Biometric Cryptosystem

Shilpi Arora[1], Akash Takawale[2], Rushikesh Karnewar[3], Rohit Bhosale[4], Shubham Tathe[5]
Department of Computer Engineering
[1] Teacher, DYPIEMR
[2,3,4,5] Student, DYPIEMR

Abstract- *Biometric cryptosystems is the combined study of cryptography and biometrics to benefit from both the 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.*

The difficulty in biometric cryptosystems comes from the fact that biometric measurements are variable and noisy: the same biometric may change between consecutive acquisitions (due to injury, ageing, even mood etc.) and noise can be introduced to a biometric signal by an acquisition device or the environment. While it would be very convenient to use biometric traits for encryption, for instance someone using his fingerprint or handwritten signature to encrypt a document and securely send it over public network, this is very difficult due to the aforementioned variability of the biometric signals and the fact that encryption and decryption operations cannot tolerate the perturbation of even a single bit. In its most basic sense, generating a cryptographic key directly from a biometric trait, for instance fingerprints, has not been very successful, as it involves obtaining an exact key from a highly variable data.

I. INTRODUCTION

In biometric based authentication, the access is granted to a person when his/her biometric traits are sufficiently matched with his/her stored biometric profile. However, there are other access scenarios, which require participation of multiple previously registered users for a successful authentication or to get an access grant for a certain entity.

In this paper, we are implementing biometrics for data security. A 64-bit key is generated from the fingerprint of user. When the user intends to send the data, he chooses a receiver from the list of users. A 128-bit key is generated by combining the receivers' and senders' keys. This key is used for encryption and decryption process. The encryption algorithm used here is Advanced Encryption Standard. It is symmetric key algorithm. So same key will be used for decryption also.

II. FEATURE EXTRACTION

1. Binarization - Image binarization is the process of turning a gray scale image to a black and white image. By the end of this process, all pixel values within the image are either zero or one, and the image has been converted to binary format. Fingerprint Image Binarization is used to transform the 8-bit Gray fingerprint image to a 1- bit image and here the value for the ridges is 0 where as it is 1 for the furrows. After this operation, the ridges in the fingerprint will be highlighted with black color while some with white. A locally adaptive binarization method is performed to binaries 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.

2. Thinning - Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide. Uses an iterative, parallel thinning algorithm. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3). And finally removes all those marked pixels after several scans. Such an iterative, parallel thinning algorithm has bad efficiency although it can get an ideal thinned ridge map after enough scans. Their method traces along the ridges having maximum gray intensity value.

III. MINUTIAE DETECTION

For minutiae detection we use the cross numbering algorithm. After the fingerprint ridge thinning, marking minutia points is relatively easy. Uses for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending. Together with the minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation.

KEY GENERATION

Algorithm for generation of key

```
Step1:-   NP <- No of minutiae points in the region of interest.
Step2:-   Rem <- NP mod 64
```

```
Step 3:-   NP <- NP – Rem //this makes NP perfect divisible by 64.
Step 4:-   I <- NP /64 //gives number of recursive iteration to perform compression of the key size to 64-bit.
Step 5:-   for 1 to I do
Drop Left 32 bit and Right 32 bit.
Divide the remaining key set into KL and KR.
Swap KL and KR.
done.
End of for.
```

The above algorithm gives a 64-bit key of a fingerprint. This key will be combined with the key of receiver's fingerprint making it a 128-bit key. This key is used in AES. AES performs 10 rounds of Bytesub transformation, Shiftrows transformation, Mixcolumns transformation and Addroundkey transformation. These rounds are performed on blocks of data, i.e. plaintext, and produces a block of cipher text.

IV. AES PROCEDURE

Rijndael is a block cipher developed by Joan Daemen and VincentRijmen.AES algorithm is can support any combination of data (128) and key length of 128, 192, and 256 bits. AES allows a 128 bit data length that can be divided into four basic operational blocks. These blocks are treated as array of bytes and organized as a matrix of the order of 4×4 that is called the state. For full encryption, Nr rounds (Nr = 10, 12, 14 for key length 128,192 and 256 respectively) of iteration are used. [7, 8]. Each round of AES is governed by the following transformations.

Biometric identifier

Universality Distinctiveness Permanence collectability Performance Acceptability Circumvention

Face	H	L	M	H	L	H	H
Fingerprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Voice	M	L	L	M	L	H	H

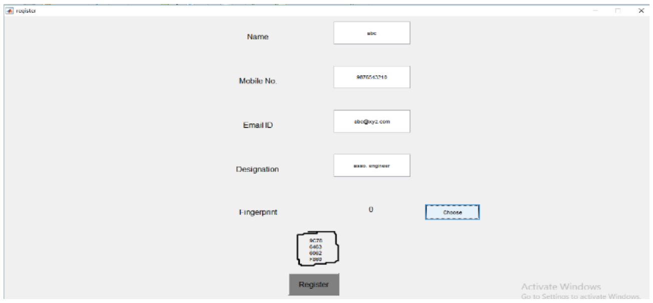
A) Bytesub transformation: It is a non linear byte Substitution, with the help of a substation table (s-box), which is generated by multiplicative inverse and affine transformation.

B) Shiftrows transformation: It is a simple byte transposition, the bytes in the last three rows of the state, depending upon the row location, is cyclically shifted; the offset of the left shift varies from zero to three bytes.

C) Mixcolumns transformation: This round is equivalent to a matrix multiplication of each Column of the states. A fix matrix is multiplied to each column vector. In this operation the bytes are taken as polynomials rather than numbers.

D) Addroundkey transformation: It is a simple XOR between the present state and the roundkey. This transformation is its own inverse. The encryption process consists of several steps. Initially an addroundkey operation is performed then a round function is applied to the data block (consisting of byte sub, shift rows, mix columns and addroundkey transformation, respectively). This round operation is performed iteratively (Nr times) depending on the length of the key. The decryption operation has exactly the same sequence of transformations as the one in the encryption operation. The transformations Inv-Byte sub, the Inv-Shift rows, the Inv-Mix columns, and the addroundkey allow the form of the key schedules to be identical for encryption and decryption.

V. RESULTS



Name: abc

Mobile No.: 9876543210

Email ID: abc@xyz.com

Designation: asso. engineer

Fingerprint: 0

9C70
6463
6062
F880

Fig.1 Generation of Key from User Fingerprint

The highlighted portion shows the 64 bit key generated. This key will be combined with the key of receiver's fingerprint making it a 128-bit key and encrypting plaintext by AES.

REFERENCES

[1] Biometric Cryptosystems : Issues and Challenges by UMUT ULUDAG, STUDENT MEMBER, IEEE, SHARATH PANKANTI, SENIOR MEMBER, IEEE, SALIL PRABHAKAR, MEMBER, IEEE, AND ANIL K. JAIN, FELLOW, IEEE.

[2] Biometric Cryptosystem: A Literature Review by Rushikesh Karnewar, Akash Takawale, Rohit Bhosale, Shubham Tathe (Student, Computer Engineering Department, DYPIEMR).

[3] https://archive.org/stream/FeatureExtractionTechniquesAndMinutiae-basedFingerprintRecognitionProcess/34-39_djvu.txt

[4] http://biometrics.sabanciuniv.edu/bc.html