iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** V **Month of publication:** May 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Crypto System Based On Revocable and Unique Session Key

Joans Annie Grace S[1], Jeyapiriya K[2]
[1]M.E Student, [2]Assistant Professor, Department of ECE
Sri Sairam Engineering College, West Tambaram, Chennai, India

Abstract*—To protect information resources from unauthorized acquisition or to prevent tampering with the information that is to be transmitted, cryptography is used. The most important aspect of any cryptographic method is the key management and its distribution. Randomly generated keys are used normally but if the generated key is short, it becomes easy to guess and if the key is long, then it becomes difficult to remember. In this approach, unique biometric traits from both the sender and the receiver are used to generate the cryptographic key from cancelable biometric templates. These generated templates are transmitted securely to either parties using key based steganography. Both these templates are concatenated using image fusion technique to form a combined template of both the sender and the receiver. A second shuffle is used to shuffle the elements of the combined template and a hash function is used generate a unique key for each session. Here the biometric data is obtained from the fingerprints of the communicating parties and processed through MATLAB. Experimental results show that the average value of hamming distance between the genuine and imposter's key is 127 bits for a 256 bit cryptographic key. This biometric based cryptosystem generates a revocable key from irrevocable biometric data and ensures that the security requirements of cryptography are achieved by cancelable biometric template and unique session key.

Keywords*—cancelable biometric template, steganography, Hamming distance, Irrevocable

I. INTRODUCTION

Any computer system requires cryptography to secure its various instances like an electronic mail using digital signatures or hash functions. Crypto systems are made up of primitives which are generally complex and breaking the underlying algorithm ultimately breaks the entire system. The cryptographic algorithm refers to the implementation of a particular pair of encryption and decryption method. A crypto system consists of algorithms for key generation, encryption and decryption. To secure a data or information cryptographically, it is a necessity that the crypto system should not be broken without the knowledge of the key used in the system. Such an encryption has no short cuts to break the system than to repeatedly try its decryption with different keys until one of them works. But the important problem remains the classical one of generating a cryptographic key that is difficult to be obtained by the attacker. The strength of a crypto system depends upon the key used in the cryptographic algorithm and the strength of the key depends on its size. If the size of the key is short, it becomes easy for the intruder to guess and if it is long, then it becomes difficult for the user to remember. This makes the user to store it in a smart card or token that can be stolen or changed. To overcome the above limitations, biometric based crypto systems are used.

Biometric is the automated recognition of the identity of an individual based on their biological and physical behavior. Examples of biometric modalities include fingerprint, iris, face, palm print, veins, palm prints, knuckles, DNA, voice, signature, typing patterns, etc. The use of biometrics in cryptography is promising as the modality is linked directly to its owner. Since these biometric traits are uniquely bound to a person, they can be used to overcome the problem of memorizing the cryptographic key and also confirms the security requirement namely non-repudiation.

The biggest problem of crypto biometric system is that the biometric modality is permanently connected to the user and can neither be stolen nor replaced [2]. Moreover, the biometric characteristics remain constant throughout the user's lifetime and are inherent. Thus, it requires revocability in case of compromise from the irrevocable biometric trait of the user [6]. With increase in use of crypto biometric systems, the privacy of user's biometric data becomes prominent. To overcome this issue, the cancelable template should not reveal the raw biometric data of the user [1]. Thus a transformed cancelable biometric template is generated to provide revocability. Therefore, there arises a need for the cryptographic key being generated, from the different users should be revocable and non-invertible [12]. And should not compromise the privacy and security of the biometric data involved in the key generation process. The remainder of the paper is organized as follows: Section II describes a short survey of the related work and in Section III the proposed methodology is discussed. The experimental results and security analysis is described in Section IV and finally, the

paper is concluded in Section V.

II. RELATED WORK

This work involves three important sub-tasks namely: (i) cancelable template (ii) transmitting the template securely to the other party (iii) cryptographic key generation.

A. Cancelable Template

Cancelable biometrics are designed to meet the requirements of biometric information protection namely, irreversibility and unlinkability. Ratha et al. [4] first used non-invertible transforms to produce cancelable biometrics that used Cartesian, polar and functional transformations. Jeong et al. [9] combined two feature extraction methods where both feature vectors are scrambled and then added to create a transformed cancelable template. Hirata [8] and Takahashi proposed a Fourier-like transform for finger-vein images and multiplying the result with a random filter. Similarly, a method of distorted transform where a circular region is built around the fingerprint minutiae and then the transform is applied. In this work, the Cartesian transformation is done followed by distortion to enhance security.

B. Secure Transmission

The cancelable template has to be transmitted securely to the other communicating party. Anil [10] and Umut proposed a secure exchange method by hiding the biometric minutiae in a host image and the transformed image is exchanged instead of the original minutiae. Lokeswara et al. [3] used LSB embedding to hide the actual data in the least significant bits of a cover image where the amount of data embedded is a significant factor. Saleh Saraireh [11] presented DWT based steganography using Haar wavelet where the data is encrypted using a filter bank cipher. In this approach, the LSB embedding is followed with no restriction on the amount of data to be embedded.

C. Cryptographic Key Generation

Cryptographic key generation transforms the biometric modality of the user to a unique key that cannot be forged. Barman et al. proposed a method by generating a key of binary numbers extracted from the fingerprint template using Euclidean distance between the minutiae. A similar proposal by Barman [12] produces a cryptographic key that is revocable if compromised. Monrose et al. [5] used the user's voice to generate the key which is used in symmetric cryptography. Many researches use multi modal biometrics that include more than one biological modality to generate the key. Here the key is generated such that it cannot be traced back to the user's original biometric data and can be replaced if it becomes compromised.

III. PROPOSED METHODOLOGY

The proposed system is organized into the following three modules.
Module I – Generation of cancelable template from the biometric features of the communicating parties.
Module II – Secure transmission of distorted template to the other communicating party.
Module III – Generation of unique cryptography key for encryption (decryption) using cancelable template.

This approach consists of the following sub sections as shown in Fig 1: feature extraction, cancelable biometric template,

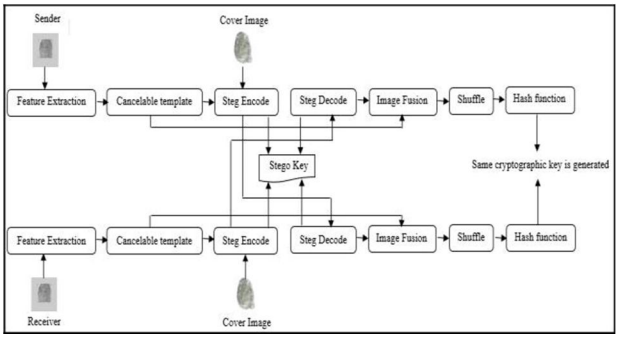


Fig 1 Outline of the proposed method

steganography, image fusion, shuffle and cryptographic key generation which are done separately in the sender and the receiver.

A. Feature Extraction

The fingerprint of the sender and receiver is obtained from a fingerprint scanner and minutiae extraction algorithm is applied. The algorithm involves the following steps:

The fingerprint image obtained is converted into a binary image by using a threshold process where pixels with value less than the threshold are given zero and above are given a one.

The binary image is thinned such that the thickness of the ridges are only a single pixel broad. Thinning does not change the location of minutiae points.

The minutiae points are extracted using crossing number method. The crossing number of a pixel is given by

$$Cn(P) = (½) \sum_{i=1} | Pi - Pi+1 | \quad (1)$$

B. Cancelable Biometric Template

The minutiae points extracted previously are distorted or scrambled randomly to produce non-invertible template known as cancelable biometric template. The image is divided into equal sized blocks depending upon its height and width [1]. Then the blocks are distorted randomly such that the minutiae points get modified from their original locations. This modification of the minutiae points provides the much needed revocability and privacy. As the minutiae points are randomly scrambled even if the template gets compromised, the attacker will not be able to get the original fingerprint of the user.

C. Steganography

The cancelable biometric template of the sender is sent to the receiver and vice versa securely through the process of steganography. LSB steganography is followed where the secret image is hidden in the least significant bit of each pixel in the cover image. Here, the transformed biometric template is hidden in a cover image preferably another fingerprint image and encrypted using a XOR key. At the receiver end, the image is decrypted with the same key and template is recovered from the least significant bits. Thus the information about the sender reaches the receiver securely and vice versa.

D. Image Fusion

The receiver now has the sender's cancelable biometric template similarly, the sender has the receiver's template. These two templates are then fused to form a single template using feature level fusion. Image fusion using feature level merges the features of the two image templates element wise to form a new image.

E. Shuffle

After image fusion, a shuffle method is introduced to shuffle the feature vectors of the fused image. Barman et al [1] used a shuffle key to shuffle the fused image. But the proposed shuffling method involves randomly rearranging the elements of the fused image without using a shuffle key. That is, the pixel values are sorted in such a way that the values corresponding to the feature vectors are rearranged following a random fashion.

F. Cryptography Key

The shuffled image is finally used to generate the cryptographic key. Here, SHA-256 hash function is used to produce a key of length 256 bits. In this hash function the input message is processed as blocks of 512 bits with each block processed through 64 rounds. In this way, the sender and the receiver generate the same cryptographic key separately and thus establish a session to communicate with each other. For each new session, the cryptographic key can be updated or replaced by changing the second shuffling.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

To evaluate the proposed system, the experiment is divided into two sections. First, the impact of LSB steganography due to data embedding and the correctness of the decoded image with respect to the encoded image are analyzed. Next, the generated cryptographic key's randomness is analyzed with different attacks that are possible when each object is compromised. For this, Hamming distance is used to measure the similarity between the genuine and imposter's keys. The histogram is plotted for each

possible attack.

A. Database

For the analysis of the proposed method fingerprints found in the database FVC 2004 are used. The database consists of our subsets of fingerprints labelled from DB1 to DB4 where DB4 is a synthetic prints database and the rest are real fingerprint database. Each database contains fingerprints of ten users with each user having eight sample prints. A genuine key is obtained by selecting a pair of prints from any of the subsets and the rest of the pairs are considered as the imposter keys.

B. Experimental Setup

A pair of fingerprints from a subset is considered to generate the genuine key and the rest are taken as imposter keys [7]. Out of the 320 fingerprints available in the set, DB4 is used as the cover image. That leaves 240 prints of which, 2 are considered for genuine keys and 238 are used for the imposter keys. The fingerprint taken from the database are then passed through MATLAB to extract the minutiae points. The extracted min1utiae points are then converted into the cancelable template by randomly distorting the location of the blocks. The block size used in the experiment is 64 which depends on the height and width of the fingerprint image. The transformed template of the sender is then sent to the receiver and vice versa using LSB steganography. The synthetic fingerprint available in the DB4 is used as the cover image. A user specified encryption key is used for both encryption and decryption which gives the pixel location on the cover image where the transformed template bits are hidden during transmission. Here, the sender and the receiver thus exchange their templates between each other using the same encryption key. Both the sender and receiver then generate the cryptographic key using hash function SHA-256 separately to produce a digest of length 256 bits.

C. Security Analysis

The results recorded from the experiment for the various possible scenarios are given below:

1) *Impact Of LSB Steganography:* To evaluate the impact of data embedding, the method proposed by Saleh. The peak signal to noise ratio between the cover image and steg image (cover image with the secret image) is calculated to evaluate the quality of the image. If the value of PSNR is greater than 36dB then the difference the cover and steg image cannot be found by the human eye. The results summarized in the table shows a PSNR value of 52dB which is very much greater than the standard 36dB. This result proves the effectiveness of LSB for secure transmission. The table also contains the overall pixel change with respect to the cover image. This proves that the entire hidden image can be extracted from the steg image and only 0.30% of the pixels in the cover image undergo changes due to hiding of

Table 1 Impact of LSB steganography

PSNR	Overall Pixel Change
52 dB	0.30%

the cancelable template.

2) *Case 1: Both Fingerprints And Shuffling Are Unknown*: In this case, the assumption is that the attacker has no information about both the sender and receiver's fingerprints and the shuffling used to compromise the generated cryptographic key. Here, unique fingerprints of the sender as well as the receiver is used to generate each key along with the shuffling method. Next, the hamming distance between the genuine and imposter's key is computed and plotted using histogram. The plot shows that the mean or average hamming distance between the keys is 50.09% that is, the attacker needs 128 bits to crack the genuine cryptographic key.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

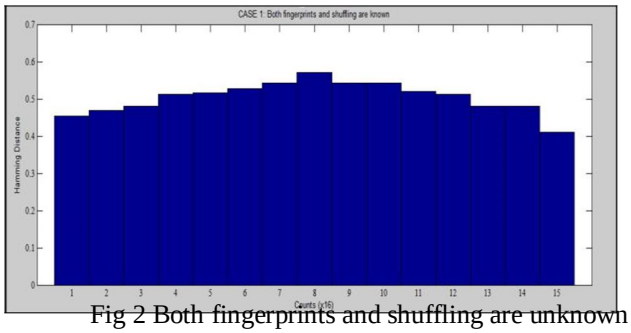


Fig 2 Both fingerprints and shuffling are unknown

3) Case 2: Known Shuffling: For this case, we consider that only the shuffling method used is compromised by the attacker. This implies that the cryptographic key is still generated from unique fingerprints of the users (the sender and receiver). From the histogram plotted, the hamming distance between the genuine and imposter keys shows a mean of 126 bits which are still needed for the attacker to find the key that equals to 49.66%.

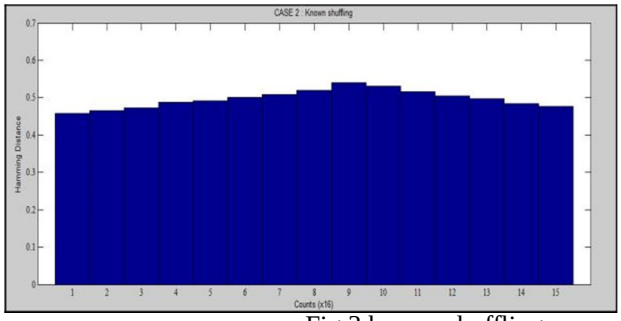


Fig 3 known shuffling

4) Case 3: One Genuine Fingerprint Is Known: In this next case, one genuine fingerprint of either the sender or the receiver is compromised by the attacker. But the attacker has no idea of the shuffling method involved. Since one of the fingerprints is compromised, the corresponding cancelable template also becomes compromised. The observation obtained from the histogram plotted for this case

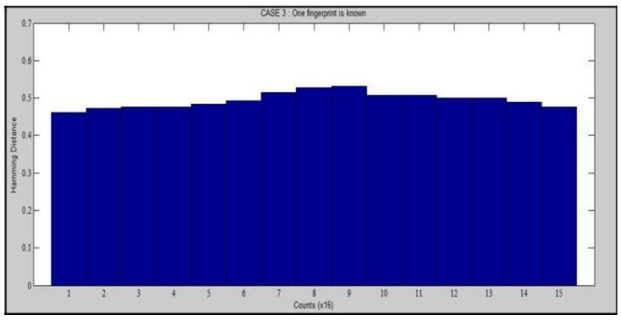


Fig 4 One genuine fingerprint is known

is that the mean hamming distance between the imposter and genuine cryptographic key is 49.6% which is a little lesser than the previous case.

5) Case 4: One Genuine Fingerprint And Shuffling Are Known: This condition states that one of the genuine fingerprints is compromised so the cancelable template generated by it also gets compromised. The difference between this case and previous one is that here the shuffling method also becomes known to the attacker. The hamming distance is computed and the histogram is plotted. Here, the mean hamming distance is observed to be 48.25% and hence the attacker requires 124 bits to guess the genuine key generated.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

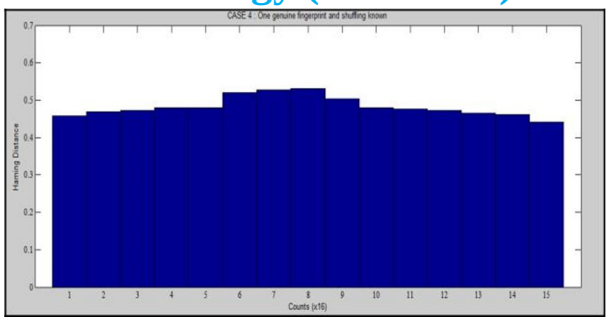


Fig 5 One genuine fingerprint and shuffling known

6) Case 5: Both Genuine Fingerprints Are Known; Shuffling Unknown: In this case, the attacker knows both the genuine fingerprints and hence both the cancelable templates are compromised but no idea of the shuffling method is known. The histogram plotted shows that the hamming distance between the keys has an average of 132 bits and 51.77% that depicts the dissimilarity of the imposter key with respect to the genuine key. It could be seen that though both the fingerprints are compromised the shuffling provides a fairly good security for the cryptographic key to be cracked.

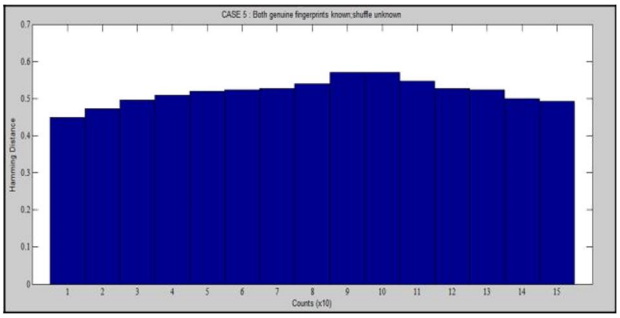


Fig 6 Both genuine fingerprints known; shuffle unknown

The all figures above represent all the cases with the mean hamming distance for each of them. Here, each bar represents a fifth of the total hamming distances calculated for each case to simplify calculations. It can be seen that the cryptographic key cannot be compromised unless the attacker knows both the genuine fingerprints used as well as the shuffling method used. The experimental results show that the minimum hamming distance is 48.25% and the maximum distance is 51%. Thus, the hamming distance between the imposter and genuine key for minimum is 124 bits and 132 bits for the maximum. And for the average case, a minimum of 2^{127} trails are required to get through a brute force attack. The below figure illustrates the hamming distance obtained for each of the cases explained above.

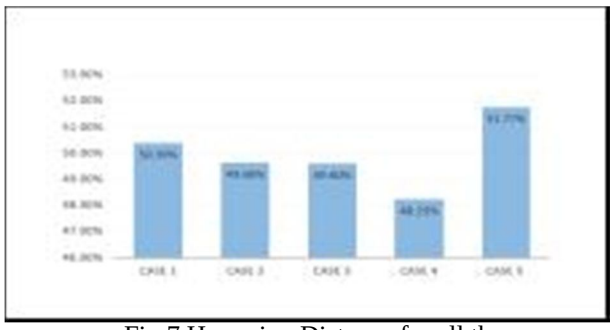


Fig 7 Hamming Distance for all the cases

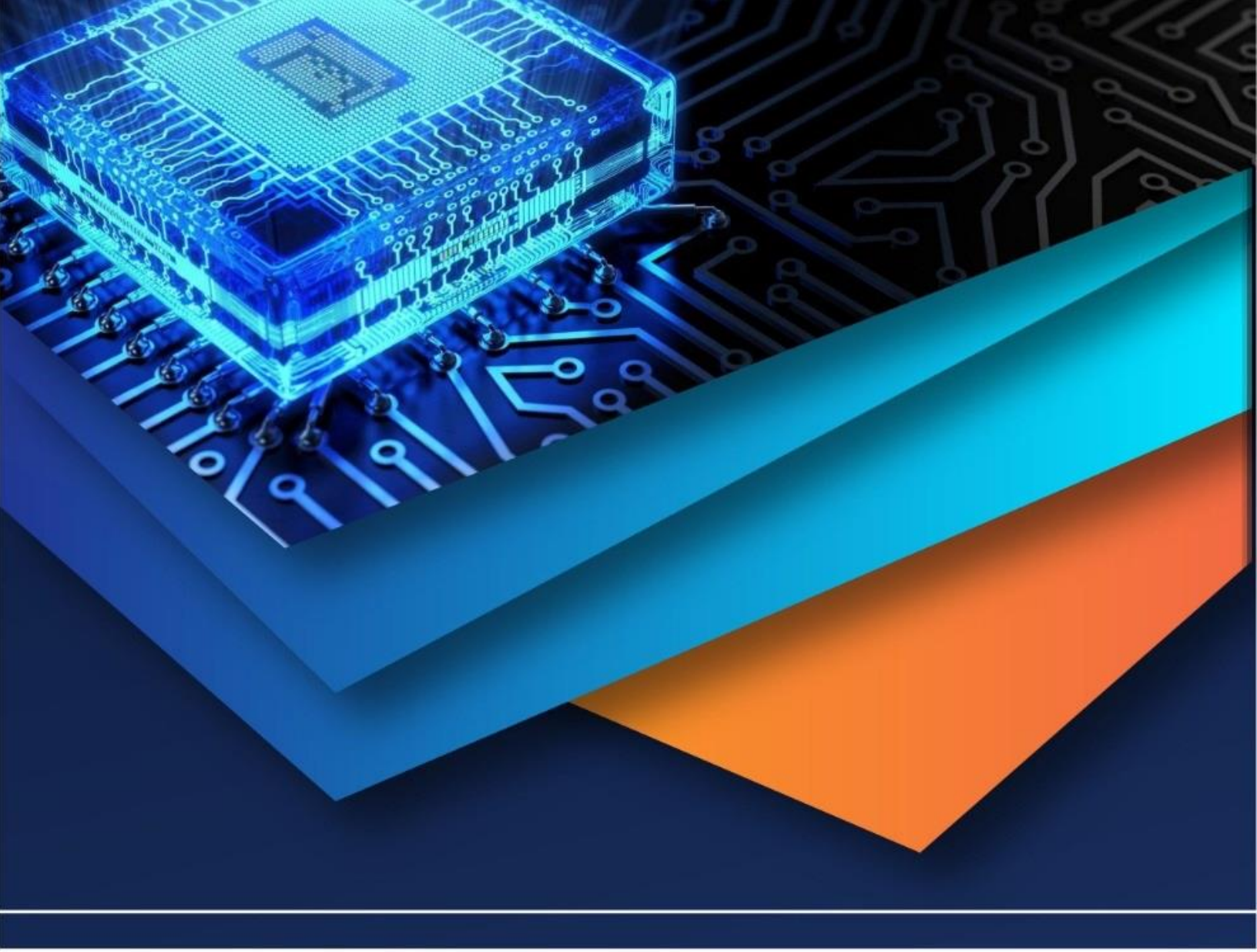
V. CONCLUSION

The key generation plays a crucial role in any crypto system which has to be secured from any kind of attacks. Using biometric

based crypto systems relieves the user from remembering long randomly generated keys. The disadvantage of using an irrevocable biometric modality is overcome by using a distorted cancelable template. The proposed system introduces a shuffling method that further adds to the security of the generated cryptographic key making it resilient against many known attacks.

REFERENCES

[1] S Barman, D Samanta and S Chattopadhyay, "Fingerprint-based crypto-biometric system for network security", EURASIP Journal on Information Security 03(04), 2015.
[2] A K Jain, K Nandakumar, A Nagar, in security and privacy in biometrics. “Fingerprint Template Protection : From Theory to Practice”
[3] (Springer London, 2013), pp.187–214.
[4] 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.
[5] N. Ratha, J. Connell, R. Bolle, and S. Chikkerur, “Cancelable Biometrics: A Case Study in Fingerprints,” Proc. Int'l Conf. Pattern Recognition, 2006.
[6] F. Monrose, M.K. Reiter, Q. (Peter) Li , and S. Wetzel. Cryptographic Key Generation from Voice (Extended Abstract).In Proceedings of the 2001 IEEE Symposium on Security and Privacy, 12 pages, May 2007.
[7] Ratha, N. K., Chikkerur, S., Connell, J. H., and Bolle, R. M.: Generating Cancellable Fingerprint Templates, IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4), 561-572, 2007.
[8] FingerprintVerificationCompetitionFVC2004,[Online].Available: http://biometrics.cse.msu.edu/fvc04db/index.html.
[9] Hirata S, Takahashi K. Cancelabel biometrics with perfect secrecy for correlationbased matching. In: Proceedings of the third international conference on advances in biometrics, ICB2009, 2009. p. 868–78.
[10] Jeong M, Lee C, Kim J, Choi J, Jaihie Kim. A changeable biometric system for appearance-based face recognition. In: Biometric consortium conference (BCC 2006), Baltimore, USA, September 19–21, 2006.
[11] A. K. Jain and U. Uludag, “Hiding biometric data,” IEEE Trans. Pattern Anal. Mach. Intelligence, vol. 25, no. 11, pp. 1493–1498, 2003.
[12] Saleh Saraireh, “A secure data communication system using cryptography and steganography,” International journal of computer networks and commuication, vol.5, no.3, May 2013,pp. 125-137.
[13] S Barman, D Samanta and S Chattopadhyay, “Revocable key generation from irrevocable biometric data for symmetric cryptography,” IEEE 3rd International conference on computer, communication, control and information, Feb 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY