A Multimodal Bio-Cryptosystem as a Model against Spoofing Attacks

Bhagya P, Mahesh P K

Abstract— With increased fraud happening, identity theft, and security attacks has becoming easier to spoof the biometric. In addition to this cryptography as become one of the main concerns about the privacy of each human and also have huge demand from public to promote a high standard secured system. Considering the main aspects of privacy and spoofing, we presents a novel multimodal cryptosystem which is having high privacy and difficult to spoof. The aim of this paper to provide a crypto-biometric system with anti-spoofing techniques with better data encryption method, increasing the robustness and complexity.

Keywords: Bio-Cryptosystem, Multimodal biometric, Fusion level

1. INTRODUCTION

Authentication systems using only one biometric trait may not provide the all properties described before, namely: universality, distinctiveness, permanence, collectability, performance, acceptability, and circumvention. This is the main interest which has actuated the current senario to multimodal biometrics, in which several biometric traits are simultaneously used [1]. The main advantage of multimodal biometric provides more robust. The term multimodal biometrics referred to the combination of different biometric traits, therefore mode refers to biometric modality. Interestingly, combining different biometric modalities is not the only way to enhance a security, as there are a number of other information sources that can be combined for that purpose. In this regard, the combination of multibiometric and cryptography methods enhances the security of privacy data. The following figure 1 shows the basic bio-crypto system technique used in most of the research. This shows the cryptosystem which stores a key and will be released once the verification is done.

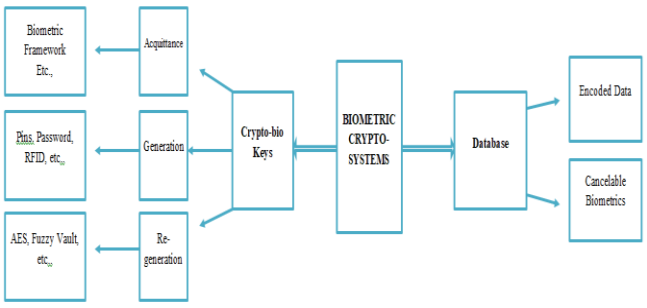


Figure 1: Basic Bio-crypto system technique

2. SPOOFING ATTACKS AND MULTIMODAL BIOMETRIC

Considering the biometric, the spoofing attacks may take in different stages from template capturing stage using sensors, feature extraction level to final level as in figure 2. Remember, none of the research has proved spoof proof, since all the systems that we have used ass been defeated. To overcome this problem and to get an anti-spoofing system, which the user agrees and which can be overcome with such defeat/attack, we use a combination of biometric for the identification. In this paper we use two types of biometric: Fingerprint and Face. The algorithms used for biometric is minutiae extraction for fingerprint and Zero mean Gabor filter for Face recognition.

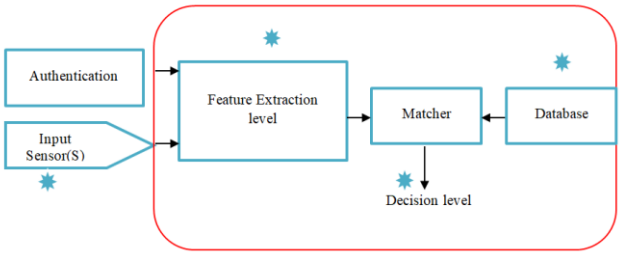


Figure 2: Different stages of attacks on a basic biometric system [2].

2.1 Zero mean Gabor filter:

Considering Brightness as a main factor, we propose Zero mean Gabor filter to increase the system robustness against brightness. From Eq.1, we know that due to odd symmetry, the imaginary part of 2-D Gabor filter is calculated as Zero. But, in the even symmetry of the 2-D Gabor filter, i.e., considering the cosine term, which is non-Zero mean. Zero mean Gabor filter, GZM σ , $\cdot$, θ (x, y), is achieved by subtracting the average of Gabor filter as shown in the below equation:

$$G^{ZM}{}_{\sigma,\lambda,\theta}(x,y) = G_{\sigma,\lambda,\theta}(x,y) - \frac{\sum_{i=-N}^{N}\sum_{j=-N}^{N} G_{\sigma,\lambda,\theta}(i,j)}{(2N+1)^2} \quad \ldots\ldots\ldots(1)$$

Revised Version Manuscript Received on 20 February, 2019.

Bhagya P, Associate professor, Department of ECE, DBIT, Bangalore, Karnataka, India.

Mahesh P K, Professor and Head, Department of ECE, ATME College of Engineering, Mysore, Karnataka, India.

where size of the filter is (2N+1) by (2N+1). This algorithm, which mainly depends on three parameters of the Gabor filter; namely σ, $\cdot$, and θ. These parameters will effects not only the accuracy of the system, but also the template size will be affected, which will be stored in database. Since, Gabor filter is a complex filter, we get both imaginary & real parts. Later, both parts are divided into sub blocks of 3x3 matrix. The average of these 9 pixels(3x3) is calculated. The mean valve is then compared with the applied threshold -0.2. each sub-block 3x3 will be replaced/encoded by 1 or 0. If the mean valve is greater than or equal to the threshold valve applied, it will be encoded as 1 else 0. Mathematically expression is as shown below:

$$b_{Real}(k,l) = u\left(\frac{\sum_{i=3k}^{3k+2}\sum_{j=3l}^{3l+2} I_{Real}(i,j)}{9} - Threshold\right)$$

$$b_{Imag}(k,l) = u\left(\frac{\sum_{i=3k}^{3k+2}\sum_{j=3l}^{3l+2} I_{Imag}(i,j)}{9} - Threshold\right) \quad \ldots.(2)$$

where IReal(i, j) and IImag(i, j) shows the real and imaginary parts and bReal(k, l) and bImag(k, l) for real parts at pixel (i, j) and sub-block(k, l) respectively. u() and Threshold depicts the unit-step response and selected threshold(-0.2), respectively.

2.2 Minutiae Key Points Extraction

Key minutiae points are extracted from fingerprint by applying pre-processing algorithm, Region Of Interest selection and lastly method to extract key minutiae points. Since, we have used the most noval approach used by most of the researchers. Histogram equalizer, Fast Fourier Transform and lastly Binarization is applied at the pre-processing stage to enhance the template image quality. Then Morphological operations [5, 6] are used to extract Region of Interest [ROI].

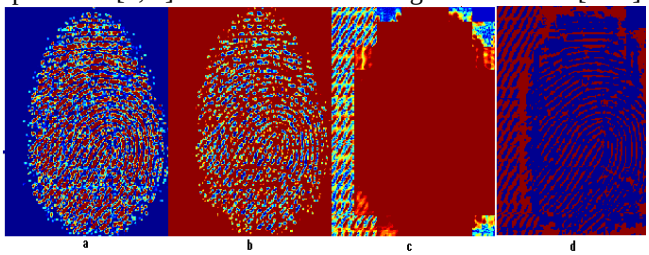
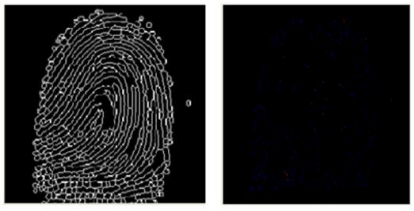


Figure 3: a) Original image, b) Histogram Enhancement, c) After FFT and d) Image after adaptive binarization.

At image enhancement stage, we use the traditional method thinning called Morphological operation. This method will in turn erodes out the foreground pixels until they are one pixel wide[6] which uses a Ridge Thinning algorithm for the Minutiae points extraction.



(a) (b)

Figure 4: a) Thinning b)and Minutiae points

2.3 Fusion level

At fusion level, we use weighted mean scheme, combining both Biometric at Weighted mean method, the fusion score is achieved as follows:

$$f = \sum_{m=1}^{M} w_m x_m \quad \ldots..(3)$$

where M is the matching stream, xm is the normalized feature valve of the mth template & wm is its corresponding weight with following condition

$$\sum_{m=1}^{M} w_m = 1 \quad \ldots..(4)$$

3. ENCODING THE MESSAGE

Substitution technique[4] is one of the classical encryption technique used in the proposed method. In substitution cipher, one piece of information replaced by another. To provide confidentiality, ciphertext could be transmitted or stored within a file system. To make the message unintelligible the character of the message with other character in substitution method while transposition cipher changes the order of characters. The algorithm used in substitution cipher, to create an offset in the character and the key is the number of alphabets to offset it. At the receiver end, reverse process takes place by converting cipher text to plain text. As an example, if we want to cipher the word "INDIA" with offset of 16 points, then we have "INDIA" ciphered as "XDTXQ". To allow someone else to read the ciphertext, the key i.e. 16 should be provided to recipient. Plaintext M transmitted over the channel from sender to receiver. Now if sender X wants to send recipient Y over insecure communication channel, sender will encrypt the message M by calculating the ciphertext C=E(K,M) and sends ciphertext to recipient Y. At the receiver, Y decrypts C by computing M=D(K,C). E and D are the algorithms used for encryption and decryption method in the process.

- **Plaintext:** *The message to be transmitted is denoted as M= <m1,m2,.....mn>. For example, M=<ATMECE>*
- **Ciphertext:** *The encrypted message or translated message is ciphertext denoted as C=<c1,c2,.....cm>. the ciphertext generated by adding the key 16 to the plaintext i.e. C=<$%^&*(>*
- **Encryption:** *C=E(M)shows the process of transferring message to ciphertext form, where M is the message, C is the ciphertext and E is method used for encryption. In substitution technique, C=E(M)=(M+K)mod(26), where K is the key.*
- **Decryption:** *M=D(C) is used to transform the ciphertext to message. In substitution technique, M=D(C)=(C-K)mod(27), where K is the key.*
- **Key:** *Key is like a set based on the inputs from the transmitter side and receiver end. The message kept secret though the third party knows the encryption process because the key used in the encryption does not know to the attacker.*

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

4. MULTIMODAL CRYPTO-BIOMETRIC SYSTEM

The following figure 5 shows a multimodal crypto-biometric system is used as proposed method, this uses two main methods, crypto-biometric and spoofing countermeasures. This proposed method provides better data encryption method, increasing the robustness and complexity. Remember, it is mandatory to user recognition before the key passes. Also this method provides a spoof proof Crypto-biometric with a good cryptographic manner.

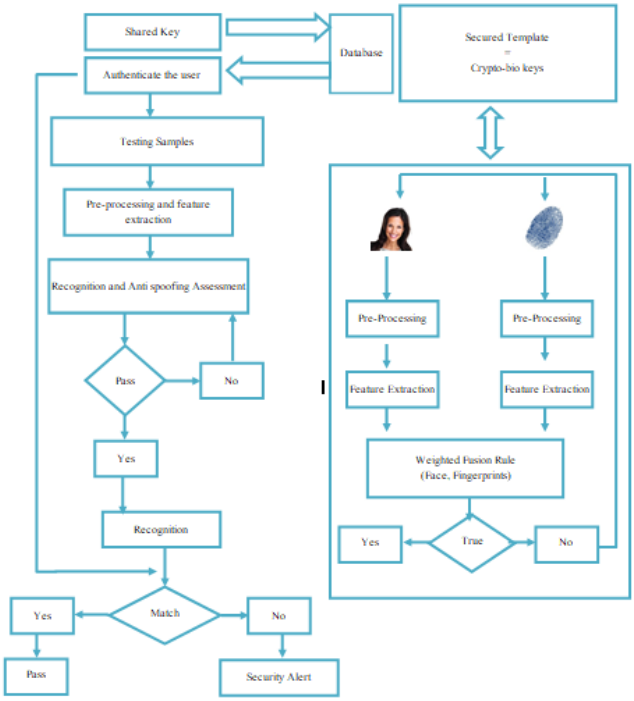


Figure 5: Proposed multimodal crypto-biometric system

4.1 Functionality and System Design

The following steps are considered for the system

i. Enrolment phase, collects the input from the user, i.e., Fingerprint and Face template
ii. The features of each user is kept in database
iii. Encryption method is executed, to create keys.
iv. These keys are shared with the user.
v. At verification end, the crypto-key is unlocked, only when the user is identified or matched with the keys.

The proposed system will definitely provide a better solution for anti-spoofing crypto-biometric system.

5. CONCLUSION AND FUTURE WORK

We propose a novel approach for multibiometric cryptography with anti-spoofing techniques. A Multibiometric-based encryption technique outperforms traditional systems in usability area. This system provides user to faith about the security of their privacy with increased robustness. In future we can experiment with different biometric modality and to come with a better multi-biometric crypto system. During the design stage, we have to make sure to get minimum error rate. At data encrypting stage, we can have an encryption scheme which gives more strength for the security against the attacks. Also, we can select different Fusion level techniques to compare and select the type which gives secured authentication with minimum error rate.

REFERENCES

1. A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, pp. 4-19, 2004.
2. Christina-Angeliki Toli and Bart Preneel, "A Bimodal Verification Cryptosystem as a Framework against Spoofing Attacks," International Journal of Intelligent Computing Research (IJICR), Infonomics Society, Volume 6-Issue 2, pp. 540 - 549, 2015.
3. Bhagya P, Dr. Mahesh P.K, "Crypto- Biometric using Substitution Encryption and Discrete Cosine Transformation for Secure Data Communication", International conference on emerging research in Electronics and Communication Technology, ICERECT 2018, PES college of Engineering, Mandya.
4. Bhagya P, Dr. Mahesh P.K, "An Efficient Approach to Fingerprint using Fuzzy Vault", in ICrtSIV 2015, Bangalore, Feb 2015, 10.3850/978-981-09-6200-5_D-37.
5. U. Uludag and A. Jain, "Securing Fingerprint Template: Fuzzy Vault with Helper Data " in Proceedings of the 2006 Conference on Computer Vision and Pattern Recognition Workshop IEEE Computer Society, 2006, pp. 163.
6. Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, "Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault" presented at Information Security and Cryptology, Beijing, China, 2005.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication