International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Multi-Purpose Key Generation Using Combination of Fingerprints

Sharda Singh[1],Dr. J. A. Laxminarayana[2]

[1]*Department of Computer Engineering, Goa College of Engineering, sharda2191@gmail.com*
[2]*Department of Computer Engineering, Goa College of Engineering, jal@gec.ac.in*

Abstract—The security of any encrypted data relies upon the cryptographic keys in use. The strong cryptographic key shall be lengthy, random and unique. A biometric feature such as fingerprint can provide the uniqueness factor, whereas randomness can be induced using different combinations of fingerprints. We propose a technique to generate the large random number by making use of combination of fingerprints.

Keywords-Biometrics; Cryptography; Fingerprints; Key Generation; Minutiae.

I. INTRODUCTION

In recent years, the progress in the communication technologies is resulting in huge transfer of the digital data in the publicly shared media. To secure these shared data, there is a significant interest shown by the researchers in the cryptographic domain leading to many innovative and efficient encryption methods. Every encryption method needs to use strong keys.

The cryptographic key shall be a large unpredictable random number [12]. There are various methods to generate such keys; some methods are proposed to generate cryptographic keys from the biometric features such as iris, fingerprints, signature etc. as in [2, 3, 4, 6, 7, 8, 9, 13].

There is a significant growth in the field of biometric technologies in past few years, and many of them are deployed according to the specific application and their acceptability to the users [3, 18].

In this paper we propose a novel technique to generate the large random number using combination of fingerprints. The motivation for this proposed method comes from the fact that biometrics are a complete source of identification and being possessed by every individual, it would work as a good source of cryptographic keys, which can easily be long, random and unique.

II. LITERATURE SURVEY

Biometric features like iris and fingerprint are used for authentication most of the times as explained in [3, 5]. In [9], efforts were made to extract the uniqueness of these biometric features and combine them to form a unique key. Further, it was attempted to generate a secure cryptographic key by incorporating multiple biometrics modalities of human being, so as to provide better security.

The proposed approach [9] is composed of three modules namely, 1) Feature extraction, 2) Multimodal biometric template generation and 3) Cryptographic key generation. Firstly, the features like minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Then, the extracted features are combined together at the feature level to obtain the multi-biometric template. Lastly, a 256-bit secure cryptographic key is generated from the multi-biometric template. Similarly, the fingerprint image was used to generate keys as in [2, 6, 8].

A combination of fingerprint and signature based key generation is explained in [7] which provided a framework for designing an asymmetric biometric cryptosystem through which a user can send and receive secure information only by using his biometric features.

As there are so many biometric features, the information shown in Table 1[3], justifies the selection of fingerprint to generate keys.

@IJMTER-2015, All rights Reserved

Table 1: Comparison of Various Biometric Technologies [3]. (Medium, high and low are denoted by M,H and L respectively)

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
Hand Geometry	M	M	M	H	M	M	M
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

The comparison in Table 1 is based on seven factors:

- Universality: How universal the identifier is? Is it possessed by everyone?
- Distinctiveness: Can it be used to distinguish people?
- Permanence: Is the identifier permanent? For how long is it there with the individual?
- Collectability: Can the identifier be captured and collected? If yes, how well?
- Performance: What is the speed of obtaining the identifier? How accurately does it get used?
- Acceptability: Is it acceptable to be used? How willing are the people to use it?
- Circumvention: how foolproof is the identifier? It should be hard to imitate it.

The biometric fingerprint is selected due to its high score in Table 1. It is found that, researchers have attempted to generate cryptographic keys using only single fingerprint [6, 8], or a fusion of two or more biometric features [4, 7, 9].

Fuzzy Vault Scheme [11] and Modified Fuzzy Vault Scheme [1] are proposed to handle the situations in which acquired biometrics are noisy due to wear and tear, improper acquisition of signal and inconsistent presentation.

In [15], a method is proposed to generate a secure key for MAC algorithm using fingerprint based cryptography system. The key is generated using fingerprint patterns, which is stable throughout person's lifetime. There is a chance that the conventionally generated password may be hacked by trial and error method. But it is not possible to break the biometrics based security system easily.

III. PRE-REQUISITES

3.1. Working of the Biometric Fingerprint

Fingerprint recognition technology extracts features from impressions made by ridges on the fingertips[5]. To generate keys from fingerprint we first and foremost need to capture the fingerprint images. We use a fingerprint capturing device for this purpose. The device can be an USB device or a parallel device with variety of sensor types.

In every human fingerprint there are certain patterns made due to ridges and valleys which are almost unique. The various patterns are ridge endings, ridge bifurcations, isolated points, deltas, pores, lakes, spurs and crossing points. In the proposed model we extract the features namely ridge bifurcation, ridge ending, crossing points and isolated points.

@IJMTER-2015, All rights Reserved

3.2. Crossing Number [10]

Crossing number is defined as the half of the sum of differences between adjacent pixels in eight connected neighborhood.This technique makes use of skeleton image / thinned image of ridge flow pattern to classify the ridge type. It uses a 3x3 window, using which neighborhood of each ridge pixel is scanned as shown in Figure 1.The crossing number is calculated as per equation (1) and the ridge pattern is classified based on the CN value for that pixel according to Table 2.

$$CN = 0.5 \sum Pi - Pi+1 \qquad \text{for } i=1 \text{ to } 8 \text{ and } P9=P1. \qquad (1)$$

P4	P3	P2
P5	P	P1
P6	P7	P8

Figure 1: 3x3 Window for Scanning Neighborhood Pixels

Table 2. Ridge Pattern Associated to Crossing Number Value.

CN	Ridge Pattern
0	Isolated Points
1	Ridge Ending
2	Ridge Continuation
3	Ridge Bifurcation
4	Crossing Point

IV. PROPOSED MODEL

We propose a novel approach to key generation, which uses a combination of fingerprints to generate the multi-purpose keys. Figure 2 shows the flow of the proposed method.

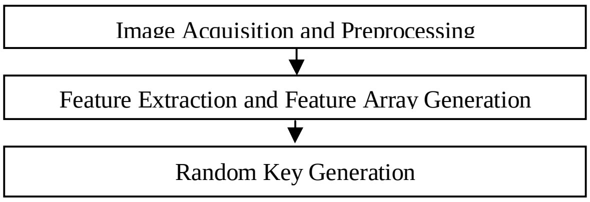

Figure 2: Flow of Proposed Method.

4.1. Image Acquisition and Preprocessing

We capture all 10 fingerprints and from them select randomly 'n' of them, where 'n' (n<10) can be explicitly specified by the user. Initially the pre- processing and feature extraction techniques as in [13, 14] are applied to the captured images followed by the proposed algorithm to generate the key.The following image processing algorithms as described in [7, 8, 9, 15] are applied.

a) *Histogram Equalization:* It enhances the contrast of the fingerprint image at the places where the ridge lines are not very prominent (caused due to low pressure on the sensor). Here the basic idea is to map the gray levels based on the probability distribution of the input gray levels.
b) *Noise removal:* this is achieved using filters like Median filter, Weiner or Gabor filter. It first estimates the noise in the image and removes the estimated noise to get the clearer image.

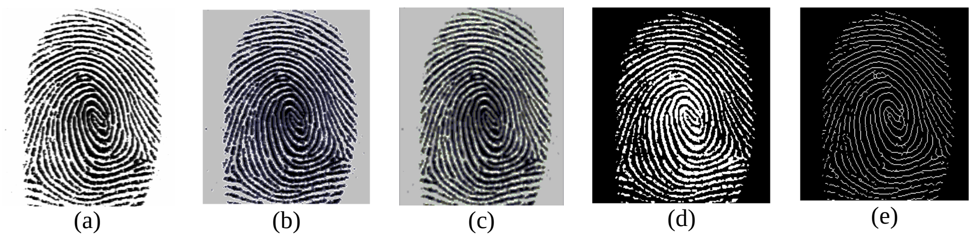

Figure 3: Results of Image Pre-Processing Techniques (a) Original Captured Image, (b)Histogram Equalization, (c)Noise Removal, (d) Binarization, (e) Thinning

@IJMTER-2015, All rights Reserved

c) *Binarization:* In this step the grey scale image is converted into binary image. This enhances the contrast between the ridge and the valleys in a fingerprint image. The image is binarized by considering the mean of all the neighboring pixels around each pixel and giving a value 1 to that pixel if its intensity is greater than the mean value and 0 otherwise.

d) *Thinning:* Application of morphological thinning operation to get the final image with a width of single pixel. The resultant image is the skeleton structure of the image.

4.2. Feature Extraction and Feature Array Generation

For every image which is pre-processed, we will extract the below listed features and store the feature coordinate into feature arrays.

1) Ridge ending points
2) Ridge bifurcation points
3) Isolated points
4) Crossover points

The features are extracted using crossing number technique. Let the extracted feature arrays are MRE, MRB, MIP, and MCR, where:

MRE: Minutiae point array for Ridge Endings.
MRB: Minutiae point array for Ridge Bifurcations.
MIP: Minutiae point array for Isolated Points.
MCR: Minutiae point array for Crossover Points.

Hence, for every fingerprint image, a collection of four 2 dimensional arrays viz., MRE, MRB, MIP, and MCR, is generated.It is proposed to create a single array FA for every image by merging all the feature arrays so generated, such that: FA= MRE+MRB+MIP+MCR, where '+' denotes concatation of arrays. It is to be noted that the total number of arrays generated is equal to n, where n is the number specified by the user.

4.3. Random Key Generation

In the following steps, we use the previously generated feature arrays (FA,) to generate the random key. The functions which are needed are:

1) next_prime(arg): returns the immediate next prime number to the argument which is passed.
2) sum_of_all(arg): returns the sum of all the arguments passed to the function.
3) random_number(arg): creates a random number using the arg value as the seed value.
4) Size_of(array): returns the no. of elements in the array.
5) xval_FA[i]: returns the x-coordinate value stored in array FA at index i.
6) yval_FA[i]: returns the y-coordinate value stored in array FA at index i.

4.3.1. Random Array Generation Based on Feature Array

For all the FA arrays, apply the algorithm as stated:

1) Create a random array R of size equal to selected FA array.
2) Calculate seed value : S=next_prime(Sx)* next_prime(Sy)
   Where: Sx=(sum_of_all(x) in FA) and Sy=(sum_of_all(y) in FA)
3) For j=1 to (size_of_FA), Use a random number generator with seed value 'S'
   a. R[j]=random_number(S).
4) For i=1 to (size_of_FA), do
   a. Calculate TX and TY as:
      i. TX=xval_FA[i]*R[i].
      ii. TY=yval_FA[i]*R[(size_of_R)-i].

b. Calculate R[i] = (TX+TY) mod S.

4.3.2. Key array generation using feature array

1) Merge all R arrays to create a new array FR.
2) Merge all FA arrays to create a new array FAA.
3) Create a string KEY with value 1, then calculate key as per algorithm explained below:
4) While size of KEY is less than 256 do
   a. Select a random number RFK between 1 to size of (FR).
   b. if FR(RFK) is odd, Concate FR(RFK) to KEY, Otherwise, Concate the KEY with product of RFKth elements of FAA.

4.3.3. Final key generation

Map the KEY string to numerical or hexadecimal format and the generated random number can be used as the required large random number for any specific encryption algorithm.

CONCLUSION

For every cryptographic algorithm, keys play an important role. Generally multiple biometrics are used to generate the key. Using multiple biometric modalities needs multiple devices for feature acquisition. The proposed methodology makes use of biometric like fingerprint to generate the key and uses only one device. As randomness is involved at many levels, starting from fingerprint selection to final key generation, the complexity of the key is increased. The generated random key can be used as seed value for pseudorandom number generator, OTP generator, for key exchange algorithms and for asymmetric cryptography.

REFERENCES

[1] Abhishek Nagar and Santanu Chaudhary, "Biometrics based Asymmetric Cryptosystem Design using Modified Fuzzy Vault Scheme", Proceedings of the 18th International Conference on Pattern Recognition(ICPR-06), pages 537-540, Aug 20-24, 2006.

[2] R. K. Sharma, "Generation of Biometric Key for Use in DES", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1 pages 312-315, November 2012.

[3] Umut Uludag, Sharath Pankanti, Salil Prabhakar and Anil K.Jain "Biometric Cryptosystems Issues and Challenges" Proceedings of the IEEE, Volume 92, issue 6, June 2004.

[4] P. Balakumar and R. Venkatesan, "Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 2, pages 349-356, September 2011.

[5] S. Soutar , D. Roberge , A. Stoianov , R. Gilroy and B.V.K.V. Kumar, " Biometric Encryption ", In R.K. Nichols, editor ICSA Guide to cryptography, pp 649 - 675, McGraw Hill New York 1999.

[6] A. Jaya Lakshmi, I. Ramesh Babu, "Design of security key Generation algorithm using Fingerprint based Biometric Modality",IOSR Journal of Engineering(IOSRJN) ISSN: 2250-3021, Vol 2, pages 325-330, Feb 2012.

[7] Abhishek Nagar, "Designing Biometrics-based Cryptosystem", Thesis report, Department of Mathematics, IIT Delhi- May 2006.

[8] R.Sesshadri and T.Raghu Trivedi, "Efficient Cryptographic Key Generation using Biometrics". IJCSTA, Vol 2, ISSN: 2229-6093.

[9] A Jagadeesan and Dr K.Duraiswamy "Secured Cryptographic key generation from multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris" in Int. Journal of Computer Science and Information Security, Vol 7, No 1, Feb 2010.

[10] Roli Bansal, Priti Sehgal and Punam Bedi, " Minutiae Extraction from Fingerprint Images - a Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

[11] A, Juels and M. Sudan, "A Fuzzy vault scheme," in Proceedings of IEEE International Symposium for Information Theory. A Lapidoth and E. Teletar, Eds., 2002, p. 408.
[12] W. Stallings, Cryptography and Network Security: Principles and Practices, Fourth Edition.
[13] Bashar Ne'ma and Hamza Ali, "Multi-Purpose Code Generation Using Fingerprint Images", Software Engineering Department, Isra Private University, Jordan, The International Arab Journal of Information Technology, Vol. 6, No. 4, October 2009.
[14] Praveen Namburu, "A Study on Fingerprint Image Enhancement And Minutiae Extraction Techniques", Thesis Report, Department of Computer Science and Engineering, National Institute of Technology, Rourkela, 2007.
[15] R.Sesshadri and T.Raghu Trivedi, " Generate a key for MAC Algorithm using Biometric Fingerprint". International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.4, December 2010.

@IJMTER-2015, All rights Reserved