Generating an Efficient Crypto-Biometric Key using Finger Print and Fuzzy Vault

Dr. Mahesh P. K1, Shashi Ranjan2 and Ravindranath K3
1, 2, 3 Department of Electronics and Communication, Don Bosco Institute of Technology, Bangalore, India
maheshpk@gmail.com, shashiranjanbe@gmail.com, ravindranath321@gmail.com

Abstract—A crypto-Biometric based system has been more convenient compared to password based systems, which enhances the security and also being user friendly, due to its maturity and reliability. Fingerprint has been studied along with biocrypt to meet the cryptographic requirement. In this paper we explore realization of fuzzy vaults with fingerprint minutiae data. Helping in hiding encryption key with the fingerprint data so as to access the secret by authorized user providing the valid fingerprint data. To achieve the more robust security over shared data RSA-2 algorithm is used to generate Cryptographic Key, hence multiple Cryptographic technique using proposed system.

Index Terms—Crypto-Biometric, CRC, Fuzzy Vaults, Galois Fields RSA-2 algorithm.

I. INTRODUCTION

Biometric system recognizes a person through a pattern recognition system through their physical and or behavioural characteristic of a person. Fingerprints are one of many forms of Biometrics used to identify an individual and verify their identity. A fingerprint is classified based is uniquely identified based on the Local ridge and furrow minute details features and on only the Global ridge and furrow structures features (ridge endings and bifurcations, also known as minutiae, see Fig. 1).

Cryptography is the study of hiding information. Cryptography mainly deals with encryption & Decryption, where Encryption is the process of converting plain text, into cipher text and Decryption is the reverse process, converting cipher text to plaintext. Cipher is generated by algorithm and each instance, by a key. Key will be known to the communicating persons only. Keys are made complex in such a way that the hackers cannot access the key information present in that. Cipher text are more secured, even if a hacker

DOI: 03.AETS.2014.5.381
© Association of Computer Electronics and Electrical Engineers, 2014
obtains the cipher image, he/she can’t extract full information because the “key “information will be provided only to communicants. Data to be transmitted is considered as plain text. Most of algorithms provide high security of data but have the main disadvantage of key management problem. By using the cryptography algorithm along with biometric system provides more Security and overcomes the problem of key management.

Methods adopted to secure a key with a biometric.

   a. Remote template matching and key storage (Biometric image is compared with corresponding template).
   b. Data is derived directly from a biometric fingerprint image.

II. RELATED WORKS

In [9], to encrypt the image and transmit over the covert channel arithmetic encoding technique is used with DES. The arithmetic encoding provides coded data values in between interval of 0 and 1. That gives security and compression over the input files[9,10].The Arithmetic Coding is efficient, for providing both security and compression simultaneously is growing more important and is given the increasing ubiquity of compressed Bio-metric files in host applications of Defence, Internet and the common desire to provide security in association with these files. In [11] the RSA algorithm is used with some modifications which enhance the speed of RSA algorithm is called RSA-1 and the algorithm which provide security more than RSA algorithm is called RSA-2 algorithm which can enhance confidentiality to the sender. The problem of RSA algorithm is solved [11] through RSA-2 algorithm, it used the numbers instead of character in the plain text are represented by encoding scheme which can be able to represent special character. In case of character and number the intruder can easily know the cipher text and author can replaced it by the special symbols with the help of decimal value into their respective ASCII code character. The RSA-2 algorithm increased the speed of encryption and decryption with enhancement of security also due to special symbol.

Uludag et al. [13] present their implementation of fuzzy vault, operating on the fingerprint minutiae features. They extend [13] where chaff points generated according to minutiae points and protected secret, which is clear in secret check block (cyclic redundancy check encoding), and chaff generation block. [12] differ from [8] work’s in decoding implementation does not include any correction scheme, since there are serious difficulties to achieve error-correction with biometric data. Developing the necessary polynomial reconstruction via error-correction has not been demonstrated in the literature. Fuzzy vault for fingerprint decodes many candidate secrets. To identify which candidate is valid a Cyclic Redundancy Check (CRC) is used. CRC is commonly used in error correction.

Geometric hashing technique to perform alignment in a minutiae-based fingerprint fuzzy vault [14] but still has the problem of limited security. That is, the maximum number of hiding points (chaff points) for hiding the real fingerprint minutiae is limited by the size of the fingerprint sensor meanwhile the size of the fingerprint images captured and the possible degradation of the verification accuracy caused by the added chaff minutiae.

III. PROPOSED METHOD

We are proposing a crypto-biometric systems method to solve the key management problem by protecting templates in biometric systems. In general, the identity theft problem is drastically exacerbated for the biometric systems, since the biometric data and the corresponding feature vectors are non-renewable. To overcome this we present our idea of implementation of the fuzzy vault, operating on the fingerprint minutiae features. And secured robust key is generated by encrypting the vault, using RSA-2 Algorithm.

A. Extracting Minutiae Points from Fingerprint

For extracting minutiae points from fingerprint, a three level approach is broadly used by researchers. These levels are listed as follows,

•Pre-processing.
•ROI selection.
•Minutia extraction.

For the fingerprint image pre-processing, Histogram Equalization [20] and FFT are used to do image enhancement. Binarization is applied on the fingerprint image. Locally adaptive threshold method [13] is used for this process. Then Morphological operations [13, 18] are used to extract Region of Interest [ROI]. In a morphological operation, the value of each pixel in the output image is based on a comparison of the
equivalent pixel in the input image with its neighbors. By selecting the size and shape of the neighbourhood, we can construct a morphological operation that is sensitive to specific shapes in the input image.

a). Pre-processing

Pre-processing is the process where the original image is made convenient to the further steps of image processing here image is expanded so that clear image is obtained to solve the problems like non continuous images histogram equalisation is used and Fourier transform is used to get expanded image so that the obtained image will be the clear image.

(a) Fingerprint Image binarization is used in order to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges (black) and 1-value for furrows (white).

![Figure 2. a) Original image, b) Histogram Enhancement, c) Enhancement by FFT and d) Image after adaptive binarization](image)

A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs [Fig.2(d)].

B. ROI Selection

We perform morphological opening on the gray scale or binary image with the structuring element. We also performed morphological closing on the gray scale or binary image resulting in closed image. The structuring element is a single structuring element object, as opposed to an array of objects both open and close. Then as the result of this approach we get the image with tight bound (leftmost, rightmost, uppermost and bottommost blocks out of the bound) and inner area.

C. Minutiae Extraction

The last image enhancement step normally performed is thinning. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide [16] uses a Ridge Thinning algorithm, which is used for Minutiae points’ extraction in our approach shown in Fig.3. The image is divided into two subfields in a checkerboard pattern.

1. In the first sub-iteration, delete pixel p from the first subfield if and only if the conditions G1, G2, and G3 are all satisfied.
2. In the second sub-iteration, delete pixel p from the second subfield if and only if the conditions G1, G2, and G3’ are all satisfied.

**Condition G1:**

\[
X_{h}(P)=1.
\]

Where,

Here, x1, x2, ......., x8, are the values of the eight neighbours of p, starting with the east neighbour and numbered in counter-clockwise order.

**Condition G2:**

\[
2 \leq \min\{n_{1}(p), n_{2}(p)\} \leq 3
\]

Where,

\[
n_{1}(p) = \sum_{k=1}^{4} X_{2k-1} \lor x_{2k},
\]

\[
n_{2}(p) = \sum_{k=1}^{3} X_{2k} \lor x_{2k+1}.
\]
Condition G3:
\[(x_2 \lor x_3 \lor x_4) \land x_5 = 0.\]

Condition G3:
\[(x_6 \lor x_7) \land x_8 = 0.\]

Two sub iterations together make up one iteration of thinning algorithm.

B). Fingerprint Vault Implementation with encryption key. Fig. 4 shows the block diagram of the proposed system. Fig. 5 explains the polynomial in Fig. 5(a) encodes the secret. It is evaluated at both genuine and chaff points in Fig. 5(b). Finally, the vault is the combination of genuine and chaff points.

The encryption portion of the system creates fuzzy vault for the message. Cryptographic key comprises of template of many samples of same data. Data points representing polynomial are stored in vault. Many random data points (chaff) to secure data points chaff is been added to vault. Resulting image consists of minutiae coordinate (x,y) and orientation angle (θ). In particular, \(GF(2^n)\) fields are used, fields are binary numbers and n is the degree of the generating polynomial [15]. A Galois field is a finite field with order \(q = p^n\) elements where p is a prime integer and \(n \geq 1\). By definition, arithmetic operations (addition, subtraction, multiplication, division, etc.) on field elements of a finite field always have a result within the field. An element with order \((q - 1)\) in \(GF(q)\) is called a primitive element in \(GF(q)\). All non-zero elements in \(GF(q)\) can be represented as \((q - 1)\) consecutive powers of a primitive element \((\alpha\) ). All elements in \(GF(2^m)\) are formed by the elements \(\{0,1,\alpha\}\). Taking the field \(GF(2^n)\) and generator polynomial \(x^3 + x + 1 = 0\), the elements of the field can be calculated, starting with an element called \(\alpha\) which is called the primitive root (in this case, \(\alpha = 2 = x\)). All elements of the field (except 0) are described uniquely by a power of \(\alpha\). For any finite field \(GF(2^n)\), \(\alpha^{2^{n-1}} = \alpha^n = 1.\)
The RSA scheme is a block cipher. Each plaintext block is an integer between 0 and \( n - 1 \) for some \( n \), which leads to a block size \( \leq \log_2(n) \). The typical size for \( n \) is 1024 bits. The details of the RSA algorithm are described as follows.

**Key generation**

1. Pick two large prime numbers \( p \) and \( q \), \( p \neq q \);
2. Calculate \( n = p \times q \);
3. Calculate \( \varphi(n) = (p - 1)(q - 1) \);
4. Pick \( e \), so that \( \gcd(e, \varphi(n)) = 1, 1 < e < \varphi(n) \);
5. Calculate \( d \) so that \( d \cdot e \mod \varphi(n) = 1 \), ie \( d \) is the multiplicative inverse of \( e \) in mod \( \varphi(n) \);
6. Get public key as \( K_U = \{e, n\} \);
7. Get private key as \( K_D = \{d, n\} \);

**Encryption**

For plaintext block \( P < n \), its cipher text \( C = P^e \mod n \);

**Decryption**

For ciphertext block \( C \), its plaintext is \( P = C^d \mod n \);

IV. EXPERIMENTAL RESULTS

The experimental analysis of our proposed approach is presented in this section. Our approach is programmed in Matlab (Matlab 7.4). The minutiae coordinates are linearly mapped to 8-bit range (e.g., the values [0, 255]) for both row and column dimensions before using them in locking/unlocking the vaults. We have tested our proposed approach with different fingerprint images. The minutiae points are extracted from the fingerprint images using the three level approaches presented in the paper. Initially, in the pre-processing stage, histogram equalization and Fourier Transform are performed on the fingerprint images to enhance them. Secondly, the binarization is applied on the fingerprint images and then the region of interest is determined. Subsequently, minutiae points are extracted. Later, the secured feature matrix is generated based on the coordinates of minutiae points. Eventually, the 1024-bit key is generated from the secured feature matrix. The fingerprint images given in Fig.5 are depicted in Fig.6.
Figure 3. Generated 1024-bit key

V. CONCLUSION

Biometrics-based Key Generation outperforms traditional systems in usability domain. Precisely it is not possible for a person to lose his/her biometrics, and the biometric signal is intricate to falsify for steal. The proposed cancellable biometric Crypto System is an all-new technique for the authentication that yields the synergistic control of biometrics. The proposed system employs intentional distortion of fingerprint in a
repeatable fashion and the fingerprint thus obtained is utilized in the cryptographic key generation. When the old fingerprint is “stolen” it is possible to obtain a “new” fingerprint just by altering the parameters of the distortion process. Subsequently, enhanced privacy for the user results as his true fingerprint is not utilized anywhere and diverse transformations for distortions can be utilized for a variety of accounts. A notable enhancement in terms of decrease in the consumed time is attained with the elimination of more steps that are redundant with the mixture of the proposed methodology. Integration of the projected technique with the existing cryptographic methodologies is uncomplicated and as well decreases key-generation and key-release issues in a remarkable manner. This methodology can be further made efficient and sophisticated with the combination of any of the evolving cryptographic systems.

REFERENCES