ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 6, Issue 3, March 2018

A Survey of Cancelable Biometric Based Key Generation Scheme using Various Cryptography Techniques

Joshi Kimee[*], Payal Chaudhari

Department of Computer Engineering, LDRP-ITR, Gandhinagar, India

E-mail: joshikimee@gmail.com

Abstract: Key management in cryptosystem has more security concerns. In traditional cryptosystem key is generated randomly and very difficult to remember. The keys generated from biometric features provide better option than traditional cryptographic key management techniques such as password based key generations. Cancelable biometric is a customized technique in biometric based cryptography, where Cancelable Biometric refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. This paper presents the survey conducted for same of the cancelable biometric key generation techniques.

Keywords: Cryptographic key generation; Biometrics; Feature extraction; Key generation; Biometric cryptography

I. INTRODUCTION

Security is the most important aspect in the field of internet and network application. It is an essential task to secure information over the network. To secure information, cryptography can be used. Cryptography play very important role in information or communication security on network. Cryptography is a technique which is used to encrypt and decrypt data or store and transmit data in a secret form [1].

In this traditional cryptography, key is generated randomly and it is very difficult to remember, hence, stored in smart card; tamper-resistant token, etc. or password based authentication method is used to control the access of cryptographic key. But these user selected passwords sometimes lost or guessed by dictionary attacks. Therefore biometric keys are proving to be better alternative to these non-memorable passwords.

1.1 Biometric

A biometric is defined as a unique, measurable, biological characteristic or trait for automatically recognizing or verifying the identity of a human being [2]. In other words, Biometric system is a method of extracting unique human identity feature and verification of this identity for reliable user authentication [3] (Figure 1).

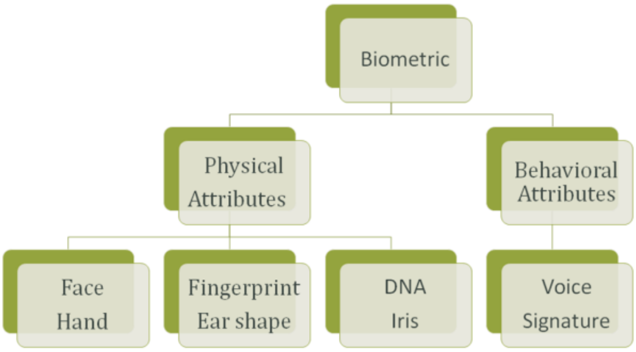

Figure 1: Biometric.

But the problem with biometrics is that once it gets compromised it cannot be reused. As a proficient solution for cancelling and reissuing biometric template cancelable biometrics has been proposed [4].

1.2 Cancelable Biometric

Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data [5]. This is a method of enhancing the security and privacy of biometric authentication. Example, Instead of enrolling with a true finger (or other biometric), the fingerprint is intentionally distorted in a repeatable manner and this new print is used. If, for some reason, the old fingerprint is stolen then an essentially a new fingerprint can be issued by simply changing the parameters of the distortion process [6] (Figure 2).

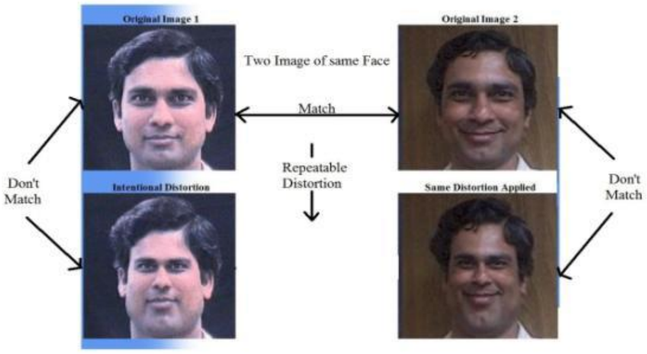

Figure 2: An example-cancelable biometric [6].

Some of the evaluation terminology used:

1.2.1 False accept rate or false match rate (FAR or FMR)

The probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, and then he is treated as genuine that increases the FAR and hence performance also depends upon the selection of threshold value [7].

1.2.2 False reject rate or false non-match rate (FRR or FNMR)

The probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected [7].

1.2.3 Genuine acceptance rate (GAR)

This is defined as a percentage of genuine users accepted by the system. It is given by GAR=100-FRR.
In the Section 2, various techniques are described. After then, the comparison of various biometric based key generation schemes. In section 3, a survey paper is concluded [7].

II. RELEATED WORK

In this section, the survey of various Biometric based key generation scheme and cancelable biometric based key generation scheme.

Arpita et al. proposed the cryptographic key is non-invertible and tracing any user’s fingerprint from the cryptographic key is not feasible. So this approach is free from the identity threat. An approach to generate and share cryptographic key from the fingerprint features (minutiae points) of sender and receiver. Both sender and receiver generate cancelable template from their own fingerprint and share it with each other. After that by using both cancelable templates, a combine template is generated and finally the symmetric cryptographic key is generated from the combine template [4].

1. Feature Extraction

Step 1: minutia points are extracted from the given fingerprint image of sender and receiver.

2. Generating Cancelable Template

```
Algorithm 1:
Input:-
1. X: X is an array of x-coordinates of all minutiae points
2. Y: Y is an array of y-coordinates of all minutiae points
3. n: n is the number of minutiae points
The minutiae points are (X[i], Y[i])
```

```
Output:-
T: T is an array of 64 signed 8-bit integers (-128 ->+127)
Procedure TRANSFORM-TEMPLATE (X, Y, n)
    //create an array of 64 random integers in the range [1,2n]
    R = new Array(64)
    for i = 1 : 64
        R[i] = random(1, 2n)
    end for
    //create an array of 64 8-bit signed integers to store the transformed template
    T = new Array(64)
    //populate the template array
    for i = 1 to 64
        if R[i] <= n
            T[i] = (X[R[i]] mod 256) - 128
        else
            T[i] = (Y[R[i] - n] mod 256) -128
        end if
    end for
    return T
End Procedure TRANSFORM-TEMPLATE
```

3. Template Exchange

Step 1: Exchange Template using RSA encryption.

4. Key Generation and Encryption Decryption

```
Algorithm 2:
Input:-
T1: An array of 64 8-bit signed integers (1st template)
T2: An array of 64 8-bit signed integers (2nd template)
Output:-
K: 128-bit integer (Symmetric key)
Procedure GENERATE-SYMMETRIC-KEY (T1, T2)
    //concatenate the templates
    T = concat (T1, T2)
    //generate 128-bit key
    K = 0
    temp = 1
    for i = 1 to 128
        if T[i] >= 0
```

```
K = K + temp //interpret as 1
end if
temp = temp * 2
end for
return K
```

After applying algorithm 1 and 2 mentioned above both sender and receiver can independently generate 128 bit key.

Subhas et al. proposed an option to revoke cryptographic key. If the key is compromised by the attacker, he is not able to know about the fingerprint data from the key. If the biometric data becomes compromised by a third party, he is not able to generate the same key from the fingerprint. This approach involves mainly three subsections, namely, Feature extraction, template generation and key generation [8].

1. Feature Extraction

Step 1: minutia points are extracted from the given fingerprint image of sender and receiver.

2. Template Generation

```
Step 1: The minutiae points are basically represented by a triplet like (mi=xi; yi; ᴓi) where mi is the $i^{th}$ minutiae point of minutiae set M and mi Ɛ M.
Step 2: di;j =((xi -xj)2 + (yi - yj)2)^1/2
Step 3: Z = n*(n-1)/2
Step 4: D8 = Sort (Unique(D))
Step 5: T(i) = 1 if i Ɛ Ds
0 if i Ɛ Ds
```

3. Key Generation

Step 1: user have to select the binary bits for key K from the template T of binary numbers in a random way. For a key K of size Nk (i.e., Nk = jKj), total N_k elements of vector T are chosen by the user as the bits of key K.

Gaurangkumar, et al. considers fingerprint data of user as an input to our system. Using this fingerprint, they extract the minutiae points as a feature vector and generate a biometric based cryptographic key. Using this biometric-based cryptographic key, they encrypt the user's data. To decrypt the message, capture the biometric fingerprint (i.e. fingerprint data) of the user and generate a biometric-based cryptographic key from the fingerprint. This approach proposed in paper can get the same biometric cryptography key from the fingerprints captured from different scanners with different quality of image [9].

Aditi et al. propose an effective scheme that has zero False Acceptance Rate and 15% False Rejection Rate over the different data set. First stable minutiae points extracted for the generation of secure key, secured one way functions are used. By this scheme, it is possible to generate a random key of size 512 bits, whose every bit is a function of the entire set of stable features, which can be compressed to 128 bits (requirement of AES) [10].

1. Feature Extraction

Step 1: For extracting minutiae point FFT and Gabor filter have been used for the enhancement of the image.

2. Secure Cancelable Cryptographic Key Generation

```
Phase 1: Registration of the user's fingerprint database
Algorithm:
(i) For all the fingerprints of a user
a) Find core point and extract all the minutiae points in the circle of radius w and core point as the center.
```

b) Select all the common minutiae points.
c) Consider k minutiae points nearest to the core point.
(ii) Calculate the parameters r and r' for each of the k minutiae.
(iii) Arrange the k points in increasing order of distances from the core and concatenate the binary string of both the parameters of the points.
(iv) Apply Secured Hash Algorithm (SHA-3) to find the hash value of the binary string formed in step (iii).
Phase 2: Key generation using fingerprint minutiae points
Algorithm:
Verification of user's fingerprint database:
(i) Take a combination of k minutiae points; find the hash using SHA-3.
(ii) If hash value matches with the hash value stored (calculated during registration). Otherwise try with another combination.
(iii) If the hash value of the fingerprint does not match with any of the combination then reject the fingerprint.

Padma et al. have presented a new cancelable biometric template generation algorithm using random projection and transformation based feature extraction and selection. Using cancelable biometric template achieved performance is better than the original template [11] (Table 1).

Method	**Key Size**	**Template Exchange**	**False Reject Rate**	**Remarks**
SA Sarkar et al. [4]	128 Bit Key	Yes		It confirms the privacy of fingerprints as well as resolves the difficulty of key storage and key distribution
P Gaurangkumar et al. [9]	As Per User Requirement	No	2.75% (GAR= 97.25%)	Generate Same Key Every time from the fingerprint captured from different scanners with different quality of image
B Aditi et al. [10]	As Per User Requirement	No	15%	FAR is 0

Table 1: Results of existing works.

III. CONCLUSION

This paper presents the basic concept of various key generation schemes. Moreover biometric fingerprint feature extraction used for encryption. Cancelable biometric provide high security than biometric. Biometric feature extracted from the user himself may be providing high security other than password based method. This paper can be useful for those who are wishing to carry out research in the direction of the Cancelable biometric based key generation scheme.

IV. REFERENCES

1. Sangeeta, K Arpneek, A Review on Symmetric Key Cryptography Algorithms. International Journal of Advanced Research in Computer Science 2017; 8:358-361.
2. S Colin, R Danny, et al. Biometric Encryption. McGraw-Hill 1999.
3. V Indu, J Sanjay, Biometric based Key-Generation System for Multimedia Data Security. IEEE Computing for Sustainable Global Development 2016.
4. S Arpita Sarkar, SK Binod, Cancelable Biometric Based Key Generation for Symmetric Cryptography. International Conference on Inventive Communication and Computational Technologies IEEE, 2017.
5. https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=1914
6. http://www.scholarpedia.org/article/Cancelable_biometrics

7. LC Archana, Biometric Fingerprint Authentication with Minutiae using Ridge Feature Extraction. International Conference on Pervasive Computing IEEE 2015.
8. B Subhas, S Debasis, et al. Revocable Key Generation From Irrevocable Biometric Data for Symmetric Cryptography. Computer, Communication, Control and Information Technology IEEE 2015.
9. P Gaurangkumar, S Debasis, Comparable Features and Same Cryptography Key Generation using Biometric Fingerprint Image. International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics IEEE 2016.
10. B Aditi, S Kapil, Secure Cancelable Fingerprint key Generation. IEEE Power India International Conference 2014.
11. PP Padma, G Marina, Multimodal Cancelable Biometrics. Int. Conf. on Cognitive Informatics and Cognitive Computing IEEE 2012.