Ear Biometric Cryptosystem

Rishika Jain

***Abstract*— Biometrics play a important role for user authentication in distributed environment .But security is main issue so Bio- cryptography is an art of science which provide security and privacy by using biometric templates. Bio-Cryptography is a progressive technology that combines biometrics with cryptography. It is a method using biometric features to encrypt and decrypt the original data. Biometric key is generated from ear biometric template. This key used for encryption and decryption the data which provides more security needs as well as authentication.**

***Index Terms*— Ear Biometric, Bio- Cryptography, Key, Advance encryption standard**

I. INTRODUCTION

Cryptography is an art of science which uses mathematics to encrypt and decrypt data which provide privacy and security. The original message to be encrypted is called plaintext and the encrypted message is called cipher text. In order to get the original data back decryption is done. A key is a value which works with cryptographic algorithms that encrypts and decrypts the data. Simple user keys are easy to remember but easily to crack. Complex keys are long bit string which is very difficult to crack but very hard to memorize. Also it can be easily attacked by using the brute force attack technique. Instead of using the traditional cryptographic techniques, Biometrics like Iris, fingerprints, voice etc. uniquely identifies a person and a secure method for stream cipher, because Biometric characteristics are ever living and unstable in nature.

This paper proposed a one of the newest bio cryptography method is Ear based cryptography. Ear biometrics is one of the passive biometrics. In this paper we explore the possibilities of key generation from Ear patterns which are used for encryption and decryption the information.

II. RELATED WORK

Many cryptographic algorithms are available for securing information, but all of them are dependent on the security of the encryption or decryption key. To overcome this dependency, biometric techniques can be applied to ensure the security of keys and documents. Different methods can be used to securely store and retrieve cipher keys from biometric characteristics.

The work done by Song Zhao, Hengjian Li, and Xu Yan for the security and Encryption of fingerprint images is more relevant to our work [1]. In this paper they proposed a novel chaotic fingerprint images encryption scheme combining with shuttle operation and nonlinear dynamic chaos system. The proposed system in this paper shows that the image encryption scheme provides an efficient and secure way for fingerprint images encryption and storage .

The core of bio-cryptography lies in the stability of cryptographic keys generated from uncertain biometrics. Hu et al. [6] investigated the effect on the generated keys when an original fingerprint image is rotated. Analysis indicates that information integrity of the original fingerprint image can be significantly compromised by image rotation transformation process. It was discovered that the quantization and interpolation process can change the fingerprint features significantly without affecting the visual image.

Also the work done by Muhammad Khurram Khan and Jiashu Zhang for implementing templates security in remote biometric Authentication systems seems relevant to us [4]. In this paper they presented a new chaos-based cryptosystem to solve the privacy and security issues in remote biometric authentication over the network.

Wu et al [8] proposed a novel biometric cryptosystem based on the most accurate biometric feature - iris. In this system, a 256-dimension textural feature vector is extracted from the pre-processed iris image by using a set of 2-D Gabor filters. And then a modified fuzzy vault algorithm is employed to encrypt and decrypt the data.

III. EAR BIOMETRIC

The term biometrics which comes from the Greek words bios, meaning life, and metrics, meaning measure. Biometrics can be measurable as physiological and/or behavioral characteristics that can be used to verify the identity of person Ear biometrics is considered to be a developing technology and not a lot of work has been done in this field in comparison with other biometric methods.

Ear has few advantages over the face. For example, its appearance does not change due to expression and it is found to be unaffected by aging process. Its color is uniform and background is predictable.

Manuscript received Feb 15, 2014.

***Rishika Jain**,Computer science & enginering,Bhagwant University.Ajmer,India.07737011632.*

ISSN: 2278 – 7798

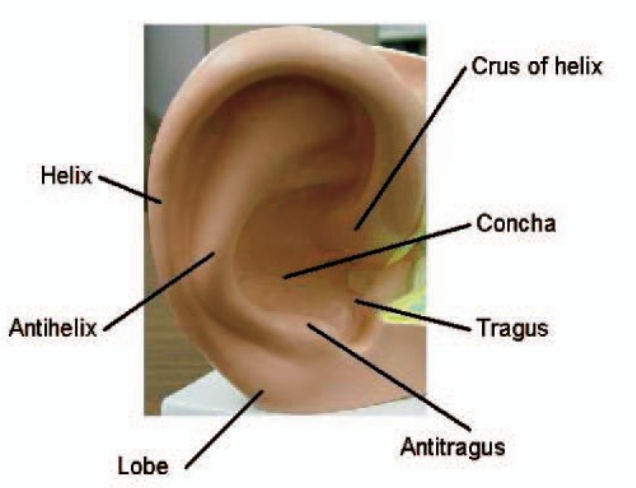

Figure 3 a. The external ear and its anatomical parts

A. Motivation

Among various physiological biometric traits such as iris, face, finger, retina; ear has received much attention in recent years as it has been found to be a reliable biometrics. The characteristics making ear biometrics much popular are given below :

Ear is remarkably consistent and does not change its shape under expressions like face. Moreover, ear has uniform color distribution.

Changes in the ear shape happen only before the age of 8 years and after that of 70 years. Shape of the ear is very much stable for the rest of the life.

Size of the ear is larger than fingerprint, iris, retina etc. and smaller than face, and hence ear can be acquired easily.

Ear images cannot be disturbed by glasses, beard or make-up.

IV. Ear Biometric Cryptosystem

A. Design Methodology

The ear cryptography system can divided into two major module –

Key generation module

Encryption and decryption module

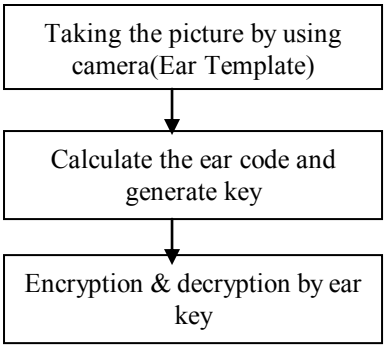

Figure 4 a. Flow Diagram of Ear Biometric Cryptosystem

B. Proposed Architecture

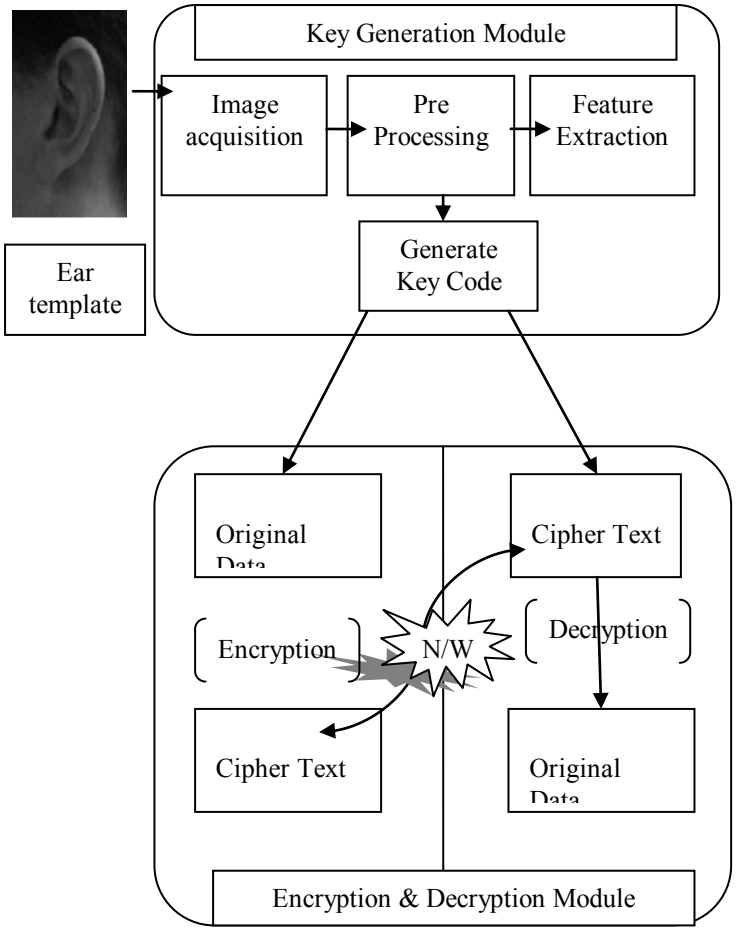

Figure 4 b. Proposed Architecture of Ear Biometric Cryptosystem

C. Proposed Algorithm

1. Key Generation from ear Algorithm

Step 1: Plain ear image has been taken.

Step 2: It has to be subjected to preprocessing unit

2.1. Image size has been altered.

2.2. Clarity of image has been maintained.

2.3. Feature extraction and segmentation .

2.4. Normalization

Step 3: 128 bit key generate from normalized image

2. Encryption & Decryption Algorithm

Step 1: Ear key apply on original data.

Step 2: Original data convert into cipher text during encryption process.

Step 3: In decryption process same key is used for finding the original data.

V. IMPLEMENTATION

Biometric feature extraction is the process in which key features of the sample biometrics are selected and enhanced

A. Key Generation Module

Image acquisition deals with the collection of raw data from subjects for specific biometric traits by using digital camera. In the preprocessing step region of Interest (ROI) is detect in the acquired image. Its also performs image clarity and altered the image size. Feature Extraction extracts the features from cropped ear template (ROI).

Key generation is a part of preprocessing step which consist of segmentation and normalization process. Segmentation is a process that divides the whole image into various segments. The main purpose of segmentation is to convert the image to something which can be easily analyzed. It is useful for estimate the boundary of biometric template and filtered from noise.

Normalization changes the ranges of pixel intensity value. For finding the accurate texture, Dogman's rubber sheet model is used which easy to map the ear feature point to a rectangular block of texture of a fixed size.

From the normalized image blocks of 128 bit should be generated. This 128 bit, extracted from the ear template is used as key.

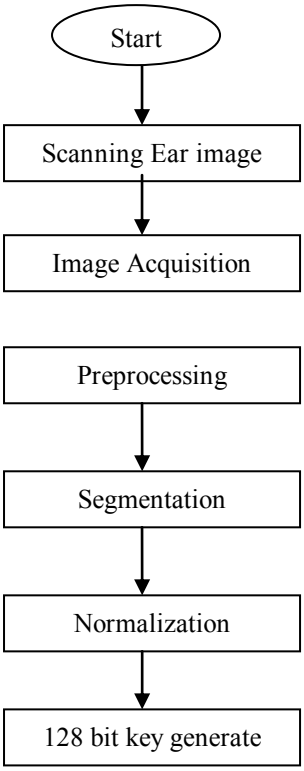

Figure 5 a. Flow Diagram of Key Generation

B. Encryption Decryption Module

To convert the plain text into the cipher text and vice versa, this 128 bit key is used as the key in advanced encryption standards(AES).AES is based on symmetric cryptography so same key is used for both encryption and decryption purpose. It only allow authenticated person to access particular system.

VI. CONCLUSION

Ear based cryptosystem is generated in this paper. Secret key is generated from the ear template. This same key is used both for encryption and decryption side.

In the future work all steps of proposed method of cryptographic key generation will be implemented and quality

properties of the generated keys will be investigated.

ACKNOWLEDGMENT

The author would like to thank the anonymous reviewers for their valuable comments and special thanks to my guide for his valuable suggestion for publishing the paper.

REFERENCES

[1] Arroyo David, Li Chengqing, Li Shujun, Alvarez Gonzalo, Halang A. Wolfgang," Cryptanalysis of an image encryption function networks," scheme based on a new total shuffling algorithm", Elsevier ,Science Direct, Volume 41, Issue 5, 15 September 2009, Pages 2613-2616.

[2] Yao-Jen Chang, Wende Zhang, Tsuhan Chen, "Biometrics-based cryptographic key generation," Multimedia and Expo, 2004. ICME '04.2004 IEEE International Conference on , vol.3, pp. 2203,2206 Vol.3, 27-30 June 2004.

[3] C. Tilborg (Ed). Encyclopedia of Cryptography and Security. Springer, 2005.

[4] Gang Zheng, Wanqing Li, Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping," Pattern Recognition, 2006. ICPR 2006. 18th International Conference on ,vol.4,pp.513–516, 2006.

[5] Andrew Teoh Beng Jin, David Ngo Chek Ling, Alwyn Goh," Biohashing : two factor authentication featuring fingerprint data and tokenized random number " April 2004,"The Journal Of The Pattern Recognition Society " , Elsevier , April 2004.

[6] Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, ijayakumar Bhagavatula, ―A pitfall in fingerprint bio-cryptographic key, Computers & Security, Volume 30, Issue 5, July 2011, pp. 311–319, 2011.

[7] Gao Tiegang, Chen Zengqiang," A new image encryption algorithm based on hyper-chaos" Elsevier, Science Direct,Physics Letters A, Volume 372, Issue 4, p. 394-400, 2007.

[8] Xiangqian Wu, Ning Qi, Kuanquan Wang, Zhang D., "An Iris Cryptosystem for Information Security", Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, pp. 1533–1536, 2008.

[9] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp.1081–1088, Sep. 2006.

[10] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems:Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, Jun. 2004.

ISSN: 2278 – 7798

Rishika Jain , have competed BTech in honors. And now doing Mtech from Bhagawant university, Ajmer(Raj).I am doing my thesis on ear based cryptography. My area of interest is image processing, cryptography and biometric field .