RESEARCH ARTICLE OPEN ACCESS

The Survey of Architecture of Multi-Modal (Fingerprint and Iris Recognition) Biometric Authentication System

Afshan Ashraf[1], Isha Vats[2]
[1]*Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali, Punjab, India.*
[2]*Department of Computer Science and Engineering, Chandigarh Engineering College, Landran, Mohali , Punjab, India.*

ABSTRACT
Biometrics based individual identification is observed as an effective technique for automatically knowing, with a high confidence a person's identity. Multi-modal biometric systems consolidate the evidence accessible by multiple biometric sources and normally better recognition performance associate to system based on a single biometric modality.Multi biometric systems are used to overcome this issue by providing multiple pieces of indication of the same identity. This system provides effective fusion structure that combines information provided by the multiple field experts based on decision-level and score-level fusion method, thereby increasing the efficiency which is not conceivable in uni-modal system.Multi-modal biometrics can be attained through a fusion of two or more images, where the subsequent fused image will be more protected. This paper discusses various fusion techniques, architecture of multi-modal biometric authentication and working of biometric fusion i.e. Iris and Fingerprint recognition that are used in multi-modal biometrics.
Keywords: Multi-modal Biometric Authentication, Iris and Fingerprint recognition, Fusion methods i.e. Score Level Fusion and Decision Level Fusion.

I. INTRODUCTION

Biometric systems automatically determine or confirm a person's identity based on his anatomical and behavioural characteristics like fingerprint, palm print, vein pattern, face and iris[1]. A method of recognizing or confirming the identity of an individual person or subject that depends on the physiological and behavioural characteristics is biometric recognition. Multimodal biometrics rise correctness by considering other very specific biological traits to limit the no of applicant for an identity. Multimodal biometric systems use more than one physiological or behavioural characteristic for enrolment, verification and identification.

A multimodal biometric authentication, which recognizes an individual person using physiological and behavioural characteristics, such as face, fingerprints, finger geometry, iris, retina, vein and speech is one of the best attractive and effective techniques. These methods are more reliable and capable than knowledge-based[2] (e.g. password) or token-based (e.g. Key) methods. Since biometric features are hardly stolen and forgotten. However, a single biometric feature sometimes fails to be exact sufficient for confirming the identity of a person. Through combining multiple modalities enhanced presentation reliability could be achieved. Due to its promising requests as well as the theoretical challenges, multimodal biometric has drawn more and more attention in current years. Iris and fingerprint multimodal biometrics are beneficial due to the use of non-invasive and low-cost picture acquisition. In this method we can easily acquire iris and fingerprint images using two touch sensors simultaneously. Existing studies in this approach [3] serve holistic features for face representation and results are shown with minorrecords set that was reported. Multimodal system also provides anti-spoofing measures by which it becomes problematic for an intruder to spool multiple biometric traits at the same time. However, an integration scheme is required to fuse the data presented by the individual modalities.

Multimodal biometric scheme has addressed some issues related to uni-modal biometrics such as; [4]

(a) Non-universality or insufficient population coverage (reduce failure to enrol rate which rises population coverage).

(b) It becomes totally unmanageable for an impostor to imitate several biometric traits of a legitimately enrolled user separately.

(c) Multimodal-biometric systems offer climbing evidence in solving the difficulty of noisy data (illness affecting voice, scar affecting fingerprint).

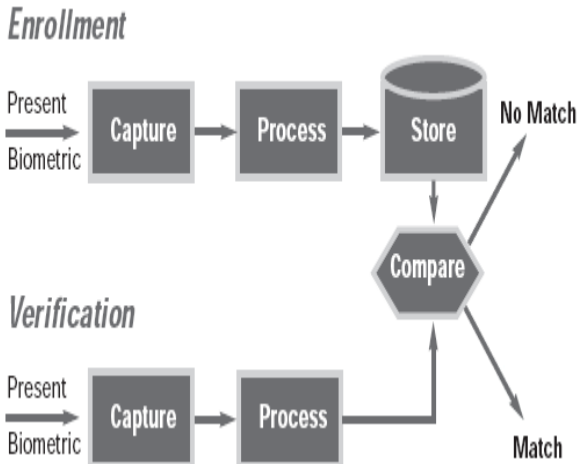

Figure no.1: Biometric Authentication [5]

II. STEPS OF MULTI-MODAL BIOMETRIC SYSTEM

The simple requirements of any biometric system are Input device, Biometric software and Databank.

A. Input Device: An input device like scanner, writing pad etc. are used to control the input which is then used by the software part.

B. Biometric Software: Software to process the input and changes it into digital form, extracts the features and compares the result[6]. In terms of correctness, the performance of a biometric system totally depends on the quality of the software.

C. Database: A databankis used to store the mathematical data which is further used for the comparison. Features extracted from the input samples are kept instead of input samples as the samples take more space and putting away features saves time for processing samples again to extract the features. The presentation of the software is most important part of a biometric system as the accuracy of the system should be contingent on quality of the software.

III. ARCHITECTURE OF MULTI-MODAL BIOMETRIC SYSTEM

The two main processes involved are enrolment or registration, confirmation and identification. Fig. 2 shows the architecture of a general biometric system.

A. *Registration Process:* In order to identify an individual, it is necessary to store the individual's features in a databank, which are extracted from the reliable samples of the biometric trait either look over or recorded using input device like writing pads[7]. These features are then matched with the features extracted from the traits of the individual necessary to be identified.

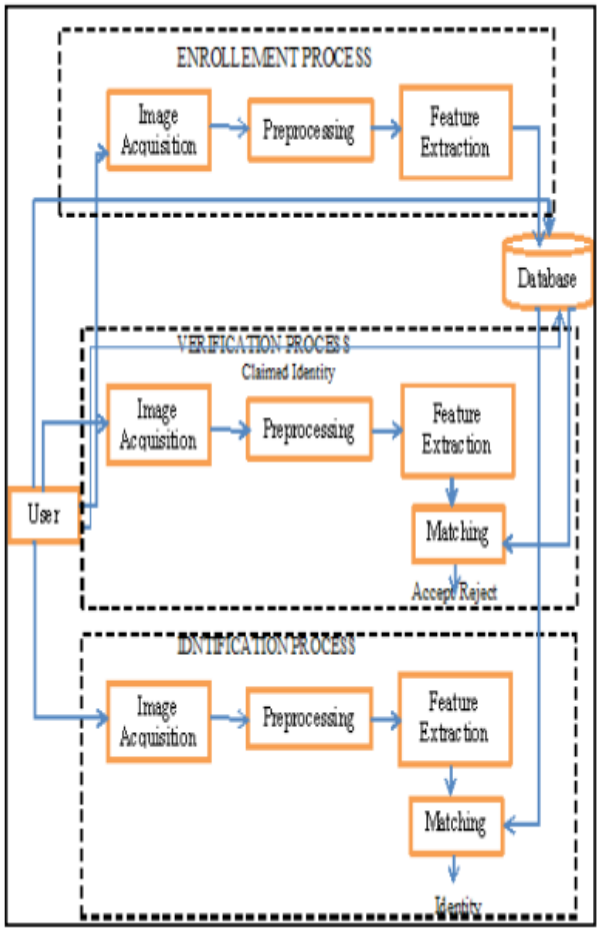

Figure no.2: Architecture of a general biometric system[7]

B. In order to extract features, the input model is pre-processed and feature extraction algorithm is applied on these pre-processed examples to form feature vectors. Instead of input models these feature vectors are stored in the databank as input samples take more space on secondary memory than mathematical files and features are computed just once which protect a lot of processing time. A classifier is trained by these feature vectors which then classifies the unknown input sample.

C. Verification: In the verification manner, the system validates a person's identity through

associating the captured biometric data with his own biometric template kept in the system database. In such a system, an individual who needs to be recognized claims an identity, mainly via PIN (Personal Identification number), a user name or a smart card and the system store uses a one to one comparison to define whether the claim is true or not [8].

D. *Identification:* In identification mode the system recognizes a genuine user by searching the templates provided by the user in the databank for a match. Therefore, the system conducts a one to several comparisons to identify an individual entity or fails to identify if the subject is not enrolled in the system database[9].

IV. LEVELS OF MULTI-MODAL BIOMETRIC FUSION SYSTEM

Biometric Fusion takes place at various levels i.e Sensor, decision and score etc. described below: [10]

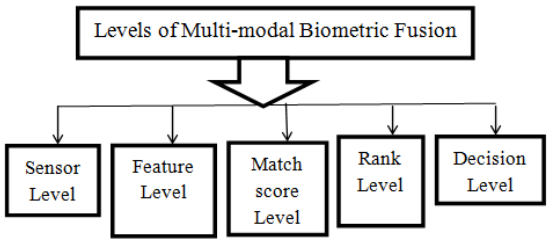

Figure no. 3: Levels of Biometric Fusion

A. Sensor level: This fusion strategy requires the raw data to be acquired from multiple sensors which can further be processed and integrated to make new data from which features can be extracted. Sensor level fusion can be done only if multiple cues of the similar biometric are obtained from multiple compatible sensors.

B. Feature level: The feature set is mined from many sources of information and is further concatenated into a joint feature vector. This novel high dimensional feature vector represents an individual. In case of feature level fusion some reduction method must be used in order to select only useful features [11].

C. Match score level: Match score is a measure between input biometric and template biometric feature vectors. Based on the similarity of feature vector and the template, every subsystem calculates its own match score value. These individual scores are finally joined to obtain a total score, which is then passed to the decision module, after which recognition is performed.

D.Rank level: Rank level fusion is normally adopted for the identification of the person rather than verification. Thus, fusion entails consolidating the ranks associated with an identity and determining a new rank that would aid in establishing the final decision.

E. Decision level: In a multi-modal biometric system, fusion is carried out at this level when only the decision output is available. Here, a separate authentication decision is computed for every biometric trait which is then combined that results in a final output. Different strategies are available to group the distinct decisions of individual modality to a final authentication decision. Fusion at this stage is regarded to be definite as far as other fusion levels are considered because very less information is available[12].

V. RELATED WORK

Satrajit Mukherjee et.al,2014[13] defined that theNovel adaptive weight and supporter based function mapping the matching scores from dissimilar biometric causes into a single merged matching score to be used by a classifier for further decision making. Differential Growth has been working to regulate these tuneable parameters with

the independent being the minimization of the covering area of the occurrence distributions of open and imposter scores in the fused score space, which are projected by Gaussian kernel density method to achieve higher level of accuracy. **Samarth Bharadwaj et.al, 2014 [14]** the paper present theReview of the features, strengths, and boundaries of existing quality evaluation technique in fingerprint, iris, and face biometric are also obtainable. lastly, a courier set of quality metrics from these three modalities are evaluate on a multimodal database consisting of 2D images, to appreciate their performance with deference to match score obtained from the state of the art recognition systems. The study of the characteristic function of excellence and match scores show that a cautious selection of admiring set of superiority metrics can provide more advantage to various applications of biometric excellence.**Vincenzo Cont et.al,2013 [15]** In this section fingerprint and iris based uni-modal and multimodal confirmation systems will be describe, analyse and evaluate. To conclude, a proto typed embedded multimodal biometric sensor will be sketch. Software and hardware proto-types have been checked against common and broadly used databases.**Sambit Bakshi et.al., 2012 [16]** in this articleachieved classification operation on the detected key points. Each set of the key points of the query image was exposed to nearest national match with respective set of key points of the database image. Hence there were two notches generated by the matching of two classes. This paper also recommends a accurate monotonic function on these dual scores to produce a single score such that the final score rate gives rise to better disjunction between unaffected and imposter scores than conservative SIFT. **Vincenzo Conti et.al. 2012 [17]** presentedthecontract with modern computing systems safety issues, focusing on biometric founded asymmetric keys generation procedure. Conservative PKI systems were based on private/public keys produced through RSA or similar algorithms. The present solution embeds biometric information on the private or public keys generation process. In addition the conforming private key depends on physical or interactive biometric features and it can be produced when it was needed. Initial from fingerprint acquisition, the biometric identifier were extracted, cyphered, and stored in tamper resilient smartcard to overcome the security difficulties of centralized databases. Biometric information is then used for user verification and for public/private keys generation.

VI. FINGERPRINT AND IRIS RECOGNITION SYSTEM

A. Fingerprint Recognition

A serious step in automatic fingerprint matching is to automatically and reliably extract minutiae features from the input fingerprint picture. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint picture. In order to ensure that the performance of an automatic fingerprint identification/verification scheme would be robust with respect to the quality of the fingerprint imageries, it would be essential to incorporate a fingerprint improvement algorithm in the minutiae extraction module.[18]

Figure no. 4: Original Image[18]

Procedure of Fingerprint Recognition System (Steps):

- *Normalization:* Normalization allows standardizing the distorted levels of variation in the gray scale values amongst ridges and valleys. Histogram equalization, as normalization method, is a process to enhance the contrast of a picture by transforming its intensity values.
- *Segmentation*: In general, only a Region of Interest is useful to be recognized for each fingerprint picture. The image area without effective ridges and furrows is first discarded since it only holds background data.
- *Minutiae Extraction:*The endings and bifurcations of the fingerprint images are known as the minutiae.

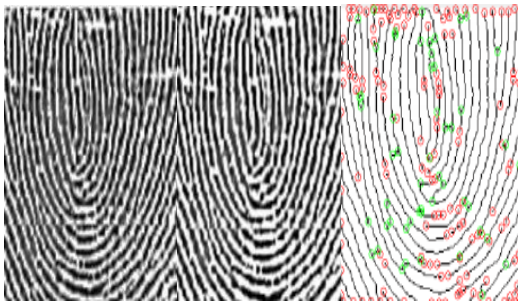

Figure no. 5(i) Normalized Image (ii) Segmented and (iii) Minutiae Features[18]

B. Iris Recognition

Iris recognition is a method of biometric authentication that uses pattern appreciation techniques based on high-resolution picture of the edges of an individual's eyes.[19]

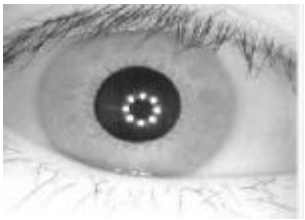

Figure no. 6: Iris Recognition[19]

Process of Iris recognition:

- *Iris Segmentation:* This involves first employing Canny Edge Detection to create an edge map.
- *Iris Localization*: In the work, in order to increase the complete speed of the system, circle detection algorithm is used.
- *Iris Normalization:* After successfully extracting the iris part from the eye picture, in order to allow comparisons between dissimilar irises, transform the extracted iris area so that it has a fixed dimension, and hence, removing the dimensional inconsistencies between eye pictures due to the stretching of the iris caused by the pupil dilation from varying levels of illumination.
- *Iris Feature Extraction:* This is the most key part of an iris recognition system and determines the system's performance to a great extent. Iris recognition produces the exact result by extracting features of the input picture and matching these features with known designs in the feature database.

Table 1: Comparison between Techniques in Fingerprint and Iris Recognition System

AUTHOR	FUSION	DATA SET
Muhammad et al.[18]	SCORE	Face, Finger vein
Mohammed et al.[19]	SCORE	Face, Speech
Dhanashree et al.[20]	FEATURE	Palmprint,Palm vein
Rattan et.al[21]	FEATURE	Face, Fingerprint
Bhagat et al[22]	FEATURE	Palmvein,face
Feifei et al[23]	SCOPE	Fingerprint, vein
Krishneswari et al[24]	FEATURE	Fingerprint, palm print
Nazmeen et al[25]	DECISION	Face, ear
Nageshkumar et al[26]	SCORE	Palmprint,Face
Krzyszof et al[27]	DECISION	Face, Speech
Mohamed et al[28]	DECISION	Fingerprint, iris
Lin hong et al[29]	DECISION	Palmprint,face
Gayatri et al[30]	FEATURE	Face,Palmprint
Mitil et al[31]	FEATURE	Palm print, fingerprint
Jegadeesan et al[32]	FEATURE	Fingerprint, iris

VII. EXISTING APPROACH

A. *The rule-based:* Fusion method includes a variety of simple rules for joining of multimodal information. These include statistical rule-depend methods like linear weighted fusion (sum and product), MAX, MIN, AND, OR, mainly voting. There are custom-defined rules that are constructed for the particular application perspective. The rule-based patterns generally perform well if the quality of temporal alignment between dissimilar modalities is good.[20]

B. *Classification-based fusion methods:* This category of techniques includes a range of classification methods that have been used to categorize the multimodal observation into one of the pre-defined classes. The techniques in this category are the(SVM) support vector machine, Bayesian inference, Dumpster–Shafer theory, active Bayesian networks, neural networks and maximum entropy model. We can further classify these methods as generative and discriminative models from the device learning perspective. For example, Bayesian inference and dynamic Bayesian links are generative models, while support vector machine and neural networks are discriminative models.

C. *Estimation-based fusion methods*: The estimation classification includes the Kalman filter, extended Kalman filter and particle filter fusion methods. These techniques have been primarily used to better estimate the state of a moving object based on multimodal data. For example, for the duty of object tracking, multiple modalities such as audio and video are fused to estimate the position of the object.

D. Scale Invariant Feature Transformation: The SIFT approach, for picture highlight era, takes a picture and changes it into an "expansive meeting of neighbourhood highlight vectors" Each of these highlight vectors is invariant to any scaling, revolution or interpretation of the picture. This methodology offers numerous highlights with neuron reactions in primate vision. To help the extraction of these highlights the SIFT calculation applies a 4 stage separating methodology:

- Scale Space
- Localization
- Assignment and Orientation [33]
- Key point Descriptor

*E. RSA Algorithm:*The RSA algorithm is based on the assumption that integer factorization is a difficult problem. This means that given a large value n, it is problematic to find the prime factors that make up n. It is most popular asymmetric key algorithm[34].

VIII. CONCLUSION

Biometric features are unique to each individual and remain unaltered throughout a person's lifetime. These features made biometrics a promising solution to the society. In this paper, a robust multimodal biometric recognition structure integrating iris and fingerprint is studied. Fusion of two biometric traits is carried out at the match score level. The domain of multi biometrics is a new and exciting area of information science study which is directed towards understanding of traits and methods for accurate and reliable personal data representation for subsequent decision making and matching. In the current years there is a significant increase in study activity directed at understanding all aspects of biometric data system representation and utilization for decision-making support, for use through public and security services, and for understanding the difficult processes behind biometric matching and recognition. Uni-modal has some disadvantages so we can go for multi-modal biometric system. In order to increase the complexity to the im-poster and to the improve the accuracy, we can go for Multi-modal biometrics.

In Future Scope, Future works could go in the direction of using Genetic algorithm or ICA in hybridization with BFO. Independent Component Analysis (ICA) is a computational method to get hidden values of random variables. ICA is basically designed for multivariate data.

REFERENCES

[1] Patil, Savitri B. "A Study of Biometric, Multimodal Biometric Systems: Fusion Techniques, Applications and Challenges." *IJCST* 3, no. 1 (2012): 524-526.

[2] Rodrigues, Ricardo N., Lee Luan Ling, and VenuGovindaraju. "Robustness of multimodal biometric fusion methods against spoof attacks." *Journal of Visual Languages & Computing* 20, no. 3 (2009): 169-179.

[3] Nageshkumar, M., P. K. Mahesh, and MN ShanmukhaSwamy. "An efficient secure multimodal biometric fusion using palmprint and face image." *arXiv preprint arXiv:0909.2373* (2009).

[4] Gawande, Ujwalla, AnushreeSapre, Apurva Jain, SanchitaBhriegu, and Shruti Sharma. "Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming

Distance Matcher." *International Journal of Engineering Inventions e-ISSN*: 2278-7461.

[5] Sree, SR Soruba, and Dr N. Radha. "A survey on fusion techniques for multimodal biometric identification." *International Journal of Innovative Research in Computer and Communication Engineering* 2, no. 12 (2014).

[6] Nair, S. Anu H. "Analysis of Image Fusion Techniques for fingerprint Palmprint Multimodal Biometric System." *International Journal of engineering Research and Applications* 1, no. 5: 77-83.

[7] Kaur, Dapinder, and GaganpreetKaur. "Level of fusion in multimodal biometrics: a review." *International Journal of Advanced Research in Computer Science and Software Engineering* 3, no. 2 (2013): 242-246.

[8] W. Yunhong, T. Tan, & A. K. Jain, Combining Face and Iris Biometrics for Identity Verification, Proceedings of Fourth International Conference on AVBPA, Guildford, UK, 2003, 805-813.

[9] S. C. Dass, K. Nandakumar, & A. K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA), Rye Brook, NY, 2005

[10] Phalguni Gupta, AjitaRattani, HunnyMehrotra, Anil Kumar Kaushik, Multimodal Biometrics System for Efficient Human Recognition, Indian Institute of Technology Kanpur, India – 208016.

[11] SangramBana, Dr.DavinderKaur, Fingerprint Recognition using Image Segmentation, (IJAEST) INTERNATIONAL JOURNAL OF ADVANCED ENGINEERING SCIENCES AND TECHNOLOGIES Vol No. 5, Issue No. 1, 012 – 023.

[12] Masek, L. (2003), ―Recognition of Human Iris Patterns ForBiometric identification‖, Thesis Report, The University ofWestern Australia.

[13] Ghoualmi, Lamis, SalimChikhi, and AmerDraa. "A SIFT-Based Feature Level Fusion of Iris and Ear Biometrics." Multimodal Pattern Recognition of Social Signals in Human-Computer-Interaction. Springer International Publishing, 2015. 102-112.

[14] Bharadwaj, Samarth, MayankVatsa, and Richa Singh. "Biometric quality: a review of fingerprint, iris, and face." EURASIP Journal on Image and Video Processing 2014.1 (2014): 1-28.

[15] Conti, Vincenzo, et al. "Fingerprint and Iris Based Authentication in Inter-cooperative Emerging e-Infrastructures." Internet of Things and Inter-cooperative Computational Technologies for Collective Intelligence. Springer Berlin Heidelberg, 2013. 433-462.

[16] Bakshi, Sambit, et al. "Score level fusion of SIFT and SURF for iris."Devices, Circuits and Systems (ICDCS), 2012 International Conference on. IEEE, 2012.

[17] Conti, Vincenzo, Salvatore Vitabile, and FilippoSorbello. "Fingerprint traits and rsa algorithm fusion technique." Complex, Intelligent and Software Intensive Systems (CISIS), 2012 Sixth International Conference on. IEEE, 2012.

[18] Muhammed Imran Razzak, RubiyahYuosf and Marzuki Khalid, "Multimodal face and finger veins biometric authentication",

ScientificResearch and Essays, Vol.5, No.17, pp. 2529-2534, 2010.

[19] Mohammed soltane, NoureddineDoghmane,"Face and speech based multimodal biometric authentication", International journal of advancescience and technology, Vol 21, No.8, pp 41-46, 2010.

[20] Dhanashreevaidhya, sheetalpawar, "Feature level fusion of palmprint and palm vein for personal authentication based on Entrophy technique",International Journal on Electronics and communication Technology, Vol.5, Issue spl-1, 2014.

[21] A.Rattani, D.R.Kishu, M.Bicego," Feature level fusion of face and fingerprint Biometrics", Biometrics: Theory, applications and systems, FirstIEEE International conference, 2007.

[22] S.F.Bahgat, S.Ghoniemy, M.Alotabi," Proposed Multimodal palm-veins- face biometric Authentication", International journal of advancedcomputer science and applications, vol-4, No.6, 2013.

[23] Feifei cui, Gongping yang, "Score level fusion of fingerprint and finger vein Recognition", Journal of Computer Information's systems: 16, 5723-5731, 2011.

[24] Krishneswari K, Arumugam S," Multimodal Biometrics using feature fusion", Journal of computer science 8(3):431-435, 2012.

[25] Nazmeenbibiboodoo, R.K.Subramanian, "Robust multi-biometric recognition using face and ear images", IJCSIS-International journal ofcomputer science and information security, Vol.6, No.2, 2009.

[26] Nageshkumar, Mahesh.PK, Shanmuka swami M.N, "A Efficient Multimodal biometric fusion using palmprint and a face image", InternationalJournal of computer science, Vol.2, Issue 3, 2009.

[27] Krzyszof, Jonas Richard, PlamenProdanov, AndrzejnDrygajlo, "Reliability- Based decision fusion in multimodal biometric verificationsystems", EURASIP Journal on advances in signal processing, Article ID 86572, 9 Pages, 2007.

[28] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari," Multimodal biometric system fusion using fingerprint and iris with fuzzy logic",International Journal of soft computing and engineering, Vol.2, Issue-6, 2013.

[29] Lin Hong, Anil Jain, "Integrating faces and fingerprints for personal identification for personal identification", IEEE Transactions on patternanalysis and machine intelligence, Vol.20, No.12, 2008.

[30] Gayathriumakantbokade, ashokM.sapkal, "Feature level fusion of palm and face for secure recognition", International Journal of Computerand Electrical Engineering, Vol.4, No.2, 2012.

[31] Mitul D. Dhameliya, JitendraP.Chaudri," A multimodal biometric recognition system based on fusion of palmprint and fingerprint",International journal of engineering trends, Vol.4, Issue 5, 2013.

[32] A.Jagadessan, Dr.K.Duraisamy,"Secured Cryptographic Key Generation from multimodal biometrics: Feature level fusion of fingerprint andIris", International Journal of computer science and information security, Vol.7, No.2, 2010.

[33] Bicego, Manuele, Andrea Lagorio, Enrico Grosso, and Massimo Tistarelli. "On the use of SIFT features for face authentication." In *Computer Vision and Pattern Recognition*

Workshop, 2006. CVPRW'06. Conference on, pp. 35-35. IEEE, 2006.

[34] Bicego, Manuele, Andrea Lagorio, Enrico Grosso, and Massimo Tistarelli. "On the use of SIFT features for face authentication." In *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on*, pp. 35-35. IEEE, 2006.