Fingerprint Bio-Crypto Key Generation using Hessian Matrix Minutiae based Feature Extraction

S.Partheeba[1] Dr.N.Radha[2]
[1]Research Scholar [2,3]Assistant Professor
[1,2,3]Department of Computer Science
[1,2,3]PSGR Krishnammal College for Women, Coimbatore, Tamilnadu, India

Abstract— *the biometric system prevents the user transmitting process and very confidential information across the insecure networks from the attackers by using the cryptography techniques. The cryptography technique using a secret key and the public key is defined for the protection of security issues. Needs the key stored in the protected place or it should be transformed in the communication process. So the biometrics using cryptography key traits of both sender and receiver avoid the key storing and improve the security. We propose an approach to generate a cryptographic key using fingerprint in an effective manner. In this approach, the fingerprint features are extracted based on the Hessian based feature extraction method. The Cryptographic key is generated based on the cancellable fingerprint template from the sender and receiver which are combined and shuffled using the SHA-1 hashing technique. Our experimental results show that effectiveness of the proposed system compared existing system in fingerprint bio-crypto key generation using scale invariant feature transform.*

Keywords— Cryptography, Hessian, Cancellable Template, SHA-1, Fingerprint, Bio-Crypto, Key

I. INTRODUCTION

Cryptography is one of the most useful fields in the wireless communication area and personal communication systems, where information security has become more and more important area of interest. Cryptographic algorithms take care of specific information on security requirements such as data integrity, confidentiality, and data origin authentication. To assure that a communication is authentic, the authentication service is of much concern. The function of authentication services is to assure the recipient that the message is from the source it claims to be. In computer security, the process of attempting to verify the digital identity of the sender of a piece of information is known as authentication. The main objective of the proposed work is to detect the quality of fingerprint which is used to encrypt the transmission data. If the image has good quality then minutiae points are extracted by using method hessian matrix feature extraction. By using a cover image the obtained cancellable template will be hidden. Then the hidden image will be transmitted from sender to receiver and receiver to sender by using Variable Least Significant Bit techniques. A cryptographic key is a very secure hash function algorithm is used a key based message authentication algorithm.

II. LITERATURE REVIEW

Priyanka Vadhera et al. [1] proposed a secure hashing algorithm and its variants. The secure hash algorithm appears to provide greater resistance to attacks, supporting the NSA's assertion that the change increased the security. The cryptographic hash function that takes an arbitrary block of data and returns a fixed-size bit string, the cryptographic hash value such that any change to the data will change the hash value. The SHA 1 hash algorithm is more secured and increases the security of the data being sent.

Danilo Gligoroski et al. [2] proposed a secure hash algorithm with only 8 folded SHA-1 steps. This paper proposed a nonlinear technique using quasigroup folds together with the mentioned principle to design hash function that has only 8 iterative steps. Besides increasing the security, the hash function shows that at least 3% faster than sha1. The SHA 1 hash function improved a security. Quasigroup folding as a tool for highly complex.

Nalini C.Iyer et al. [3] proposed on the implementation of secure hash algorithm-1 using FPGA. The SHA is famous message compress standard used in computer cryptography, it can compress a long message to become a short message abstract. SHA 1 implemented using Verilog source code is divided into three modules, namely Initial, Round and Top module. The SHA-1 achieves a higher working frequency and also higher throughput.

Sanjay Kanade et al. [4] proposed an effective protocol to share crypto-biometric keys securely. Another protocol was proposed to generate and share session keys that are being changed for each communication session. Without the need of trusted third party certificates, this protocol achieved mutual authentication between the client and the server. When the user verification was successful, it yields a long key so that it produced a strong link between the user identity and his cryptographic keys. It also facilitated easy online updating of the templates that were cancellable. The protocols were evaluated for biometric verification performance on a subset of the NIST-FRGCv2 face database successfully. However, it does not accommodate for multi-biometric modalities.

Nalini K. Ratha et al. [5] proposed on generating cancellable fingerprint templates. This work proposed a demonstrate several methods generate multiple cancellable identifiers from fingerprint images, a user can be given as many biometric identifiers as needed by issuing a new transformation key then identifiers can be cancelled and replaced. Compare the performance of several algorithms such as Cartesian, Polar and Surface folding transformation of the minutiae positions.

Cai Li et al. [6] proposed a new security analysis framework where the information-theoretic approach and computational security were combined. This paper constructed a fingerprint-based Multi Biometric Cryptosystem (MBC) using decision level fusion. The work mainly consists of two parts namely, a new bio-cryptosystem-oriented security analysis framework and a practical fingerprint-based MBCD construction. Hash functions are utilized in the construction of the MBCD to

protect each single biometric trait further. However, consumes more storage space.

Madhuri et al. [7] proposed fingerprint recognition using robust local features. A techniques use minutiae points for fingerprint representation and matching. Fingerprint recognition technique which uses local robust features for fingerprint representation and matching. The technique performs well in presence of rotation and able to carry out recognition in presence of partial fingerprints. SURF identifies important feature points commonly called key points in the image, it uses hessian matrix for detecting key points. If the feature extraction enhanced fingerprint image are extracted.

F.A.Afsar et al. [8] proposed fingerprint identification and verification system using minutiae matching. The minutiae based approach to fingerprint identification and verification and serves as a review of the different techniques used in the development of minutiae based automatic fingerprint identification system(AFIS). The fingerprint classification of the matching enhances the performance of the matching process to good results on 95% of Accuracy. The fingerprint minutiae based on FAR of 1% was obtained for an FRR of 7% for this process.

B.Raja Rao et al. [9] proposed fingerprint parameter based cryptographic key generation. The proposed work mainly concentrates on the approach to reduce the cost associated with lost keys, addresses non-repudiation issues and also provides increased security of digital content. There by, they have used ECC (elliptic curve cryptography) algorithm for providing higher security with good performance in terms of computational and bandwidth requirements.

Sheena et al. [10] Introduced a comparison of SIFT and SURF algorithm for the recognition of an efficient iris biometric system. SIFT and SURF methods will extract the local feature points of the iris and then determine the scale invariant key points in the iris image and then express these key points using the local patterns around the key points. The experiment of algorithm works will be fast in SURF.

III. METHODOLOGY

- Fingerprint acquisition and Quality check
- Minutiae point extraction using Hessian based algorithm
- VLSB steganography
- SHA-1 hashing

A. Minutiae Point Extraction using Hessian Matrix

If the image has good quality then the minutiae points are extracted by using our proposed method which includes minutiae extraction by using Hessian based extraction method. It has three main parts such as minutiae point detection, local neighborhood description, and matching. Filtering the image with a square is much faster if the integral image is used:

$$S(x,y) = \sum_{i=0}^{x}\sum_{j=0}^{y} I(i,j) \quad (1)$$

The sum of the original image within a rectangle can be evaluated quickly using the integral image, requiring evaluations at the rectangle's four corners. SURF uses a blob detector based on the Hessian matrix to find points of interest. The determinant of the Hessian matrix is used as a measure of local change around the point and points are chosen where this determinant is maximal.

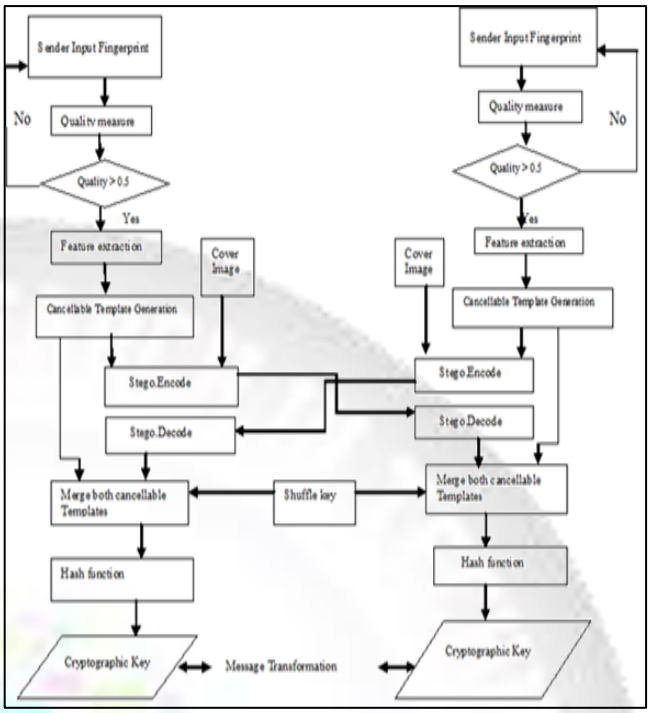

Fig. 1: Framework of proposed work

In contrast to the Hessian-Laplacian detector by Schmid, SURF also uses the determinant of the Hessian for selecting the scale, as is also done by Lindeberg. Given a point p=(x, y) in an image I, the Hessian matrix H(p, σ) at point p and scale σ, is:

$$H(p,\sigma) = \begin{pmatrix} L_{xx}(p,\sigma) L_{xy}(p,\sigma) \\ L_{xy}(p,\sigma) L_{yy}(p,\sigma) \end{pmatrix} \quad (2)$$

Where $L_{xx}(p,\sigma) L_{xx}(p,\sigma)$ etc. are the second-order derivatives of the gray scale images.

The goal of a descriptor is to provide a unique and robust description of an image feature, e.g., by describing the intensity distribution of the pixels within the neighborhood of the point of interest. Most descriptors are thus computed in a local manner; hence a description is obtained for every point of interest identified previously.

The dimensionality of the descriptor has a direct impact on both its computational complexity and point-matching robustness/accuracy. A short descriptor may be more robust against appearance variations, but may not offer sufficient discrimination and thus give too many false positives.

The first step consists of fixing a reproducible orientation based on information from a circular region around the interest point. Then we construct a square region aligned to the selected orientation, and extract the SURF descriptor from it.

B. SHA-1 Hashing

The stego-image is sent to the receiver from sender and vice-versa. After receiving cancellable template from counter partner it is merged with its own cancellable template that means sender has its own cancellable template TCS and received cancellable template TCR from a receiver. Then the cryptography key is generated by the merged templates by using SHA-1 hashing function. Then

merged cancellable fingerprint template is divided into two equal parts of the same size. The divided values are denoted as:

$$V_1 = [v_1 \dots . vn/_2] \quad (3)$$

$$V_2 = [vn/_{2+1} \dots v_n] \quad (4)$$

The elements in two parts are shuffled by using modulo operation and stored in another vector. The shuffled vector is combined and denoted as:

$$SV = [SV_1 \cup SV_2) \quad (5)$$

The elements of vector are also shuffled by this manner. Then each corresponding element of a shuffled the vector is merged by using XOR operation. For this, each element is converted into binary numbers and bitwise XOR operation is followed followed by all elements of shuffled vectors. The result of bitwise XOR operation is stored in vector given as,

$$F_c = \int F_c = \int bitwiseXOR\,(x_i, y_i) \quad (6)$$

Then, the final cryptographic key is generated by using SHA-1 hash function. The vector F_c is divided into different blocks of size 512 bits each. A vector (K) of size 512 bits of all zeroes are generated as initial hash value. Then other block is XORed with initial hash value and output is stored in another vector and so on. Finally, the cryptographic key is generated based on final hash value.

The basic SHA-1 algorithm is presented as follows:

- The algorithm starts off by initializing the five sub-registers of the first 160-bit register X labeled H_0, H_1, H_2, H_3, H_4 as follows:H_0=67452301; H_1=EFCDAB89; H_2=98BADCFE; H_3=10325476; H_4=C3D2E1F0;
- From here onwards, SHA-1 iterates through each of the 512-bit message blocks viz. m_0, m_1, m_2, … , m_{n-1}. For each of the message block, do the following:
- Write m_j as a sequence of sixteen 32-bit words,

$$m_j = W_0 \,||\, W_1 \,||\, W_2 \,||\, \dots \,||\, W_{15}$$

- Compute the remaining sixty four 2-bit words as follows:
- $W_t = (W_{t-3}$ xor W_{t-8} xor W_{t-14} xor $W_{t-16})$
- Cyclic shift of W_t by 1 i.e. $S^1(W_t)$
- Copy the first 160 bit register into the second register as follows:

  A= H_0; B= H_1; C=H_2; D=H_3; E= H_4;
- This step involves a sequence of four rounds, corresponding to four intervals 0<=t<=19, 20<=t<=39, 40<=t<=59, 60<=t<=79. Each round takes as input the current value of register X and the blocks W_t for that interval and operates upon them for 20 iterations as follows:
- For t = 0 to 79,
- $T=S^5(A)+f_t(B,C,D)+E+W_t+K_t$
- E=D;D=C; C= S^{30}(B);
- B=A; A=T
- Once all four rounds of operations are completed, the second 160-bit register (A, B, C, D, E) is added to the first 160-bit register (H_0, H_1, H_2, H_3, H_4) as follows:
- $H_0 = H_0 + A$;
- $H_1 = H_1 + B$;
- $H_2 = H_2 + C$;
- $H_3 = H_3 + D$;
- $H_4 = H_4 + E$;
- Once the algorithm has processed all of the 512-bit blocks, the final output of X becomes the 160-bit message digest.
- The final digest is used as cryptographic key.

IV. Experimental Result

The proposed work is evaluated in tool MATLAB 2014a version is used throughout the implementation. We have used FVC2002 data base for taking fingerprints and 120 images have been used for obtaining various results. We have used Hessian matrix algorithm for extracting minutiae point and VLSB steganography technique for hiding the variable amount of data in every individual pixel of each sector's cover file. For this process, we have used MDT (modular distance technique) algorithm. The metrics like FAR (0.33%), FRR (0.1%) and Accuracy of 94% are evaluated for comparison of the existing and the proposed system.

A. *False Acceptance Rate*

False Acceptance rate (FAR) is defined as the probability in which the system incorrectly authorizes the non-authorized person due to incorrectly matching the biometric input with the template.

$$FAR = \frac{wrongly\ accepted\ individuals}{total\ number\ of\ wrong\ matching} \quad (7)$$

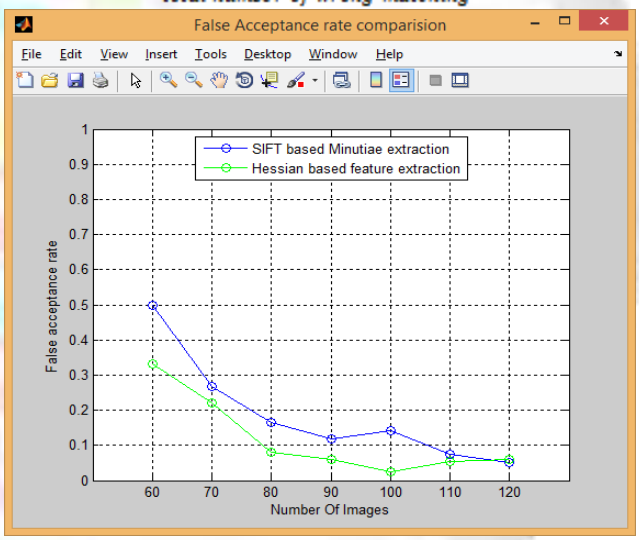

Fig. 2: Comparison of false acceptance rate between existing and proposed system

In the above Fig.2, shows the resulted False Acceptance Rate (FAR) obtained in the proposed as 0.33% for 120 images and existing technique is analysed and resulted as 0.5% for 120 images, it is observed that the proposed technique results in lesser False Acceptance Rate for all the persons, whereas the existing techniques results with higher percentage of False Acceptance Rate.

B. *False Rejection Rate*

False rejection rate is defined as the probability in which the system incorrectly rejects the access of an authorized person due to failing of matching biometric input with the template.

$$FRR = \frac{wrongly\ rejected\ individuals}{total\ number\ of\ correct\ matching} \quad (8)$$

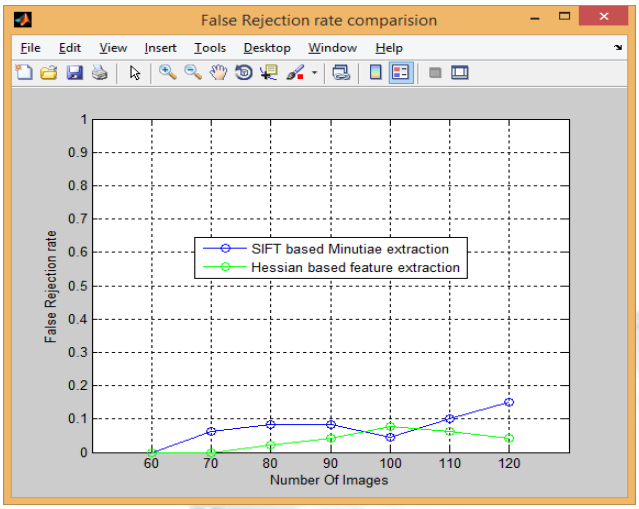

Fig.3 Comparison of false rejection rate between existing and proposed system

In the above Fig.3, the comparison of False Rejection Rate (FRR) obtained in the proposed as 0.1% for 120 images and existing technique is analyzed and resulted as 0.2%, it is observed that the proposed technique results in lesser False Rejection Rate when compared to the existing technique.

C. Accuracy

Accuracy is defined as the proportion of the true outcomes (both true positives and true negatives) among the sum of cases observed. It is calculated as follows:

$$Accuracy = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \quad (26)$$

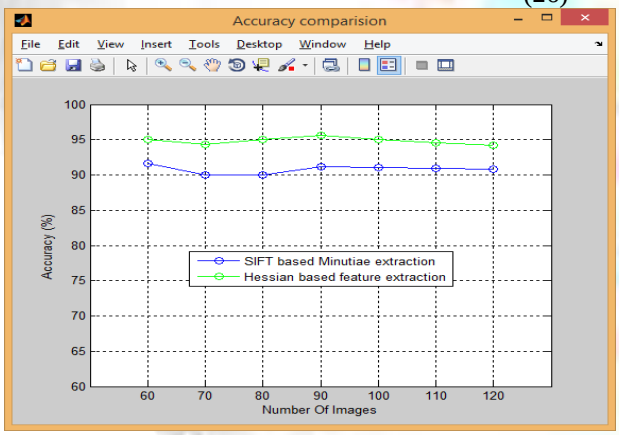

Fig. 4: Comparison graph for difference in existing and proposed system

In the above Fig.4, the comparison of Accuracy 94% obtained in the proposed and accuracy as 91% of existing technique SIFT based is analyzed and resulted From the result, it is observed that the Hessian based minutiae technique results in better accuracy when compared to the Morphological based minutiae technique.

D. Summary of the performance analysis of proposed techniques and existing system

Techniques	FAR	FRR	Accuracy
SIFT based minutiae extraction	0.5%	1.2%	91%
Hessian matrix based minutiae extraction	0.33%	0.1%	94%

Table 1: Comparison table for existing and proposed system

V. CONCLUSION

The proposed work addresses the secured transmission of data using a cryptographic technique. The Hessian matrix and hash algorithms are used to improve the accuracy and security of cancellable template from one end to other end. The proposed approach in the feature extraction process had done using hessian matrix algorithm for minutiae points. The cancellable template hiding process will be done with steganography. Then hash function using cryptographic key generation. Finally, 256- bit bio-crypto key is generated for secured transmission over networks and has been shared between sender and receiver. In future, multi-modal biometric traits can be used for the key generation and different cryptographic algorithms can be used to improve the security and overall performance.

REFERENCES

[1] A. Jagadeesan, K. Duraiswamy "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris", (IJCSIS) International Journal of Computer Science and Information Security, vol.7, no.2, 2010.

[2] Sunil V. K. Gaddam, Manohar Lal, "Efficient Cancellable Biometric Key Generation Scheme for Cryptography", International Journal of Network Security, vol.11, no.2, pp. 61-69, 2010.

[3] A.K Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition", IEEE international journal of transactions on circuit and systems for video technology, vol. 14, no. 1, pp. 1-21, 2004.

[4] M.S. Durairajan, Dr.R.Saravanan,"Biometrics based key generation using Diffie- Hellman Key Exchange for enhanced security Mechanism", International Journal of Chem. Tech Research, vol.6, no.9, pp. 4359- 4365, 2014.

[5] Barman, S., Samanta, D., & Chattopadhyay, S. (2015). "Fingerprint based crypto-biometric system for network security". EURASIP Journal on Information Security, no.1, pp.1-17, 2015.

[6] N.Lalithamani, Dr.K.P.Soman, "An Effective Scheme for Generating Irrevocable cryptographic key from Cancelable Fingerprint Templates", International journal of Computer Science and Network security, vol. 9, no. 3, 2009.

[7] Deepika Sahu, Rashmi Shrivas, "Minutaie based fingerprint matching for Identification and Verification", International journal of science and Research, vol. 5, no. 3, 2016.

[8] A.Jagadeesan, T.Thillaikarasi and Dr.K. Duraisamy, "Cryptographic key generation from multiple biometric modalities:Fusing minutiae with iris feature", International journal of computer applications, vol. 2, no.6, 2010.

[9] K.Hemanth, Srinivasulu Asadi, Dabbu Murali, N.Karimulla, M.Aswin, " High Secure Crypto Biomertic Authentication Protocol", International Journal of Computer Scince and Information Technologies, vol.2, no.6, pp. 2496-2502, 2011.

[10] R.Divya, V.Vijayalakshmi, "Analysis of Multimodal Fusion Based Authentication Techniques for Network",

International Journal of Security and its Applications, vol.9, no.4, PP.236-246, 2015.

[11] Ms.S.Malathi, Dr.C.Meena, "Partial Fingerprint matching based on SIFI Features", International Journal on Computer Science and Engineering, vol. 2, no. 4, pp. 1411-1414, 2010.

[12] Bhosale Swapnali B, Kayastha Vijay S and HarpaleVarsha K, "Feature extraction using SURF algorithm for object recognition", International journal of Technical Research and applications, vol. 2, no. 4, pp. 197-199, 2014.

[13] Danilo Gilgoroski, Smile Markovski and Svein J.Knapskog, A Secure hash algorithm with only 8 folded SHA-1 steps", International journal of computer science and network security, vol. 6, no. 10, pp. 194-205, 2006.

[14] Thulasimani Lashmanan and Madheswaran Muthusamy, "A novel secure hash algorithm for public key digital signature schemes", The international Arab journal of information technology, vol. 9, no. 3, pp.262-267, 2012.

[15] Cai Li, Jiankun Hu, Josef Pieprzyk and Willy Susilo, "A new bio cryptosystem oriented security analysis framework and implementation of multi biometric cryptosystems based on decision level fusion", IEEE journal transactions on information forensics and security, vol. 10, no. 6, pp. 1193-1206, 2015.

[16] Feng Hao, R.Anderson, J.Dairgman, "Combining crypto with biometrics effectively", IEEE transactions on computer, vol. 55, no.9, pp. 1081-1088, 2006.

[17] Sanjay kanade, Dijana Petrovska-Delacretaz and Bernadette Dorizzi, "Generating and sharing biometrics based session key for secure cryptographic applications", IEEE international conference, vol. 4, pp. 1-7, 2010.

[18] Sumeet Kaur, Savina Bansal, R.K Bansal, "Steganography and classification of image steganography techniques", IEEE International conference on computing for sustainable global development, vol.14, pp. 870 - 875, 2014.

[19] Y. J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation", IEEE international conference on Multimedia and Expo, vol. 3, no. 4, pp. 2203-2206, 2004.

[20] Chang Chou Lin and Wen Hsiang Tsai, "Secret image sharing with steganography and authentication", ELSEVIER Journal of systems and software, vol. 73, no. 3, pp. 405-414, 2004.

[21] Cheng- Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang and Hung-Min Sun, "Adaptive data hiding in Edge areas of images with spatial LSB domain systems", IEEE journal of transactions on information Forensics and security", vol. 3, no. 3, pp. 488-497, 2008.