Multimodal Biometric Authentication using Cryptosystem

R. Sharmiladevi
Department of ECE
Anna University Regional Campus-
Tirunelveli.

Dr. Gokulakrishnan
BE.,ME.,Ph.D
Department of ECE
Anna University Regional Campus-
Tirunelveli.

***Abstract*:-Multimodal are generally much more imperative to fraudulent technologies, because it is harder to fake multiple biometric characteristics than to forge a single biometric characteristic thus provide higher accuracy rate and higher protection from spoofing. The proposed enhanced multimodal authentication cryptosystem is based on feature extraction using Iris, retina and fingervein and key generation using RSA.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,GAR,FAR,

1 INTRODUCTION

With new advances in digital technologies, security and access control are essential requirements.Biometrics is a best way to secure data when compared to traditional methods such as password, PIN, etc…The term biometrics has been originated from the prehistoric Greek terms: bios means life and metros means measure. Biometrics is used to identify individual person uniquely using their physical, chemical or behavioral traits [1]. The use of unimodal biometrics traits susceptible to noise, bad capture, and other inherent problems make unsuited for all applications.

Multimodal systems remove some of the drawbacks of the uni-biometric systems by grouping the multiple sources of information.These systems utilize more than one physiological or behavioral characteristic for enrollment and identification/verification. When choose multimodal biometric system, some factors are need to considered .They are application nature, method adopt, number of traits used, cost etc…[2].

The goal of multimodal biometrics is to reduce False accept rate, False reject rate, Failure to enroll rate, Susceptibility to artifacts or mimics. This system may be classified as four that is architecture, Sources that provide multiple evidence, Level of fusion, Methodology used for integrating the multiple verifiers. Only Biometric system is not sufficient to provide security but also if it is combined with cryptography provide good security [3].

Cryptography plays a significant role in this digital advancement. To secure data which is transmitting between sender and receiver. Many cryptographic algorithms are available. In addition to accuracy, multimodal biometric systems may 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[4].

Multimdal biometrics are implemented based on fusion of unibiometrics[5]. Biometric traits (iris, retina and finger vein) of an individual is combined and the combined features are encrypted using asymmetric cryptographic (RSA) algorithm and stored in a database.Verification is done by comparing the current template with the decrypted values.RSA increases genuine acceptance rate and reduces false acceptance rate.

2. FUSED MULTIMODAL BIOMETRIC SYSTEM

Fused multimodal biometric system 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. Iris, retina, and finger vein [6]. The feature extraction of three biometric traits fused using 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.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.

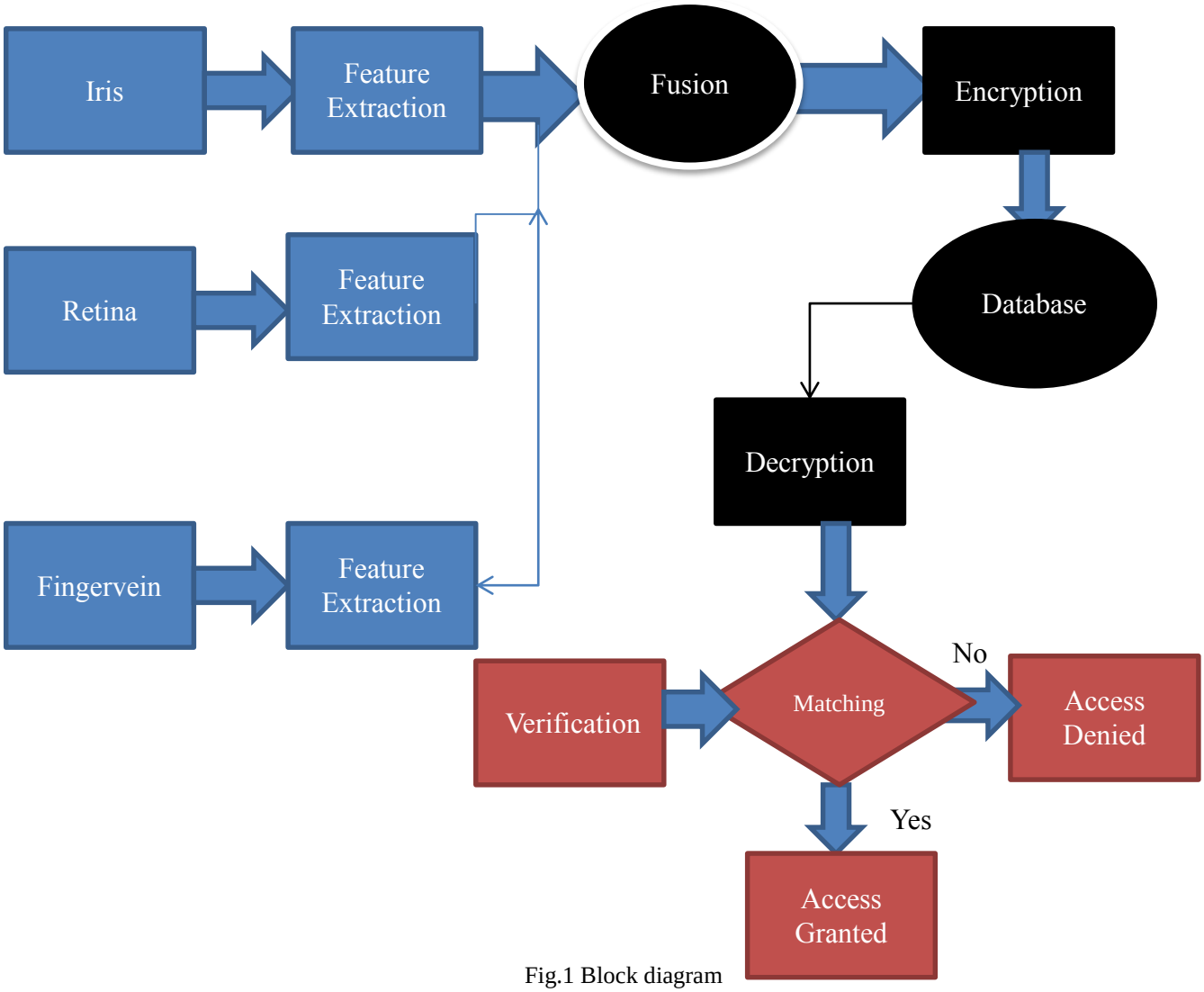


Fig.1 Block diagram

3. FEATURE EXTRACTION

The feature is extracted from Iris, retina and finger vein of an individual.The extracted features are:

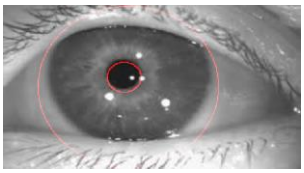
3.1 Iris recognition

Iris image of eye is segmented by integro-differential operator [7] (act as a circular edge detector)which finds the centre coordinates and radius of both iris and pupil [8].It extracts the geometric features of iris [9]. The operator is given below,

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} I(x,y) / 2\pi r \right| \quad (1)$$

The operator searches over the image domain I(x,y) for the maximum in the blurred partial derivative with respect to increasing radius r of the normalized contour integral of I(x,y) along a circular arc of radius r and centre coordinates (x_0, y_0). The symbol $*$ denotes convolution and $G_\sigma(r)$ is a smoothing function such as a Gaussian of scale σ.

Fig.2(a) Original image

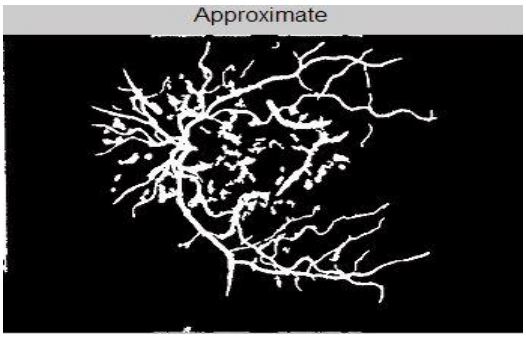


(b) Extracted boundary

3.2 Retina recognition

The retinal vasculature is rich in structure and hence it is supposed to be a characteristic of each individual eye [10]. It is claimed to be the most secure biometrics since it is not easy to change or replicate the retinal vasculature[11]. The image as in Fig. 3(a) acquisition involves the cooperation of the subject, entails contact with the eye piece 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

3.3 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 [12]. 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 [13]. 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).

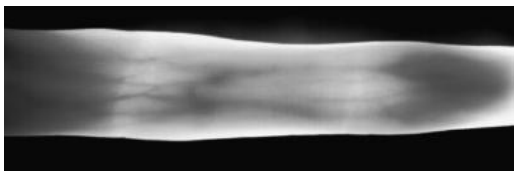
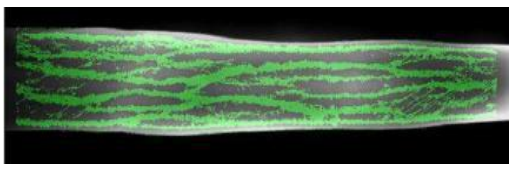


Fig.3(a) Original image



(b) Extracted vein pattern

4. 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 Iris, 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 , 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[14] was implemented in the fused matrix of the stored template, which was then verified with the fused matrix of the present query[15].

5.RSA

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 [16], which is a public key cryptography.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.RSA(Rivest, Shamir and Adleman) was explained by the steps shown below:

5.1 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 keys).

iii. Find the quotient of n, Φ (n)

Where **,**

$$\Phi(n) = (p-1)(q-1) \quad (2)$$

iv. Choose an e such that **1 < e < Φ(n),** and such that e and Φ(n). Where 'e' is kept as the public key exponent.

v.Determined (using modular arithmetic) which satisfies the congruence relation.

$$d = 1 \pmod{\Phi(n)} \quad (3)$$

d is to be the modular multiplicative inverse of 'e'.

5.2 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

$$C \equiv me \pmod{n} \quad (4)$$

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

5.3 Decryption:

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

$$m \equiv Cd \pmod{n} \quad (5)$$

6. SIMULATION RESULTS

The three biometric traits Iris, retina and finger vein of an individuals 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.

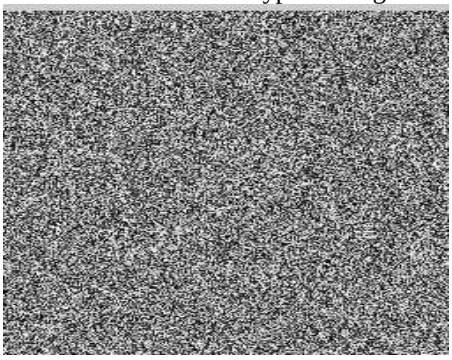


Fig. 5 Encryption of Fused Biometric

The final encrypted information is then stored in the database and decrypted value is matched with the current query. For each biometric such as iris, 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. 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 Iris [17], retina [18] and finger vein [19] based on fused matrix values using correlation.

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 [20]. 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 Iris was trained and performance was calculated based on extracted points with current query for an identity using FAR and GAR. GAR of 72% and FAR of 10% for Iris. 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 performance of Iris using RSA has a GAR of 82.2% and FAR of 4.25%, whereas without RSA, GAR was 72% and FAR was 10%.The performance of the retina using RSA has a GAR of 85.25% and FAR of 3.50%, whereas without RSA, the GAR was 78% and FAR was 6.74%. The performance of finger vein using RSA has a GAR of 90.5% and FAR of 1.5%, whereas without RSA, the GAR was 80% and FAR was 5.02%. The performance of multimodal biometric(fusion of Iris, 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%. 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 multimodal system has reduced FAR of 0.01% and increases GAR of 95.3% respectively, and its performance compared to unimodal biometric systems such as iris, retina and finger vein without 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 Iris have GAR of 82.2% and FAR of 4.25%, RSA with retina have GAR of 85.25% and FAR of 3.50%, RSA with finger vein have GAR of 90.5% and FAR of 1.5% .

7. CONCLUSION

The feature level fusion technique is used for the design of multimodal biometric traits such as Iris, 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 Iris, 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.

8.REFERENCE

1 Pocovnicu,Adrian."Biometric security for cell phones,".Informatica Economica, 13.1 (2009): 57.
2 Anwar, Farhat, Rahman, and Azad. "Multibiometric systems based verification technique," European Journal of Scientific Research, 34.2(2009): 260-270.
3 Gaikawad, kumar S., and S. N. Kini."A Survey of Multi-Biometric Cryptographic Security System,"
4 Terence Sim, 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.
5 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 2010, p. 92-102.
6 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.
7 Karen,Kevin Bowyer."Genetically identical irises have texture similarity that is not detected by iris biometrics," Journal Computer Vision and Image Understanding,115,2011 1493–1502.
8 Vanaja Roselin, E. Chirchi and L. M. Waghmare, "Feature Extraction and Pupil Detection Algorithm Used for Iris Biometric Authentication System", International Journal of Signal Processing, Image Processing vol.6, 2013, pp.141-160.
9 Nicolaie Popescu-Bodorin, Valentina E. Balas," Learning Iris Biometric Digital Identities for Secure Authentication: A Neural-Evolutionary Perspective Pioneering Intelligent Iris Identification, Recent Advances in Intelligent Engineering Systems", Series: Studies in Computational Intelligence, Springer, Vol. 378, 2012, pp. 409-434
10 Diego Marín, Arturo Aquino, Manuel Emilio Gegundez-Arias,"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.
11 Maneesh Upmanyu, Anoop M. Namboodiri, 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.
12 Ajay Kumar, Yingbo Zhou."Human Identification Using Finger Images", IEEE Transactions on image processing,vol. 21, no. 4, April 2012, pp. 2228-2244.
13 Lee E, Lee H, & Park K." Finger vein recognition using minutia-based alignment and local binary pattern-based feature extraction,"International Journal of Imaging Systems and Technology, 2009, 179–186.
14 Abhishek K. Nagar, Student Member, IEEE, Karthik Nandakumar, Member, IEEE, and Anil K. Jain, Fellow, IEEE,"Multibiometric Cryptosystems Based on Feature-Level Fusion," IEEE Tractions on Information Forensics and Security, vol.7, no.1, February 2012.
15 Qin H, Qin, L, Xue L, He X, Yu C & Liang, X."Finger-vein verification based on multi-features fusion Sensors," 13, 2013,15048–15067.
16 Christof Paar, Jan Pelzl. "Understanding Cryptography," ISBN 978-3-642-04100-6, Springer, 2010.
17 Marques Santos, Luís Ducla Soares, and Paulo Lobato Correia."iris verification system with secure template storage,"18th European Signal Processing Conference (EUSIPCO-2010) Aalborg, Denmark, August 23-27, 2010.
18 Lajevardi S, Arakala A, Davis S, & Horadam K."Retina verification system based on biometric graph matching,"IEEE Transactions on Image Processing, 22, 3625–3635,2013.
19 Song W, Kim T, Kim H, Choi J, Kong H & Lee S. "A finger-vein verification system using mean curvature," Pattern Recognition Letters, 32,1541–1547,2011.
20 Houda Benaliouche and Mohamed Touahria,"Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint", Computer Science Department, University of Ferhat Abbas Setif 1, Pole 2 - El Bez, 19000 Setif, Algeria.