ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

A Biometric Based Hybrid Approach to Secure End to End Communication with Symmetric Key Cryptography

Aparna K H[1], Shyjith M B[2], Ambikadevi Amma T[3]

P.G. Student, Department of Computer Science and Engineering, JCET, Palakkad, Kerala, India[1]

Assistant Professor, Department of Computer Science and Engineering, JCET, Palakkad, Kerala, India [2]

Professor, Department of Computer Science and Engineering, JCET, Palakkad, Kerala, India [3]

ABSTRACT: This work is motivated from the urge to develop a sound crypto biometric system that is free from concerns such as privacy of biometrics, sharing of biometric data between communicating parties, generating revocable key from irrevocable biometric, unwanted processing of low quality inputs etc., which all forms the mainframe matter of interest. It uses fingerprint as basic biometric and acquires it from sender and receiver simultaneously. This is processed and its quality is determined through Gabor filter processing. Feature extraction is done for a good quality input and certain transformations are made on it on both sides and the transformed templates are exchanged through a novel key based steganography. The templates are fused and shuffled thus providing a provision for revocability. An indexing based approach is employed for final key generation, thus generating a unique cryptographic key at both sides independently. Since neither the symmetric cryptographic key nor the original fingerprint is being stored there is no need of any kind of database security. Processing time is substantially reduced by the filtering of low quality inputs which is a main concern in all traditional biometric systems. It also throws light on to extending the work for multiple sender/receiver systems with the same kind of biometric bindings, safety and security, heralding the end of typed passwords.

KEYWORDS: Crypto biometrics, Gabor filter, Steganography, Biometric fusion, Revocability, Symmetric Key.

I. INTRODUCTION

The modern networking technologies have altered the way communication is usually done. Security is a very crucial aspect that must be considered in order to evenly safeguard ones invaluable data and hence it needs to be enhanced and nurtured to fortify the statistics, data and personnel accounts. Many eminent means and methods are available today for acquiring security in varied environments.so as far as data sharing in network is concerned a secured framework needs to be developed in emergency as the threats in networks are increasing day by day. Any networking personnel today will be familiar with the attacks like DNS, DNS spoofing, man in middle, smurf attacks, heap overflow etc. To sum up, we can say that security in communication can be achieved through mainly two ways: one secure the whole network for communication or else secure the message to be communicated. By all means the second option appears to be more appealing than the former. So somehow wrap up the message being transmitted.

Cryptography has been regarded as the part and parcel of any security framework from the ever old ancient ages. We can witness a new form of cryptography rooting at least once in every decade. Even when different data hiding forms like steganography, watermarking, signatures etc. emerging and spreading, almost all encoders depended on some or other kind of crypto techniques for ensuring their message security. Two procedures form the basis of any cryptographic technique- encryption and decryption and the aid for these two procedures are – keys. Thus key management is considered as the most difficult yet most important part of any cryptographic framework. Keys can be symmetric or asymmetric depending upon the type of cryptography adopted. The lack of proper binding between message and the sender rendered a serious security loophole as a properly guided brute force attack can easily cook up the cryptographic keys. This knowledge led to the biometric key concept.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Securing the message in a proper biometric vault can of course add a layer of security to the message transferred but as generally said – every coin has two sides, biometrics do have many predicaments associated with it: irrevocability of biometrics and need for enrolment process being the major botheration, others like sharing the biometric data between the sender and receiver, privacy of biometrics also do their own contributions. The researchers were hence forced to make up a unified framework which intertwined cryptography and biometrics- called crypto-biometrics, which helped them to divide the whole concern into two: i.e.,the primary concern of key generation is taken away by the biometrics and the authenticity of the users are automatically verified before the cryptographic decoding is performed thus binding the message and the user, tightly.

Our work primarily focuses on generation of unique cryptographic keys at the sender end and receiver end, thus enabling the proper binding of user with the message in a cutting edge fashion, which joins the fingerprint biometrics of sender and receiver in an absolutely unpredictable manner and uses this information to generate keys at both end separately thus eliminating the need for sharing of ultimate cryptographic key. Also we propose a method to revive the crypto key in a session wise manner so that there is no need to store the key for subsequent sessions, as each session utilizes a different key for encryption-decryption process, thus masking the message through an entirely different cypher text easy for an imposter to fake or reproduce. In addition to this we propose an algorithm to check the quality of the input fingerprint at the first stage, so that the processing of low quality fingerprint can be eliminated. Even if the fingerprints are unclear or improper minutiae points will be extracted which would subsequently lead to not so strong cryptographic keys being generated. If they are eliminated in the first trial it can save us from a lot of unwanted processing as well as save a lot of system resources. As the biometric itself is not used directly, there is practically zero chance for compromising the privacy of biometric trait.

The remaining of this paper is organized as follows. Section II summarizes the basic methodologies adopted in this work, like biometric transformations, fusion of biometrics, key generation from biometrics, feature extraction etc. it also briefly discusses about various methods of fusing biometrics etc. Next section explains the proposed system in detail with the needed block diagrams. Subsequently we discuss the results and future work possible in this field. Then we conclude the work with the references.

II. RELATED WORK

This work mainly consists of five major subtasks, namely: 1) Quality checking 2) Transformations on biometric templates 3) Secure transmission of biometric data 4) Fusion of biometrics 5) Key generation from biometrics. There exists a few works related to each of these subtasks which are briefly discussed in this section.

A. Quality checking

Providing quality inputs is not always practical since this depends upon so many environmental factors in one way or another. As this work focuses on fingerprint biometric – a scanner or any other machine that take the input fingerprint image is concerned and that would depend on factors such as proper alignment of fingerprint, lightings in the surroundings, proper dots per pixels settings in the machine, format of storing the image, cuts and bruises in the finger etc. Minutiae based approach is very much sensitive to noise and deformations. For instance false ridge endings and bifurcations may appear due to blurred or over inked problems. More over ridge endings and bifurcations may disappear when a finger is pressed too hard or too light i.e. the performance of minutiae extraction algorithms relies heavily on the quality of the fingerprint. If the quality of the image is checked first, then it is possible to reject the image with very poor quality. It is therefore desirable to design an automatic scheme that examines and quantifies the quality of the acquired fingerprint image before it is processed.

Normally three different point-of-views are considered for any biometric sample quality [3] namely, 1) Character 2) Fidelity 3) Utility. Fingerprint is usually defined as a measure of the clarity of ridges and valleys and the extractability of features used for identification like minutiae, core or delta points. Algorithms used for fingerprint image quality estimation can be broadly divided into 1) those that use local features of the image 2) those that use global features of the image and 3) those that address the problem of quality assessment as a classification problem. A method proposed by Ratha and Bolle [4] for image quality estimation in the wavelet domain which is suitable for WSQ compressed fingerprint images. But it cannot be used for uncompressed fingerprint images, since wavelet transforms consumes much computation. Sufficient methods are not yet developed in spatial domains for accurate estimation of fingerprint

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

image quality. Quality can be determined by measuring the variance of gray levels, which is computed in a direction orthogonal to the orientation field in each block, in the work proposed by Hong et al [3]. Since this method is based on the orientation field and it doesn't take into consideration the ridge frequency into account. But if the image is noisy precise orientation field cannot be determined.

A two dimensional Gabor filter is a linear filter that acts as band pass spatial filter with the ability to tune to certain orientation and spatial frequency. Its Impulse Response Function (IRF) also known as carrier is a complex sinusoid which is modulated by an elliptical shaped Gaussian envelope. A filter bank is a combination of Gabor filters calculated at different scales and orientations. It is generally employed to compute the Gabor feature. It helps to recognize the object irrespective of its geometric transformation. These Gabor features elegantly represent ridge structures and hence can be directly employed to detect features required. The quality checking in this paper is inspired from the concept on the paper [3] by Lin Lin Shen et al, where it doesn't take the orientation as a main factor and hence its precision is not much affected by the surrounding noises.

B. Transformation of biometric templates

Ratha et al [6] proposes three kinds of transformations possible on biometric templates so as to make them cancellable or revocable. 1) In Cartesian transformations approach the minutiae space is divided into rectangular cells which are numbered in a sequence. A transformation key is used to shift the rectangular cells to a new location thus relocating the minutiae points. 2) In Polar transformation approach the coordinate space is divided into polar sectors, numbered in sequence and the sector position is changed using a translation key. 3) In Functional transformation approach the transformation is modelled using a vector valued function, which is an electric potential field parameterized by a random distribution of charges. Compared to the latter two approaches Cartesian transformation is most simple to adopt and proceed. The transformation key can be made absolutely independent for sender and receiver thus making the transformations absolutely unpredictable for an outsider. Also by changing these transformation keys the whole mode can be varied without much logical changes in the procedures.

C. Secure transmission of biometric data

Simply passing the cancellable biometric templates is also possible as a method but cannot be considered fully secured. Some kind of data hiding techniques can be employed so as to make a notion that apparently nothing is being shared or passed. Watermarking and steganography are commonly adopted data hiding schemes. Rather than adopting a simple LSB steganography, a more complex one like key based steganographic embedding [5] can be adopted. This would add another layer of protection for the steganographic scheme being used.

Read the original image and the image which is to be hidden in the original image and shift the image to hide in the cover image by X bits. And the original image or cover image with 240 which is 11110000 i.e. four MSB's set to 0. Because of this only four LSB's are considered further. The shifted hidden image and the result of the previous step are bitored. This makes changes only in the X LSB bits so that the image is hidden in the original image. The reverse process is done for decoding process.

D. Biometric Fusion

As far as biometric templates are concerned normally five kinds of fusion techniques are adopted [7].

1. Sensor level: This fusion strategy requires the raw data to be acquired from multiple sensors which can be further processed and integrated to generate new data from which features can be extracted. Sensor level fusion can be done only if the multiple cues of the same biometric are obtained from multiple compatible sensors.
2. Feature level: The feature set is extracted from the multiple sources of information and is further concatenated into a joint feature vector. This new high dimensional feature vector represents an individual. In case of feature level fusion some reduction technique must be used in order to select only useful features.
3. Match score level: Match score is a measure of the similarity between the input biometric and template biometric feature vectors. Based on the similarity of feature vector and the template, each subsystem calculates its own match score value. These individual scores are finally combined to obtain a total score, which is then passed to the decision module, after which recognition is performed.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

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

5. Decision level: In a multi biometric system, fusion is carried out at this level when only the decisions output by the individual biometric matchers are available. Here, a separate authentication decision is computed for each biometric trait which is then combined to result in a final vote. Different strategies are available to combine the distinct decisions of individual modality to a final authentication decision. Fusion at this level is considered to be rigid compared to the other fusion schemes due to the availability of limited information.

All these techniques are not suitable in all scenarios. The mode of fusion need to be adopted depends highly on mainly the inputs and requirement of the output as well as the kind of algorithm adopted. This work adopts the feature level fusion technique as the fusion method.

E. Key Generation from Biometrics

Biometric trait would be in some or other template format and that needs to be converted to a key format, so that it can be used for encoding in any encryption algorithm like AES, DES, and RSA etc. Keys are the most important part of any symmetric key cryptographic system. Hence that part needs to be made fully clean and clear so that no kind of security problems are likely to emerge. Normally the keys are numbers as they are readily available without a limit and easily modifiable and easy to manipulate too. Keys when made binary become even more safe as it contains only bit strings of zeros and ones and hence very much random. It is very much difficult to brute force the key because of its randomness.

Key generation algorithm depends on the available input and the expected output of the system. Starting from a simple representation of the pixel values of the image the keys can be even the hash value of the adjacent pixels in the image [1]. A work of fuzzy extractor directly uses a different approach called fuzzy commitment scheme. A novel approach in the paper [2] of Samantha et al uses a new approach, a simple yet effective one based on indexing of the available minutiae data to generate a single key. It yields a 256 bit key from a fingerprint template which adds the security in such a way that it doesn't even disclose the original pixel values of the minutiae points on the fingerprint template. This is a very simple approach easy to understand and implement.

III. PROPOSED SYSTEM

In this section we discuss our proposed approach in detail. An overview of our approach is shown in Fig 1. The ultimate aim of this work is to produce symmetric keys at sender and receiver end separately without sharing the final key- which enables the sender to encrypt and send the message and receiver to receive and decrypt properly. For this sender and receiver are asked to enter their fingerprints in to the system separately at their own end systems. They are first passed through a quality checking module which enables the system to filter out low quality fingerprints and inform the user that the fingerprint entered is of low quality and hence you need to re-enter the fingerprint for further processing. After this the sender and receiver extract the minutiae points from their own fingerprints. These extracted minutiae points are transformed in to a cancellable form called cancellable template, which introduces revocability to the irrevocable fingerprint biometric.

These templates are then exchanged between the two parties through a method of steganography. The stego key (K_g) is used by both parties for secure steganographic use. It is generated from a password (pwd) using PRNG. After this exchange the decoded templates are fused together through a concatenation based feature level fusion technique. This combined template is then used for extraction of keys through an indexing based approach which helps us to directly derive the final key so that no intervening can create any kind of fake keys of length 256 bits in an easy way. This key is then used to encrypt the message through AES encryption and send to the receiver where it can easily decrypt it by using key produced at its end for that session. Any other key cannot decrypt the message other than the one genuinely created at the receiver side.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

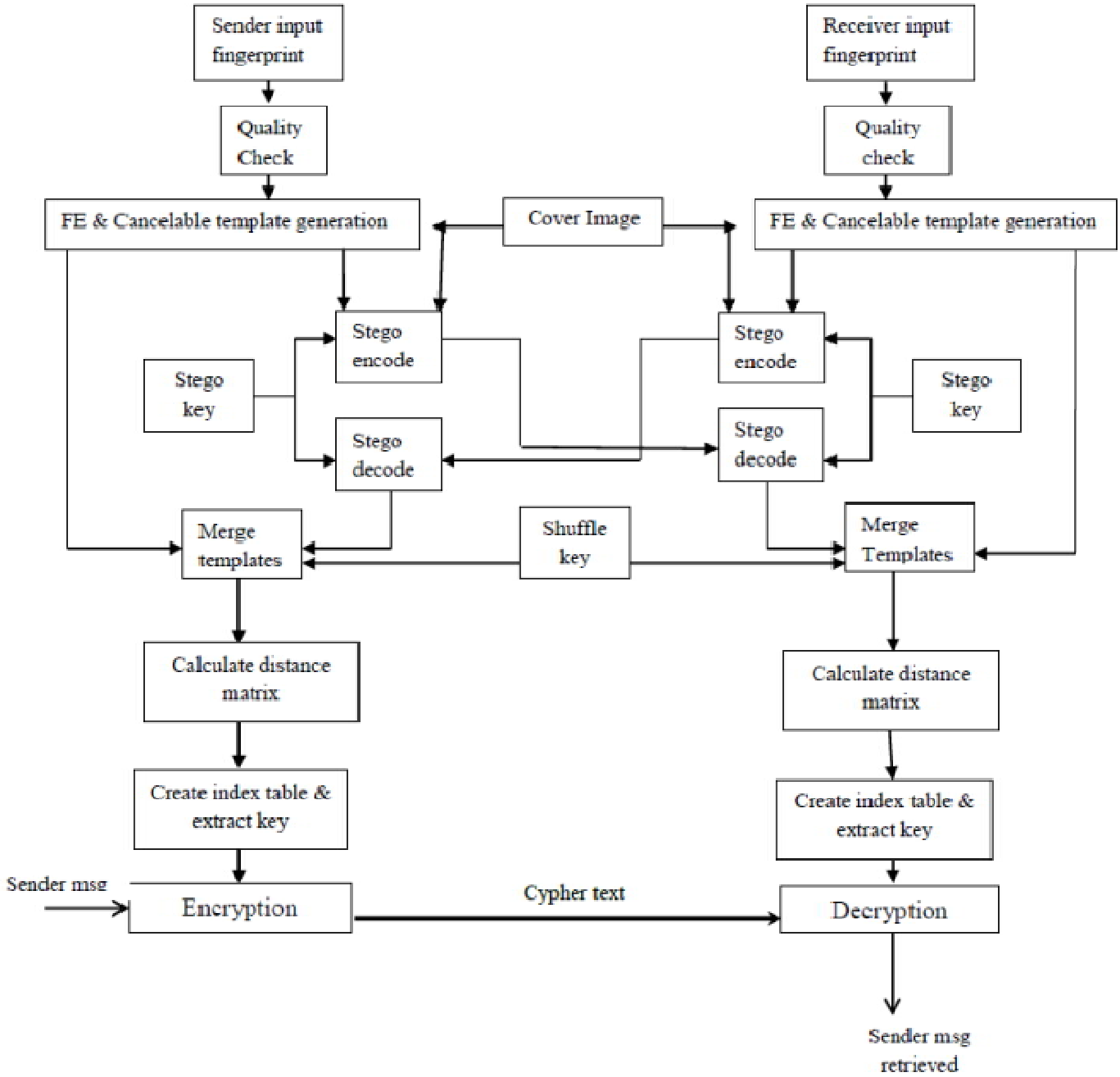

Fig. 1 The proposed system

A. Key generation algorithm

Input: 1. Fused template of sender and receiver (X & Y coordinates)
2. Shuffle key (K_{shuff})

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Algorithm:

1. Template (fused) is taken as input having the X and Y location values.
2. All distances ($d_{i,j}$) between distinct minutiae points of the fused template are computed and stored in a matrix D.

$$d_{(i,j)} = \sqrt{(x_i-x_j)^2 + (y_i-y_j)^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

3. Sort out the distance between each minutiae points and store only unique distances in a vector UA.

$$U_A = [\, u_1,u_2,u_3,u_4 \ldots\ldots\ldots\ldots u_q] \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

4. Map these unique distances into another vector FTA in such a way that the value of ui, will be stored at a location of that vector whose index value is equal to ui.

$$F_{TA}[uk] = uk \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

5. Fill in the empty positions with zero $F_{TA}[t] = 0$, where t Ɇ UA

6. Generate the key from this in such a way that put a zero at K[i] if $F_{TA}= 0$ and if F_{TA} != 0 put a one for the key.

Output: The final cryptographic key K

B. Shuffle key updation algorithm

Another important highlight of our work is its ability to update its cryptographic keys for each session. This updation further helps us to secure the transaction because even if a single key gets compromised, and the attacker captures subsequent messages he/she is not in a position to decrypt the message using the captured key in any way. For this we introduce another randomizing measure named K_{shuff} or shuffle key into the system. Then the revocability of cryptographic key is achieved with not only the cancellable fingerprint template but also with the shuffle key. The initiation for updation can be done by sender/receiver [1].

C. Quality checking algorithm

For a good quality image block with local ridge orientation the values of one or several Gabor features are much bigger than that of the others. For poor quality image blocks or background blocks without local ridge orientation the values of m Gabor features are close to each other. So the standard deviation values of both foreground or background segmentation as well as quality estimation. A primary segmentation is done on the fingerprint as foreground and background area blocks to avoid extraction of features in the noisy background areas of the image.

Input: Fingerprint image (scanned output in any standard format .tif, .jpeg, .bmp etc...)

Algorithm:
1. Divide the image in to N blocks of a standard size WxW (say 6x6).
2. Compute the m WxW Gabor matrices using standard Gabor filter equation in Matlab.
3. Compute m Gabor features and the standard deviation value G for each block centered at pixel (i,j).
4. If G for a block is less than a threshold value T_b, mark that block as a background block and otherwise mark it as foreground. Thus a primary segmentation is made in the fingerprint input.
5. The quality field value for a foreground block is defined to have one of the values: good or poor. The block is marked ‘poor’ and if its G value is less than a given threshold T_q. otherwise mark it as ‘good’.
6. Compute the quality index for the whole image using the following formula,

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

QI =1 -- (No of poor foreground blocks /No of foreground blocks)…….. (4)

7. A fingerprint is classified good if its QI value is greater than a threshold T_Q and else classified as unclear.

IV. SIMULATION AND RESULTS

The work is simulated using Matlab 12.We have tested the system using fingerprint images from publically available fingerprint databases FVC 2000, FVC 2008, FVC 2004. We propose to generate transformation keys (s_k,r_k), randomly using pseudo random number generator using, a sender entry and a receiver entry asthe seed value.

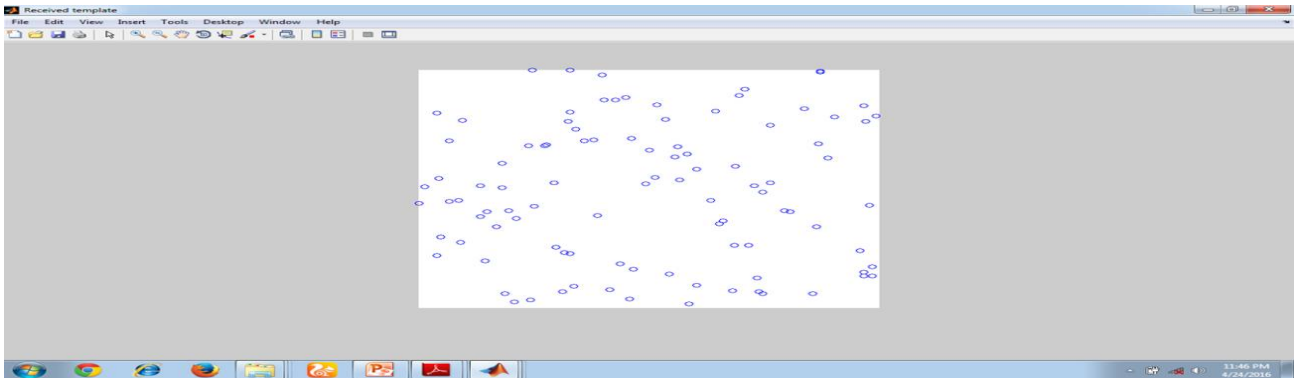

Fig. 2 Fused Template

The cover images are chosen separately by the sender and receiver from a set of synthetic fingerprint database CASIA fingerprint dataset. The exchanged templates are fused together using a concatenation based feature level fusion technique. The fused template is shown in figure 2. The distance matrix containing the distances between the various minutiae points of the fused template is recorded and based on these distances the final cryptographic key is generated as a string of binary bits of 0's and 1's. This key is used to encrypt the input message using AES encryption algorithm (Figure 3).

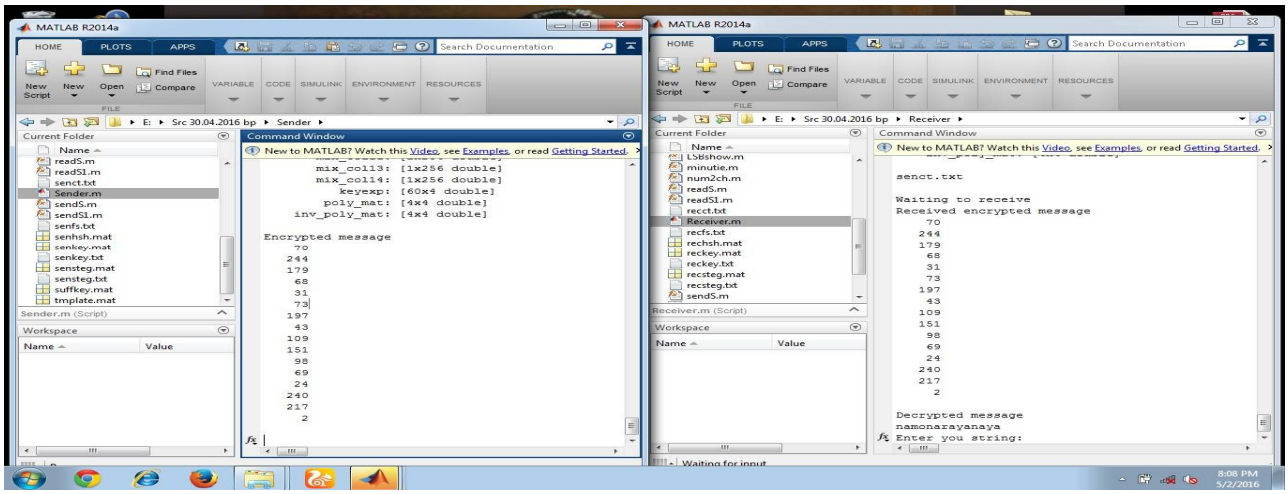

Fig. 3 Encryption and Decryption

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Thetheory of symmetric key encryption algorithm is that only the same key used for encryption can decrypt the original message precisely. When tested, we can clearly see through that the key generated as a result of algorithm processing at the receiver can decrypt the message accurately whereas any other key randomly generated is unable to perform the decryption properly. A comparison measure of the two methods of key generation is given in table 1. A set of fingerprints were used for analysis and each pair takes a different amount of time to perform the key generation, depending on its quality. But on an average the indexing based key generation takes much a lesser time than the former method.

V. CONCLUSION

Security in communication has become very much in evitable in this ever pirated world. The only way to bind a message to its owner is through biometrics. Including this biometrics in to key generation can make it more complex for the intruder to predict the key and hence loot the message. Keeping this as the key idea, we have adopted a novel approach which combines the biometric traits of both sender and receiver and finally generates a key from the same. As per the adopted schemes same key i.e. a symmetric one would be generated at each peer entity, without the actual sharing of cryptographic key. A more impenetrable hashing algorithm can be implemented so as to make it more secure. Also the selection of biometrics can be altered like including the palm print or iris image can cause more randomness in the final key generated. As it is normally seen with all biometric systems there is no need of any kind of database to be implemented, not even to store the final key so as to make it use for subsequent sessions. Thus it totally frees the user from the overhead of introducing any kind of database security into the system. Thus a safe and secure two way session wise communication can be reliably established with much lesser overhead through this proposed work. Works can be extended in the light of including multiple sender/receiver systems in the communication scenario.

REFERENCES

1. Subhas Barman, Debasis Samanta and Samiran Chattopadhyay, “Fingerprint-based crypto-biometric system for network security”, Springer open journal, April 2015.H. Simpson, Dumb Robots, 3rd ed., Springfield: UOS Press, 2004, pp.6-9.
2. Subhas Barman , Debasis Samanta and Samiran Chattopadhyay, “Fingerprint Based Symmetric Cryptography”, IEEE High performance computing and applications(ICHPCA) International conference on 22-24 dec 2014.
3. LinLin Shen, Alex Kot and WaiMun Koo, “Quality measures of fingerprint images”, in proc. Audio video based person Authentication , 2001, pp 266-271, Springer open journal.
4. Ratha and Bolle, “Fingerprint Image Quality Estimation”, pp 819-823, ACCV 2000.
5. V Lokeswara Reddy, A Subramanyam, P Chenna Reddy, “Implementation of LSB Steganography and its Evaluation for Various File Formats”. Int. J. Adv. Netw. Appl. 02(05), 868–872 (2011).M. Young, The Technical Writer’s Handbook, Mill Valley, CA: University Science, 1989.
6. NK Ratha, S Chikkerur, JH Connell, RM Bolle, “Generating Cancellable Fingerprint Templates”, IEEE Trans. Pattern Anal. Mach. Intell. 29(4), 561–572 (2007).
7. S.R.Soruba Sree, Dr. N.Radha. “A Survey on Fusion Techniques for Multimodal Biometric Identification”, International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.