Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Cryptographic Key Generation with Multimodal Biometrics

[1]Priti Shende, [2]GirishAuti, [3]AkshayJagtap, [4]ShubhamRajput
[1,2,3,4] Electronics and Telecommunication, DYPIET Pimpri Pune

Abstract - A biometric system depending on one biometric feature is not a reliable system. Identification based on multiple biometric features is best option to overcome the disadvantages of single feature biometric system. The main aim is to incorporate the biometric feature of user into cryptographic key to make biometric system more secure. We go one step further to try to incorporate the multiple biometric features into cryptographic key generation to provide more security. In this paper, we have proposed an approach to design a biometric system with cryptographic key generation. This approach is consisting of three stages 1) Feature extraction 2) Multimodal biometric template generation 3) Cryptographic key generation. In this approach, the features, facial and minutiae points are extracted from face and fingerprint images respectively. The extracted features are fused together at feature level to generate templates. From these templates, cryptographic key is generated.

Keywords - Biometric, Multimodal, Cryptographic key, Minutiae points, Fingerprint, Face.

I. INTRODUCTION

The need of reliable and secure personal authentication is increased in today's electronically wired information society. Traditionally, a user can be verified depending on ID card or token (what he/she possesses) or depending on password or PIN (what he/she knows). But there are number of disadvantages of such system. The ID card may be lost, stolen or misplaced. Password may be forgotten or stolen. Therefore such a system does not provide security as compared to biometric system.

Biometric refers to the authentication based on physical, behavioral or chemical characteristics of human. Biometric characteristics are unique to each user. The biometric system has shown the various significance in the field of reliability, mobility and security compared with knowledge-based and token-based authentication systems. There are mainly two types of biometric system: 1) Unimodal 2) Multi-modal. The biometric systems that uses single feature (i.e. Unimodal biometric system) has number of limitations such as noisy data, intra class variation, interclass similarities, non-universality, spoofing. These limitations can be overcome with the help of multi-modal biometric system.

Multi-modal biometric system can be used to increase the performance and efficiency of biometric system. In recent times, Multimodal biometric fusion technique got more attention as they are useful to increase the efficiency of a system. Now, we get much further to incorporate the cryptographic key generation with multimodal biometric system. This will help to increase the efficiency and performance of the system.

@IJMTER-2015, All rights Reserved

In our approach, we have considered two biometric traits 1) Face and 2) Fingerprint.

Face Recognition

Face recognition is basically depending on the facial pattern and the positioning of facial features. Face recognition is very complex method of biometric recognition. In face recognition, the image is captured using camera, webcam, etc. The features are extracted from the captured image and template is generated from extracted feature. The generated template is compared with template which is stored in database. Depending on comparison result, the person is get accepted or rejected.

Fingerprint Recognition

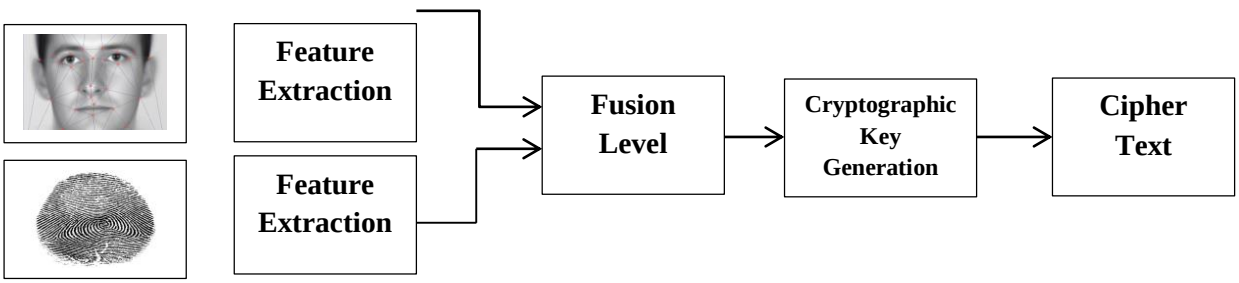
Fingerprint is unique and unchangeable biometric trait. Fingerprint is made up of series of ridges and furrows. Fingerprint recognition is one of the oldest recognition technique that is most successful. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as minutiae points.

One recent development, biometric cryptosystems [1] combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc [2]. Of late, the enhanced performance of cryptographic key generated from biometrics in terms of security has obtained massive reputation amongst the researchers and experimenters [3] and in the recent past, researchers have attempted towards merging biometrics with cryptography in order to enhance overall security, by eliminating the necessity for key storage using passwords [4-7]. Even though it is highly infeasible to break cryptographic keys generated from biometrics, the attackers are still in with a possibility of sneaking through cryptographic attacks. One effective solution with added security will be the incorporation of multimodal biometrics into cryptographic key generation; so as to achieve incredible security against cryptographic attacks.

Here, we present a proficient approach for the secure cryptographic key generation based on multiple modalities namely, Face and fingerprint. Initially, the fingerprint features (minutiae points) are extracted from the fingerprint image. Similarly, the facial features are extracted from the face image The two extracted features, minutiae points and facial texture are then fused at feature level to construct the multimodal biometric template. Fusion at the feature level is accomplished using the processes namely, shuffling, concatenation and merging. Finally, multi biometric template obtained is used to generate the secure 128-bit cryptographic key that is capable of providing better user recognition and security.

II. BASIC PRINCIPLES

A. Block Diagram



@IJMTER-2015, All rights Reserved

Fig: Block Diagram Of Cryptographic Key generation With Multimodal Biometric

B. Algorithm

Step 1: Start.
Step 2: Take the face and fingerprint images from database.
Step 3: Extract the features from face and fingerprint images using principal component analysis (PCA).
Step 4: Find the threshold values of features which are extracted from images.
Step 5: Combine the threshold values of both images.
Step 6: Apply cryptographic algorithm to generate cryptographic key.

C. Procedure

The proposed approach consist of following procedures:

1. Input as face and fingerprint
   This is the initial stage of our proposed approach. In this stage, the face and fingerprint images are captured and given to next stage.

2. Feature Extraction
   This is the second stage. The features are extracted from both face and fingerprint images using Principal component analysis.

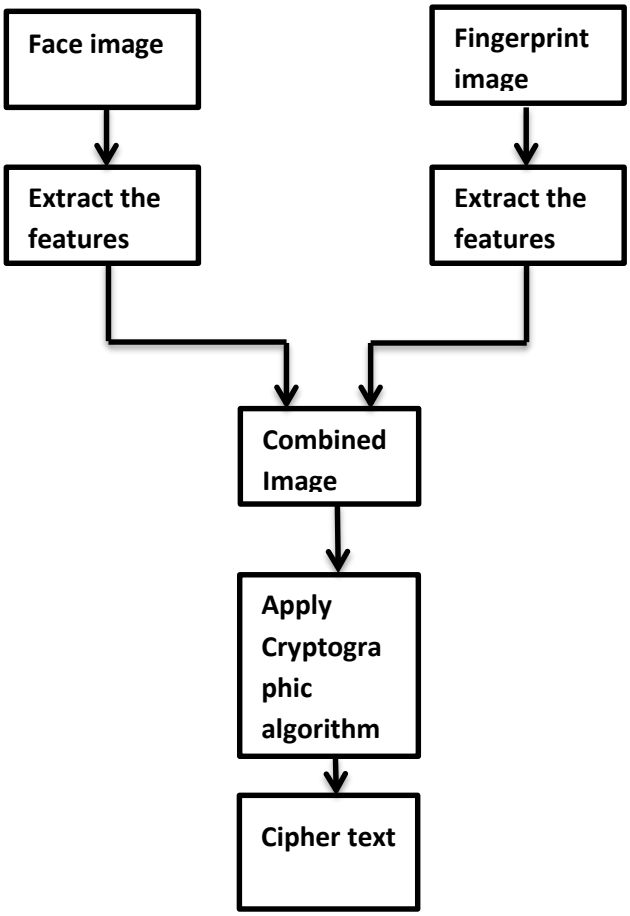
3. Combine image
   At this stage, the feature extracted from the face and fingerprint image are fused together.

4. Apply cryptographic key algorithm
   Cryptography is the science of encrypting and decrypting written communication. It comes from the Greek word kryptos, meaning hidden, and graphia, meaning writing. Cryptanalysis is the process of trying to decrypt encrypted data without the key. Plain text: This is the original message or data that is fed into the algorithm as a input. The secret key is also an input to the algorithm. An encryption algorithm is applied to convert the plain text into cipher text. Cipher text is a scrambled message which is depend on plain text and secret key.

5. Cipher text
   Finally after applying cryptographic algorithm to the fused image of both face and fingerprint there will be the conversation of plain text into unknown format is called cipher text.

D. Flowchart

@IJMTER-2015, All rights Reserved



III. CONCLUSION

The current generation of biometric authentication devices offers cost and performance advantages over manual security procedures. Cryptographic key generation with multimodal biometrics system will increase security due to the use of the cryptographic key.

Accuracy of our system will be more than that of the other system. These methods have shown that, using biometrics for identification or verification-based security systems and cryptosystems, is a promising technology.

REFERENCE

[1] Umut Uludag, Sharath Pankanti, Salil Prabhakar, Anil K.Jain, "Biometric Cryptosystems Issues and Challenges", in Proceedings of the IEEE, vol. 92, pp. 948-960, 2004.

[2] P.Arul, Dr.A.Shanmugam, "Generate a Key for AES Using Biometric for VOIP Network Security", Journal of Theoretical and Applied Information Technology, vol. 5, no.2, 2009.

[3] N. Lalithamani and K.P. Soman, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme", European Journal of Scientific Research, vol.31, no.3, pp.372-387, 2009.

[4] A. Goh and D.C.L. Ngo, "Computation of cryptographic keys from face biometrics", International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1–13, 2003.

@IJMTER-2015, All rights Reserved

[5] F. Hao, C.W. Chan, "Private Key generation from on-line handwritten signatures", Information Management & Computer Security, vol. 10, no. 2, pp. 159–164, 2002.
[6] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces", in proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394 - 401, December 2007.
[7] N. Lalithamani and 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, March 2009.
[8] A Proposal for a Biometric Key Dependent Cryptosystem by K. Hassanain1 ,M. Shaarawy, E. Hesham2, P a g e 42 Vol. 10 Issue 11 (Ver. 1.0) October 2010 Global Journal of Computer Science and Technology.
[9] B. Kiran Bala and J.Lourdu Joanna, "Multi Modal Biometrics using Cryptographic Algorithm" available on http://www.euroessays.org
[10]A. Jagadeesn and Dr. K. Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometric" available on http://www.arxiv.org

@IJMTER-2015, All rights Reserved