Paper 19

A STUDY ON MULTIFACTOR AUTHENTICATION MODEL USING FINGERPRINT HASH CODE AND IRIS RECOGNITION

Krishna Prasad K. [#1] **& Dr. P.S. Aithal**[*2]

[#] Research Scholar, College of Computer and Information Science, Srinivas University, Mangaluru-575001, Karnataka, India

[*] College of Computer and Information Science, Srinivas University, Mangaluru-575001, Karnataka, India

E-mail: karanikrishna@gmail.com

Abstract

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. This model proposes instead of password iris of the user, which is also one of the strongest physiological biometrics recognition systems. The iris is absolutely fashioned by way of eighth month of adults, and remains stable throughout the life span. In recent years, the usage of Iris for human identification has substantially grown due to the tremendous advantages with traditional or usual or normal authentication techniques based on private identity numbers (PINs) or passwords. In fact, given that iris is intrinsically and uniquely related to a character, they can't be forgotten, without difficulty stolen or reproduced. But, the use of Iris may additionally have some drawbacks related to viable safety breaches. On the grounds that iris traits are limited and immutable, if an attacker has get access to the database where they are saved, the system security may be irreparably compromised. To deal with this hassle, an iris structure with template protection becomes very much essential. In this paper the different methods of iris recognition are studied with its features. This paper also discusses about multifactor authentication model.

Keywords: Fingerprint Recognition, Fingerprint Hash code, Iris Recognition, Multifactor Authentication Model, Template Protection.

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 or similar components like biometric sensor module, feature extractor module, a matching module, decision-making module and system database [1-2]. System makes use of different capturing devices with an intention to acquire biometric traits to an automated system. These include camera and scanning devices to capture images, speakers for recording voice, the special type of sensors to capture behavioral traits, computer hardware, and software to extract, purify or enhance, store and compare the characteristics or features of biometric traits [3-5].

Cell phones have become important electronic device or equipment in human life. Clients get to their messages, informal organizations, financial balances, and different sites by means of cell phones. Portable equipment makers, working framework and application engineers take a collection of safety efforts because of the individual, private as well as the touch sensitive nature of the data move away in cell phones. The utilization of biometric authentication on cell phones began with cameras. Initially, cell phone producers have included biometric validation or identification frameworks like the increasingly well known unique fingerprint recognition system [6-10]. 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 [11-15].

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 [16-20].

The iris is absolutely fashioned by way of the eighth month of adults and remains stable throughout the lifespan. Statistically extra accurate than even DNA matching since the opportunity of irises being same is 1 in 10^{78}. In this paper, we develop a conceptual model for user identification using fingerprint Hash code and Iris. This paper has seven sections. Section 1 describes introductory theory related to fingerprint, Hash code and Iris recognition. Section 2 explains about brief literature review of Multifactor Authentication Model developed by many researchers. Section 3 narrates Objectives of the study. Section 4 describes methodologies used for fingerprint Hash code generation using Euclidean distance. Section 5 describes a conceptual model for user identification using fingerprint Hash code and Iris. Section 6 makes an analysis of new model using ABCD analysis. Section7 concludes the paper.

2. BACKGROUND 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) [21] 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 is 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 [22]. Aloul, F. et al., (2009) [23] 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) [24], 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% [25]. Delac, K., & Grgic, M. (2004, June) [26] 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) [27] 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) [28] 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) [29] 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 [30-31-27].

Yoo, J. H. et al., (2007, December) [32] 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) [33] 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.

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 and Iris recognition. Fingerprint alone not gives full security; in order to improve the security of the system fingerprint hash code is combined with iris of the user. The main objectives of this study are given below.

- To propose an alternative approach for User Authentication using Multifactor with Fingerprint Hash code and Iris.
- To analyze the new model using ABCD analysis.

4. FINGERPRINT HASH CODE GENERATION USING EUCLIDEAN DISTANCE

Figure 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.

The step by step procedure to develop Hashcode by making use of Euclidean distance matrix on a binary fingerprint image is explained below. The algorithm also shows the pseudo code [13].

```
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)
```

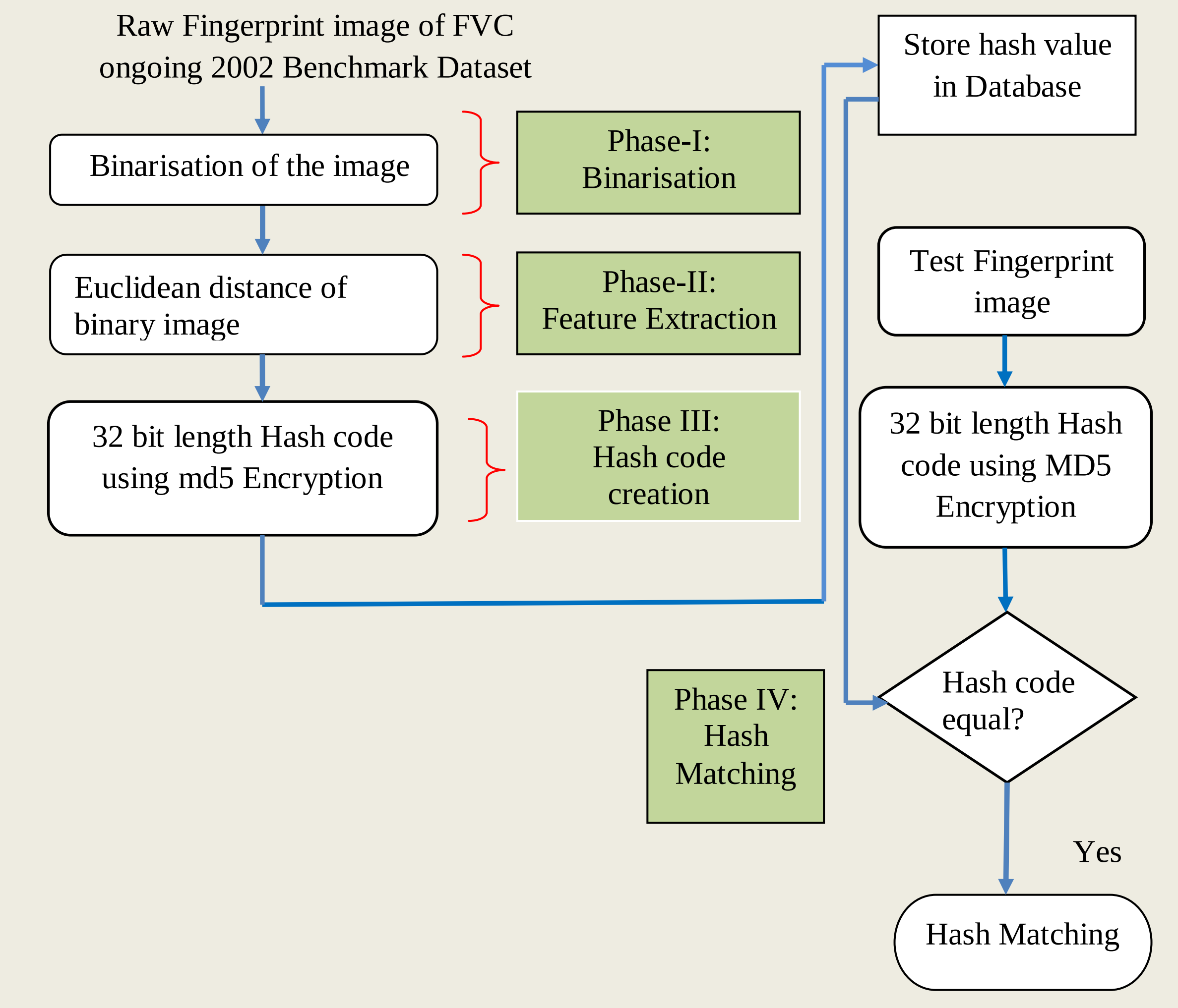
Raw Fingerprint image of FVC ongoing 2002 Benchmark Dataset
Binarisation of the image
Phase-I: Binarisation
Euclidean distance of binary image
Phase-II: Feature Extraction
32 bit length Hash code using md5 Encryption
Phase III: Hash code creation
Store hash value in Database
Test Fingerprint image
32 bit length Hash code using MD5 Encryption
Hash code equal?
Phase IV: Hash Matching
Yes
Hash Matching

Figure 1: Methodologies used for Fingerprint Hash code generation [13]

5. MULTIFACTOR AUTHENTICATION MODEL USING FINGERPRINT HASH CODE AND IRIS RECOGNITION

Figure 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 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.

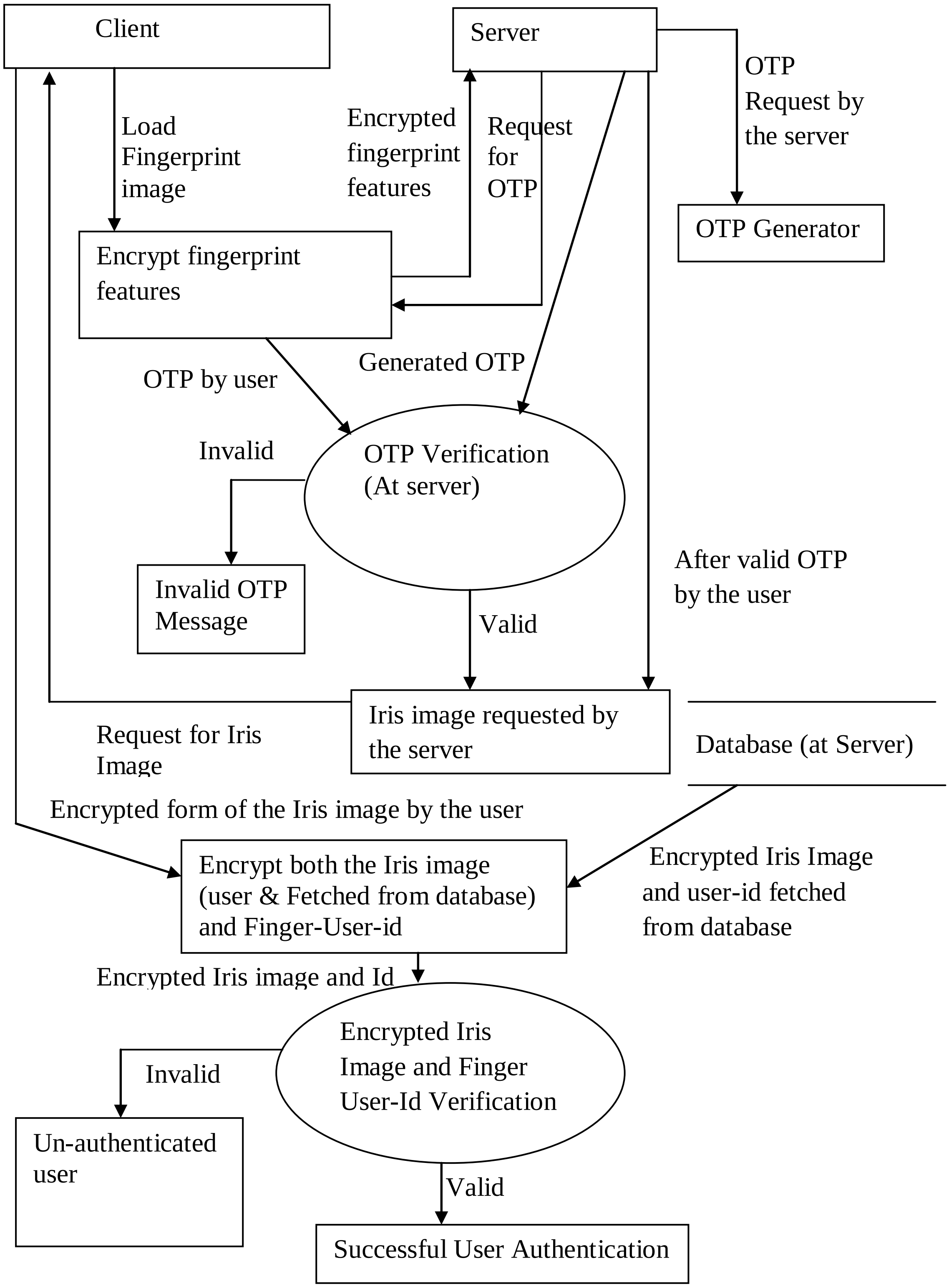
Client
Server
Load Fingerprint image
Encrypted fingerprint features
Request for OTP
OTP Request by the server
OTP Generator
Encrypt fingerprint features
Generated OTP
OTP by user
Invalid
OTP Verification (At server)
Invalid OTP Message
After valid OTP by the user
Valid
Iris image requested by the server
Database (at Server)
Request for Iris Image
Encrypted form of the Iris image by the user
Encrypt both the Iris image (user & Fetched from database) and Finger-User-id
Encrypted Iris Image and user-id fetched from database
Encrypted Iris image and Id
Encrypted Iris Image and Finger User-Id Verification
Invalid
Un-authenticated user
Valid
Successful User Authentication

Figure 2: Dataflow Diagram of Proposed Multifactor Authentication

The client mobile phone automatically takes this OTP and is compared with server generated OTP at the server side. If OTP is verified, server requests for the Iris of the user. The server verifies the iris image using neural network with the already stored iris template in its database. Since Iris image is stored in encrypted format, it's not possible to recover original information so easily. So if an intruder gets stored hash codes from the database, still authentication cannot become successful. If both Iris image and Fingerprint Hash code match then user is considered as an authenticated user. In other words authentication process successfully completes when OTP, Iris image, and Fingerprint Hash code matches. If anyone out of Fingerprint Hash code or Iris image 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. This model is used in Smart mobile phones for authentication purpose.

6. 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 [34-36].

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 Iris image 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.
- The database makes use of SHA-256 algorithm for Hash generation, which makes hash code very robust.
- 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 Mobile banking or any other mobile based secured authentication systems.
- 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.
- 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.
- User does not need to remember anything, Fingerprint hash code and Iris recognition system automatically does verification.

Constraints

- The user should have good configuration mobile camera or high resolution and pixel based mobile camera embedded in heir smart phones.
- While capturing Iris image user should focus and see the mobile camera straight and in fixed angle to capture right Iris image for recognition purpose.
- Lower mobile network coverage makes a denial to the system because of not getting the OTP in time.
- Iris recognition system makes the system costlier.

Disadvantages

- Biometric Fingerprint is less emphasized in verification or authentication process in Multifactor Authentication model.
- The User cannot be verified or authenticated without proper Iris image.
- Multifactor Authentication Model used in this study is not suitable for a system which does not utilize a mobile phone like a biometric attendance system.
- Multifactor Authentication Model used in this study requires client-server architecture and not helpful for a standalone system.

7. CONCLUSION

Authentication frameworks in light of multiple factors 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 not full secret and secured, 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 fingerprints and 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 this Multifactor Authentication model acts as identity-key or index-key to uniquely identify individual persons. Fingerprint Hash code, combined with Iris image with the aid of the neural network 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 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] 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. & 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] Krishna Prasad, K. & Aithal, P.S. (2018). 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), 1-13. DOI: IJIRMET1602012001.

[15] 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.

[16] 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.

[17] Krishna Prasad, K. & Aithal, P.S. (2018). A Comparative Study on Fingerprint Hash Code, OTP, and Password based Multifactor Authentication Model with an Ideal System and Existing Systems. *International Journal of Applied and Advanced Scientific Research,* 3(1), 18-32. DOI: http://doi.org/10.5281/zenodo.1149587.

[18] Krishna Prasad, K. & Aithal, P. S. (2018). A Novel Tuning Based Contrast Adjustment Algorithm for Grayscale Fingerprint Image. *Saudi Journal of Engineering and Technology (SJEAT),* 3(1), 15-23. DOI: http://10.21276/sjeat.2018.3.1.3.

[19] Krishna Prasad, K. & Aithal, P.S. (2018). ABCD Analysis of Fingerprint Hash Code, Password and OTP based Multifactor Authentication Model. *Saudi Journal of Business and Management Studies,* 3(1), 65-80. DOI: http://10.21276/sjbms.2018.3.1.10.

[20] Krishna Prasad, K. & Aithal, P.S. (2018). A Study on Pre and Post Processing of Fingerprint Thinned Image to Remove Spurious Minutiae from Minutiae Table**.** *International Journal of Current Research and Modern Education*, 3(1), 197-212. DOI: http://doi.org/10.5281/zenodo.1174543.

[21] 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.

[22] Bemmel, V., & Mian, S. (2009). U.S. Patent No. 7,512,567. Washington, DC: U.S. Patent and Trademark Office.

[23] Aloul, F. A., Zahidi, S., & El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In AICCSA (pp. 641-644).

[24] 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.

[25] Angulo, J., & Wästlund, E. (2011, September). Exploring touch-screen biometrics for user identification on smart phones. In IFIP Prime Life International Summer School on Privacy and Identity Management for Life (pp. 130-143). Springer Berlin Heidelberg.

[26] 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.

[27]. 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.

[28] 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.

[29] Kumar, D., & Ryu, Y. (2009). A brief introduction of biometrics and fingerprint payment technology. International Journal of advanced science and Technology, 4, 25-38.

[30] 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.

[31] 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.

[32] 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.

[33] 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.

[34] Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2015). Application of ABCD Analysis Model for Black Ocean Strategy.

[35] Aithal, P. S. (2016). Study on ABCD analysis technique for business models, business strategies, operating concepts & business systems.

[36] Aithal, P. S., Shailashree, V. T., & Kumar, P. M. (2016). ABCD analysis of Stage Model in Higher Education.

****