International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 6 | ISSN : 2456-3307

A Study on Image Encryption Using Key Matrix Generation from Biometric Mixed Fingerprint Image for Two Level Security

M. D. Randeri[1], S. D. Degadwala[2], A. Mahajan[3]
[1] M. E. Student, Computer Engineering, Sigma Institute of Engineering, Vadodara, Gujarat, India
[2]Head of Computer Department, Sigma Institute of Engineering, Vadodara, Gujarat, India
[3]Assistant Professor, Computer Department, Sigma Institute of Engineering, Vadodara, Gujarat, India

ABSTRACT

In recent Era, Security has been most important issue to be considered with different forward looking and preventing measures. Several cryptographic algorithms are developed for encryption and decryption using a secret key. The issue with this strategy is that user ought to recall the key or store the key in a database, which make the framework under danger. Once the put away key is bargained, at that point an attacker can get to the private information effectively. To maintain uniqueness of key, a biometric feature such as fingerprint can be used, whereas randomness can be induced using different combinations of fingerprints. In this paper, we propose a technique to generate the key matrix by extracting minutiae points from mixed fingerprints of the sender and receiver. This system contains four phases. One is Enrolment Phase, second is Authentication Phase, third is Key Generation phase and last is Cryptographic phase. For encryption of the original image using generated key matrix, we use Hill cipher.
Keywords *:* Fingerprints, Minutiae points, Cryptography, Hill Cipher.

I. INTRODUCTION

As of late, the advance in the correspondence innovations is bringing about exchange of data in the openly shared media. To secure these, there is a huge intrigue appeared by the researchers in the cryptographic area prompting numerous creative and productive encryption strategies. Each encryption technique needs to utilize secure keys. The cryptographic keys might be an arbitrary number or password. There are different techniques to produce such keys; a few strategies are proposed to create cryptographic keys from the biometric for example, iris, fingerprints, signature and so forth as in [1, 3, 4, 5]. There is a critical development in the field of biometric innovations in recent years, and many of them are deployed according to the specific application and their acceptability to the users. Fingerprints have been utilized for over a century and are the most generally utilized type of biometric recognizable proof. This unique mark of an individual is interesting and stays unaltered over a person's lifetime. On a finger, the unique patterns formed by the ridges make up fingerprints. A valley is the area between two consecutive ridges. Among various minutiae types, the ridge endings and bifurcations are utilized commonly. Ridge endings are point where the ridge terminates and bifurcation are points where a single ridge divides into two ridges. In this paper, we propose a new technique of encrypting an image using key matrix, which is generated from mixed fingerprints of sender and receiver. The proposed technique has four phases namely:

Enrolment phase, Authentication phase, Key Generation phase and Cryptographic phase. In enrolment phase, the fingerprints of both sender and receiver are acquired and stored on the server along with identification key generated from their minutiae points. In authentication phase, the sender's given fingerprint and the fingerprint stored on the server is compared. If the matching score is within threshold value, the authentication is successful. If authentication is successfully completed, the sender generates mixed fingerprint image from his/her own fingerprint and receiver's finger print from server. Then in Key generation phase, cryptographic key matrix is generated from this mixed finger print image. Here we will generate 4x4 key matrix. Finally in cryptographic

phase, the original image is converted into 256x256 matrix form and divided into 4x4 sub matrices. Each sub matrix is encrypted using Hill cipher with previously generated key matrix. Encrypted image is created by combining each encrypted sub matrix in same order.

Rest of the paper is organized as follows, Section I contains introduction of cryptography, fingerprints and proposed approach, Section II contains related work, Section III explains the methodology to be used in the proposed work, Section IV describes the overall algorithm of encryption and decryption and Section V concludes the paper.

II. RELATED WORK

Many researchers have developed various techniques for image encryption using different cryptographic keys generated from biometrics.

In [7], Ziad E. Dawahdeh, Shahrul N. Yaakob and Razif bin Othman combined Elliptic Curve Cryptography (ECC) with Hill Cipher to improve security of Hill Cipher for image encryption. They used self invertible key matrix which is dependent of ECC and elliptic curve discrete logarithms problems are difficult to retrieve the key. The approach is applied only to greyscale images, need to be modified for RGB images.

In [8], Panduranga H T and Naveen Kumar S K described an approach for partial image encryption using dual stage Hill Cipher. In this approach, two self-invertible key matrices are generated from the original key and used in two stages of encryption using Hill Cipher.

In [1]. A technique is described by Subhas Barman, Debasis Samanta and Samiran Chattopadhyay which uses cancellabele fingerprint templates of sender as well as receiver to generate a secret key. They produced revocable key from unique finger impression for symmetric cryptography The symmetric cryptography based on session key can use this generated secret key.

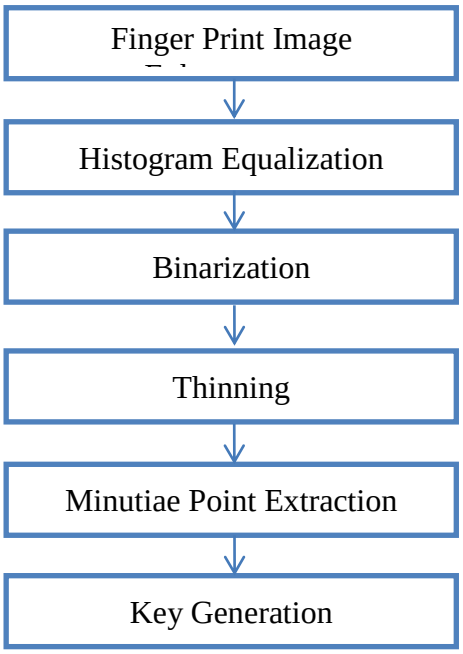
In [5], Sharda Singh, Dr. J. A. Laxminarayan proposed methodology which used combination of fingerprints to generate pair of keys for RSA algorithm. The random key was generated by extracting minutiae points from fingerprints and forming a key array. From that key array, the key pair for RSA encryption and decryption was generated. As randomness is involved at many levels, the complexity of key is expected to be very high.

In [4], M. Marimuthu and A. Kannammalp presented the simplified approach for generating cryptographic keys to reduce the complexity of traditional cryptosystem. They generated a 256 bit secure key by incorporating dual fingerprints of human being and extracting their features. Their results demonstrated the efficiency and better security.

III. METHODOLOGY

In the proposed technique, for generating identification key for each user, we have extracted minutiae points from the user's fingerprint image.

A. Identification key generation



Finger print Image Enhancement

However, in practice, the fingerprint image may not be clear because of the noise elements. Noise elements may present due to variations in skin or scars, mugginess, improper contact with the scanning device. Hence, to improve the clarity of ridges against the valleys by decreasing the noise elements, various image enhancement techniques.

Histogram Equalization

The first histogram of the original fingerprint image is of the bimodal type, the histogram after equalization involves the range from 0 to 255 and perception impact is upgraded.

Fingerprint Image Binarization

The procedure to get a binary image from a given greyscale image is called Binarization. It makes clear the differentiation between the ridges and valleys, so that minutiae extraction is encouraged. Binarization results in a binary image having ridges as foreground and valleys as background.

Thinning

Thinning is the way toward lessening the thickness of each line of ridges to a single pixel. The prerequisites of a thinning algorithm are A) The thinned fingerprint image ought to be of single pixel width without any disruptions. B) Each ridge ought to be as thin as its middle pixel. C) Wipe out noise and singular pixels. D) No further evacuation of pixels ought to be conceivable after thinning procedure.

Minutiae Extraction

Figure 1 : Minutiae Features [2]

The vast majority of the finger-scan technologies depend on Minutiae. Minutiae-based systems speak to the fingerprint by its features like terminations and bifurcations.

The Crossing Number (CN) strategy is utilized for minutiae extraction. By analyzing the neighbourhood of each ridge pixel utilizing 3x3 window, the ridge endings and bifurcations are removed. For a ridge pixel P the crossing number CN is calculated as

$$CN = 0.5 \sum_{i=0}^{9} |P_i - (P_{i+1})| \, , P_9 = P_1$$

Where P_i is the pixel value in the neighbourhood of P [5].

Eight neighbourhood pixels are scanned anti-clockwise for pixel P.

- If the central pixel is valued one and has only one valued neighbour, then it is an end point.
- If the central pixel is valued one and has three one valued as neighbour, then it is a bifurcation.

The pixel would be classified by CN value property after processing of a ridge pixel CN.
Minutiae are described in three co-ordinate system as (x,y,θ). In the first place, all x co-ordinates, y co-ordinates and θ co-ordinates are added independently. The resultant average values of X and Y co-ordinates are in decimal and the co-ordinate θ is in radian.

Step 1: The binary values XBi, YBi and θBi of Xi, Yi and θi for given i^{th} minutiae are taken.
Step 2: In order as follows, all the binary values are merged.
MBi= X Location (9bits) + X Location (9bits) + angle (3 bits)
Step 3: the merged binary string MBi is converted to decimal for obtaining the single coordinate value M1i.

B. Cryptographic key matrix generation from mixed fingerprints

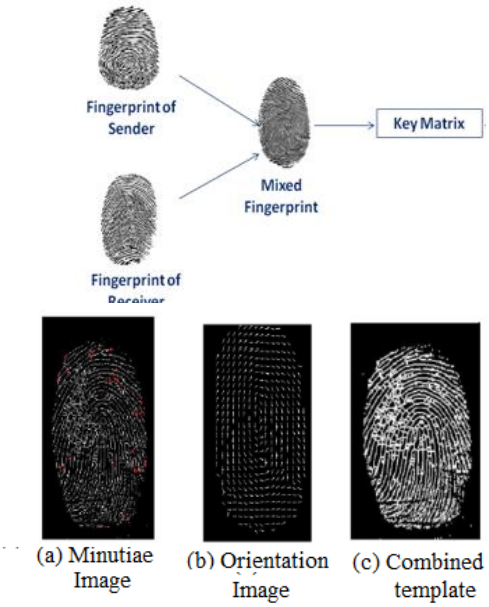


Figure 2 : Key Matrix Generation

The fingerprints of sender and receiver are taken. From one fingerprint the minutiae and reference points are taken, whereas from second orientation and reference

points are taken to make combined minutiae template. This generated combined minutiae template is used to generate cryptographic key matrix using key generation algorithm.

C. Encryption using Hill Cipher

In 1929, the mathematician Lester Hill invented a block cipher, called Hill cipher. It is kind of substitution cipher in which each letter of plaintext is substituted by the corresponding cipher text letter by applying m linear equations. Each alphabets a, b, .. z are allotted a number like 0,1..25. For m = 3, the system can be described as follows:

$$C_1 = (K_{11}P_1 + K_{12}P_2 + K_{13}P_3) \bmod 26$$
$$C_2 = (K_{21}P_1 + K_{22}P_2 + K_{23}P_3) \bmod 26$$
$$C_3 = (K_{31}P_1 + K_{32}P_2 + K_{33}P_3) \bmod 26$$

In matrix and column vector format, it can be written as follows:

$$C = K \times P$$

$$\begin{bmatrix} C1 \\ C2 \\ C3 \end{bmatrix} = \begin{bmatrix} K11 & K12 & K13 \\ K21 & K22 & K23 \\ K31 & K32 & K33 \end{bmatrix} \times \begin{bmatrix} P1 \\ P2 \\ P3 \end{bmatrix} \bmod 26$$

Here, P and C are column vectors describing the plaintext and cipher text. K is a 3x3 encryption key matrix.

Decryption is the reverse process of encryption, thereby requiring inverse of the key matrix K^{-1}.
$KK^{-1}=K^{-1}K=I$, where I is the Identity matrix. By calculating K^{-1} with C, P is retrieved.
It can be expressed as
For encryption:

$$C = E_K(P) = KP$$

For decryption:

$$P = D_K(C) = K^{-1}C$$

I. PROPOSED SYSTEM

Figure 3 shows the encryption process of our proposed approach. On the secured server, the fingerprint images for all users are stored along with their respective identification key. Before the transfer of an original image from sender to receiver, it follows two levels of security. First, the sender's identification key is generated from its fingerprint image and compared with that stored on the server. Once the sender is authenticated, the fingerprints of both sender and receiver are mixed, minutiae points from one fingerprint and region points from other one are extracted to form key matrix. Using the generated key matrix as key for Hill cipher, the original image is encrypted and sent to the receiver.

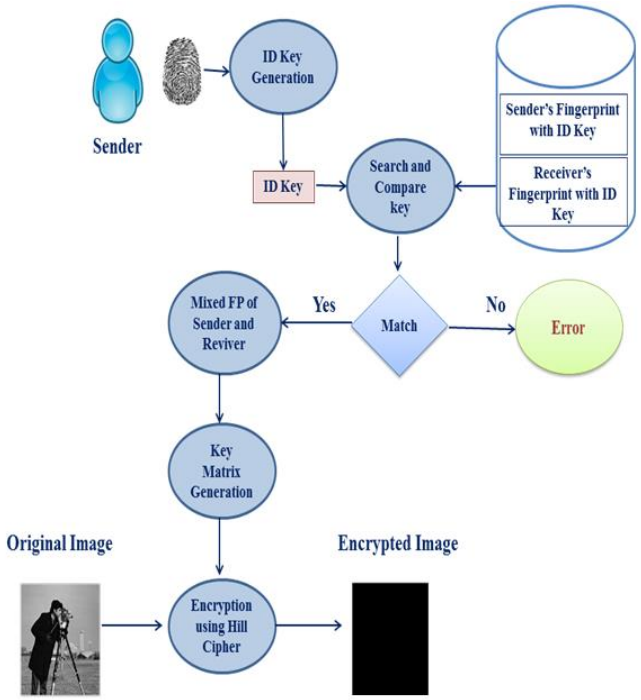


Figure 3: Encryption Process

At receiver side, the same authentication process follows and inverse key matrix is generated for decrypting the encrypted image and retrieving the original image back.

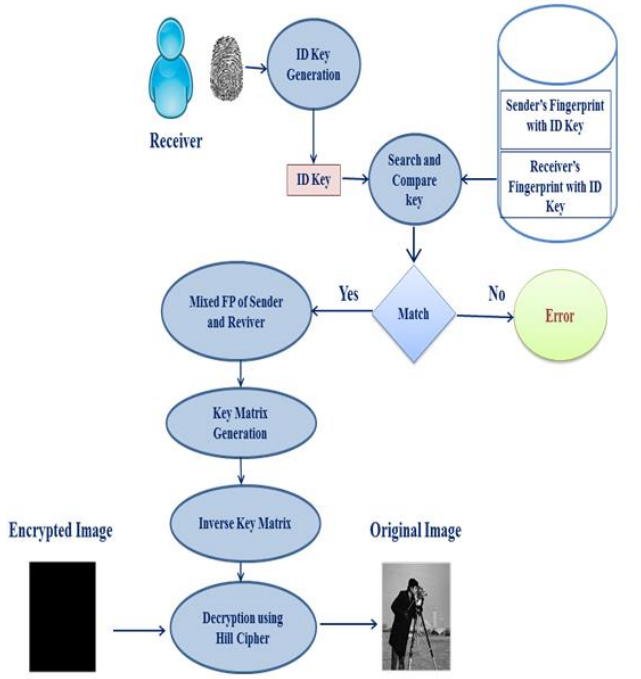


Figure 4: Decryption Process

IV.CONCLUSION

In this paper, we have proposed a novel approach for providing two level security to images being transferred in an open world. First the sender is verified by its fingerprint and identification key, and then key matrix is generated by extracting minutiae points from the mixed fingerprints of both sender and receiver. Using the generated secured key matrix, the original image is encrypted and sent to the receiver. The receiver decrypts the image using inverse key matrix. This way we can ensure more secure transfer of images around the internet.

V. REFERENCES

[1] Subhas Barman, Debasis Samanta and Samiran Chattopadhyay, "*Fingerprint-based crypto-biometric system for Network security*", EURASIP Journal on Information Security, Springer (2015).

[2] Mrs. Afreen Fatima Mohammed, "*Biometric Based Authentication Using Two-Stage Fingerprint Privacy Protection for File Storage on Server*", IJCSMC, Vol. 5, Issue. 3, March 2016, pg.377 – 387.

[3] Mofeed Turky Rashid, Huda Ameer Zaki, "*RSA Cryptographic Key Generation Using Fingerprint Minutiae*", Iraqi Journal for Computers and Informatics(IJCI), volume 1, issue 1, 2014.

[4] M.Marimuthu, A.Kannammal, "*Dual Fingerprints Fusion for Cryptographic Key Generation*", International Journal of Computer Applications, volume 122, July 2015.

[5] Sharda Singh, Dr. J. A. Laxminarayana, "*RSA Key Generation Using Combination of Fingerprints*", IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, (AETM'15).

[6] Goutham L, Mahendra M S, Manasa A P, Mr. Prajwalasimha S N4, "*Modified Hill Cipher Based Image Encryption Technique*", (IJRASET), Volume 5 Issue IV, April 2017.

[7] Dawahdeh, Z.E., Yaakob, S.N., Razif bin Othman, R., "*A New Image Encryption Technique Combining Elliptic Curve Cryptosystem with Hill Cipher*", Journal of King Saud University Computer and Information Sciences (2017).

[8] Panduranga H T, Naveen Kumar S K, "*Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique*", International Journal of Computer Applications (0975 – 8887) Volume 60– No.16, December 2012.

[9] F. Abundiz-Perez, C. Cruz-Hernandez, M. A. Murillo-Escobar, R. M. Lopez-Gutierrez, A. Arellano-Delagado, "*A Fingerprint Image Encryption Scheme based on Hyperchaotic Rossler Map*", Hindawi, volume 2016.

[10] Gang Zheng, Wanqing Li, Ce Zhan, "*Cryptographic Key Generation from Biometric Data using Lattice Mapping",* International Conference on Pattern Recognition, IEEE, 2006.

[11] N. Lalithamani, Dr. K.P. Soman, "*An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancellable Fingerprints Biometrics".* International Conference on Advances in Recent technologies in Communication and Computing, IEEE, 2009.

[12] G. Patel, G. Panchal, "*A Chaff-point Based Approach for Cancellable Template Generation of Fingerprint Data",* Springer International Publishing, ICTIS, 2017.

[13] R. K. Nichols, "*ICSA Guide to Cryptography",* McGraw-Hill, chapter 22.

[14] B. K. Sy, A. P. Kumara Krishnan, "*New Trends and Developments in Biometrics",* INTECH publisher, pp 191-218.

[15] R. K. Jangid, Noor Mohmmad, A, Didel, S. Taterh, "*Hybrid Approach of Image Encryption using DNA cryptography and TF Hill Cipher Algorithm",* International Conference on Communication and Signal Processing, IEEE, 2014.