Advanced Bio-Crypto System with Smart Card

Ansi R R, Anusree L

Abstract— ***Biometric cryptosystems has widespread applications in this era. Generally associated to a personal device for privacy protection, biometric references are stored in secured electronic devices such as smart cards, and systems are using cryptographic tools to communicate with the smart card and securely exchange biometric data. The biometrics used in this paper is fingerprint. In many areas, fingerprint recognition is used to improve the security and privacy. In this paper, we propose a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity called combined minutiae template, stored in both database and smart card. Smart cards are widely acknowledged as one of the most secure and reliable forms of electronic identification. Combining smart card technology with biometrics provides the means to create a positive binding of the smart card to the cardholder thereby enabling strong verification and authentication of the cardholder's identity. Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember a memorable password or passphrase etc. Fingerprint has been integrated in the RSA algorithm for biometric public/private key generation. Using RSA algorithm, we can generate a biometric based asymmetric keys from the biometric template of a user stored in the database. We grant authentication and using these keys we can encrypt/decrypt message. New approaches have endeavored towards merging biometrics with cryptography, so as to increase overall security of the system.***

Index Terms—Combination, fingerprint, minutiae, privacy, RSA, Key generation, MATLAB.

I. INTRODUCTION

Biometrics is a security solution based on something you know, have, and are. Fingerprint recognition is an active research area in nowadays. In many areas, fingerprint recognition is used to improve the security and privacy [1]. Traditional encryption is not suitable for fingerprint privacy protection because here decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker. The main problem statement of existing system is security. In the existing system, single fingerprint is scanned and it is stored in database. In authentication process stored fingerprints is matched with the enrollment fingerprint. This type of system didn't provide full security and privacy to the users. Lower security, the hackers can easily hack the secured information. To avoid this, here we use fingerprint combinational [2] biometric authentication in this system.

Biometric application, fingerprint, has taken part a major role to identify a particular person uniquely. In this paper, we propose a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity [3]. During the enrollment, the system captures two fingerprints from two different fingers [10]. We extract the minutiae positions [6] from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints [5]. Based on this combined minutiae template [2] is generated and stored in a database. In the authentication [11], the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching [7] process is proposed for matching the two query fingerprints against a combined minutiae template [8]. We can choose these two fingers randomly.

Existing system does not specify how we can protect a secret data using combination. To overcome this in our proposed system we generate keys [5] from combined minutiae using RSA [9] and using these keys, we are able to encrypt and decrypt the message. Cryptography and biometrics [12] play a key role in security applications. Biometric cryptosystems combine both biometrics and cryptography [13] to afford the advantages of both for security purposes. This technique provides the advantages like better security levels for data transmission and eliminating the must to memorize passwords or to carry tokens etc. In this approach for generating cryptographic key [15], fingerprint has been selected as the biometrics feature.

II. RELATED WORKS

The proposed work is inspired from a number of researches which are related to cryptography and cancellable biometric techniques. Goh and Ngo combined have proposed a new system based on face biometrics [4]. The work adopted the biometric locking approach of Soutar et al. Here the features are the Eigen-projections which are extracted from the face image, each of which is then mixed with a random string and quantized into a single bit.

Arun Rossa, Anil Jaina, James Reismanb (2003) discussed hybrid technique which has the entire image is taken into account while constructing the ridge feature map. Minutiae matching are used to determine the translation and rotation parameters relating the query and the template images for ridge feature map extraction. Itering and ridge feature map extraction are implemented in the frequency domain thereby speeding up the matching process. ltered query images are catched to greatly increase the one-to-many matching speed. The hybrid matcher performs better than a minutiae-based Fingerprint matching system [7].

Jo et al. [9] proposed a simple technique for the generation of digital signatures and cryptography communication with the aid of biometrics. The generation of the signature is necessary in such a way that it becomes possible to verify the same with a cryptographic algorithm in existence like the RSA without altering its own security constraint and infrastructure.

Shweta Malhotra, Chander Kant Verma(2013) proposed Multimodal biometrics, many unimodal have several problems such as noisy data, spoof attacks etc. which cause

Revised Version Manuscript Received on August 13, 2015.

Ansi R R, Department of ECE, LBS Institute of Technology for Women, Thiruvananthapuram, Kerala, India.

Anusree L, Department of ECE, LBS Institute of Technology for Women, Thiruvananthapuram, Kerala, India.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

data insecure. To overcome these problems multimodal biometrics is used. Multimodal biometrics allows fusing two or more characteristics into single identification. It leads to more secure and accurate data. In this paper, we have combined two characteristics one physical and one behavioral and further a key is added to the template to make it more secure. The template is finally stored in database [12].

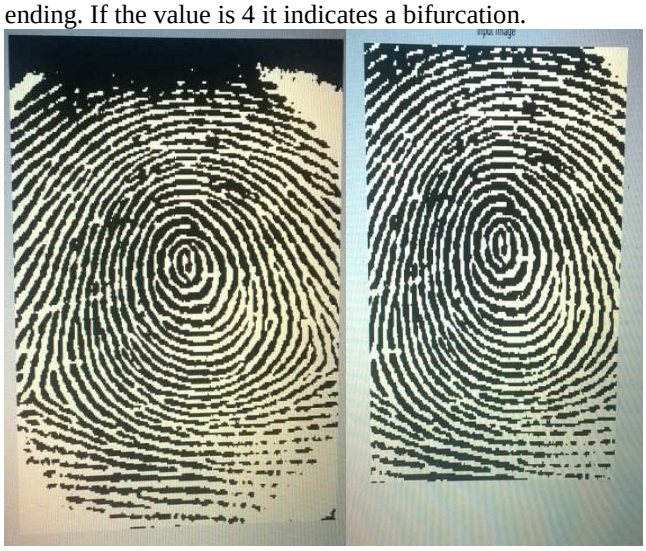
III. PROPOSED METHODOLOGY

Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields. In biometric cryptosystems, a cryptographic key is generated from the biometric template of a user stored in the database in such a way that the key cannot be revealed without a successful biometric authentication. We are using combined fingerprint patterns as the biometrics feature, because it is stable throughout person's life time. Using RSA, generating a strong bio-crypt key from the combined minutiae template. Several steps have been achieved in order to generate combined biometric as follow:

A. Minutiae Extraction

A fingerprint is the pattern of ridges on the surface of a fingertip. Each individual has unique fingerprints. The uniqueness of a fingerprint is exclusively determined by local ridge characteristics. The two most prominent ridge characteristics are ridge ending and bifurcation. A ridge ending is defined as the point at which ridge terminates. A ridge bifurcation is defined as the point at which ridges separates.

Minutiae [14] defined as the minute details of the fingerprint [3].There are mainly three steps in minutiae extraction. Binarization is the process that converts the gray scale image to binary image .So the intensity of the image has only two values, black and white. The objective of thinning is to make the ridges in to unit-width. Third step is minutiae detection, from the binary thinned image, the minutia are detected by using a 3x3 windows. Then set 2 matrices one for ridge ending and another for bifurcation. Move a 3x3 window locally and check whether the middle element is a zero or not. If it is zero indicates either ridge ending or bifurcation. Then find the sum of 3x3 window. If the value is 2 it indicates ridge ending. If the value is 4 it indicates a bifurcation.



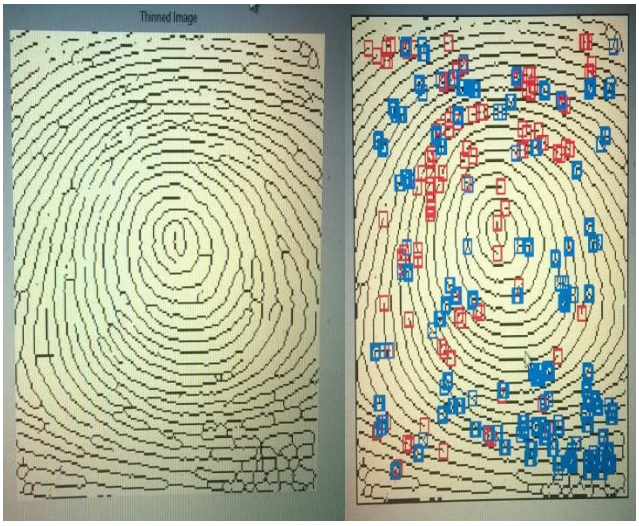


Fig. 1. Minutiae Extraction

B. Orientation Detection

The orientation image represents an intrinsic property of the fingerprint image and defines invariant coordinates for ridges and follows in a local neighbourhood. By viewing a fingerprint image as an oriented texture, a number of methods have been proposed to estimate the oriented field of fingerprint images. We have developed least square orientation estimation algorithms. Given normalized image G, the main steps of the algorithm are as follows:

1) Divide normalized image into blocks of size w×w (16×16).

2) Define a filter and compute the gradients , $\partial_x(i,j)$ and $\partial_y(i,j)$ at each pixel (i, j).

3) Estimate the local orientation of each block centered at pixel (i, j) using below equations:

$$V_x(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\partial_x(u,v)\partial_y(u,v) \quad (1)$$

$$V_y(i,j) = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (\partial_x^2(u,v)\partial_y^2(u,v)) \quad (2)$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\frac{Vy(i,j)}{Vx(i,j)} \quad (3)$$

where $V_x(i,j)$ and $Vy(i,j)$ represents the local orientation of the fingerprint along the x and y-directions and $\theta(i,j)$ is the least square estimate of the local ridge orientation

4) The estimated local ridge orientation (i,j) may not always be a correct estimate. So a low pass filtering is performed to reduce noises

5) Filtering performed using below equation:-

$$\emptyset_x'(i,j) = \sum_{u=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} \sum_{v=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} W(u,v)\emptyset_x(i-uw,j-vw) \quad (4)$$

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

$$\emptyset_y'(i,j) = \sum_{u=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} \sum_{v=-\frac{w_\emptyset}{2}}^{\frac{w_\emptyset}{2}} W(u,v)\emptyset_y(i-uw, j-vw) \quad (5)$$

where $\emptyset_x'(i,j)$ is the real part of $\theta(i,j)$and $\emptyset y'(i,j)$ is the imaginary part of $\theta(i,j)$.

6) Compute the local ridge orientation at (i, j) using the below equation **:**

$$O(i,j) = \frac{1}{2}\tan^{-1}\frac{\emptyset_y'(i,j)}{\emptyset_{x'}(i,j)} \quad (6)$$

where O(*i,j*) is the noise free final ridge orientation. With this algorithm, a fairly smooth orientation field is obtained.

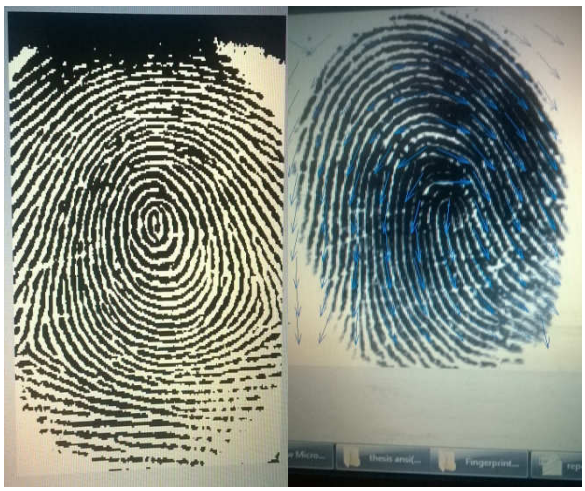


Fig. 2.Orientation Detection

C .Reference Points Detection

The reference points detection process is motivated by Nilsson , who first propose to use complex filters for singular point detection. A fingerprint image can be said to have two structures, the global structure and the local structure. Direct use of the local structure in the identification/ verification process is sensitive to noise, i.e. poor performance for low quality fingerprints can be foreseen. Compared to the local structure the global structure is more stable even when the fingerprint is of poor quality. First align the reference and the unknown fingerprint before using the local structure for the identification/verification. Here global structure of the fingerprint is used. When the two fingerprints are aligned (registered) we can match the local structure for certain points on the basis of the neighborhood content more robustly than by extracting minutiae positions and matching on the basis of the geometric position distribution of the minutiae. For the alignment we need certain landmark points. Given a fingerprint, the main steps of the reference points detection are summarized as follows:

1) Compute the orientation ***O*** from the fingerprint using the orientation estimation algorithm.

$$Z = \cos(2\boldsymbol{O}) + j\sin(2\boldsymbol{O}) \quad (7)$$

2) Calculate a certainty map of reference point

$$C_{ref} = Z * T'_{ref} \quad (8)$$

$$T_{ref} = (x+iy).\frac{1}{2\pi\sigma^2}.\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \quad (9)$$

where $Tref$ is the kernel for reference point detection

3) *Calculate an improved certainty map*

$$C'_{ref} = \begin{cases} C_{ref}.\sin\left(Arg\left(C_{ref}\right)\right) & ; \ if\ Arg(C_{ref}) > 0 \\ 0 & ; \ otherwise \end{cases} \quad (10)$$

where $Arg(Cref)$ returns the principal value of the argument of z.

4) Locate a reference point should two conditions: (i) the amplitude of of the point (hereinafter termed as the certainty value for simplicity) is a local maximum, and (ii) the local maximum should be over a fixed threshold

5) Repeat step (4) until all reference points are located.

6) If no reference point is found ,we take maximum certainty value in the whole fingerprint image as the reference point.

D .Combined Minutiae Template Generation

Combined minutiae template is generated in mainly two steps: Minutiae Position Alignment and Minutiae Direction Assignment. In minutiae position alignment, among all the reference points of a fingerprint for enrollment, we define a reference point with the maximum certainty value as the primary reference point. Therefore, we have two primary reference points $\mathbf{R_a}$ and $\mathbf{R_b}$ for fingerprints A and B respectively. $\mathbf{R_a}$ is located at $\mathbf{r_a}=(\mathbf{r_x}, \mathbf{r_y})$ and $\mathbf{R_b}$ is located at $\mathbf{r_b}=(\mathbf{r_x}, \mathbf{r_y})$.The position alignment is performed by using below equation:

$$(P_{ic})^T = H.(P_{ia} - r_a)^T + (r_b)^T \quad (11)$$

In minutiae direction assignment, Each aligned minutiae position P_{ic} is assigned with a direction θ_{ic} . The direction alignment is performed by using below equation:

$$\theta_{ic} = O_b(x_{ic}, y_{ic}) + \rho_i\pi \quad (12)$$

where ρ_i is an integer 1, if mod (length of ridge ending, 2) > 0. Otherwise it is 0.

By using above two equations, we generate combined minutiae template M_c. Once all the N aligned minutiae positions are assigned with directions, a combined minutiae template $M_C = \{m_{ic} = (P_{ic}, \theta_{ic}), 1 \le i \le N\}$ is used for enrollment.

E. Two-Stage Fingerprint Matching

The two-stage fingerprint matching process including query minutiae determination and matching score calculation. In the proposed method, during the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints A and B respectively. We extract the minutiae positions from fingerprint A, the orientation from fingerprint B using some existing techniques .Then, by using our proposed coding strategies, a combined minutiae template is generated based on the minutiae positions. Finally, the combined minutiae template is stored in a database. In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints A1 and B1 from fingers

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

A and B. Then we extract the minutiae positions from fingerprint A1 and the orientation from fingerprint B1. Reference points are detected from both query fingerprints. This extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold.

1) Query Minutiae Determination

The minutiae positions of PA1 of fingerprint A1, the orientation OB1 of fingerprint B1 and the reference points of the two query fingerprints are determine in this stage.

2) Matching Score Calculation

Calculate a matching score between *MQ* and *MC* based on the assumption that the matching score is greater than a threshold value grant the access.

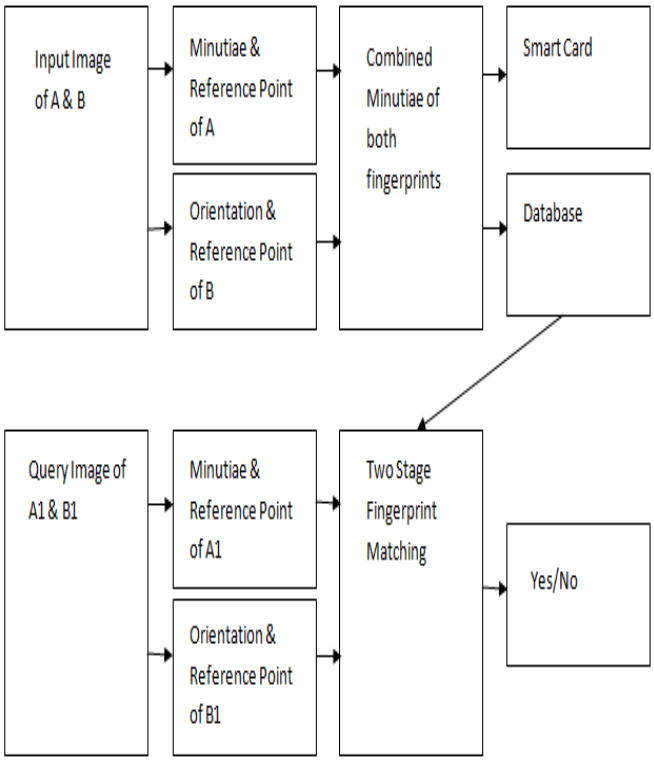


Fig. 3. Proposed fingerprint privacy protection system

IV. THE BIOMETRICS WITH SMART CARD

Using smart card technology significantly enhances privacy in biometric ID systems. The use of a smart card here allows building up a distributed database where every user is the carrier of his own biometric reference, hence alleviating the previous privacy concern. The smart card provides the individual with a personal database, a personal firewall and a personal terminal. It secures personal information on the card through advanced cryptography and digital signatures to prevent alteration or replacement of biometric data and to prevent cloning of the card. This allows the individual to control access to their biometric information and eliminates the need for central database access during identity verification. When used in combination with biometrics, a smart card ID becomes even more personal and private. A biometric provides a strong and unique binding between the cardholder and the personal database on the card, identifying the cardholder as the rightful owner of this card. The biometric cannot be borrowed, lost, or stolen like a PIN or a password, and so strengthens the authentication of an individual's identity. Because of their cryptographic processing capabilities, smart cards can be used in ID systems to increase the trustworthiness of terminals. Using the combination of smart card technology with biometrics for identification and authentication of individuals provides the most efficient implementation of a secure authentication system.

V. CRYPTOGRAPHIC KEY GENERATION FROM COMBINED BIOMETRICS

A. RSA based Asymmetric Cipher Methodology

One of the first algorithms implementing the public key infrastructure was developed in 1977 by Rivest, Shamir and Adleman . This well-known algorithm named RSA has been and is considered as the most widely accepted and implemented general-purpose approach to public-key encryption. The basic points of this algorithm are:

- p and q are very large prime numbers; they are private;
- $n = p*q$ is public;
- $\Phi(n)$ is the Eulero function;
- e is a number smaller of $\Phi(n)$ and co-prime to it; it is public;
- d is a number such that $e * d = 1 \bmod \Phi(n)$; it is private.

where e is named public exponent and d is named private exponent. In the RSA algorithm, both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, the public key (PU) is defined as $\{e, n\}$ and the private key (PU) is defined as $\{d, n\}$.

The encryption process for a generic message M is performed through the equation (13):

$$C = Me \bmod n \quad (13)$$

The decryption of the message C is performed through the equation (14):

$$M = Cd \bmod n \quad (14)$$

The main characteristic of this algorithm is that to determine d given e and n is infeasible.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

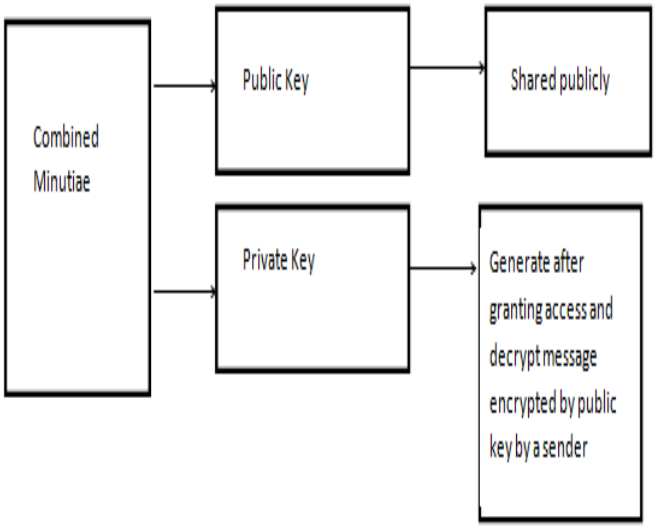


Fig. 4. Key generation.

In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys [16]. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key. In this system keys are generated from combined minutiae template.

VI. RESULTS AND DISCUSSION

In the enrollment phase, two fingerprints are captured from two different fingers (See fig.5). We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template.

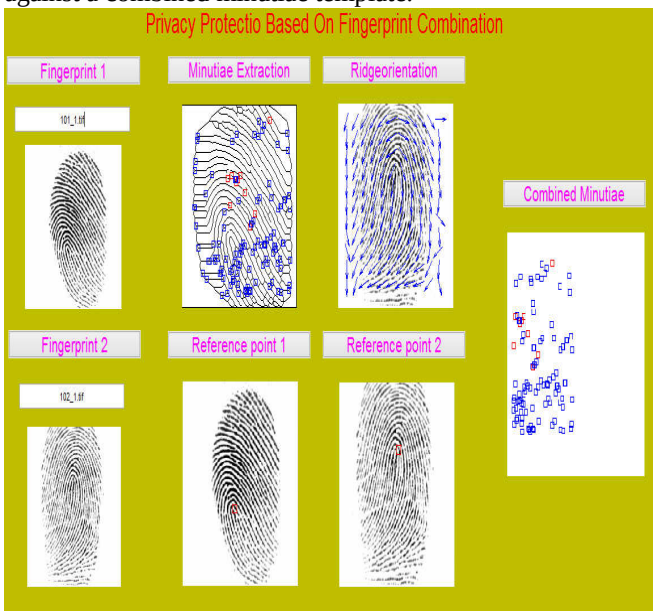


Fig. 5.Enrollment phase

In the enrolment phase, the biometric trait is acquired and processed to extract its own distinctive features. Biometric trait representation is encrypted and stored in tamper-resistant device, i.e. smartcard. During the authentication phase, the enrolled biometric identifier is used together with the query biometric identifier for user authentication and public/private key pair generation. The link between biometric traits and the cipher algorithm is a pair of prime number .In the public key generation phase (See Fig. 6.) the user must enroll in the system/platform giving his fingerprint.

After enrolment phase, the identifier is extracted and stored in the user's smartcard. Using the information contained in the identifier, the public key is generated and distributed. This public key is used to encrypt the message typed by a sender.

Fig. 6. The biometrics with smartcard

During the authentication phase (See Fig. 7.), the user gives his smart card and fingerprints through the sensor. These two inputs are processed: if the user is correctly authenticated, then the system will grant the access. So user can generate his private key and this private key is used to decrypt the message encrypted by a sender.

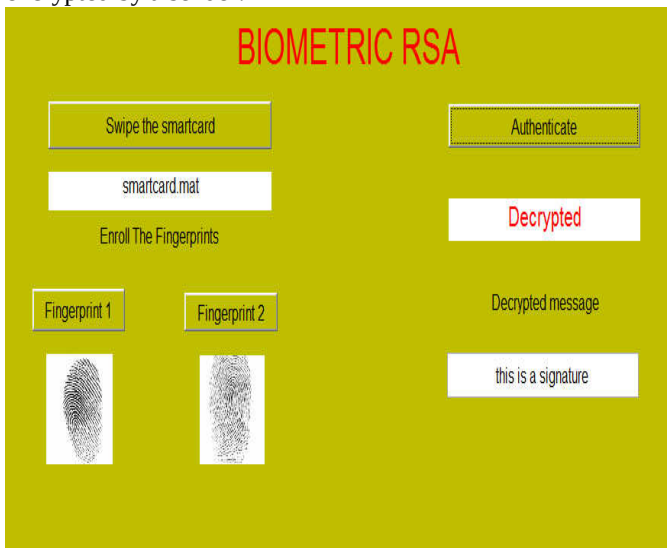


Fig. 7.Enrollment phase

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.

A. Evaluating the Performance of the Proposed System

In order to evaluate the effectiveness of the our proposed approach, we considered both the FMR (FALSE MATCH RATE) and FNMR (FALSE NON MATCH RATE).FVC2002 DB1 database was used for this evaluation. The database consists of 80 images made up of 10 individuals with 8 prints for each. The accuracy was determined by following FVC testing protocol that uses 280 [((8*7) /2) * 10] genuine and 45 [((10*9) /2)] impostor comparisons.

- False match rate = number of false acceptances / no:-of identification attempts
- False non- match rate = number of false rejection / no of identification attempt.

For a high security scenario FMR of 1% is not acceptable because it means that for one hundred attempts to access the system by impostors one of them will be succeeded. It is an extremely high rate for this kind of application. For decreasing the FMR rate the DT (Decision threshold) must be increased and as consequence the FNMR will simultaneously increase. In our example, suppose the DT is fixed on 0.48 as showed in figure 8. In that case, the FMR(0.48) is 0,0001 (0,01%) guaranteeing that for ten thousand attempts to access by impostors only one of them would be succeeded which is an acceptable rate for the application. Nevertheless, it must be admitted simultaneously a FNMR rate of 0.1568 (15%) meaning that fifty percents of the genuine attempts to access will be denied. In that case, the system is more save but also more rejected by users, because the high number of unsuccessful attempts of genuine access.

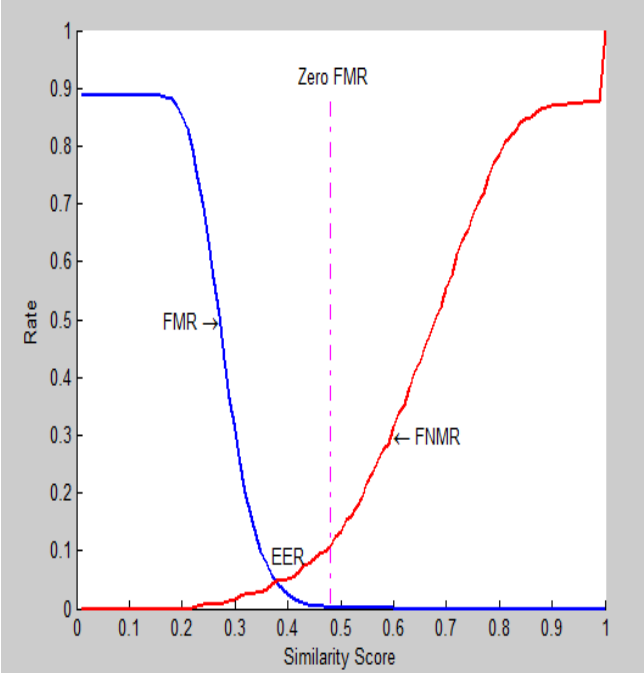


Fig. 8. Decision threshold (0.48) fixed for a high security scenario.The FMR value is 0.0001 (0,01%) and the FNMR is 0.1568 (15,6%).

VII. CONCLUSION

This method introduces a novel system for fingerprint privacy protection by combining two different fingerprints into a new identity. In this paper fingerprint traits have been integrated in the RSA algorithm to develop a new asymmetric cipher system, so that this process will be unpredictable for hackers. In the enrollment phase, two fingerprints are captured and processed to generate combined minutiae template, stored in user smartcard. During the authentication phase, the enrolled biometric identifier is used together with the query biometric identifier for user authentication and public/private key pair generation. The experimental results show that our system achieves, low false match rate and high false non-match rate ensure that unauthorized person will not be allowed access. Thus we are able to increase the level of security.

REFERENCES

1. Sheng L and Alex C. Kot, “Fingerprint Combination For privacy Protection,” in Proc. IEEE transactions on information forensics and security, vol. 8, no. 2, February 2013
2. A. Othman and A. Ross, “Mixing fingerprints for generating virtual identities,” in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.
3. Safnitha P Y and Sheena Kurian K, “Fingerprint image enhancement with emphasis on histogram equalization adaptively”, UGC sponsored national conference on information and communication technologies at BPC college piravom, march 2014.
4. T. Connie, A. Teoh, M. Goh, and D. Ngo, “ Palm hashing: A novel approach for cancellable biometrics," Information processing letters, vol. 93, no. 1, pp. 1-5, 2005.
5. Sayani Chandra, Sayan Paul, Bidyutmala Saha and Sourish Mitra, “Generate an Encryption Key by Using Biometric Cryptosystems to Secure Transferring of Data over a network” IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 12, Issue 1 (May. - Jun. 2013), PP 16-22
6. K. Nilsson and J. Bigun, “Localization of corresponding points in fingerprints by complex filtering,” Pattern Recognit. Lett., vol. 24, no. 13,pp. 2135–2144, 2003.
7. Arun Rossa, Anil Jaina, James Reismanb, “A hybrid Fingerprint matcher”, 2003 Published by Pattern Recogninition, Elsevier Science Ltd 36 (2003) 1661 – 1673, Elsevier Publication
8. X. Jiang andW.Yau, “Fingerprint minutiae matching based on the local and global structures,” in Proc. 15th Int. Conf. Pattern Recognition, 2000, vol. 2, pp. 1038–1041.
9. J. G. Jo, J. W. Seo, and H. W. Lee, “Biometric digital signature key generation and cryptography communication based on fingerprint," First Annual International Workshop 2007, LNCS 4613, pp. 38-49, Springer Verlag, 2007.
10. L. Hong, Y. F. Wan, and A. Jain, “Fingerprint image enhancement: Algorithm and performance evaluation,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 20, no. 8, pp. 777–789, Aug. 1998.
11. Fingerprint Verification competition, For accessing fingerprint database, http://bias.csr.unibo.it/fvc2004/download.asp, accessed on 20.05.2014.
12. Shweta Malhotra, Chander Kant Verma , “A Hybrid Approach for Securing Biometric Template”, International Journal of Engineering and Advanced Technology (IJEAT), ISSN: 2249 – 8958, Volume-2, Issue-5, June 2013.
13. Vincenzo Contiand, Salvatore Vitabile and Filippo Sorbell, “Fingerprint Traits and RSA Algorithm Fusion Technique”, 2012 Sixth International Conference on Complex, Intelligent, and Software Intensive Systems.
14. ANSI INCITS 378. Information technology - Finger Minutiae Format for Data Interchange,2004.
15. Christian Rathgeb, Andreas Uh, “A survey on biometric cryptosystems and cancelable biometrics”, EURASIP Journal on Information Security 2011, 2011:3, http://jis.eurasipjournals.com/content/2011/1/3, 2011:3,
16. Kai Xi, Jiankun Hu, “Bio-Cryptography”, Handbook of Information and Communication, Peter Stavroulakis,Mark Stamp (Eds.) Security, pp. 129-157, c Springer 2010[3] Feng Hao, Ross Anderson, John Daugman, “Combining cryptography with biometrics effectively”, Technical Report No. 640, 2005, UCAM-CL-TR-640, ISSN 1476-2986

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication Pvt. Ltd.