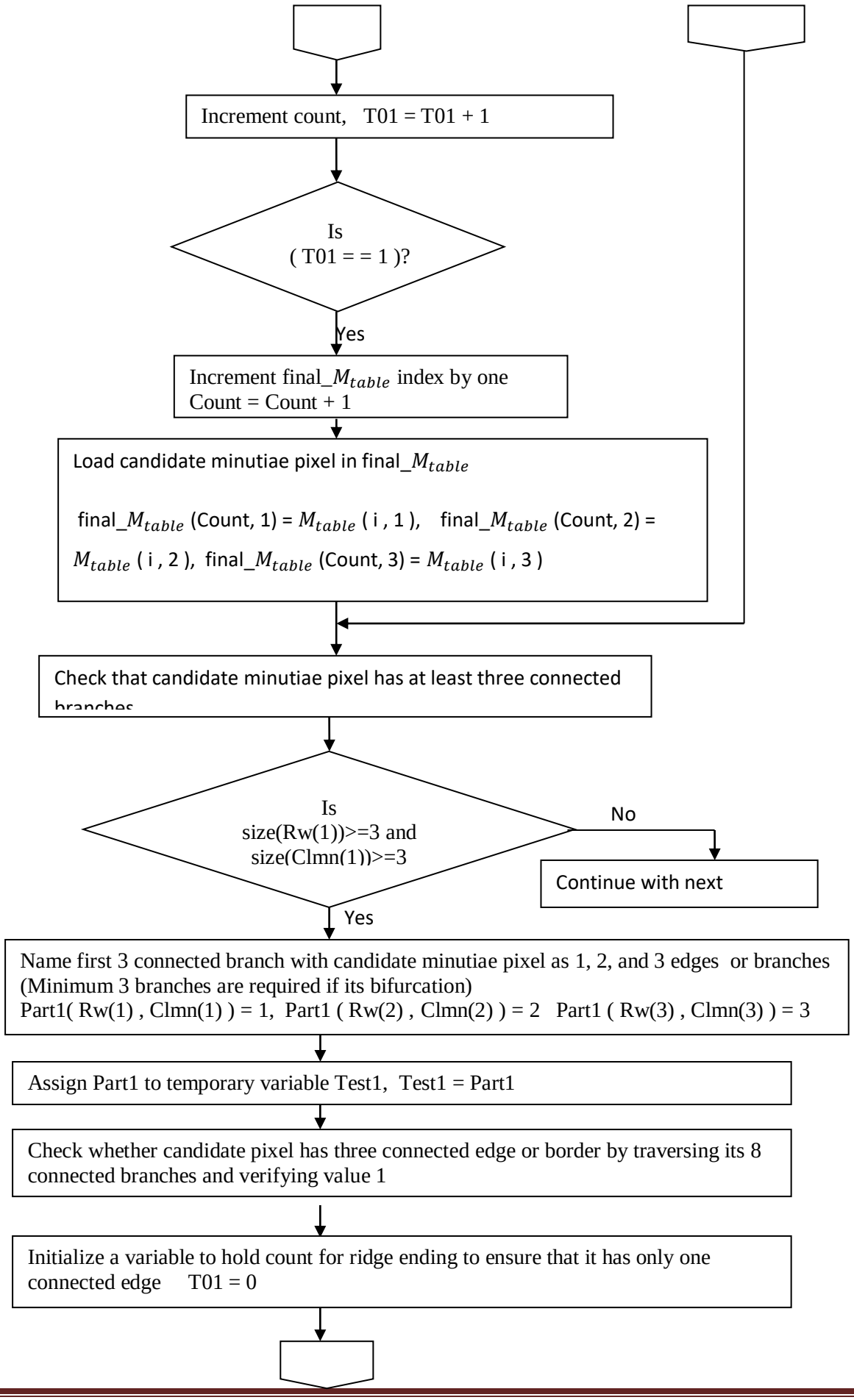


Figure 13.7: Workflow of Post Processing of Minutiae Table

The flowchart of post-processing spans across multiple pages, so flowchart symbol off-page connector are used to connect the flowchart symbols. The off-page connector is shown below.




Is
No
Yes
Create a window Test with value zero of size w× w
Test = zeros (param, param)
Find the maximum value of non-zero index position of row matrix Rw
Max= size (Rw. 1)
Check the connected branch of Part1 with candidate minutiae pixel or simply check for value, -2.
If
(PartI(Rw(z) ,
Clmn(z)) = -2) ?
Traverse from first position of Rw to
Yes
Reassign Test window with value 1 for all connected branches of candidate minutiae pixel
Test(Rw(z) , Clmn(z)) = 1 ;
Check whether candidate pixel has only one connected edge or border by traversing its 8 connected branches and verifying value 1
Initialize a variable to hold count for ridge ending to ensure that it has only one connected edge T01 = 0
Is
(Borders(p)= =0) &
(Borders(p+1)= =1))?


Increment count, T01 = T01 + 1
Is
(T01 = = 1)?
Yes
Increment final_M_{table} index by one
Count = Count + 1
Load candidate minutiae pixel in final_M_{table}
final_M_{table} (Count, 1) = M_{table} (i , 1), final_M_{table} (Count, 2) = M_{table} (i , 2), final_M_{table} (Count, 3) = M_{table} (i , 3)
Check that candidate minutiae pixel has at least three connected branches
Is
size(Rw(1))>=3 and
size(Clmn(1))>=3
No
Continue with next
Yes
Name first 3 connected branch with candidate minutiae pixel as 1, 2, and 3 edges or branches (Minimum 3 branches are required if its bifurcation)
Part1(Rw(1) , Clmn(1)) = 1, Part1 (Rw(2) , Clmn(2)) = 2 Part1 (Rw(3) , Clmn(3)) = 3
Assign Part1 to temporary variable Test1, Test1 = Part1
Check whether candidate pixel has three connected edge or border by traversing its 8 connected branches and verifying value 1
Initialize a variable to hold count for ridge ending to ensure that it has only one connected edge T01 = 0

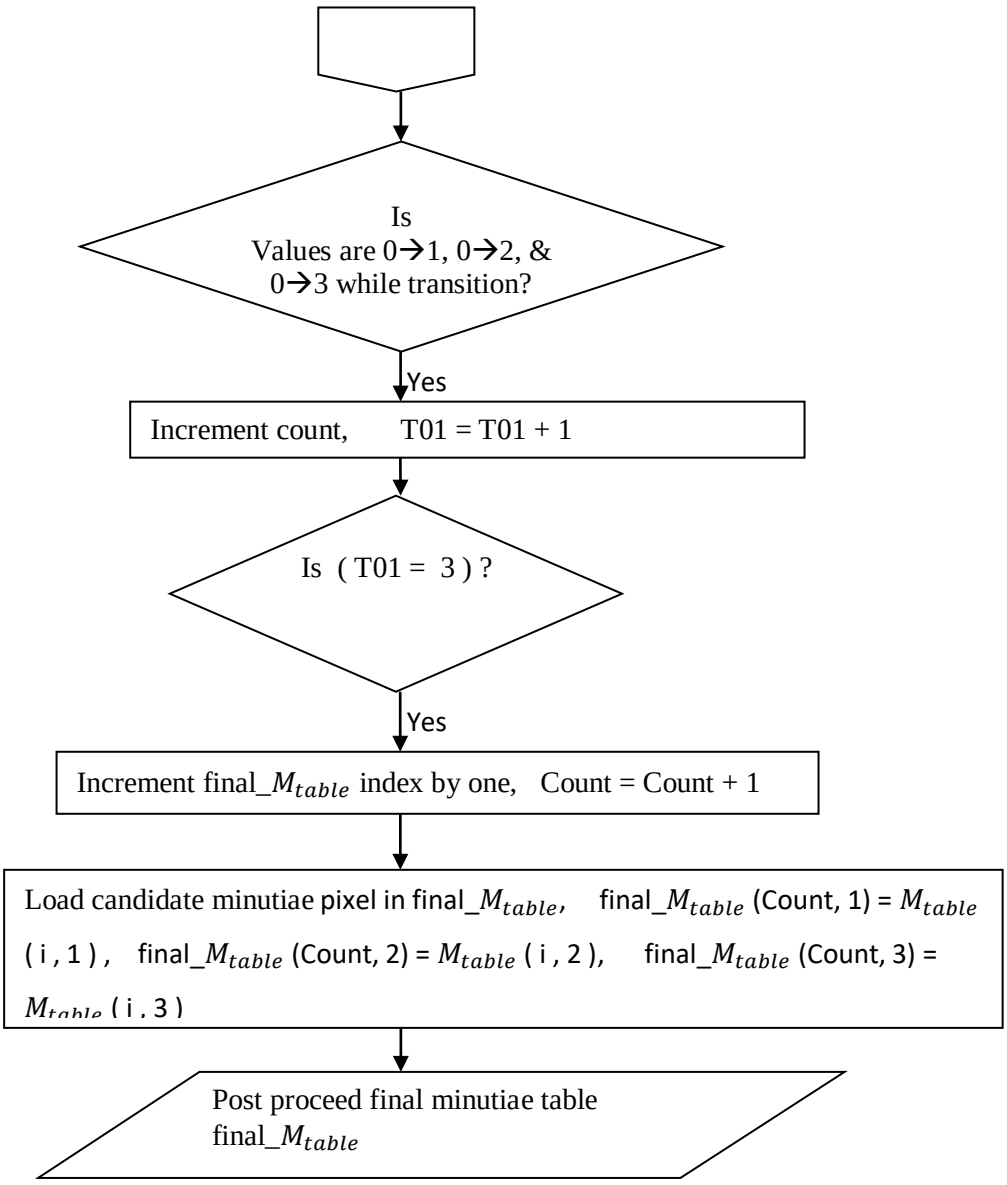


Figure 13.8: Flow chart for post processing of Minutiae Table

Table 13.3: Total number of ridge ending and bifurcation pixels before and after post processing operation

Sr. No	**Image name**	**Total number of ridge ending and bifurcation pixels before post processing operation**	**Total number of ridge ending and bifurcation pixels after post processing operation**
1	101_1	419	11
2	101_5	324	77
3	102_2	1015	55

4	103_3	623	32
5	104_4	450	52
6	104_7	811	582
7	104_8	488	02
8	105_8	829	67
9	106_6	693	54
10	109_3	819	18
11	109_8	879	26
12	110_3	666	18
13	110_8	900	23

6. APPLICATIONS OF MINUTIAE TABLE

After obtaining Final Minutiae Table, through post-processing phase, next to these minutiae details are further converted into a form which is suitable or compatible to convert into hash code. In order to convert Hash code, we can use MD5 or SHA-256 Hash algorithm. These Hash code can uniquely identify a person or can act as index key or identity key. One of the application of Minutiae Table for Hash code generation and how that Hash code can act as one of the factors in Multifactor Authentication Model is explained below [10].

Initially on the client side using an interface user loads fingerprint image into the system. At first Finger image, foreground feature is extracted from the background using segmentation Later, using Gabor filtering fingerprint image features are extracted. These features are encrypted and sent to the server. As soon as these features arrive at the server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered mobile phone user. Client system prompts a message to enter OTP, which is received to the registered mobile phone of the user. The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side. If OTP is verified, server requests for the password, the user enters the password through the client-side interface and entered password reaches to the server. The server verifies the user entered a password with the already stored password in its database. Since database password is stored in encrypted format. The password which is stored in the database in encrypted form and finger user-id hash code is encrypted one again to enhance security. So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match then a user is considered as an authenticated user. In other words authentication process successfully

completes when OTP, Password, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered as a un-authorized user. If OTP not matches then the user is blocked from further steps in the authentication process. In this research study, this is not implemented as server and client in different machines.

13.7 CONCLUSION

In Automatic Fingerprint Identification System (AFIS) preprocessing of a fingerprint play crucial role in enhancing the performance of matching and identification accuracy. After applying fingerprint image preprocessing on raw fingerprint, which includes filtering, enhancement, binarization, and segmentation thinned image or Skeletonization processes or techniques. Further skeleton or thinned image is preprocessed to remove white areas occupied by the noise. Again preprocessed thinned image is further post-processed to remove some false minutiae from minutiae table and which is generated through crossing number theory. In this paper, we have discussed preprocessing, feature extraction, and post-processing with its theory, algorithm, workflow diagram, and flowchart. The final minutiae table obtained after post-processing can be effectively used for generating Fingerprint Hash code, which can be used as index-or identity key in order to uniquely identify an individual person or as one factor in Multifactor Authentication Model.

REFERENCES

[1] K. Krishna Prasad, & Aithal, P.S., "A Critical Study on Fingerprint Image Sensing and Acquisition Technology," International Journal of Case Studies in Business, IT and Education (IJCSBE), 1(2), pp. 86-92, 2017. DOI: http://dx.doi.org/10.5281/zenodo.1130581

[2] K. Krishna Prasad, & Aithal, P.S., "A Conceptual Study on Image Enhancement Techniques for Fingerprint Images," International Journal of Applied Engineering and Management Letters (IJAEML), 1(1), pp. 63-72, 2017. DOI: http://dx.doi.org/10.5281/zenodo.831678

[3] K. Krishna Prasad, & Aithal, P.S., "Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image," International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), pp. 8-19, 2017. DOI: http://dx.doi.org/10.5281/zenodo.835608

[4] K. Krishna Prasad, & Aithal, P.S., "Fingerprint Image Segmentation: A Review of State of the Art Techniques," International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), pp. 28-39, 2017. DOI: http://dx.doi.org/10.5281/zenodo.848191

[5] K. Krishna Prasad, & Aithal, P.S., "A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization," International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), pp. 27-39, 2017. DOI: http://dx.doi.org/10.5281/zenodo.896653

[6] K. Krishna Prasad, & Aithal, P.S., "Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images," International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), pp. 51-65, 2017. DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[7] K. Krishna Prasad, & Aithal, P.S., "A conceptual Study on Fingerprint Thinning Process based on Edge Prediction," International Journal of Applied Engineering and Management Letters (IJAEML), 1(2), pp. 98-111, 2017. DOI: http://dx.doi.org/10.5281/zenodo.1067110

[8] K. Krishna Prasad, & Aithal, P.S., "A Study on Fingerprint Hash Code Generation using Euclidean Distance for Identifying a User," International Journal of Management, Technology, and Social Sciences (IJMTS), 2(2), pp. 116-126, 2017. DOI: http://doi.org/10.5281/zenodo.1133545

[9] K. Krishna Prasad, & Aithal, P.S., "An Alternative Approach to Fingerprint Hash Code Generation based on Modified Filtering Techniques**,"** International Journal of Innovative Research in Management, Engineering And Technology, 2(12), pp. 1-13, 2017. DOI: IJIRMET1602012001.

[10] K. Krishna Prasad, & Aithal, P.S., "A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP," International Journal of Advanced Trends in Engineering and Technology, 3(1), pp. 1-11, 2018. DOI: http://doi.org/10.5281/zenodo.1135255.

[11] K. Krishna Prasad, & Aithal, P.S., "A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code," International Journal of Computational Research and Development, 3(1), pp. 13-22, 2018. DOI : http://doi.org/10.5281/zenodo.1144555.

[12] K. Krishna Prasad, & Aithal, P.S., "A Comparative Study on Fingerprint Hash Code, OTP, and Password based Multifactor Authentication Model with an Ideal System and Existing Systems," International Journal and Advanced Scientific Research, 3(1), pp. 18-32, 2018. DOI: http://doi.org/10.5281/zenodo.1149587.

[13] V. Espinosa-Duro, "Mathematical Morphology approaches for fingerprint Thinning," In Proceedings of the IEEE 36th Annual 2002 International Carnahan Conference on Security Technology, pp. 43-45, 2002.

[14] M. Ahmed, & R. Ward, "A rotation invariant rule-based thinning algorithm for character recognition," In Proceedings of the IEEE Transactions on Pattern Analysis and Machine Intelligence, 24(12), pp.1672-1678, 2002.

[15] P. M Patil, S. R. Suralkar, & F. B. Sheikh, "Rotation invariant thinning algorithm to detect ridge bifurcations for fingerprint identification," In Proceedings of the IEEE 17th International Conference on In Tools with Artificial Intelligence, pp. 8, 2005.

[16] X. You, B. Fang, V. Y. Y. Tang, and J. Huang, " Multiscale approach for thinning ridges of fingerprint", in Proc. Second Iberian Conference on Pattern Recognition and Image Analysis, volume LNCS 3523, pp. 505–512, 2005.

[17] E. Newham, "The biometric report," SJB services, 733, 1995.

[18] A. A. Moenssens, Fingerprint techniques.Chilton, 1975.

[19] T. Y. Zhang, & C. Y. Suen, "A fast parallel algorithm for thinning digital patterns," *Communications of the ACM*, 27(3), pp. 236-239. 1985.

[20] C. Arcelli, & G. S. Di Baja, "A width-independent fast thinning algorithm," In Proceedings of the IEEE Transactions on Pattern Analysis and Machine Intelligence, (4), pp. 463-474, 1985.

[21] S. Kasaei, M. Deriche, & B. Boashash, "Fingerprint feature extraction using block-direction on reconstructed images". In Proceedings of the IEEE TENCON'97 Region 10

Annual Conference on Speech and Image Technologies for Computing and Telecommunications., 1, pp. 303-306, 1997.

[22] D. Maltoni, D. Maio, A. K., Jain, & S. Prabhakar, "Handbook of Fingerprint Recognition," Annals of Physics. 54, 2003.

[23] M. U. Akram, A. Tariq, S. A. Khan, & S. Nasir, "Fingerprint image: pre-and post-processing," International Journal of Biometrics, 1(1), pp. 63-80, 2008.

[24] S. Tabbone, & L. Wendling, "Multi-scale binarization of images," Pattern Recognition Letters, 24(1-3), pp. 403-411, 2003.

[25] J. Yang, L. Liu, and Y. Fan, "A modified Gabor filter design method for fingerprint image enhancement", Pattern Recognition Letter, 24(12), pp.1805–1817, 2003.

Chapter 14

ABCD ANALYSIS OF FINGERPRINT HASH CODE, PASSWORD AND OTP BASED MULTIFACTOR AUTHENTICATION MODEL

Authentication is the usage of one or multiple mechanisms to show that who you declare or claim to be. Authentication ensures that users are granted to some resources or services after verifying their identity. The essential characteristics of every authentication system are to provide high security for their users. Multifactor authentication model always improves or enhances the security compared to single-factor authentication model. This new model makes use of three factors-biometric Fingerprint Hash code, One Time Password (OTP), and Password. Fingerprints are not fully secret compare to passwords, because if passwords are leaked which can be easily revocable using another password and which is not true in case of fingerprint biometric security system. If an authentication system uses only fingerprint biometric features, it is not easy to change fingerprint, because fingerprint is static biometric, which never change much throughout the lifespan. In this paper, as per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, (5) Customer Issues, (6) Service Provider issues, and (5) Performance Evaluation matrix issues. The constituent critical elements of Multifactor Authentication model determinant issues are listed under the four constructs - advantages, benefits, constraints and disadvantages of the ABCD technique and tabulated. The analysis has brought out many critical constituent elements, which is one of the proofs for the success of the new methodology.

Keywords: Multifactor Authentication Model, Fingerprint Hash Code, ABCD analysis, Constituent Critical Elements.

14.1 INTRODUCTION

By definition, authentication is using one or multiple mechanisms to show that who you declare or claim to be. As soon as the identity of the human or machine is demonstrated, then human or machine is authorized to grant some services. Three worldwide referred authentication process are (1) Token supported authentication, (2) Biometric supported authentication, and (3) Knowledge supported authentication.

Token supported authentication makes use of key cards, bank cards, and smart cards. Token supported authentication system sometimes uses knowledge supported techniques to improve security. Biometric supported authentication strategies, together with fingerprints, iris scan and facial reputation aren't yet extensively adopted [1-2]. The essential flaws of this technique are that such systems can be costly, and the identification process may be slow and regularly unreliable. However, this form of technique presents the highest level of protection. Knowledge supported authentication is most commonly and widely used authentication technique and encompass both text-based and image-based passwords. The image-based techniques can be further subdivided into two classes: recognition-primarily based and recall based graphical techniques. The use of recognition based strategies, a person is provided with a set of images and the user is authenticated through recognizing and identifying the images, which is registered at the time of registration process. In recall based techniques it's essential that user has to reproduce something like a pattern, which is created or drawn at the time of registration process.

One time password can be generated in two forms. (1) Time-synchronized OTP: In time-synchronized OTPs the person has to enter the password within a time frame or within a stipulated time, in other words, OTP having lifespan only for few amount of time after that time it will get expired and another OTP will be generated. (2) Counter-synchronized OTP: In Counter-synchronized OTP, instead of regenerating OTP after the stipulated time, a counter variable is coordinated or synchronized between client device and server.

Automatic Fingerprint Identification System (AFIS) consists of different techniques like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [3-10]. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or readers. There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause a difference in Hash code [11-14]. Based on the different Methods of Fingerprint Hash code generation, it reveals that fingerprint hash code does not suit exclusively for authentication or security purpose. But it uniquely identifies an individual person or human being through a Hash code key.

It is well known that we can improve the performance of any system by comparing it with a hypothetical, predicted system of that kind called Ideal system [15]. The word Ideal system refers to the system which has utmost characteristics, which cannot be improved further. It is

what our mind tells ultimate and which reached the pinnacle of success in the respective field, which can be compared to all other systems of similar type, which lacks in some qualities [16]. The less-efficient system can be converted into the ideal system with the aid of research and continuous innovation in that field. Many objects we can consider as ideals like an ideal gas, ideal fluid, ideal engine, ideal switch, ideal voltage source, ideal current source, ideal semiconductor and ideal communication technology and all of these are considered as standards to improve the quality and performance of similar type. Recently many ideal systems are studied, which includes ideal business system [16], ideal education system [17-20], ideal technology system [15], ideal strategy [21], ideal energy source [22], ideal library system [23], ideal banking system [24-25], ideal software [26], ideal optical limiter [27], ideal analysis model [28] and ideal mobile banking system [29]. The ideal system of any kind can be placed in mind, while improving the characteristics of practical devices/ systems and reach ideal system or considered to be a pinnacle of success. Some of the ideal systems with respect to Authentication System are listed in Table 14.1.

Table 14.1: List of Ideal components with respect to Authentication System

Sr. No	Ideal System Components/ Characteristics	Definition of Ideal Systems Components/ Characteristics
1	Ideal Speed	The time taken by the Automatic Verification or Authentication System to authenticate the registered user.
2	Ideal Data Transfer Rate	Any amount of data can be transferred from source to destination without any delay or within null unit of time duration (In client Server Model)
3	Ideal Signaling efficiency	The quality of signal is 100% efficient in all aspects.
4	Ideal Security	100% protection of Registered user means no intruder can able to break the system anyway.
5	Ideal Availability	Service can be available any part of the world anytime.
6	Ideal Bandwidth	The volume of Information per unit of time that a system can handle is unlimited or uncountable.
7	Ideal False Acceptance Rate	The percentage of system incorrectly classifies the input pattern to an unregistered user is zero.
8	Ideal False Rejection Rate	The probability that the Authentication framework unable to identify a match between the authentic people is always zero.
9	Ideal Equal Error Rate	Acceptance and rejection mistakes are identical in the system and which is equal to zero.
10	Ideal Failure to Enroll Rate	The unsuccessful attempt made to enrol in database or template of an Automatic Fingerprint Identification System by the input is

		zero.
11	Ideal Accuracy Rate	Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high.

In this paper, a new Multifactor Authentication Model based on Fingerprint Hash Code, Password, and OTP is discussed. In this model fingerprint Hash code is used as index-key or identity key. Initially, the user loads static Fingerprint image and which is converted to Hash Code through the programme. Later time synchronized OTP is checked and verified and the last password is prompted by the server and verified by the server. Finally, the password is prompted and verified by the server. The remaining part of the paper is organized as follows. Section 2 explains about ABCD Model. Section 3 describes Multifactor Authentication model. Section 4 describes OTP generation. Section 5 describes ABCD analysis of new Multifactor Authentication Model. Section 6 identifies the critical constituent elements of these determinant factors. Section 7 concludes the paper.

14.2 ABCD ANALYSIS FRAMEWORK

Many techniques are available in the literature, to investigate the individual characteristics, system traits, and effectiveness of an idea or concept, the effectiveness of a method to know its merits and demerits and also business value in the society. The individual traits or organizational effectiveness & techniques in a given surroundings may be studied the usage of SWOT analysis, SWOC evaluation, PEST analysis, McKinsey7s framework, ICDT version, Portor's 5 force model and so on. Recently a new model is introduced to these analysis areas called ABCD analysis framework [30], which is used for analyzing business concept, business system, new technology, new model, new idea/concept etc. In the qualitative evaluation the use of ABCD framework, the new idea or new system or new strategy or new generation or new model or new concept is further analyzed studied or analyzed using critical constituent elements. In the quantitative evaluation the use of ABCD framework [31], can be used to assign appropriate score or rating for each critical constituent elements, which is calculated through empirical research. The final score is calculated and based on the score the new idea or new system or new strategy or new generation or new model or new concept can be accepted or rejected. Consequently, ABCD evaluation framework may be used as a research tool in these regions and is easy but systematic study or analyzing method is essential for business concept or systems or models or ideas or strategy evaluation [30-47].

14.3 Multifactor Authentication Model Using Fingerprint Hash Code, OTP, and Password

Figure 14.1 shows Dataflow Diagram of Multifactor Authentication model used in this study. Initially on the client side using an interface user loads fingerprint image into the system. First, using Euclidean distance fingerprint image features are extracted, which is explained in Section 3 and 4.

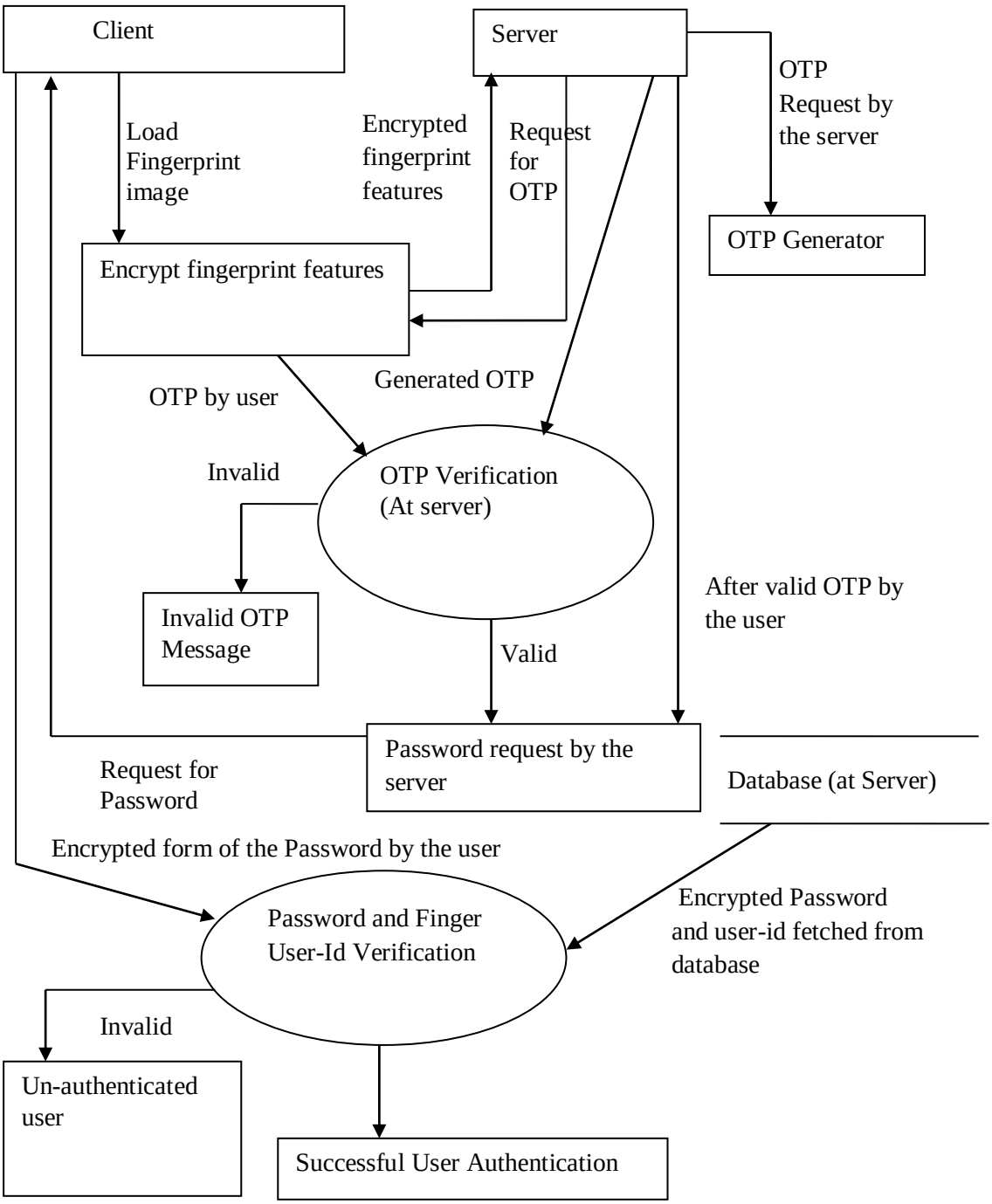


Figure 14.1: Dataflow Diagram of Proposed Multifactor Authentication

These features are encrypted and sent to the server. As soon as these features arrive at a server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered mobile phone user. Client system prompts a message to enter OTP, which is received to the registered mobile phone of the user.

The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side. If OTP is verified, server requests for the password, the user enters the password through a client-side interface and entered password reaches to the

server. The server verifies the user entered a password with the already stored password in its database. Since database password is stored in encrypted format. The password which is stored in the database in encrypted form and finger user-id hash code is encrypted one again to enhance security.

So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match them user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Password, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered an unauthorized user. If OTP not matches then the user is blocked from further steps in the authentication process. In this research study, this is not implemented as server and client in different machines. The model of this approach is implemented on the same machine using MATLAB 2015a.

14.4 ONE TIME PASSWORD GENERATOR

In this research work, One Time Password Generator is responsible for generating OTP. This is a function located on the server. In this study, Time synchronized OTP is generated by combining some features. The time for which OTP is valid is administrative specific, for simplicity we consider in this work as 2 minutes. The algorithm for generating OTP is explained below.

Algorithm:

Step-1: Generate the Hash code for input fingerprint using MD5 Hash Function.
Step-2: Extract system Date and Time.
Step-3: Extract seconds separately.
Step-4: Consider only integer part of the seconds.
Step-5: A 4 × 4 sized matrices of the random number is generated.
Step-6: Date and Time are converted into string data type.
Step-7: Random matrix is concatenated with Date and Time string.
Step-8: Hash code of the input fingerprint image is concatenated with result of Step-7.
Step-9: Hash code is generated for combined string obtained from Step-8.
Step-10: A random number is generated between1 to 32.
Step-11: If the random number is in between 1 to 8 (including both) then extracts first 8 characters of the Hash code of size 32 characters generated in Step-8.
Step-12: If the random number is in between 9 to 16 (including both) then extract next 8 characters (from position 9 to 16) of the Hash code of size 32 characters generated in Step-8.
Step-13: If the random number is in between 17 to 24 (including both) then extract next 8 characters from position 17 to 24) of the Hash code of size 32 characters generated in Step-8.
Step 14: If the random number is in between 24 to 32 (including both) then extract next 8 characters from position 24 to 32) of the Hash code of size 32 characters generated in Step-8.

14.5 ABCD ANALYSIS OF MULTIFACTOR AUTHENTICATION MODEL

Multifactor Authentication Model used in this research work can be analyzed using ABCD Analysis Aithal, P. S. et. al., (2015), proposed ABCD analyzing framework to analyze a new model to observe and understand its effectiveness in imparting value to its stakeholders. The

ABCD analysis effects in an organized listing of Business or new Model with advantages, Benefits, constraints, and disadvantages in a systematic way or form. The complete framework is divided into various issues, the area which new model is focused. Various key properties and affecting the area of the new model may be identified and analyzed under each area of issues identified before.

Later some of the critical constituent element for each identified issue is recognized and analyzed and which is shown in Figure 2. This method of analysis is simple and also offers a guideline to identify and examine the effectiveness of the new model in this context. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, (5) Customer Issues, (6) Service Provider issues, and (5) Performance Evaluation matrix issues.

(1) Security Issues

Security is very important in the Authentication process. An ideal security refers that a system which is impossible for an intruder to break or impossible for the unregistered user to access the system. In the Authentication process, security refers safeguarding the user personal data used for the authentication process, which includes, Fingerprint Hash code, Password, One Time Password (OTP). The affecting factors of Security issues include Fingerprint Hash code, Password, and OTP under key properties or levels like user level, network level, and Database or template level are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(2) User-friendly Issues

The user-friendliness of Multifactor Authentication Model signifies that user should able to get access to the system effortless or easily without remembering anything or very minimum amount of data. The affecting factors under key properties like Response time, Access time, Automatic Process, Speed, and Availability are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(3) Input Issues

Input ensures that registered user should able to get access to the system or authenticated with very less or no input or automatically. The affecting factors under key properties like Minimum Possession, Least input, Input Selectivity, Ubiquitous Data, Reliability, Usability, Efficiency, Input security and execution time are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(4) Process Issues

Process Issues ensures that user should able to complete authentication process without any fault, fast and completely. The affecting factors under key properties like Atomicity, Consistency, Isolation, Availability, effort free, and High durability are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

(5) Performance Evaluation matrix issues refer all the performance evaluation matrices normally used for the authentication system. The affecting factors under key properties like False Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to enroll rate, Accuracy Rate, and Execution are determinant factors under the constructs Advantages, Benefits, Constraints, and Disadvantages of the new model.

Each determinant issue has sub-issues called key attributes used for analyzing the advantages, benefits, constraints and disadvantages, the four constructs of the framework.

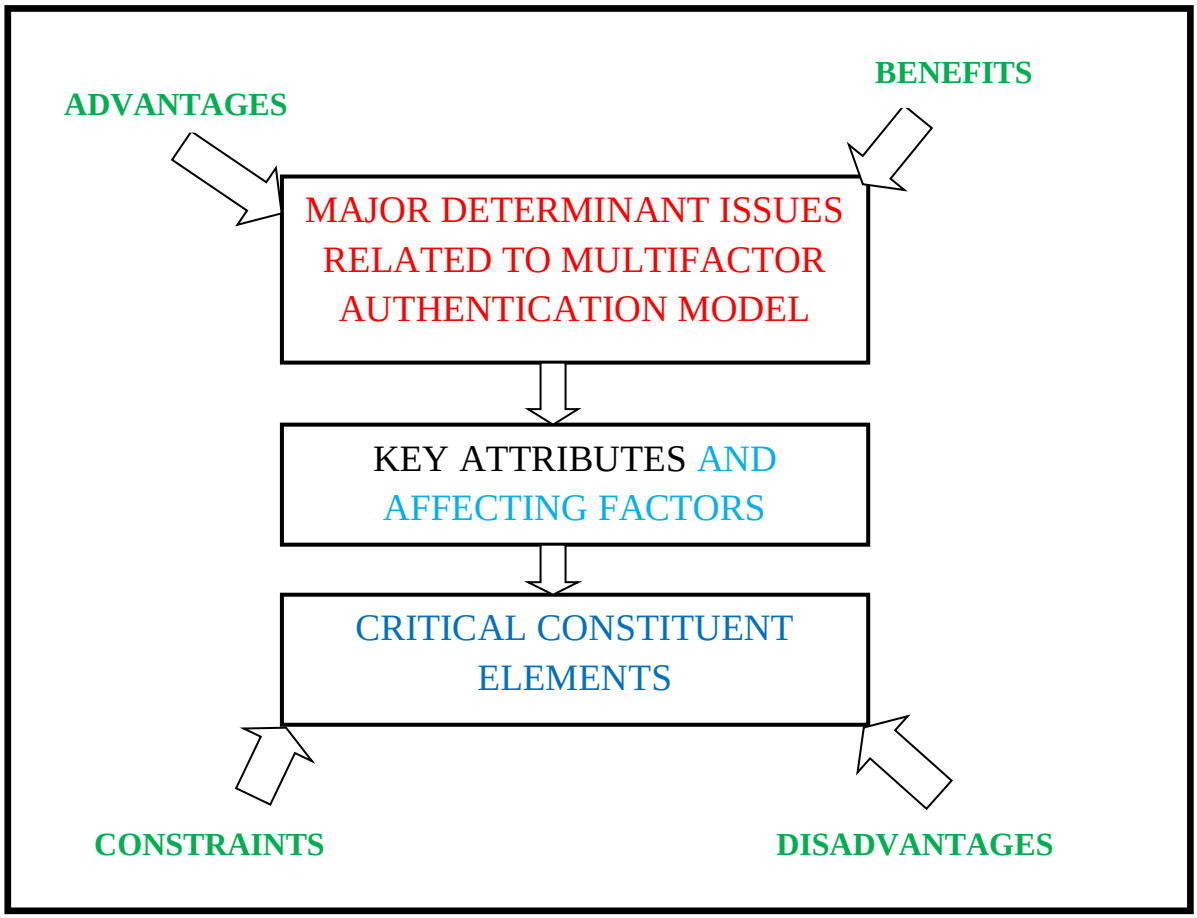


Figure 2: Block diagram of Issues affecting the Fingerprint Hash code, Password, OTP based Multifactor Authentication Model

The factors affecting the various determinant issues of Multifactor Authentication Model for each key attributes under four constructs are derived by a qualitative data collection instrument namely, focus group method and are listed in Table 14.2.

Table 14.2: Analysis of Fingerprint Hash code, Password, and OTP-Multifactor Authentication Model for Verification purpose

Determinant Issues	Key Attributes	Advantages	Benefits	Constraints	Disadvantages
Security Issues	User level security (For	Easy to secure using personal devices like	increases demand Cloud Drive,	High Security of the Cloud	Acceptance by the user

	Biometric Image-Hash code)	mobile phone, Laptop, USB drive, and private cloud drive	Mobile, Pen drive, and laptop	Drive, USB device, Laptop, and Mobile Phone is questionable	
	Network Level Security	Non-reversible, Non-Revocable Hash code,	Customer faith increases Can attract new customer	tampering of data	Network failure due to some uncontrollable circumstances
	Database or Template Security	Single Hash value is used for comparing, Non revertible Hash code	Efficient memory use, Database is easily manageable	Database table requires values in Hash form	Database failure, Server failure
User-friendly Issues	Response time	Increased rate of growth of authentication process	Increased customer pool	Requires high configuratio n system and efficient algorithms	Hardware and Software cost
	Access time	User Instantaneous authentication	Reduced Queuing, Reduced waiting process	Requires good network, memory, and processor	Hardware and software cost
	Speed	Increased Authentication request per unit time	Increased customer satisfaction, retention and acquiring new customers becomes easy	Requires high configured system and reduced time complexity	Hardware and software cost, High bandwidth network,
	Automatic process	Minimum prior information of the system required	Increased customer satisfaction,	Ability to make difference between registered and unregistered user,	Utilization of the hardware and software resources are too high complex backend design of user

				processing power	interface
	Availability	Ubiquitous authentication	Reduced request queue	Dedicated server and network	24 × 7 working server
Input Issues	Minimum Possession	minimum knowledge parameters required for authentication	User get authenticated anywhere without carrying anything	Capacity of the system to differentiate between registered user and intruder with minimum data	Lack of information
	Minimum input	Simple User authentication from customer point of view	Reduced I/O operation	Requirement of unique and robust parameter for user Authenticati on	Lack of information
	Input Selectivity	Reduced error in inputting	Increased Customer comfort and satisfaction	User ability to identify correct image	Negligence of the user in selection of input
	Ubiquitous input	Ubiquitous Authentication process	Increased user satisfaction	Requirement of high configuratio n system and network availability	Misuse of Authentication system, More intruder will try to break the system
	Reliability	Improved consistency of the system	Improved user satisfaction	Operating cost	Significant startup and Maintenance cost
	Usability	One parameter for multipurpose like fingerprint image	Reduced parameter requirement for authenticatio n	The ability of the software to make distinction between different context of	Intruder or un-registered user tries to get multipurpose parameter used in the authentication process.

				the same parameter	
	Efficiency	Increased number of requests	Accurate results, error-free output	Quality of the input	Inability to handle error-prone or partial input
	Security	User personal data protection	Trust and faith over system increases	Uniqueness, permanence, Universality, and revocability	Cost of the system becomes high.
	Execution time	Increased growth rate in authentication	Trust and faith over system increases	Requires good time and space complexity algorithm	Requirement of Good configuration system increases cost
Process Issues	Atomicity	Authentication process Rollback or Commit at the time of system failure	Authentication failure is very rare or practically zero.	Need of good fault tolerance techniques.	Requires separate programme for database protection /safeguards
	Consistency	Ensures consistent state at the time of system failure	Authentication process ensures consistency,	Need of good fault tolerance techniques.	Database management and safe guarding requires extra efforts and cost
	Isolation	Authentication process gets isolation property	Enhanced user trust and satisfaction	Need for good lock-based concurrency control system	Database management and lock-based concurrency control requires extra cost
	Availability	Ubiquitous authentication	Reduced request queue	Dedicated server and network	24 × 7 working server
	Effort free	User freely and easily interacts with authentication system	User enjoys working with system, Increased user trust, and satisfaction	Requires navigational and narrative user interface, Input should	Complex design of user interface and programme increases cost

				be selective rather than enter	
	Durability	Changed Password and Biometric-ID durable for long time	Revocability can be done easily, if password or finger-id is compromised	Need of good fault tolerance techniques.	Database management and safeguarding requires extra efforts and cost
Performance Evaluation matrix issues	False acceptance rate	The ability of the system to differentiate registered and the unregistered user can be tested.	Improved biometric matching and identification rate	The fingerprint unique property	Not useful to identify the performance of non-biometric factors.
	False Rejection Rate	Ability of Authentication system to identify registered user can be improved	Biometric Matching rate and registered user identification can be improved	Unique fingerprint feature should be used for registered user identification	Not useful to identify performance of non-biometric factors
	Equal Error Rate	Ability of Authentication system to identify rejection and acceptance rate can be easily studied	Biometric Matching rate, registered user, and un-registered user identification error can be improved	Unique fingerprint feature should be used for registered and unregistered user identification	Not useful to identify performance of non-biometric factors like password
	Failure to enroll rate	The capacity of the authentication system in identifying person when some specific features are	Biometric matching rate, enroll rate failure can be improved	Sophisticated feature enhancement techniques are essential	Not useful to identify performance of non-biometric factors

		missing can be studied easily			
	Accuracy Rate	The overall matching performance and accuracy can be easily studied	Overall quality of matching can be studied, analyzed, and improved	Sophisticated filtering, feature enhancement techniques are essential Good false rejection and acceptance rate are compulsory	Not useful to identify performance of non-biometric factors
	Execution time	The rate of users get authenticated increases per unit time.	Trust and faith over system increases	Requires good time and space complexity algorithm	Requirement of Good configuration system increases cost

14.6 Critical Constituent Elements as per ABCD Model

The important constituent factors of determinant issues are listed beneath the four constructs - advantages, benefits, constraints and disadvantages of the ABC model and tabulated in Tables 14.3 to14. 6.

Table 14.3: Advantages of Multifactor Authentication Model for Verification purpose

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	Mobile/Smart Phone	Structure of locking pattern
			Password strength
		USB-pen Drive	Password strength of third-party software
			Usage of USB (Public/ Private)
		Laptop	Password strength
		Private cloud drive	Security strength of cloud drive
			Accessibility strength of image by programme/software
		Non-reversible Hash code in network level	Strength of cryptographic programs/ Hash code in network level
		Revocable Hash code	Ability or how fast the system having capacity to change password and finger-id, when compromised

		Non-reversible Hash code in network level	Strength of cryptographic programs/ Hash code in template level
2	User-friendly issues	Increased rate of growth of authentication process	Conversion time required to convert fingerprint image to hash-id
			Time required for fetching password and decrypting
			Network speed for OTP
			Speed of Matching function
		Increased Authentication request per unit time	Ability of concurrent authentication
			Efficiency of Hash code matching rate
		Minimum prior information of the system required	The ability of the system to authenticate without prompting anything or with minimum input (only by selection or automatic)
		Ubiquitous authentication in user-friendly issue	The system used for authentication
			Availability of network
3	Input Issue	Minimum Knowledge parameters	The ability of the system to authenticate without prompting or without accepting more input from the user. (only password)
		Simple User authentication from customer point of view	Number of Input
			Narration used in the interface
		Reduced error in inputting	The way the input are provided to the system (Selection rather than entering)
		Ubiquitous Authentication process in input	The device used for authentication process
			Availability of network
		Consistency of the system	Reliability of the system
			The working efficiency of the system
		Multipurpose parameter	The ability of the unique fingerprint features to make different actions in different instances
		Increased number of requests	The execution time of the system
			Features or quality of input
		User personal data	Security mechanisms used in

		protection	authentication process
			Security used for protecting input
		Increased growth rate in authentication due to input	The structure of the input
			Execution time of the algorithm used (time complexity)
4	Process Issues	Authentication process Rollback or Commit at the time of system failure	Strength of RDBMS
			RDBMS transaction atomicity property
		Ensures consistent state at the time of system failure	Strength of RDBMS
			RDBMS transaction consistent property
		Authentication process gets isolation property	Strength of RDBMS
		Ubiquitous authentication in process issue	RDBMS transaction atomicity property
			The device used for authentication process
			Availability of network
		User freely and easily interacts with authentication system	Simple user interface
			Navigational and narrative interface
		Changed Password and Biometric-ID durable for a long time	Management and maintenance of Database
			Safeguarding of database
5	Performance Evaluation matrix issues	The Ability of the system to differentiate registered and the unregistered user can be tested.	The fingerprint image unique feature
			Quality of the fingerprint image
			False Acceptance Rate
		The Ability of Authentication system to identify registered user can be improved	The fingerprint image unique feature
			Quality of the fingerprint image
			False Rejection Rate
		The Ability of Authentication system to identify, reject and accept a fingerprint image can be easily studied	The fingerprint image unique feature
			Quality of fingerprint image
			Difference between Acceptance and Rejection Rate
		The capacity of the authentication system in identifying person when some specific features are missing can be studied easily	The fingerprint image unique feature
			Quality of the fingerprint image
			Ability of the system to convert hash code from partial fingerprint image

		The overall matching performance and accuracy can be easily studied	The fingerprint image unique feature
			Quality of the fingerprint image
			Rejection rate
			Acceptance rate
		Increased growth rate in authentication due to performance issue	The structure of the input
			Execution time of the algorithm used (time complexity)

Table 14.4: Benefits of Multifactor Authentication Model for Verification purpose

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	Increases demand Cloud Drive, Mobile, Pen drive, and laptop	Usage of cloud drive for authentication process
			Usage of mobile phone for authentication process
			Usage of pen drive for authentication process
			Usage of Laptop for authentication process
		Increased customer faith and attracts new customer	Security in all aspects of network
			Simple and easy way to input
			Time is taken for authentication process
		Efficient memory use, Database is easily manageable	One hash code for comparison and matching
			Cryptographically Encrypted Hash code
			Non reversible Hash code
2	User-friendly issues	Increased customer pool	Quality of multifactor authentication model
			Response time
			Simple method of inputting
			Speed of authentication process
		Reduced Queuing and Reduced waiting process	Good access time
			Simple method of inputting
			Speed of authentication process
		Increased customer satisfaction, retention and acquiring new customers becomes easy	Good Access time
			Good Response time
			Simple method of inputting
			Speed of authentication process

		Increased customer satisfaction,	Automatic process
			Good Access time
			Good Response time
			Simple method of inputting
			Speed of authentication process
3	Input Issue	Ubiquitous authentication with minimum possesition of data	The device used for authentication process
			Availability of network
		Reduced I/O operation	Minimum number of input
			Quality of input
		Increased Customer comfort and satisfaction	Automatic process
			Selection input method
			Good Response time
			Simple method of inputting
			Speed of authentication process
		Reduced parameter requirement for authentication	Multipurpose usability of single input
			Type of input
		Accurate results, error free output	Reliability of the system
			Efficiency of the input
			Quality of input
		Trust and faith over system increases	Increased security
			Increased execution time
			Reliability of the system
			Efficiency of the input
			Type and quality of input
			Security used for protecting input
4	Process Issues	Authentication failure is very rare or practically zero.	Strength of RDBMS
			RDBMS transaction atomicity property
			Ability of the system to handle crashes or failures
		Ensures a safe state at the time of system failure	Strength of RDBMS
			RDBMS transaction consistent property
			Ability of the system to handle crashes or failures
		Enhanced user trust and satisfaction	Strength of RDBMS
			RDBMS transaction atomicity property
			Protected and private authentication process

			Isolation transaction property of DBMS
		Reduced request queue	Availability of authentication system
			Availability of network
			Speed of authentication
		Increased user trust, happiness, and satisfaction	Simple user interface
			Navigational and narrative interface
			Speed of authentication
			Effort free input and process
		Revocability can be done easily if password or Finger-id is compromised	Fast fingerprint-id change option
			Fast password change option
			Hash code representation of fingerprint features and password
5	Performance Evaluation matrix issues	Improved biometric matching and identification rate	The fingerprint image unique feature
			Quality of the fingerprint image
			Ideal false acceptance rate or simply zero.
		Biometric Matching rate and registered user identification can be improved	The fingerprint image unique feature
			Quality of the fingerprint image
			Ideal False Rejection Rate or simply zero
		Biometric Matching rate, registered user, and un-registered user identification error can be improved.	The fingerprint image unique feature
			Quality of fingerprint image
			Ideal Difference between Acceptance and Rejection Rate
		Biometric matching rate, enrol rate failure can be improved	The fingerprint image unique feature
			Quality of the fingerprint image
			The capacity of the system to generate Hash code when partial minutiae details are present in fingerprint image.
		Overall quality of matching can be studied, analyzed, and improved	The fingerprint image unique feature
			Quality of the fingerprint image
			Rejection rate
			Acceptance rate
		Trust and faith over system	The structure of the input

		increases	Execution time of the algorithm used (time complexity)
			Over performance of the system

Table 14.5: Constraints of Multifactor Authentication Model for Verification purpose

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	High Security of the Cloud Drive, USB device, Laptop and Mobile Phone is questionable	Security architecture used in Cloud Drive
			Third party software security architecture used in USB devices
			Password strength used in Laptop login process
			Mobile phone pattern lock rigid structure and strength of password
		Good network architecture	Connectivity and security
			Redundancy
			Standardisation
			Disaster recovery
			Growth
		Cryptographically Hash representation of fingerprint image	The fingerprint feature used for Hash code generation
			The strength of Hash code.
			The rate of difficulty for decrypting Hash code.
2	User friendly issues	Requires high configuration system and efficient algorithms	RAM size
			OS and its architecture (32bit 0r 64-bit)
			Processor used
			Single processor/ Multiprocessor
			Clock speed
			Time and space complexity of algorithms used.
		Ability to make difference between registered and un-registered user and Processing power	The features used for identification purpose
			RAM size
			Processor used, Clock speed
			Single processor/ Multiprocessor
			Time and space complexity of algorithms used.
		Dedicated server and network in user-friendly	All the features of server required for efficiency

		issue	All the features of network required for efficiency
3	Input Issue	Capacity of the system to differentiate between registered user and intruder with minimum data	The quality of input
			The features used for identification
			All the features of high end configuration system
		Requirement of unique and robust parameter for user Authentication	The quality of input
			The features used for identification
			The salting process used in Hash generation
		User ability to identify correct image	The input selected through selection
			Understandability level of the user
		Operating cost	Cost of the high-end processor
			Cost of the Authentication system
		The ability of the software to make distinction between different context of the same parameter	The feature selected for multipurpose
			The strength of software
			Quality of input
		Quality of the input	Number of minutiae details in fingerprint image
			The correctness of the OTP
			Right password
		Uniqueness, permanence, Universality, and revocability	The features used for generating Hash code
			The database quality to achieve all template protection characteristics
4	Process Issues	Need of good fault tolerance techniques.	Strength of RDBMS
			RDBMS transaction's atomicity, consistency, and isolation property
			The fault tolerance technique used in RDBMS.
			The strength of lock based concurrency control used in RDBMS
		Dedicated server and	All the features of server required

		network	for efficiency
			All the features of network required for efficiency
		Requires navigational and narrative user interface Input should be selective rather than entering	Te explanation displayed in user interface
			Navigational control used in interface
			Input type (selection rather than entering)
5	Performance Evaluation matrix issues	The fingerprint unique property used for identification/Matching	Features used to generate Hash code.
			Quality of Hash code
			The stored Hash code in Database
		Requires good time and space complexity algorithm	The algorithm used for Hash code
			Memory utilized by the algorithm
			Configuration of the system used for authentication

Table 14.6: Disadvantages of Multifactor Authentication Model for Verification purpose

Sl. No	Issue	Factors affecting	Critical Constituent Elements
1	Security Issues	User level security acceptance by the user	Security architecture used in Cloud Drive, UDB drive, Laptop and mobile.
			Inconvenience in handling these drives
			Security aspect is questionable in third party software
		Network failure	Single point of failure in hardware
			Power problems or issues
			Routing problems
			Human error
		Tampering of data	Un-authorized access to data
			Network failure
		Database failure or server failure	Hardware failure
			File corruption
			File system damage
2	User friendly issues	Hardware and software cost	Cost of RAM
			Cost of Processor

			Cost of the computer system
			OS cost
			Authentication system cost
		Network cost	Bandwidth cost
			Data cost
		High utilization of hardware and software	High utilization of memory and processor
			Space and time complexity
		Complex backend design of interface	To design simple user interface for user
		24 × 7 service	High utilization of processor, and memory
			More power consumption
3	Input Issue	Lack of information	Only fingerprint image are selected
			User personal details are not taken by the system.
		Negligence of the user in selection of input	Lack of concentration of the user
		Misuse of authentication system / More intruder will try to break the system	Continuous availability of the system.
		Significant startup and Maintenance cost	Cost of the high-end processor
			Cost of the Authentication system
		Intruder or un-registered user tries to get multipurpose parameter	Continuous availability of the system.
			Usability of the parameter
		Inability to handle error prone or partial input	Minutiae details are fully missing
4	Process Issues	Requires separate programme for database protection/safeguards	Management of the database
			Essentiality of the Database protection
		Requires lock based concurrency control system	For acquiring isolation property of the database transaction
		Continuous availability of the server increases cost	Requirement of Ubiquitous availability of the server
			Requirement of efficiency of the system
		Complex design of user interface and programme increases cost	Requirement of effort-free authentication process

5	Performance Evaluation matrix issues	Acceptance rate, Rejection rate, Equal error rate, failure to enrol rate, accuracy only used for biometric performance evaluation	Performance evaluation matrices of biometrics data

14.7 CONCLUSION

We have studied the Multifactor Authentication Model based on Fingerprint Hash Code, Password, and OTP using ABCD analysis framework. As per ABCD analysis various determinant issues related to Multifactor Authentication Model for Verification/Authentication purpose are: (1) Security issues, (2) User-friendly issues, (3) Input issues, (4) Process issues, (5) Customer Issues, (6) Service Provider issues, and (5) Performance Evaluation matrix issues. The analysis identified the affecting factors for various determinant issues under four constructs advantages, benefits, constraints, and disadvantages. The analysis shows that new model gives good security at network and database level. The Hash code is no reversible and also minimum numbers of input are used for the authentication process.

REFERENCES

[1] Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image Authentication. *Journal of Computer Science and Information Technology*, *7*, 195-206.

[2] M'raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). *Hotp: An hmac-based one-time password algorithm* (No. RFC 4226).

[3] Krishna Prasad, K., & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 86-92. DOI: http://dx.doi.org/10.5281/zenodo.1130581.

[4] Krishna Prasad, K., & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[5] Krishna Prasad, K., & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608.

[6] Krishna Prasad, K., & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[7] Krishna Prasad, K., & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[8] Krishna Prasad, K., & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied*

Engineering and Management Letters (IJAEML), 1(2), 51-65. DOI: http://dx.doi.org/10.5281/zenodo.1037627.
[9] Krishna Prasad, K., & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 98-111. DOI: http://dx.doi.org/10.5281/zenodo.1067110
[10] Krishna Prasad, K., & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 116-126. DOI : http://doi.org/10.5281/zenodo.1133545.
[11] Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. *International Journal of Advanced Trends in Engineering and Technology*, 3(1), 1-11. DOI : http://doi.org/10.5281/zenodo.1135255.
[12] Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code. *International Journal of Computational Research and Development*. 3(1), 13-22. DOI : http://doi.org/10.5281/zenodo.1144555.
[13] Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.
[14] Das, P. P., Chakrabarti, P. P., & Chatterji, B. N. (1987). Distance functions in digital geometry. *Information Sciences*, *42*(2), 113-136.
[15] Aithal, P. S., & Shubhrajyotsna Aithal, (2015). Ideal Technology Concept & its Realization Opportunity using Nanotechnology, *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 4(2), 153 - 164. DOI: http://doi.org/10.5281/zenodo.61591.
[16] Aithal, P. S. (2015). Concept of Ideal Business & Its Realization Using E-Business Model, *International Journal of Science and Research (IJSR)*, 4(3), 1267 - 1274. DOI : http://doi.org/10.5281/zenodo.61648.
[17] Aithal, P. S., & Shubhrajyotsna Aithal, (2016). Impact of On-line Education on Higher Education System. *International Journal of Engineering Research and Modern Education (IJERME), 1(*I), 225-235. DOI : http://doi.org/10.5281/zenodo.161113.
[18] Aithal, P. S., & Shubhrajyotsna Aithal (2015). An Innovative Education Model to realize Ideal Education System. *International Journal of Scientific Research and Management (IJSRM)*, 3(3), 2464-2469. DOI: http://doi.org/10.5281/zenodo.61654.
[19] Aithal, P. S., & Shubhrajyotsna Aithal, (2014). Ideal education system and its realization through online education model using mobile devices. *Proceedings of IISRO Multi Conference 2014, Bangkok*, 140 – 146. ISBN No. 978-81-927104-33-13.
[20] Aithal, P. S., (2016). Review on Various Ideal System Models Used to Improve the Characteristics of Practical Systems. *International Journal of Applied and Advanced Scientific Research*, 1(1), 47-56. DOI: http://doi.org/10.5281/zenodo.159749.

[21] Aithal, P. S. (2016). The concept of Ideal Strategy & its realization using White Ocean Mixed Strategy, *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 171-179. DOI : http://doi.org/10.5281/zenodo.161108.
[22] Sridhar Acharya, P. and Aithal, P. S., (2016). Concepts of Ideal Electric Energy System for production, distribution and utilization. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 367-379. DOI : http://doi.org/10.5281/zenodo.161143.
[23] Aithal, P. S., (2016). Smart Library Model for Future Generations. *International Journal of Engineering Research and Modern Education (IJERME)*, 1(1), 693-703. DOI : http://doi.org/10.5281/zenodo.160904.
[24] Aithal, P. S. (2016). Ideal Banking Concept and Characteristics. *International Research Journal of Management, IT and Social Sciences (IRJMIS)*, 3(11), 46-55. DOI: http://dx.doi.org/10.21744/irjmis.v3i11.311.
[25] Aithal, P. S. (2016). A Comparison of Ideal Banking Model with Mobile Banking System. *International Journal of Current Research and Modern Education (IJCRME)*, 1(2), 206-224. DOI: http://dx.doi.org/10.5281/ZENODO.198708.
[26] Aithal, P. S., & Vaikuth Pai, T., (2016). Concept of Ideal Software and its Realization Scenarios. *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 826-837. DOI : http://doi.org/10.5281/zenodo.160908.
[27] Shubrajyotsna Aithal, & Aithal, P. S., Bhat, G. K. (2016). Characteristics of Ideal Optical Limiter and Realization Scenarios using Nonlinear Organic Materials – A Review. *International Journal of Advanced Trends in Engineering and Technology (IJATET)*, 1(1), 73-84. DOI : http://doi.org/10.5281/zenodo.240254.
[28] Aithal, P. S., Suresh Kumar P. M. (2017). Ideal Analysis for Decision Making in Critical Situations through Six Thinking Hats Method. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 1-9. DOI: http://dx.doi.org/10.5281/zenodo.838378.
[29] Krishna Prasad, K., & Aithal, P.S. (2017). A Customized and Ideal Mobile Banking Technology Using 5G Technology. *International Journal of Management, Technology and Social Science (IJMTS)*, 2(1), 25-37. DOI: http://dx.doi.org/10.5281/zenodo.820860.
[30] Aithal, P. S., Shailashree, V. T., Suresh Kumar, P. M. (2015). A New ABCD Technique to Analyze Business Models & Concepts, *International Journal of Management, IT and Engineering (IJMIE)*, 5(4), 409-423. DOI : http://doi.org/10.5281/zenodo.61652.
[31] Aithal, P. S. (2016). Study on ABCD Analysis Technique for Business Models, Business strategies, Operating Concepts & Business Systems, *International Journal in Management and Social Science*, 4(1), 98-115. DOI : http://doi.org/10.5281/zenodo.161137.
[32] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy. *International Journal of Applied Research (IJAR)*, 1(10), 331-337. DOI: http://doi.org/ 10.5281/zenodo.163424.
[33] Aithal, P. S., Shailashree, V. T., & Suresh Kumar P. M., (2016). ABCD analysis of Stage Model in Higher Education. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 11-24. DOI: http://doi.org/10.5 281/zenodo.154233.
[34] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Analysis of NAAC Accreditation System using ABCD framework. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 30-44. DOI: http://doi.org/10. 5281/zenodo.154272.

[35] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Application of ABCD Analysis Framework on Private University System in India. *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 159-170. DOI : http://doi.org/10.5281/zenodo.161111.
[36] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). The Study of New National Institutional Ranking System using ABCD Framework, *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 389–402. DOI : http://doi.org/10.5281/zenodo.161077.
[37] Aithal, S., & Aithal, P. S. (2016). ABCD analysis of Dye doped Polymers for Photonic Applications, IRA-International Journal of Applied Sciences, 4 (3), 358-378. DOI: http://dx.doi.org/10. 21013/j as.v4.n3.p1.
[39] Aithal, P. S., Shailashree, V. T. & Suresh Kumar, P. M., (2016). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 846-858. DOI : http://doi.org/10.5281/ zenodo.62022.
[40] Varun Shenoy, & Aithal P. S., (2016). ABCD Analysis of On-line Campus Placement Model, IRA-International Journal of Management & Social Sciences, 5(2), 227-244. DOI: http://dx.doi.org/10.21013/jmss .v5.n2.p3.
[41] Aithal, P. S., Shailashree V. T. & Suresh Kumar P.M. (2016). Factors & Elemental Analysis of Six Thinking Hats Technique using ABCD Framework. *International Journal of Advanced Trends in Engineering and Technology (IJATET)*, 1(1), 85-95. DOI : http://doi.org/10.5281/zenodo.240259.
[42] Aithal, P. S. & Suresh Kumar, P. M. (2016). CCE Approach through ABCD Analysis of 'Theory A' on Organizational Performance. *International Journal of Current Research and Modern Education (IJCRME)* 1(1), 169-185. **DOI:** http://dx.doi.org/10. 5281/zenodo.164704**.**
[43] Aithal, P. S. (2017). ABCD Analysis of Recently Announced New Research Indices. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(1), 65-76. DOI: http://doi.org/10.5281/ zenodo. 583644.
[44] Aithal, P. S. (2017). Factor Analysis based on ABCD Framework on Recently Announced New Research Indices, *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 1(1), 82-94. DOI: http://dx.doi.org/1 0.5281/zenodo.584105.
[45] Aithal, P. S., (2017). ABCD Analysis as Research Methodology in Company Case Studies. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 40-54. DOI: http://dx.doi.org/10.5 281/zenodo.891621.
[46] Aithal, Architha., Aithal, P. S. (2017). ABCD Analysis of Task Shifting-An optimum Alternative Solution to Professional Healthcare Personnel Shortage. *International Journal of Health Sciences and Pharmacy (IJHSP)*, 1(2), 36-51. DOI: http://dx.doi.org/10.5281/zenodo.1038975.
[47] Varun Shenoy & Aithal, P. S., (2017). Quantitative ABCD Analysis of IEDRA Model of Placement Determination. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 1(2), 103-113. DOI: http://dx.doi.org/10.5281/zenodo.1133691.

Chapter 15

A Comparative Study on Fingerprint Hash Code, OTP, and Password based Multifactor Authentication Model with an Ideal System and Existing Systems

Authentication is the process to validate the user identity and to grant some resources or services to the user. Authentication process uses many factors like password, biometrics, or One Time Password. Multifactor authentication model always gives higher security than single-factor authentication model. Fingerprint Hash code is not used for full security or authentication purpose but it can be combined with other security elements like password or OTP in order to enhance security. Fingerprint Hash code acts as a key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. In this paper based on focus group interaction, first, we define an Ideal Authentication System. The Ideal Authentication System used in this study consists of different components like Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices. In this paper, we also compare new Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password with existing authentication systems. The traditional user-id, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions and Indian Aadhaar card registration process are the different existing systems used in this study to compare with the new model.

Keywords: *Authentication, Multifactor Authentication Model, Fingerprint Hash code, OTP, Ideal Authentication System.*

15.1 INTRODUCTION

By definition, authentication is using one or multiple mechanisms to show that who you declare or claim to be. As soon as the identity of the human or machine is demonstrated, then human or machine is authorized to grant some services. Three worldwide referred authentication process are (1) Token supported authentication, (2) Biometric supported authentication, and (3) Knowledge supported authentication.

Token supported authentication makes use of key cards, bank cards, and smart cards. Token supported authentication system sometimes uses knowledge supported techniques to improve security. Biometric supported authentication strategies, together with fingerprints, iris scan and facial reputation aren't yet extensively adopted [1-2]. The essential flaws of this technique are that such systems can be costly, and the identification process may be slow and regularly unreliable. However, this form of technique presents the highest level of protection. Knowledge supported authentication is most commonly and widely used authentication technique and encompass both text-based and image-based passwords. The image-based techniques can be further subdivided into two classes: recognition-primarily based and recall based graphical techniques. The use of recognition based strategies, a person is provided with a set of images and the user is authenticated through recognizing and identifying the images, which is registered at the time of registration process. In recall based techniques it's essential that user has to reproduce something like a pattern, which is created or drawn at the time of registration process.

One time password can be generated in two forms. (1) Time-synchronized OTP: In time-synchronized OTPs the person has to enter the password within a time frame or within a stipulated time, in other words, OTP having lifespan only for few amount of time after that time it will get expired and another OTP will be generated. (2) Counter-synchronized OTP: In Counter-synchronized OTP, instead of regenerating OTP after the stipulated time, a counter variable is coordinated or synchronized between client device and server.

Automatic Fingerprint Identification System (AFIS) consists of different techniques like preprocessing, enhancement, segmentation, thinning, feature extraction, post-processing, minutiae orientation and alignment [3-10]. Fingerprint Hash code acts as the key, which can uniquely identify every person. So it can be replaceable with user-id or username and can work along with text-based or picture based or pattern based passwords. The fingerprint hash code is not constant with biometric sensors or readers. There are many types of research are carried out translation and rotation invariant fingerprint hash code generation but even small or pixel changes cause a difference in Hash code [11-14]. Based on the different Methods of Fingerprint Hash code generation, it reveals that fingerprint hash code does not suit exclusively for authentication or security purpose. But it uniquely identifies an individual person or human being through a Hash code key.

A service model or system called ideal system, when that must have the following characteristics [15]:

- An ideal model/system should capable of incorporating changes in services, or inclusion/deletion/updating of new/old services without affecting its overall framework or performance.

- Postulation made in the model/system should be minimal.
- The service should be accessible all time 24×7 basis, around the year 365 days.
- The user interface should be simple, user-friendly and highly explanatory.
- The response time should be very good.
- The error rate should be zero or nullified.
- Security should be very high or unauthorized access or use data by the unregistered user should be prevented.

In this paper, we discuss an ideal Multifactor Authentication System which is finest in terms of all its characteristics or fulfils every aspects or need of all its stakeholders. Multifactor Authentication Model is an advanced technology to protect user and user credentials from an intruder in the highly secured way. The paper is discussed in six sections. Section 1 describes introductory theory about fingerprint biometrics, Hash code, and Ideal system. Section 2 explains about an Ideal system. Section 3 describes Ideal Authentication Model. Section 4 describes Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password. Section 5 makes a comparison of new Multifactor Authentication Model with different existing Authentication systems. Section 6 concludes the paper with findings of the comparative study.

15.2 AN IDEAL SYSTEM

It is well known that we can improve the performance of any system by comparing it with a hypothetical, predicted system of that kind called Ideal system [15]. The word Ideal system refers to the system which has utmost characteristics, which cannot be improved further. It is what our mind tells ultimate and which reached the pinnacle of success in the respective field, which can be compared to all other systems of similar type, which lacks in some qualities [16]. The less-efficient system can be converted into the ideal system with the aid of research and continuous innovation in that field. Many objects we can consider as ideals like an ideal gas, ideal fluid, ideal engine, ideal switch, ideal voltage source, ideal current source, ideal semiconductor and ideal communication technology and all of these are considered as standards to improve the quality and performance of similar type. Recently many ideal systems are studied, which includes ideal technology system [15], ideal business system [16], ideal education system [17-20], ideal strategy [21], ideal energy source [22], ideal library system [23], ideal banking system [24-25], and ideal mobile banking system [29]. The ideal system of any kind can be placed in mind, while improving the characteristics of practical devices/ systems and reach ideal system or considered to be a pinnacle of success [15-29].

15.3 IDEAL AUTHENTICATION SYSTEM

Ideal Authentication System is a system which has properties like highly user-friendly, ubiquitous services, always available, very cheaper and 100% efficient in all aspects. An ideal or error-free biometric system should make an accurate and correct decision on every test sample regardless of any performance degrading factors like variation or differences in inter-class, similarities in intra-class, different representation for enrolled and sample data, and extreme noise and low sample data quality. Some of the ideal systems with respect to Authentication System are listed in Table 15.1.

Table 15.1: List of Ideal components with respect to Authentication System

Sr. No	Ideal System Components	Definition of Ideal Systems/Components
1	Ideal Speed	The time is taken by the Automatic Verification or Authentication System to authenticate the registered user
2	Ideal Data Transfer Rate	Any amount of data can be transferred from source to destination without any delay or within null unit of time duration (In client Server Model)
3	Ideal Signalling efficiency	The quality of the signal is 100% efficient in all aspects.
4	Ideal Security	100% protection of Registered user means no intruder can able to break the system anyway.
5	Ideal Availability	Service can be available any part of the world anytime.
6	Ideal Bandwidth	The volume of Information per unit of time that a system can handle is unlimited or uncountable.
7	Ideal False Acceptance Rate	The percentage of system incorrectly classifies the input pattern to an unregistered user is zero.
8	Ideal False Rejection Rate	The probability that the Authentication framework unable to identify a match between the authentic people is always zero.
9	Ideal Equal Error Rate	Acceptance and rejection mistakes are identical in the system and which is equal to zero.
10	Ideal Failure to Enroll Rate	The unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input is zero.
11	Ideal Accuracy Rate	Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high.

As shown in Figure 15.1, we have proposed an Ideal Authentication Model, which consists of different components like Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices.

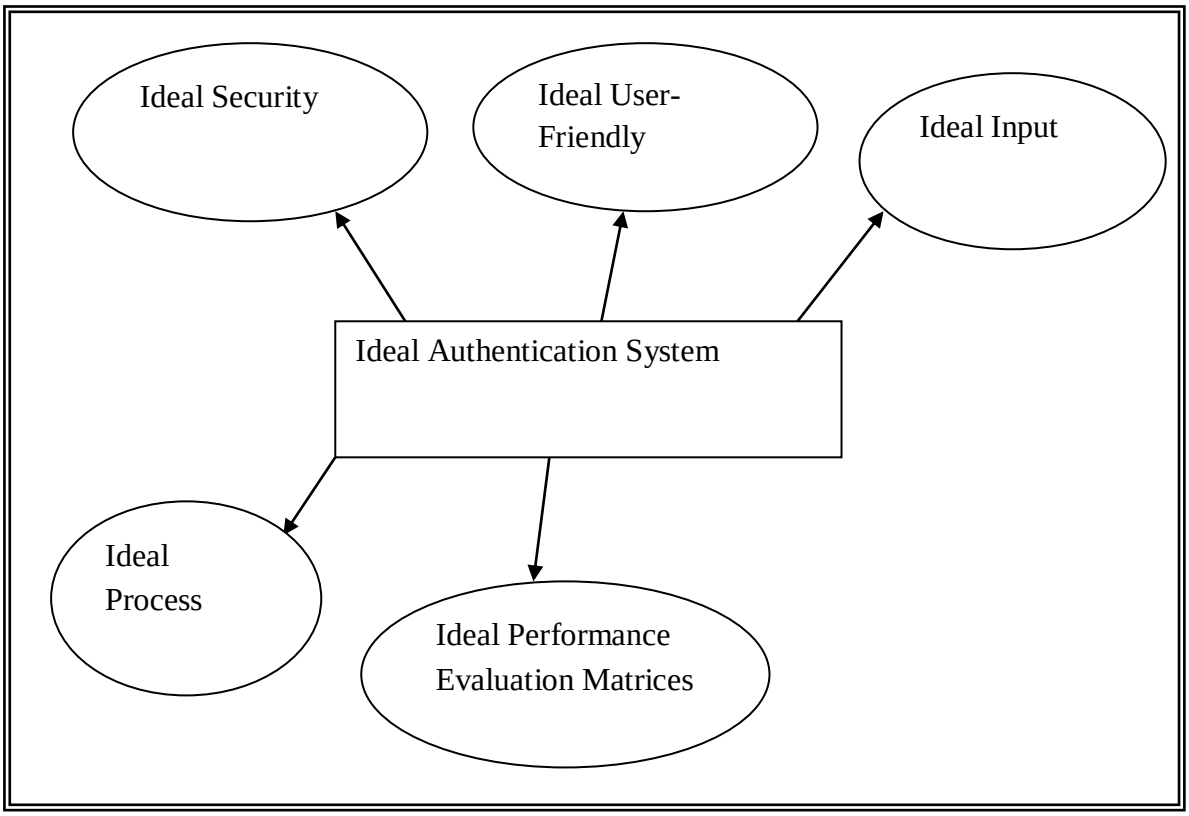


Figure 1: Ideal Authentication System Model

15.3.1 Ideal Security

In Ideal Authentication System, Ideal Security refers a system, which is impossible for an intruder to break the system or impossible for the unregistered user to access the system. Ideal Security model improves or makes the system robust by maintaining security mechanism at various levels like user level, network level, template or database level. Security can be enhanced to maximum or optimal level by the use of multifactor authentication model. Table 15.2 shows Ideal security various components technologies and benefits.

Table 15.2: Description of various characteristics of Ideal Security

Sr. No	Characteristics	Descriptions
1	High User level Security	Minimum data is remembered by the user for the authentication process. To realize this use Physiological or Behavioral biometrics
2	High Network level Security	Difficult to get original data or information. Decrypting of the message by the unknown user becomes impossible.
3	Ideal Template level or Database level security	Non revertible template or impossible to get actual information.

4	Multifactor Authentication Security	Use more than one factor for authentication like Biometrics, One Time Password (OTP), and Password.

15.3.2 Ideal User-Friendly

The goal of the ideal user-friendly component is that user should able to get access to the system effortless or easily without remembering anything or very minimum amount of data. Ideal user-friendly system should have some characteristics, which are listed in Table 3 to call itself as Ideal.

Table 3: Description of various characteristics of Ideal User-Friendly

Sr. No	Characteristics	Description
1	High Response Time	User should get Authenticated as early as possible or with least amount of time
2	High Access Time	User should get access to the system with least amount of time
3	Automatic Process	User should able to get authenticated automatically without entering anything on the screen or just by standing infront of the system
4	High speed	The execution time for authentication should be very minimum
5	High Availability	Anytime, Anywhere, Anyplace or simply ubiquitously available
6	Effort free	The user should able to work with the system effortless or freely.

15.3.3 Ideal Input

Ideal Input ensures that registered user should able to get access to the system or authenticated with very less or no input. In an Ideal Authentication system, the Ideal input having different characteristics, which are listed out in Table 15.4.

Table 15.4: Description of various characteristics of Ideal Input [Source: Aithal, P. S. & Pai T, Vaikunta [26])

Sr. No	Characteristics	Description
1	Minimum possessions	Users will be carrying only one data or no data along with them to get authenticated
2	Minimum input	The number of data or instruction to the system is as minimum as possible
3	Input Selectivity	Select input data rather than remembering and entering
4	Ubiquitous Data	Anytime, Anywhere, and Anyplace able to input or feed data

5	Reliability	The input should not have any imperfections. It should not fail during execution
6	Usability	The input should have infinite usability for various applications.
7	Efficiency	The provided input should have 100% efficiency with an intention to get accurate results.
8	Input Security	The input should be protected from intruder
9	Short execution time	The input provided to the system should execute with a minimum amount of time.

15.3.4 Ideal Process

In an Ideal Authentication system, Ideal process refers user should able to complete authentication process without any fault, fast and completely. The different characteristics, of the Ideal process, are listed out in Table 15.5.

Table 15.5: Description of various characteristics of Ideal Process

Sr. No	Characteristics	Description
1	High Atomicity	The Authentication process should complete fast without any errors or should not abort in between if it has started.
2	Ideal Consistency	After the authentication process system should end up with the consistent state.
3	Maximum Isolation	The intermediate state of Authentication process should be invisible to other users.
4	High Availability	Anytime, Anywhere, Anyplace or simply ubiquitously available
5	Effort free	Authentication process should be effortless.
6	High durability	After a transaction completes, the changes made should persist even in the case of unexpected system failure. If user credentials like password or biometric are changed, it should persist, if that process completes just before the failure.

15.3.5 Ideal Performance Evaluation Matrices

In Ideal Authentication System, Ideal Performance Evaluation Matrices refers all the performance evaluation matrices normally used for the authentication system. This component is having scope in the biometrics-based authentication system. The different characteristics, of Ideal Performance Evaluation Matrices, are listed out in Table 15.6.

Table 15.6: Description of various characteristics of Ideal Performance Evaluation Matrices

Sr. No	Characteristics	Description
1	Ideal False Acceptance Rate	The percentage of system incorrectly classifies the input pattern to an unregistered user is zero.
2	Ideal False Rejection Rate	The probability that the Authentication framework unable to identify a match between the authentic people is always zero.
3	Ideal Equal Error Rate	Acceptance and rejection mistakes are identical in the system and which is equal to zero.
4	Ideal Failure to Enroll Rate	The unsuccessful attempt made to enroll in database or template of an Automatic Fingerprint Identification System by the input is zero.
5	Ideal Accuracy Rate	Because of False Rejection Rate and False Acceptance Rate is zero, the accuracy of the system becomes high.
6	Ideal Execution time	Automatic Verification or Authentication process should complete as early as possible for the registered user.

15.4. Multifactor Authentication Model Using Fingerprint Hash Code, OTP, and Password

Figure 15.2 shows Dataflow Diagram of Multifactor Authentication model used in this study. Initially on the client side using an interface user loads fingerprint image into the system. First, using Euclidean distance fingerprint image features are extracted, and converted into Hash code.

These features are encrypted and sent to the server. As soon as these features arrive at a server in encrypted form, the server receives that and request for One Time Password from OTP generator. OTP generator is a module or function, which is located at server machine. Time synchronized OTP is sent to the registered mobile phone user. Client system prompts a message to enter OTP, which is received to the registered mobile phone of the user.

The user enters that OTP through the client interface and this OTP is compared with server generated OTP at the server side. If OTP is verified, server requests for the password, the user enters the password through a client-side interface and entered password reaches to the server. The server verifies the user entered a password with the already stored password in its database. Since database password is stored in encrypted format. The password which is stored in the database in encrypted form and finger user-id hash code is encrypted one again to enhance security.

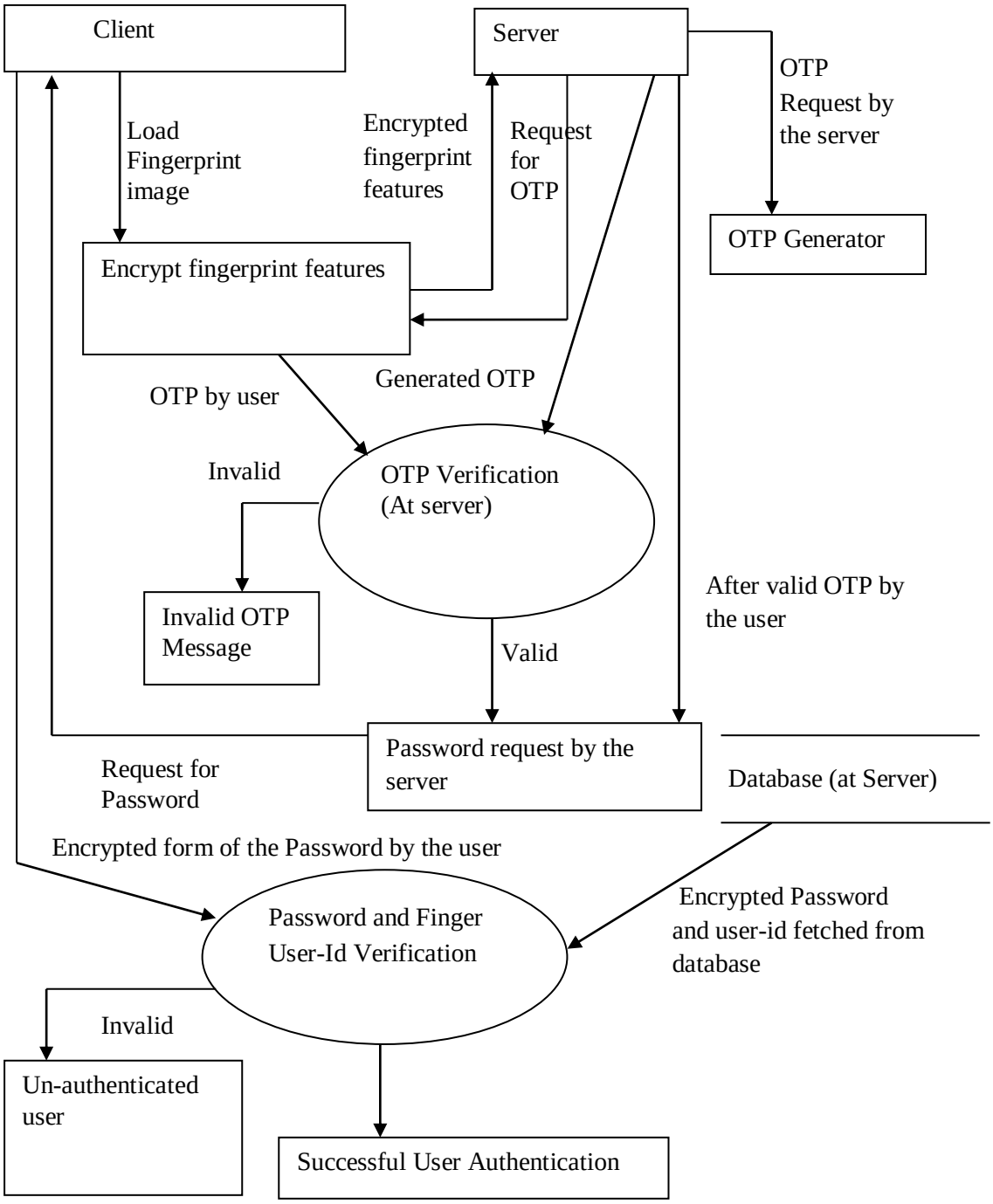


Figure15. 2: Dataflow Diagram of Proposed Multifactor Authentication

So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both password and Fingerprint Hash code match them user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Password, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Password does not matches user is considered an unauthorized user. If OTP not matches then the user is blocked from further steps in the authentication process. In this research study, this is not implemented as server and client in different machines. The model of this approach is implemented on the same machine using MATLAB 2015a.

15.4.1 One Time Password Generator

In this research work, One Time Password Generator is responsible for generating OTP. This is a function located on the server. In this study, Time synchronized OTP is generated by combining some features. The time for which OTP is valid is administrative specific, for simplicity we consider in this work as 2 minutes. The algorithm for generating OTP is explained below.

Algorithm:

Step-1: Generate the Hash code for input fingerprint using MD5 Hash Function.
Step-2: Extract system Date and Time.
Step-3: Extract seconds separately.
Step-4: Consider only integer part of the seconds.
Step-5: A 4 × 4 sized matrices of the random number is generated.
Step-6: Date and Time are converted into string data type.
Step-7: Random matrix is concatenated with Date and Time string.
Step-8: Hash code of the input fingerprint image is concatenated with the result of Step-7.
Step-9: Hash code is generated for combined string obtained from Step-8.
Step-10: A random number is generated between1 to 32.
Step-11: If the random number is in between 1 to 8 (including both) then extracts first 8 characters of the Hash code of size 32 characters generated in Step-8.
Step-12: If the random number is in between 9 to 16 (including both) then extract next 8 characters (from position 9 to 16) of the Hash code of size 32 characters generated in Step-8.
Step-13: If the random number is in between 17 to 24 (including both) then extract next 8 characters from position 17 to 24) of the Hash code of size 32 characters generated in Step-8.
Step 14: If the random number is in between 24 to 32 (including both) then extract next 8 characters from position 24 to 32) of the Hash code of size 32 characters generated in Step-8.

15.5 Comparison of New Multifactor Authentication Model with existing Systems

Here we compare Multifactor Authentication Model based on Fingerprint Hash code, OTP, and Password with different existing systems of the same kind or slightly different systems or any system which makes use of biometric or password or username or OTP for authentication. The different system considered in this study are the traditional user-d, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions, and Indian Aadhaar card registration process. These comparisons help to understand where this model stands in terms of its features compare to the existing systems.

The new model is compared with all the existing models under four constructs as Advantages, Benefits, Constraints, and Disadvantages [30-42]. Table 15.7, Table 15.8, Table 15.9, and Table 15.10 shows Advantages, Benefits, Constraints, and disadvantages comparative study of new Multifactor Authentication Model with traditional username and password based Internet/Mobile Banking System respectively.

Table 15.7: Advantages comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

Sl. No	New Multifactor Authentication Model	Traditional user-id and password based Internet/Mobile Banking System
1	The Nonreversible Fingerprint Hash code is used in network level Highly secured encrypted user-id and password are used in network level Fingerprint Hash code is used in network level	Highly secured encrypted user-id and password are used in network level
2	Fingerprint Hash-id is used for identification purpose which is in Hash or encrypted form	User-id is used for identification purpose which is in Hash or encrypted form
3	Easily revocable Fingerprint Hash-id and password which is in Hash or encrypted form	Easily revocable user-id and password which is in Hash or encrypted form
4	High template protection is ensured	High user-id and password protection is ensured in database level
5	The system having ability to authenticate with one knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry)	The system having ability to authenticate with two knowledgebase input (user-id by selection, OTP is entered by viewing and Password by knowledge base entry)
6	Depending on the device and network Provides ubiquitous authentication	Depending on the device and network Provides ubiquitous authentication
7	Interactive and explorative user interface	Interactive and explorative user interface
8	One knowledge base parameter input	Two knowledge base parameter inputs
9	Simple User authentication from customer point of view	Simple User authentication from customer point of view but user-id also remembered along with password
10	Reduced error in inputting due to one selection type input.	Input error little more due to lack of selection input.
11	Due to Hash code user, personal data or input are secured.	Due to encrypted data user personal data or input are secured.
12	Due to RDBMS transaction property atomicity, consistency, and isolation properties are ensured.	Due to RDBMS transaction property atomicity, consistency, and isolation properties are ensured.
13	Changed Password and Biometric-id durable for a long time.	Changed Password and User-id durable for a long time.
14	All the fingerprint performance evaluation matrices like False	User-id and Password give highest accuracy rate.

	Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to Enroll Rate, and Accuracy Rate gives good accuracy or matching rate.	
15	Lifespan or validity of OTP is very less, say 2 minutes.	OTP used for financial transaction having more validity.

Table 15.8: Benefits comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

Sl. No	New Multifactor Authentication Model	Traditional user-id and password based Internet/Mobile Banking System
1	Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers.	Security in all aspects of network and database and reduced execution time increased customer faith and also attracted new customers. But due to password attacks, users require advanced way of authentication like biometrics.
2	Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient.	Cryptographically encrypted user-id and password only stored in database, which makes database memory utilization very less and efficient.
3	Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input.	OTP is used only for financial transactions.
4	Ubiquitous authentication with one knowledge base input.	Ubiquitous authentication with two knowledge base inputs.
5	Authentication failure is very rare or practically zero compare to any other biometrics-based authentication.	An authentication failure occurs when user-id, password or both becomes wrong.
6	Revocability can be done easily if password or Finger-id is compromised. In most of the fingerprint-based authentication system, revocability of fingerprint is not so easy.	Revocability is done easily if the password is compromised.
7	Due to RDBMS transaction property, at the time of system failure.	Due to RDBMS transaction property, ensures a safe state at the time of system failure.
8	The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction.	The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input already enhanced user trust, happiness, and satisfaction. But the user needs still more security for their data and transactions.

Table 15.9: Constraints comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

Sl. No	New Multifactor Authentication Model	Traditional user-id and password based Internet/Mobile Banking System
1	Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working.	Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working.
2	Good RDBMS management and disaster recovery techniques are essential.	Good RDBMS management and disaster recovery techniques are essential.
3	Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption.	Requires high configuration system and efficient algorithms for user-id and password encryption.
4	Requires navigational and explorative user interface.	Requires navigational and explorative user interface, and Input should be selective rather than entry type.
5	While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification.	Unique user-id is selected for collusion free user-id and for effective user identification.

Table 15.10: Disadvantages comparative study of new Multifactor Authentication Model v/s traditional user-id and password based Internet/Mobile Banking System.

Sl. No	New Multifactor Authentication Model	Traditional user-id and password based Internet/Mobile Banking System
1	Network cost for OTP	Network cost for OTP in financial transactions.
2	Network and server Failures will shut down the Authentication process	Network and server Failures will shut down the Authentication process
3	Complex backend design of user interface	Complex backend design of user interface
4	Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in authentication process.	The negligence of the user in entering the input and Lack of concentration of the user increases the non-matching rate in authentication process.
5	Requirement of continuous availability of the server increases cost	Requirement of continuous availability of the server increases cost

Table 15.11, Table 15.12, Table 15.13, and Table 15.14 shows Advantages, Benefits, Constraints, and disadvantages [30-42] comparative study of new Multifactor Authentication Model with Apple iPhone X facial recognition system. Here the comparison is not more

useful because the Apple iPhone X facial recognition used for mobile locking and not for secured transaction or authentication.

Table 15.11: Advantages comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

Sl. No	New Multifactor Authentication Model	Apple iPhone X Facial Recognition System
1	Nonreversible Fingerprint Hash code is used in network level	Face recognition image are stored on the mobile phone. Authentication is done locally.
2	Fingerprint Hash code alone is not used for the purpose of authentication. Authentication is done with the aid of Fingerprint Hash code, OTP, and Password.	Face of the user image alone is used for authentication/recognition purpose.
3	Hashed fingerprint gives more security	The unhashed Face image is an easy target for Hackers.
4	Multiple inputs are necessary for authentication or matching, which includes Fingerprint Hash code, OTP, and Password	Only face image of the user is needed for Authentication/Matching/Verification purpose.
5	At least one knowledge base input is required (password)	None of the Knowledgebase input is used for Authentication/Matching/Verification purpose.
6	System is not easily mimicable	The system is easily mimicable.

Table 15.12: Benefits comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

Sl. No	New Multifactor Authentication Model	Apple iPhone X facial recognition system
1	Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers	Not implemented in large scale due to security failure in its infant stage only.
2	Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient.	Not used in Client-Server architecture.
3	Both fingerprint-id and passwords are protected by OTP means OTP is first	OTP is not used in verification or matching process.

	entry type input.	
4	Ubiquitous authentication with one knowledge base input.	Ubiquitous matching with no knowledge base inputs.
5	Authentication failure is very rare or practically zero compare to any other biometrics-based authentication.	Authentication/matching failure occurs when face image is hacked by the intruder

Table 15.13: Constraints comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

.Sl. No	New Multifactor Authentication Model	Apple iPhone X facial Recognition System
1	Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working.	Not used in network, used in local system
2	Good RDBMS management and disaster recovery techniques are essential.	Not used in client-server architecture
3	Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption.	Requires high configuration system and efficient algorithms for processing of facial features from face image
4	Requires navigational and explorative user interface.	Not having much scope for interface because no entry type input required. Input is captured through a mobile camera.
5	Provides good security architecture through multifactor authentication model.	Good security architecture is essential

Table 15.14: disadvantages comparative study of new Multifactor Authentication Model v/s Apple iPhone X facial Recognition System

.Sl. No	New Multifactor Authentication Model	Apple iPhone X facial Recognition System
1	Network cost for OTP	Not suitable for network feature comparison.
2	Network and server Failures will shut down the Authentication process	The client-server architecture is not implemented.
3	Complex backend design of user interface	user interface having not much scope due to lack of manual input.
4	Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process.	Negligence of the user in storing face image in unsecured places causes security failure.

Table 15.15, Table 15.16, Table 15.17, and Table 15.18 shows Advantages, Benefits, Constraints, and disadvantages [30-42] comparative study of new Multifactor Authentication Model with HDFC OTP Checkout for online transactions.

Table 15.15: Advantages comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

Sl. No	New Multifactor Authentication Model	HDFC OTP Checkout for online transactions
1	Nonreversible Fingerprint Hash code is used in network level.	Highly secured encrypted OTP is used in network level
2	The system having ability to authenticate with one knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry)	The system having the ability to authenticate without knowledgebase input.
3	Depending on the device and network Provides ubiquitous authentication	Depending on the device and network Provides ubiquitous authentication
4	Interactive and explorative user interface	Interactive and explorative user interface
5	One knowledge base parameter input	No knowledge base parameter inputs
6	Simple User authentication from customer point of view	Simple User authentication from customer point of view
7	Reduced error in inputting due to one selection type input.	More Reduced error in inputting due to lack of selection or entry types input.
8	Due to Hash code user, personal data or input are secured.	Due to encrypted data user personal data or input are secured.
9	Lifespan or validity of OTP is very less, say 2 minutes.	OTP used for financial transaction having less validity.

Table 15.16: Benefits comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

Sl. No	New Multifactor Authentication Model	HDFC OTP Checkout for online transactions
1	Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers	Security in all aspects of network and database and reduced execution time increased customer faith and also attracted new customers. When the mobile phone is stolen users requires advanced way of authentication like biometrics.
2	Cryptographically encrypted one hash code and password only stored in the database, which makes database	Cryptographically encrypted user-id and password only stored in the database, which makes database memory utilization

	memory utilization very less and efficient.	very less and efficient.
3	Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input.	Only OTP is used for authentication/transaction purpose.
4	Ubiquitous authentication with one knowledge base input.	Ubiquitous authentication with OTP
5	Authentication failure is very rare or practically zero compare to any other biometrics-based authentication	An authentication failure occurs when OTP is wrong, which very rare or uncommon.
6	The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction.	The simple, Navigational, and explorative user interface, the speed of authentication, and lack of manual input already enhanced user trust, happiness, and satisfaction. But the user needs still more security for their data and transactions.

Table 15.17: Constraints comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

Sl. No	New Multifactor Authentication Model	HDFC OTP Checkout for Online Transactions
1	Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working.	Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working.
2	Good RDBMS management and disaster recovery techniques are essential.	Good RDBMS management and disaster recovery techniques are essential.
3	Requires high configuration system and efficient algorithms for fingerprint Hash code creation and for encryption.	Requires high configuration system and efficient algorithms for OTP encryption.
4	Requires navigational and explorative user interface.	Requires simple interface due to lack of knowledgebase input.
5	While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification.	Unique user-id is selected for collision-free user-id and for effective user identification but verification is done only through OTP.

Table 15.18: Disadvantages comparative study of new Multifactor Authentication Model v/s HDFC OTP Checkout for online transactions

Sl. No	New Multifactor Authentication Model	HDFC OTP Checkout for Online Transactions
1	Network cost for OTP	Network cost for OTP
2	Network and server Failures will shut down the Authentication process	Network and server Failures will shut down the Authentication process
3	Complex backend design of user interface	Simple backend design of user interface
4	Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process.	No manual input, which reduces error in input.
5	Requirement of continuous availability of the server increases cost	Requirement of continuous availability of the server increases cost

Table 15.19, Table 15.20, Table 15.21, and Table 15.22 shows Advantages, Benefits, Constraints, and disadvantages [42-51] comparative study of new Multifactor Authentication Model with Indian Aadhaar card registration process.

Table 15.19: Advantages comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

Sl. No	New Multifactor Authentication Model	Indian Aadhaar card registration process.
1	Nonreversible Fingerprint Hash code is used in network level	Highly secured encrypted OTP is used in network level
2	The system having the ability to authenticate without knowledgebase input (Hash-id by selection, OTP is entered by viewing and Password by knowledge base entry)	The system having ability to authenticate without knowledgebase input.
4	Interactive and explorative user interface	Interactive and explorative user interface
5	One knowledge base parameter input	No knowledge base parameter inputs
6	Simple User authentication from customer point of view	Simple User authentication from customer point of view
7	Reduced error in inputting due to one selection type input.	More Reduced error in inputting due to lack of selection or entry types input.
8	Due to Hash code user, personal data or input are secured.	Due to encrypted data user personal data or input are secured.
9	Lifespan or validity of OTP is very less, say 2 minutes.	OTP used for financial transaction having little bit more validity.
10	Fingerprint thumb capturing will not	Registration process involving fingerprint

	fail frequently for kids.	thumb image captures requires many attempts for kids.

Table 15.20: Benefits comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

Sl. No	New Multifactor Authentication Model	Indian Aadhaar card registration process
1	Security in all aspects of network and template, Simple and easy way to input, reduced execution time can become influence parameters for Increased customer faith and also can attract new customers	Not having scope for authentication. Its one-time registration for a single user.
2	Cryptographically encrypted one hash code and password only stored in the database, which makes database memory utilization very less and efficient.	Cryptographically encrypted user-id and biometric only stored in the database, which makes database memory utilization more but efficient.
3	Both fingerprint-id and passwords are protected by OTP means OTP is first entry type input.	Both fingerprint template and OTP makes authentication/transaction process.
5	Authentication failure is very rare or practically zero compare to any other biometrics-based authentication.	An authentication failure occurs when thumb minutiae details vary with a dry finger or cold weather, or finger damage or cut.
6	The simple, Navigational, and explorative user interface, the speed of authentication, and Effort free input and process can have chances to enhance user trust, happiness, and satisfaction.	Simple, Navigational, and explorative user interface, speed of registration, and lack of manual input already enhanced user trust, happiness, and satisfaction.

Table 15.21: Constraints comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

Sl. No	New Multifactor Authentication Model	Indian Aadhaar card registration process
1	Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working.	Good Network architecture, network availability, and Network availability of mobile service provider's are essential for smooth working.
2	Good RDBMS management and disaster recovery techniques are essential.	Good RDBMS management and disaster recovery techniques are essential.
3	Requires high configuration system and	Requires high configuration system and

	efficient algorithms for fingerprint Hash code creation and for encryption.	efficient algorithms for OTP encryption.
4	Requires navigational and explorative user interface.	Requires simple interface due to lack of knowledgebase input.
5	While selecting fingerprint features for Hash code, unique features should be selected for collision-free Hash code and for effective user identification.	Unique user-id is selected for collision-free user-id and for effective user identification but verification is done only through OTP.

Table 15.22: Disadvantages comparative study of new Multifactor Authentication Model v/s Indian Aadhaar card registration process

Sl. No	New Multifactor Authentication Model	Indian Aadhaar card registration process
1	Network cost for OTP	Network cost for OTP
2	Network and server Failures will shut down the Authentication process	Network and server Failures will shut down the registration process
3	Complex backend design of user interface	Complex backend design of user interface
4	Negligence of the user in selection of input and Lack of concentration of the user increases the non-matching rate in the authentication process.	No manual entry type input, which reduces error in input.
5	Requirement of continuous availability of the server increases cost	Requirement of continuous availability of the server increases cost
6	The quality of the fingerprint capturing or sensing technology does not affect the system	The quality of the fingerprint capturing or sensing technology affects the system

15.6 CONCLUSION

In this paper initially, we have discussed an ideal system characteristic with respect to Ideal Authentication System. Ideal Authentication system consists of different components, which includes Ideal Security, Ideal User-Friendly, Ideal Input, Ideal Process, and Ideal Performance Evaluation Matrices. We have compared Fingerprint Hash code, OTP and Password-based Authentication Model with existing systems, which includes, the traditional user-id, password-based internet/mobile banking system, Apple iPhone X face recognition system, HDFC OTP Checkout for online transactions and Indian Aadhaar card registration process. Some of the important findings of the comparative study are mentioned below.

- One time captured static fingerprint image are not vulnerable to climate or weather condition changes compared to any other biometric-based authentication system like Indian Aadhaar Card registration process.
- The new multifactor Authentication model requires less knowledgebase input compared to traditional user-id and password based Internet/Mobile banking authentication [52-55].

- If the user takes care and ensures user-level security through external devices like USB drive or Private cloud drive, we can eliminate password factor from authentication process.
- The new Multifactor Authentication model produces good performance evaluation matrices, which includes False Acceptance Rate, False Rejection Rate, Equal Error Rate, Failure to Enroll Rate, and Accuracy Rate for Fingerprint Hash code compare to any other Hash code based matching systems.

REFERENCES

[1] Parmar, H., Nainan, N., & Thaseen, S. (2012). Generation of secure one-time password based on image Authentication. *Journal of Computer Science and Information Technology*, *7*, 195-206.

[2] M'raihi, D., Bellare, M., Hoornaert, F., Naccache, D., & Ranen, O. (2005). *Hotp: An hmac-based one-time password algorithm* (No. RFC 4226).

[3] Krishna Prasad, K., & Aithal, P.S. (2017). A Critical Study on Fingerprint Image Sensing and Acquisition Technology. *International Journal of Case Studies in Business, IT and Education (IJCSBE),* 1(2), 86-92. DOI: http://dx.doi.org/10.5281/zenodo.1130581.

[4] Krishna Prasad, K., & Aithal, P.S. (2017). A Conceptual Study on Image Enhancement Techniques for Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(1), 63-72. DOI: http://dx.doi.org/10.5281/zenodo.831678

[5] Krishna Prasad, K., & Aithal, P.S. (2017). Literature Review on Fingerprint Level 1 and Level 2 Features Enhancement to Improve Quality of Image. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 8-19. DOI: http://dx.doi.org/10.5281/zenodo.835608

[6] Krishna Prasad, K., & Aithal, P.S. (2017). Fingerprint Image Segmentation: A Review of State of the Art Techniques. *International Journal of Management, Technology, and Social Sciences (IJMTS),* 2(2), 28-39. DOI: http://dx.doi.org/10.5281/zenodo.848191

[7] Krishna Prasad, K., & Aithal, P.S. (2017). A Novel Method to Contrast Dominating Gray Levels during Image contrast Adjustment using Modified Histogram Equalization. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 27-39. DOI: http://dx.doi.org/10.5281/zenodo.896653

[8] Krishna Prasad, K., & Aithal, P.S. (2017).Two Dimensional Clipping Based Segmentation Algorithm for Grayscale Fingerprint Images. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 51-65. DOI: http://dx.doi.org/10.5281/zenodo.1037627.

[9] Krishna Prasad, K., & Aithal, P.S. (2017). A conceptual Study on Fingerprint Thinning Process based on Edge Prediction. *International Journal of Applied Engineering and Management Letters (IJAEML),* 1(2), 98-111. DOI: http://dx.doi.org/10.5281/zenodo.1067110.

[10] Krishna Prasad, K., & Aithal, P.S. (2017). A Study on Fingerprint Hash Code Generation Using Euclidean Distance for Identifying a User. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, 2(2), 116-126. DOI : http://doi.org/10.5281/zenodo.1133545.

[11] Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Multifactor Authentication Model Using Fingerprint Hash Code, Password and OTP. *International Journal of Advanced Trends in Engineering and Technology*, 3(1), 1-11. DOI : http://doi.org/10.5281/zenodo.1135255.

[12] Krishna Prasad, K. & Aithal, P. S. (2018). A Study on Fingerprint Hash Code Generation Based on MD5 Algorithm and Freeman Chain Code. *International Journal of Computational Research and Development*. 3(1), 13-22. DOI : http://doi.org/10.5281/zenodo.1144555.

[13] Tulyakov, S., Farooq, F., Mansukhani, P., & Govindaraju, V. (2007). Symmetric hash functions for secure fingerprint biometric systems. *Pattern Recognition Letters*, *28*(16), 2427-2436.

[14] Das, P. P., Chakrabarti, P. P., & Chatterji, B. N. (1987). Distance functions in digital geometry. *Information Sciences*, *42*(2), 113-136.

[15] Aithal, P. S., & Shubhrajyotsna Aithal, (2015). Ideal Technology Concept & its Realization Opportunity using Nanotechnology, *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 4(2), 153 - 164. DOI: http://doi.org/10.5281/zenodo.61591.

[16] Aithal, P. S. (2015). Concept of Ideal Business & Its Realization Using E-Business Model, *International Journal of Science and Research (IJSR)*, 4(3), 1267 - 1274. DOI : http://doi.org/10.5281/zenodo.61648.

[17] Aithal, P. S., & Shubhrajyotsna Aithal, (2016). Impact of On-line Education on Higher Education System. *International Journal of Engineering Research and Modern Education (IJERME), 1(*I), 225-235. DOI : http://doi.org/10.5281/zenodo.161113.

[18] Aithal, P. S., & Shubhrajyotsna Aithal (2015). An Innovative Education Model to realize Ideal Education System. *International Journal of Scientific Research and Management (IJSRM)*, 3(3), 2464-2469. DOI: http://doi.org/10.5281/zenodo.61654.

[19] Aithal, P. S., & Shubhrajyotsna Aithal, (2014). Ideal education system and its realization through online education model using mobile devices. *Proceedings of IISRO Multi Conference 2014, Bangkok*, 140 – 146. ISBN No. 978-81-927104-33-13.

[20] Aithal, P. S., (2016). Review on Various Ideal System Models Used to Improve the Characteristics of Practical Systems. *International Journal of Applied and Advanced Scientific Research*, 1(1), 47-56. DOI: http://doi.org/10.5281/zenodo.159749.

[21] Aithal, P. S. (2016). The concept of Ideal Strategy & its realization using White Ocean Mixed Strategy, *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 171-179. DOI : http://doi.org/10.5281/zenodo.161108.

[22] Sridhar Acharya, P. and Aithal, P. S., (2016). Concepts of Ideal Electric Energy System for production, distribution and utilization. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 367-379. DOI : http://doi.org/10.5281/zenodo.161143.

[23] Aithal, P. S., (2016). Smart Library Model for Future Generations. *International Journal of Engineering Research and Modern Education (IJERME)*, 1(1), 693-703. DOI : http://doi.org/10.5281/zenodo.160904.

[24] Aithal, P. S. (2016). Ideal Banking Concept and Characteristics. *International Research Journal of Management, IT and Social Sciences (IRJMIS)*, 3(11), 46-55. DOI: http://dx.doi.org/10.21744/irjmis.v3i11.311.

[25] Aithal, P. S. (2016). A Comparison of Ideal Banking Model with Mobile Banking System. *International Journal of Current Research and Modern Education (IJCRME)*, 1(2), 206-224. DOI: http://dx.doi.org/10.5281/ZENODO.198708.

[26] Aithal, P. S., & Vaikuth Pai, T., (2016). Concept of Ideal Software and its Realization Scenarios. *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 826-837. DOI : http://doi.org/10.5281/zenodo.160908.

[27] Shubrajyotsna Aithal, & Aithal, P. S., Bhat, G. K. (2016). Characteristics of Ideal Optical Limiter and Realization Scenarios using Nonlinear Organic Materials – A Review. *International Journal of Advanced Trends in Engineering and Technology (IJATET)*, 1(1), 73-84. DOI : http://doi.org/10.5281/zenodo.240254.

[28] Aithal, P. S., Suresh Kumar P. M. (2017). Ideal Analysis for Decision Making in Critical Situations through Six Thinking Hats Method. *International Journal of Applied Engineering and Management Letters (IJAEML)*, 1(2), 1-9. DOI: http://dx.doi.org/10.5281/zenodo.838378.

[29] Krishna Prasad, K., & Aithal, P.S. (2017). A Customized and Ideal Mobile Banking Technology Using 5G Technology. *International Journal of Management, Technology and Social Science (IJMTS)*, 2(1), 25-37. DOI: http://dx.doi.org/10.5281/zenodo.820860.

[30] Aithal, P. S., Shailashree, V. T., Suresh Kumar, P. M. (2015). A New ABCD Technique to Analyze Business Models & Concepts, *International Journal of Management, IT and Engineering (IJMIE)*, 5(4), 409-423. DOI : http://doi.org/10.5281/zenodo.61652.

[31] Aithal, P. S. (2016). Study on ABCD Analysis Technique for Business Models, Business strategies, Operating Concepts & Business Systems, *International Journal in Management and Social Science*, 4(1), 98-115. DOI : http://doi.org/10.5281/zenodo.161137.

[32] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy. *International Journal of Applied Research (IJAR)*, 1(10), 331-337. DOI: http://doi.org/ 10.5281/zenodo.163424.

[33] Aithal, P. S., Shailashree, V. T., & Suresh Kumar P. M., (2016). ABCD analysis of Stage Model in Higher Education. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 11-24. DOI: http://doi.org/10.5 281/zenodo.154233.

[34] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Analysis of NAAC Accreditation System using ABCD framework. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 30-44. DOI: http://doi.org/10. 5281/zenodo.154272.

[35] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). Application of ABCD Analysis Framework on Private University System in India. *International Journal of Management Sciences and Business Research (IJMSBR)*, 5(4), 159-170. DOI : http://doi.org/10.5281/zenodo.161111.

[36] Aithal, P. S., Shailashree, V. T., & Suresh Kumar, P. M. (2016). The Study of New National Institutional Ranking System using ABCD Framework, *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 389–402. DOI : http://doi.org/10.5281/zenodo.161077.

[37] Aithal, S., & Aithal, P. S. (2016). ABCD analysis of Dye doped Polymers for Photonic Applications, IRA-International Journal of Applied Sciences, 4 (3), 358-378. DOI: http://dx.doi.org/10. 21013/j as.v4.n3.p1.

[39] Aithal, P. S., Shailashree, V. T. & Suresh Kumar, P. M., (2016). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 846-858. DOI : http://doi.org/10.5281/ zenodo.62022.

[40] Varun Shenoy, & Aithal P. S., (2016). ABCD Analysis of On-line Campus Placement Model, IRA-International Journal of Management & Social Sciences, 5(2), 227-244. DOI: http://dx.doi.org/10.21013/jmss .v5.n2.p3.

[41] Aithal, P. S., Shailashree V. T. & Suresh Kumar P.M. (2016). Factors & Elemental Analysis of Six Thinking Hats Technique using ABCD Framework. *International Journal of Advanced Trends in Engineering and Technology (IJATET)*, 1(1), 85-95. DOI : http://doi.org/10.5281/zenodo.240259.

[42] Aithal, P. S., Shailashree V. T & Suresh Kumar P. M., (2016). Analysis of ABC Model of Annual Research Productivity using ABCD Framework. *International Journal of Current Research and Modern Education (IJCRME)*, 1(1), 846-858. DOI : http://doi.org/10.5281/zenodo.62022.

[43] Aithal, P. S. & Suresh Kumar, P. M. (2016). Opportunities and Challenges for Private Universities in India. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 88-113. DOI : http://doi.org/10.5281/zenodo. 161157.

[44] Padmanabha Shenoy, & Aithal, P. S., (2016). A Study on History of Paper and possible Paper Free World. *International Journal of Management, IT and Engineering (IJMIE)*, 6(1), 337-355. DOI : http://doi.org/10.5281/zenodo. 161141.

[45] Aithal, P.S., (2015). Comparative Study on MBA Programmes in Private & Public Universities - A case study of MBA programme plan of Srinivas University, ***International Journal of Management Sciences and Business Research (IJMSBR),*** 4(12), 106-122. DOI : http://doi.org/10.5281/zenodo.163884.

[46] Aithal P. S., & Shubhrajyotsna Aithal (2016). Impact of On-line Education on Higher Education System. *International Journal of Engineering Research and Modern Education (IJERME)*, 1(1), 225-235. DOI : http://doi.org/ 10.5281/zenodo.161113.

[47] Aithal P. S., and Suresh Kumar P. M., (2016). Analysis of Choice Based Credit System in Higher Education. *International Journal of Engineering Research and Modern Education (IJERME)*, 1(1), 278-284. **DOI :** http://doi.org/ 10.5281/zenodo.161046.

[48] Varun Shenoy and Aithal P. S., (2016). Changing Approaches in Campus Placements - A new futuristic Model, *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 766 – 776. DOI : http://doi.org /10.5281/zenodo.160966.

[49] Prithi Rao, and Aithal, P.S. (2016). Green Education Concepts & Strategies in Higher Education Model, *International Journal of Scientific Research and Modern Education (IJSRME)*, 1(1), 793-802. DOI : http://doi.org/ 10.5281/zenodo.160877.

[50] Aithal, P. S. & Shubhrajyotsna Aithal (2016). Ekalavya Model of Higher Education – an Innovation of IBM's Big Data University. *International Journal of Current Research and Modern Education (IJCRME)*, 1(2), 190-205. **DOI:** http://dx.doi.org/10.5281/ZENODO.198704**.**

[51] Aithal, P. S. & Shubhrajyotsna Aithal, (2016). A New Model for Commercialization of Nanotechnology Products and Services. *International Journal of Computational Research and Development*, 1(1), 84-93. **DOI :** http://doi.org/10.5281/zenodo.163536.

[52] De Marsico, M., Galdi, C., Nappi, M., & Riccio, D. (2014). FIRME: face and iris recognition for mobile engagement. *Image and Vision Computing*, 32(12), 1161-1172.

[53] Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. *International Journal of advanced science and Technology*, 4, 25-38.

[54] Aithal, P. S. (2016). A Review on Advanced Security Solutions in Online Banking Models, International Journal of Scientific Research and Modern Education (IJSRME), 1(1), 421-429. DOI : http://doi.org/10.5281/zenodo.160971.

[55] Aithal, P. S. (2015). Biometric Authenticated Security Solution to Online Financial Transactions. *International Journal of Management, IT and Engineering (IJMIE)*, 5(7), 455-464, DOI : http://doi.org/10.5281/zenodo.268875.

****

Reviewers

Dr. P. S. AITHAL
Professor,
College of Computer and Information Sciences
Srinivas University, Mangalore, India.

Dr. NASIB SINGH GILL
Professor, Dept. of Computer Science and Applications,
M.D. University, Rohtak – 124001
Haryana, India.

Dr. B. H. SHEKAR
Professor,
Department of Computer Science,
Mangalore University, Mangalore, India.

About Srinivas University:

Srinivas University, Mangalore, is a Private Research University in Mangalore, Karnataka, India established in 2013 by Karnataka State Act. No.42. Recognized by UGC & Member of Association of Indian Universities, New Delhi. The various colleges under Srinivas University are;

College of Business Management & Commerce

College of Computer & Information Sciences

College of Social Science &Humanities

College of Engineering & Technology

College of Hotel Management & Tourism

College of Physiotherapy

College of Allied Health Sciences

College of Education

Srinivas Publication
(An International Publisher for Academic & Scientific Journals and Book)
Srinivas University,
A. Shama Rao Foundation,
G.H.S. Road, Mangalore-575001,
Karnataka State, India.
Emil: srinivaspublication@srinivasgroup.com
Website: www.srinivaspublication.com

ISBN 978-81-938040-3-2