Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 109 – 116

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Biometric Authentication using Fused Multimodal Biometric

D. Jagadiswary[a], D. Saraswady[a,b,*]

[a]Department of Electronics & Communication Engineering, Pondicherry Engineering College, Puducherry, India
[b] Department of Electronics & Communication Engineering, Pondicherry Engineering College, Puducherry, India

Abstract

Biometrics are basically based on the expansion of pattern recognition systems. At present, electronic or optical sensors like cameras and scanning devices are used to capture images, recordings or measurements of a person's 'unique' characteristics. These technologies are being utilized across a range of applications like security, prevention of cyber crime and border control, public aid/social benefits, customs, immigration, passport and healthcare identity verification, as well as commercial enterprises use. Most biometric systems that are typically use a single biometric trait to establish identity have some challenges like Noise in sensed data which increases False Acceptance Rate (FAR) of the system, Non-universality which reduces Genuine Acceptance Rate (GAR). Hence the security afforded by the biometric system mitigates its benefits. In this paper, we propose a Fused Multimodal systems which also have several advantages over unibiometric systems such as, enhanced verification accuracy, larger feature space to accommodate more subjects and higher security against spoofing. The proposed enhanced multimodal authentication system is based on feature extraction(using fingerprint, retina and fingervein) and key generation (using RSA). The experimental evaluation implemented using MATLAB 2014, illustrates the significance improvement in the performance of multimodal biometrics with RSA have GAR of 95.3% and FAR of 0.01%.

Keywords: Multimodal Biometric; Fingerprint; Finger Vein; Retina; RSA

[1]Email: jagadiswary@pec.edu

[2]Email: dsaraswady@pec.edu

1. INTRODUCTION

Individual biometric personalities like iris, DNA, Voice recognition, fingerprint, retina and finger vein can be labeled as unibiometric systems because it rely on a single biometric source for recognition. Unibiometric systems have some disadvantages like erratic biometric basis due to sensor, low quality of specific biometric trait of the authentic user. In addition, high-security applications and large-scale civilian recognition systems place stringent

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.187

accuracy necessities that cannot be met by obtainable unibiometric systems. To deal with the requirements of such applications, it is necessary to move, beyond the traditional pattern of biometric recognition [1] usually based on a single source of biometric information and also consider systems that consolidate evidence from multiple biometric sources for recognition. However, the consolidation of information presented by these multiple cures can result in a more accurate determination or certification of individuality. Hence biometric systems are designed to recognize a person based on information acquired from multiple biometric sources. Such systems are referred as multibiometric systems [2], are expected to be more accurate compared to unibiometric systems that rely on a particular segment of biometric affirmation. Accuracy enhancement, which is the primary motivation for using multibiometric systems [3], happens due to two reasons. Firstly, the fusion of multiple biometric sources effectively increases the dimensionality of the feature space and reduces the overlap between the feature distributions of dissimilar individuals. In addition to that, a combination of multiple biometrics is more exclusive to an individual than a single biometric trait. Due to noise, imprecision, or inherent drift (caused by factors like ageing) in a subset of the biometric sources can be compensated by the discriminatory information provided by the remaining sources. In addition to accuracy, multimodal biometric systems [4] may also offer the following advantages over unibiometric systems viz., alleviate the non-universality problem and reduce the failure to enroll errors, provide a degree of flexibility in user authentication, enable the search of a large biometric database in a computationally efficient manner and increase the resistance to spoofing attacks[5]. Multimodal biometric[6] implemented based on fusion of unibiometric. Fusion level has different techniques such as sensor level, feature level, score level, decision level, and rank level [7]. In this scenario, feature level fusion was used in the proposed technique. Proposed biometric traits like fingerprint, retina and finger vein were combined with asymmetric cryptographic algorithm RSA, is used in biometric template which is stored in the database thereby increases genuine acceptance rate and reduces false acceptance rate.

2. FUSED MULTIMODAL BIOMETRIC SYSTEM

Fused multimodal biometric system [8] includes two modules namely Enrollment module and Verification module which is below in Fig.1. In Enrollment module, a suitable user interface incorporating the biometric sensor or reader is needed to measure or record the raw biometric data of the user. The feature is extracted in the proposed biological traits, e.g. fingerprint, retina, and finger vein [9]. The feature extraction of three biometric traits fused using feature level fusion and encrypted using RSA and stored in a database for desired authentication and verification. This then facilitates the next process of verification module, in which the user claims an uniqueness and the scheme verifies whether the claim is genuine or imposter.

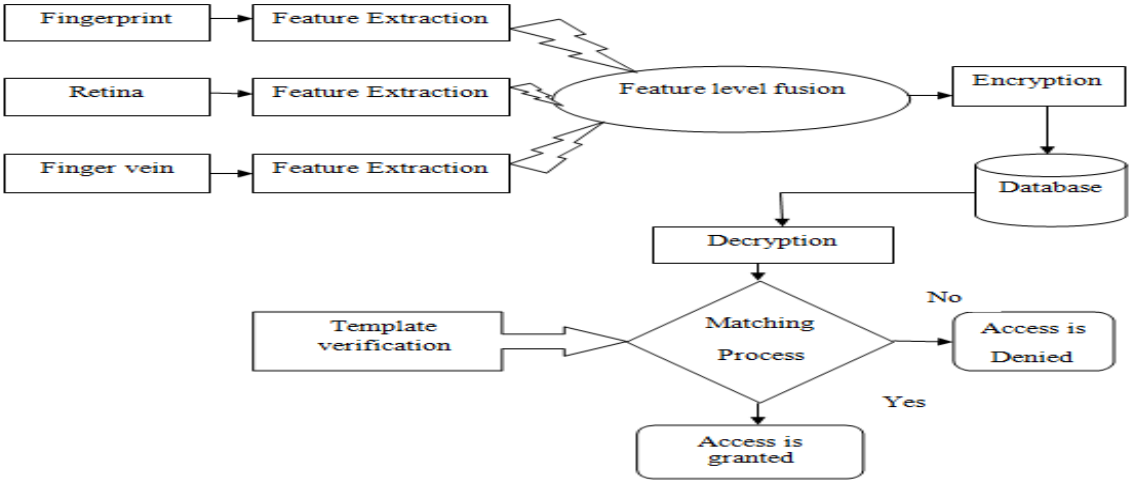


Fig.1Block diagram of the proposed system

The newly captured biometric traits of the individual are compared against the stored data is used to

determine the user identity. The query is compared only to the template corresponding to the claimed identity (a one-to-one match) after decryption.

3. FINGERPRINT RECOGNITION

Fingerprint recognition technology, which extracts features from impressions made with the distinct ridges on the fingertips. The fingerprints can be either flat or rolled. A flat print covers only an impression of the central area between the fingertip and the first knuckle, whereas a rolled print captures ridge on both sides of the finger which is utilized in our biometric system. An image of the fingerprint is captured by an optical scanner, enhanced, and converted into a template as shown in Fig.2(b). Minutiae are points of interest formed by the corners or forking of the abrasion skin ridges on every finger. Minutiae points mainly focussed on location, orientation of ridge flow and its type (i.e. Ridge ending or bifurcation) which makes an individual's fingerprint unique. The flow of the friction skin ridges also forms the patterns – the whorl, arch and loop of each finger. In this paper, Minutiae extraction is used based on termination (immediate ending of a ridge;) and bifurcation(with the point at which a single ridge splits into two ridges) [10].

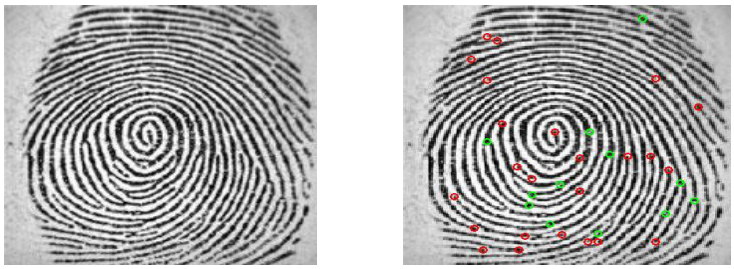


Fig.2 (a) Original image (b) Extracted minutiae points

4. RETINA RECOGNITION

The retinal vasculature is rich in structure and hence it is supposed to be a characteristic of each individual eye [11]. It is claimed to be the most secure biometrics since it is not easy to change or replicate the retinal vasculature[12]. The image as in Fig. 3(a) acquisition involves the cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on behalf of the user. The extraction of vessel segmentation, shown in Fig.3 (b) in the retina using Kirch's template using thresholding techniques based on eight different orientations is used in the proposed biometric system.

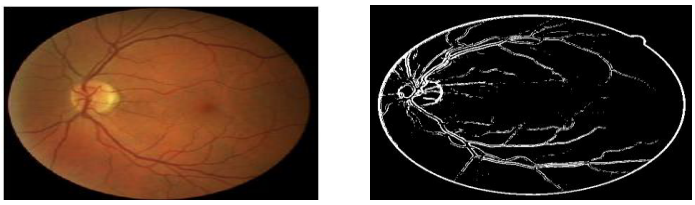


Fig. 3 (a) Original image (b) Blood vessel segmentation

5. FINGERVEIN RECOGNITION

A finger is placed between the infra-red light source and camera. The infra-red light was absorbed by the hemoglobin in the blood vessels and the pattern of veins in the palm is captured as a pattern of shadows. An image of a finger captured [13]. Under infra-red light contains not only the vein pattern, but also irregular shading produced by the various thicknesses of the finger bones and muscles. Infra-red light is used to capture an image of a

finger that shows the vein pattern, which is also reflected fluctuation in the blood vein, depending on temperature, physical conditions, etc. To identify a person with high accuracy, the pattern of the thin/thick and clear/unclear veins in an image must be extracted equally. The pattern of finger vein pattern extracts based on the repeated line tracking method and the maximum curvature method is shown in Fig.4(b).

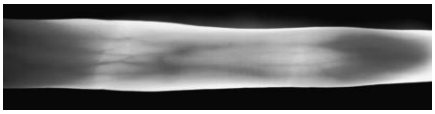
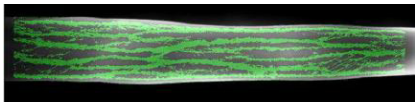


Fig.4 (a) Original image



(b) Extracted vein pattern

6. FEATURE LEVEL FUSION

Feature level fusion refers to combining different feature sets that are extracted from multiple biometric sources. When the feature sets are non homogeneous (e.g., the feature sets of different biometric modalities like fingerprint, retina and finger vein) concatenate them to form a single feature set. When the multiple feature sets correspond to different samples of the same biometric trait that are processed using the same feature extraction algorithm [14], then feature level fusion can be considered as a template update or template improvement. It improves recognition accuracy over other fusion technique. In this research work, the feature level fusion technique was implemented in the fused matrix of the stored template, which was then verified with the fused matrix of the present query [15].

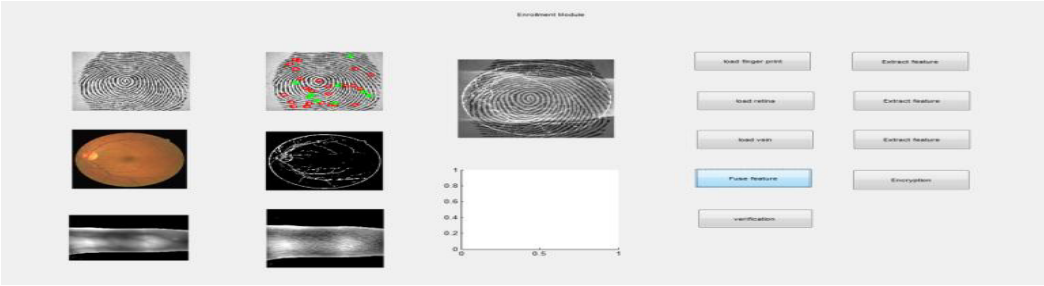


Fig. 5 Steps involved in Feature Level Fusion

7. MODIFIED DRSA (MDRSA)

The multimodal biometric system consists of multiple traits of individual information, so it is necessary to secure the template from the database. Thus the proposed system, used to encrypt the template is RSA, which is a public key cryptography. Comparing with the existing RSA, in order to acquire fine eminence of the decrypted image, the modification had done in the decryption stage of RSA using symmetry properties of an algorithm. MDRSA(Modified Decrypted Rivest, Shamir and Adleman) was explained by the steps shown below:

7.1 Key Generation:

i. Choose two distinct prime numbers p and q.
ii. Find n such that n = p*q. (n will be used as the modulus for both the public and private keys).
iii. Find the quotient of n, Φ (n)
Where, **Φ (n) = (p-1) (q-1).**
iv. Choose an e such that **1 < e < Φ(n),** and such that e and Φ(n). (e and Φ(n) are relatively prime). Where 'e' is kept as the public key exponent.
v. Determined (using modular arithmetic) which satisfies the congruence relation.
$$d = 1 \pmod{\Phi(n)}.$$
This is often computed using the Extended Euclidean Algorithm. e and Φ(n) are relatively prime and d is to be the modular multiplicative inverse of 'e'.

The public key has modulus n and the public (or encryption) exponent. The private key has a modulus 'n' and the private (or decryption) exponent 'd', which is kept secret.

7.2 Encryption

i. Person "A" transmits his/her public key (modulus n and exponent e) to Person B, keeping his/her private key secret.
ii. When Person" B" wishes to send the message "M" to Person A, he first converts M to an integer such that $0 < m < n$ by using agreed upon reversible protocol known as a padding scheme.
iii. Person B computes, with Person A's public key information, the cipher text c corresponding

$$C \equiv m^e \pmod n$$

iv. Person B now sends message "M" in cipher text, or C, to Person A.

7.3 Decryption:

i. Person A recovers m from c by using his/her private key exponent, d, by the computation

$$m \equiv C^d \pmod n.$$

ii. Given m, Person A can recover the original message "M" by reversing the padding scheme.

$$C \equiv m^e \pmod n,$$
$$C^d \equiv (m^e)^d \pmod n$$
$$C^d \equiv m^{de} \pmod n.$$

iii. By the symmetry property,

$$m^{de} \equiv m^{de} \pmod n.$$

Since $de = 1 + k\Phi(n)$, we can write

$$m^{de} \equiv m^{1 + k\Phi(n)} \pmod n,$$
$$m^{de} \equiv m(m^k)^{\Phi(n)} \pmod n$$
$$m^{de} \equiv m \pmod n$$

From Euler's Theorem, we can show that this is true for all 'm' and the original message

$$C^d = m \pmod n, \text{ is obtained.}$$

8. SIMULATION RESULTS

The security level of the proposed multimodal biometric system was designed using a GUI in MATLAB 2014.. Initially the three biometric traits fingerprint, retina and finger vein are chosen for multimodal fusion and the required features of fingerprint, retina and finger vein are extracted using various techniques like minutia extraction, blood vessel extraction and maximum curvature method respectively. The extracted features are fused using feature level fusion and then encrypted using RSA as per Fig. 6.

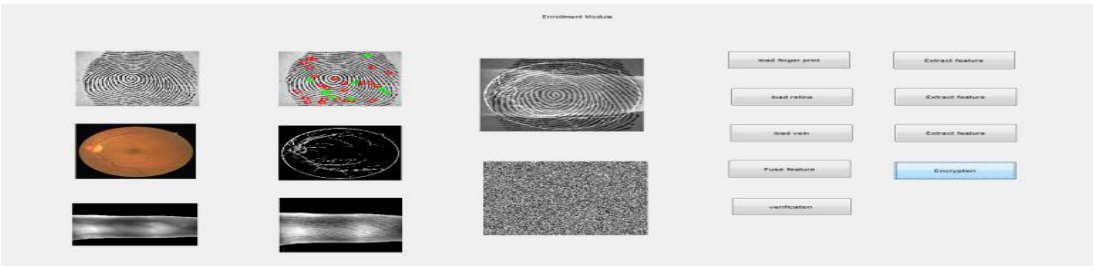


Fig. 6 Encryption of Fused Biometric

The final encrypted information is then stored in the database and decrypted image is matched with the current query. For each biometric such as fingerprint, retina and finger vein are trained with unimodal identity is simulated and depends upon the matching performance, False Acceptance Rate (FAR) and Genuine Acceptance

Rate (GAR) are calculated for both multimodal and unimodal with RSA and without RSA. Whenever verification is considered necessary for the system, first the system has to produce keys for query user as in Fig. 7.

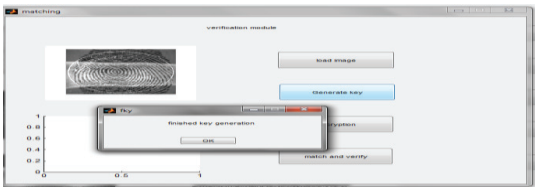


Fig. 7 Key generation process

Fig. 8 Decryption of Fused Biometric from database

The generated key used to search the template for decryption until the key matches. The key is used to decrypt the template and the decrypted template is used to match with current query which is a fusion of three biometric traits fingerprint, retina and finger vein based on fused matrix values using correlation as in Fig.8 and Fig.9.

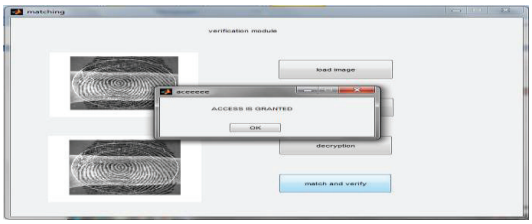


Fig. 9 Process of Matching and Verification

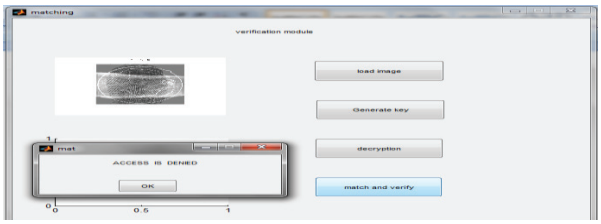


Fig. 10 Access Denied by the system

In this scenario, if the query template is not matched to the stored template, system denied the access of the user as in Fig. 10. The performance of the proposed system analyzed by matching the performance between enrollment module and verification module for the current query template to identify an individual for authorization. False acceptance rate and Genuine acceptance rate are calculated based on genuine and imposter authentication during a verification module. The false acceptance rate should be low which means imposter is not allowed to authenticate and genuine acceptance rate should be high which means genuine user is allowed to authenticate. The simulated performance of multimodal was compared with unimodal and then it was plotted on ROC curve FAR versus GAR.

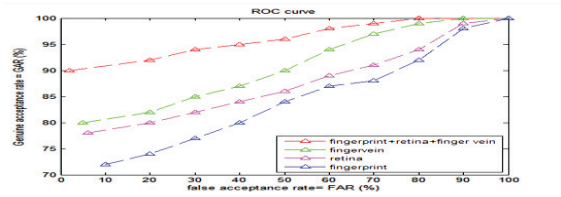


Fig.11 GAR Vs FAR without RSA

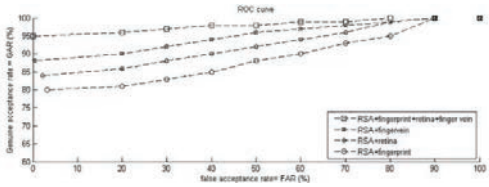


Fig. 12 GAR Vs FAR with RSA

The samples of unimodal biometric traits such as fingerprint, retina and finger vein are trained without RSA and then multimodal biometric trait such as fingerprint, retina and finger vein was also implemented using feature level fusion techniques without RSA. The fingerprint was trained and performance was calculated based on matching minutiae points with current query for an identity using FAR and GAR. GAR of 72% and FAR of 10% for fingerprint. Similarly, the retina was trained based on blood vessel pattern and its GAR of 78% and FAR of 6.74%. The Finger vein was trained based on vein pattern in finger and its GAR of 80% and FAR of 5.02%. The multimodal biometric was trained based on fused matrix values using correlation and it's GAR of 90% and FAR of 2.06%. The performance of finger print using RSA has a GAR of 80.2% and FAR of 3.25%, whereas without RSA,

GAR was 72% and FAR was 10%. The comparative curves were shown in Fig.14.

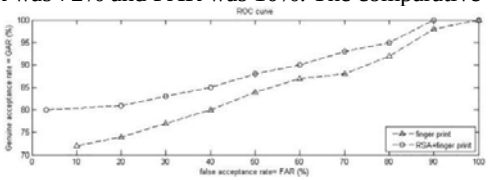


Fig. 14 GAR Vs FAR with and without RSA for FingerPrint

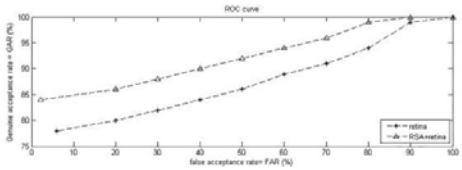


Fig. 15 GAR Vs FAR with and without RSA for Retina

The performance of the retina using RSA has a GAR of 84.2% and FAR of 2.2%, whereas without RSA, the GAR was 78% and FAR was 6.74%. The comparative curves were shown in Fig.15. The performance of finger vein using RSA has a GAR of 87.6% and FAR of 0.52%, whereas without RSA, the GAR was 80% and FAR was 5.02%. The comparative curves were shown in Fig.16.

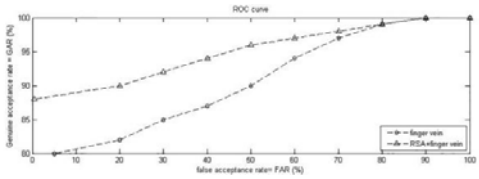


Fig. 16 GAR Vs FAR rate with and without RSA for FingerVein

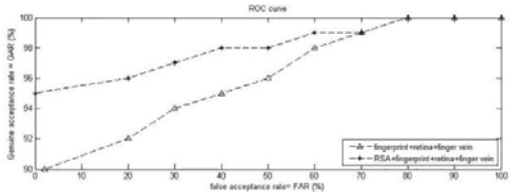


Fig.17 GAR Vs FAR with and without RSA for Fused Biometric

The performance of multimodal biometric(fusion of fingerprint, retina and finger vein) based on fused matrix values using RSA has a GAR of 95.3% and FAR of 0.01% whereas without RSA, GAR was 90% and FAR was 2.06%. The comparative curves were shown in Fig.17. However, in order to increase the accuracy of multimodal biometric as a whole, fusion at feature level fusion, and encrypting using security algorithm has been performed. The overall performance of multi-modal system has reduced FAR of 0.01% and increases GAR of 95.3%, respectively, and its performance compared to unimodal biometric systems such as fingerprint, retina and finger vein with RSA.The performance of multimodal biometric based on fused matrix values using RSA have GAR of 95.3% and FAR of 0.01%, RSA with fingerprint have GAR of 80.2% and FAR of 3.25%, RSA with retina have GAR of 84.2% and FAR of 2.2%, RSA with finger vein have GAR of 87.6% and FAR of 0.52% .

9. CONCLUSION

The feature level fusion technique is used for the design of multimodal biometric traits such as fingerprint, retina and finger vein, which protects the multiple templates using RSA has been implemented using MATLAB R2014. A realistic security analysis of the multimodal biometric cryptosystem has also been conducted using fingerprint, finger-vein and retina, which provide a remarkable improvement performance in a multimodal biometric cryptosystem using RSA. The overall performance of multimodal system has increased with GAR by 95.3% and reduced with FAR of 0.01%, which is compared to unimodal biometric using RSA.

Future work can be further extended by accurately modeling feature extraction techniques and managing the database more effectively and evaluating the matching methodology and its performance of biometric system using different level of fusion.

REFERENCES

[1] Abhishek Nagar, Karthik Nandakumar, Anil K. Jain, and Dekun Hu, “Multibiometric Cryptosystems Based on Feature-Level Fusion”, *IEEE Transactions on Information forensics and security*, vol. 7, no. 1, February 2012, pp. 255–268.

[2] Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma , “Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm”, *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, Volume 1, Issue 3, 2012, pp. 7–13.

[3] Bo Fu, Simon X. Yang, Jianping Li, and Dekun Hu, “Multibiometric Cryptosystem: Model Structure and Performance Analysis”, *IEEE Transactions on information forensics and security*, vol. 4, no. 4, December 2009, pp. 867–882.

[4] Koen Simoens, Julien Bringer, Herve Chabanne, and Stefaan Seys, “ A Framework for Analyzing Template Security andPrivacy in Biometric Authentication Systems”, *IEEE Transactions on Information forensics and security*, vol. 7, no.

2, April 2012, pp. 833-841.

[5] Terence Sim, Sheng Zhang, Rajkumar Janakiraman, and Sandeep Kumar, "Continuous Verification Using Multimodal Biometrics", *IEEE Transactions on pattern analysis and machine Intelligence*, vol. 29, no. 4, April 2007, pp.687-700.

[6] Ajay Kumar, Vivek Kanhangad, and David Zhang, "A New Framework for Adaptive Multimodal Biometrics Management", *IEEE Transactions on Information forensics and security*, vol. 5, no. 1, March 2010p, p. 92-102.

[7] W. Stallings, *Cryptography and Network Security*, Prentice Hall, Fourth Edition, 2005.

[8] A. J. Menezes, P. C. Van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*, *CRC Press Series on Discrete Mathematics and Its applications*, CRC Press, 1997, pp. 756-799.

[9] Samarth Bharadwaj, Mayank Vatsa* and Richa Singh, "Biometric quality: a review of fingerprint, iris, and face", EURASIP Journal on Image and Video Processing 2014, pp. 2014-34.

[10] Anil K. Jain, Fellow, Jianjiang Feng, Member, "Latent Fingerprint Matching", *IEEE Transactions on pattern analysis and machine intelligence*, vol. 33, no. 1, January 2011, pp. *88-100.*

[11] Diego Marín, Arturo Aquino, Manuel Emilio Gegundez-Arias, José Manuel Bravo, "A New Supervised Method for Blood Vessel Segmentation in Retinal Images by Using Gray-Level and Moment Invariants-Based Features", *IEEE Transactions on medical imaging*, vol. 30, no. 1, January 2011, pp. 146-158.

[12] Maneesh Upmanyu, Anoop M. Namboodiri, Kannan Srinathan, and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol", *IEEE Transactions on Information forensics and security*, vol. 5, no. 2, June 2010, pp.225-268.

[13] Ajay Kumar, Yingbo Zhou, "Human Identification Using Finger Images", *IEEE Transactions on image processing*, vol. 21, no. 4, April 2012, pp. 2228-2244.

[14] Blakley G. R. ,'Safeguarding cryptographic keys' in Proc. National Computer Conf., vol. 48, (1979), pp. 313–317.

[15] Tuyls P., Kevenaar T., Schrijen G. J., Staring T., and Van Dijk M., 'Security displays, enabling secure communications' in Proc. First Int. Conf. Pervasive Computing, Boppard Germany, Springer-Verlag Berlin LNCS, vol. 2802, 2004, pp. 271–284.

D. Jagadiswary is a Ph.D. student at Pondicherry Engineering College, Puducherry, India, in the Department of Electronics and Communication Engineering. She received the Master's Degree in Information Security from the Pondicherry university in 2009. Her research interests include security analytics and Cryptography. Mail Id: jagadiswary@pec.edu

D. Saraswady is a Professor in the Department of Electronics and Communication Engineering, Pondicherry Engineering College, Puducherry , India. She published 16International Journals, 4 National Journals, 10 International Conferences and 15 National Conferences. Her research interests includes Security, Cognitive Networks, Wireless Communication and Image Processing. Mail Id: dsaraswady@pec.edu