SECURE CANCELABLE BIOMETRIC BASED GROUP KEY GENERATION SCHEME USING HOMOMORPHIC ENCRYPTION

1Kimie Joshi, 2Payal Chaudhari
1PG Scholar, 2Lecturer

1Department of computer engineering,
1LDRP-Institute of technology and Research, Gandhinagar, India.

Abstract: In the 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 key sometimes lost or guessed by dictionary attacks. Therefore biometric keys are proving to be better alternative to these non-memorable passwords. But the problem with biometrics is that once it gets compromised it cannot be reused. As a proficient solution for this problem, cancelable biometrics has been proposed. Cancelable biometric refers to the intentional distortion of biometric feature. In this paper, we present a cancelable biometrics based group key generation. The Proposed algorithm facilitates to update the key when the number of members are added in or revoked from group. We aim to use Homomorphic encryption for group key generation.

Keywords: Biometric, Symmetric cryptography, cryptographic key generation, cancelable template, Minutia extraction, Group Key Generation

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

Cancelable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. [3] 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 a new fingerprint can be issued by simply changing the parameters of the distortion process.
II. RELATED WORK

There are existing schemes which provide cancelable or non cancelable biometric based key generation. In [2] Indu et al proposed a scheme for generating biometric key using traditional algorithms like MD5 and SHA. Two cryptographic keys of size 128 bits and 512 bits are generated using Hash Function. The key generated by algorithms are compared on two factors like entropy and key space. SHA-12 approach can be used to generate more secure biometric key than MD5 Algorithm.

In [5] Arpita et al proposed a scheme for generating a cryptographic key that 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 is 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. From both cancelable templates, a combine template is generated and finally the symmetric cryptographic key is generated from the combine template.

In [6] Gaurangkumar et al proposed a scheme for generating biometric cryptography key from the fingerprints captured from different scanners with different quality of image. 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.

In [7] Subhas el 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.

In [8] 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. From 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).

In [9] 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.

OUR CONTRIBUTION

All these existing scheme have provided cancelable or Non-cancelable biometric key generation. All of them have presented the key generation for two party communication. None of them have addressed multiparty key generation. In our current work we address this issues. Our proposed scheme facilities a group key generation from cancelable biometric template. The Scheme also supports dynamic group size.

III. PROPOSED METHOD

In this present work an approach is proposed to generate and share cryptographic key from the fingerprint features (minutiae points) of multiple user. All Users generate cancelable template from their own fingerprint and Encrypt it with group owner’s public key to share it with Group Owner. After receiving Encrypted cancelable template Group Owner apply additive homomorphic encryption and generate combine Encrypted cancelable templates and finally the cryptographic key is generated from the template. An overview of the approach is shown in Figure 3.
Once Group Key is generated and if another user wants to join Group. The whole process of encryption is not repeated for new user. Directly add the user’s Encrypted cancelable template with combine. If a revocation occurs then, revoked user’s template is removed. Encrypted Cancelable template as shown in figure4.

3.1 The Different tasks involved in this approach are discussed in the following:
1. Generation of private and public key
2. Feature Extraction from Fingerprint
3. Cancelable Template Generation
4. Encryption of Cancelable Template & Share
5. Apply Additive Homomorphic Encryption on Template & Key Generation
6. Share the Key

3.1.1 Generation of private and public key
Public Key & Private key of each user is generated by using any efficient public key encryption algorithm such as RSA(Rivest-Shamir-Adleman).

3.1.2 Feature Extraction from Fingerprint of User[5]
In this approach minutia points are extracted from the given fingerprint image of sender and receiver. The steps involved in minutia extraction are as follows:

a) Image Binarization:
Image Binarization convert grayscale image into binary image. One can choose a threshold value and choose all the pixels above that value as white and below that value as black. This process is one of the simplest for Binarization.

b) Thinning:
Thinning plays an important role. Thinning is used to remove selected image from binary sources and is particularly used for skeletonization. All lines will be reduced to a single pixel thickness. It reduces amount of data to be processed and Reduce time.

c) Minutiae Extraction:
Minutiae points are extracted from the fingerprint image. Bifurcations, ridge ending and other features are found in this method. This algorithm returns \((x, y)\) as a minutiae point where \((x, y)\) denote \((x, y)\)-coordinate value. Figure Shows minutiae point. These values are stored in two vectors \((X, Y)\). Vector \(Vx\) contains \(x\)-coordinate values and vector \(Vy\) contains \(y\)-coordinate values of minutiae points.

\[
Vx = [xi], \text{ where } i=1 \text{ to } n \\
Vy = [yi], \text{ where } i=1 \text{ to } n
\]

![Figure 5: Minutiae Points](image)

For example, assume that 8 minutiae points are extracted. Let the points be \((280,113), (289,115), (284,120), (327,111), (332,104), (358,91), (360,86), (352,81)\)

Then \(X\) and \(Y\) are:

![Figure 6: X and Y coordinate values](image)

3.1.3 Cancelable Template Generation
In this step the fingerprint template of the user is transformed into non-invertible forms, called cancelable template. This is because if the original biometric data is compromised, the biometric traits will be useless. So, it is required to convert the irrevocable biometric data into revocable one before it is use in cryptography. The process is as follows: From the \(X\) and \(Y\) arrays generated in previous step, a template is created. The template array is of 128 elements. For generating this template, following steps are followed:

3.1.3.1 Create lookup table
A 128-element array of unsigned integers is created. Each element of the array will contain integer values from 1 to \(2n\). Let the array be \(R\).

3.1.3.2 Fill the lookup table
Each element of the 128-element lookup table is assigned a random integer between 1 and \(2n\).

3.1.3.3 Create template array
A new 128-element array \(T\) of signed 8-bit integers is created.

3.1.3.4 Fill the template array
The template array is assigned values from \(X\) and \(Y\) arrays using the lookup table \(R\). The algorithm for generating cancelable template is as follows:

**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 128 element

Procedure TRANSFORM-TEMPLATE (X, Y, n)

//create an array of 128 random integers in the range [1,2n]
R = new Array(128)
for i = 1 : 128
   R[i] = random(1, 2n)
ext for

//create an array of 128 element to store the transformed template
T = new Array(128)
//populate the template array
for i = 1 to 128
   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

3.1.4 Encryption of Cancelable Template & Share
Once Cancelable Template is generated, User Encrypt the own Cancelable Template using Group Owner’s Public Key. For Encryption RSA Algorithm is used.

3.1.5 Apply Additive Homomorphic Encryption on Template & Key Generation
Let the encrypted templates be T1,T2,T3,........,Tn of 128-element arrays. A new template is created is created by using Additive Homomorphic Encryption.
Logical converts integer into an array of logical values. Any nonzero element of array is converted to logical 1 (true) and zeros are converted to logical 0 (false).

Algorithm 2:
Input:
- T1....TN: An array of 128 size
Output:
- K: 128-bit integer (Symmetric key)

Procedure GENERATE-SYMMETRIC KEY (T1..TN)

//Add the templates
T = T1+T2+T3+.....+TN

//generate 128-bit key
   K= logical(mod(T,2))

End Procedure GENERATE-SYMMETRIC KEY

Once Group Key is generated and if another user wants to join Group. The whole process of encryption is not repeated for new user. Directly add the user’s Encrypted cancelable template with combine Encrypted Cancelable template.

Algorithm 3:
Input:
- T: A Combine Encrypted Cancelable template of 128 size
Output:
K: 128-bit integer (Symmetric key)
Procedure GENERATE-SYMMETRIC KEY (T,Tₙ)

//Add the templates
New T = T + Tₙ

//generate 128-bit key
K= logical(mod(New T,2))

//Revocation Of User
New T= T-Tₓ(If X user is revocke)

End Procedure GENERATE-SYMMETRIC-KEY

3.1.6 Share Key
Once Symmetric Group Key is generated Group Owner Sends the Key to all user using any encryption algorithm

IV. EXPERIMENTS

4.1 Database:
In this work publicly available fingerprint database FVC 2002 DB1 is used to generate cryptographic key.

4.2 Experimental Setup:
This work is implemented with intel®Core™ i3 processor with 1,70GHZ clock speed in MATLAB17a running with Windows10OS

4.3 Experimental Results:
For this Example, Four different fingerprint images are taken as an input fingerprint of user. The minutia points or features are extracted from the fingerprint images. By applying Algorithm 1 mentioned above on the extracted minutia points the generate cancelable template values for user is as follows –

Cancelable template of User1 (T₁) :
8 -17 14 -34 -118 103 111 -104 -2 72 90 89 91 24 114 34 104 19 87 -82 41 -87 14 93 16 17 93 30

Cancelable template of User2 (T₂) :

Cancelable template of User3 (T₃) :

Encrypted Cancelable template of User1 :
148 23 255 230 400 458 358 230 243 458 23 230 384 75 230 243
319 230 243 400 75 384 230 400 400 230 243 63 23 230 212 230 243 458 63 230 458 63 230
Performance analysis of the proposed approach is shown in Figure 7. It is observed that as we increase the number of user it increases the time.
V. SECURITY ANALYSIS

In this approach, the encrypted cancelable template are transmitted over an insecure channel and hence they can be considered as public. Here both cancelable templates are hidden with the help of encryption. Thus, the attacker will not be able to extract cancelable templates. For example when the user sends its cancelable template to the group owner using group owner’s public key. The Group Owner after receiving the encrypted template decrypt it with its private key. So without the knowledge of the private key it is impossible for an attacker to get the cancelable template. In this proposed approach, User does not share their original fingerprint images or raw fingerprint features. They share the non-invertible cancelable templates of their fingerprints. The cancelable transformation used in our approach, is a one way transformation and there is no inverse transformation is possible. The cryptographic key is non-invertible and tracing any candidate fingerprint from the cryptographic key is not feasible. So the approach is free from fingerprint identity threat. The key can be generated by an attacker only when all cancelable templates are compromised. It is very difficult to compromise the all cancelable templates as they are transmitted over network after encoding. Whenever a cryptographic key is required to be updated, a new cancelable template is generated by changing the parameter of algorithm applied for generation of cancelable template. Every new cancelable template generates a new cryptographic key.[5]

VI. CONCLUSION

In traditional cryptographic approach, maintaining security of large key is important. The cryptographic keys are not linked with user, thus difficult to remember. This present work proposed an approach where the cryptographic key is generated using cancelable template of the user and generate group key. This Scheme also Support a dynamic group size.

References