CANCELABLE BIOMETRIC BASED KEY GENERATION FOR SYMMETRIC CRYPTOGRAPHY: SURVEY

ASWATHY MADHU[1], LASHMA K[2]

[1]M. Tech. Student, Computer Science and Engineering, Sree Buddha College of Engineering, Kerala, India.
[2]Assistant Professor, Computer Science and Engineering, Sree Buddha College of Engineering, Kerala, India.

Abstract - *In order to solve the problem of attacking the data, cryptographic algorithms along with key generation would be proposed. For symmetric cryptography the sender and the receiver uses the same key for encryption and the decryption process. Strength of the cryptography is based on the hardness of the keys that are used in the cryptographic algorithms. A key should be strong enough so that it is not easily guessable and not feasible to break within real times. Cryptographic keys can be generated by different methods. In this paper, Biometrics are incorporated with cryptography to create better security system. The cryptographic key is generated by using the fingerprint features of the user. Tracing any candidate biometric trait from the cryptographic key is not feasible. One of the problem with biometrics is that once it gets compromised it cannot be reused.*

Key Words: **Fingerprint Biometrics, Symmetric key cryptography, Cryptographic key generation.**

1. INTRODUCTION

These days, information travels so rapidly and the information to deal with is really huge too. So, information security is one of the biggest issues that are arising nowadays and thus cryptography is used to strengthen the fact that the volatile information does not fall into wrong hands. Cryptographic algorithms are divided into two types: symmetric key cryptography algorithms and asymmetric key cryptography algorithms. In symmetric key cryptography, the sender and the receiver uses same key to encrypt and decrypt the data with the help of encryption and decryption algorithms whereas in asymmetric key cryptography pair of keys are used private key and the public key. The public key is announced publicly and the private key is set as secret.

In a public-key encryption system, the public key is used for encryption process, while the private key i.e secret key is used for decryption process. Symmetric algorithms such that data encryption standard (DES), 3DES which use long keys of size 56 bit, 168 bits, advanced encryption standard (AES) uses 128,192 or 256 bits which make the user very difficult to keep in mind such a long key. To overcome these limitations, biometrics has been incorporated with cryptography to create better and robust security system.

In a crypto-biometric system, cryptography provides high level security whereas biometrics incorporates non-repudiation so that no need to carry passwords or tokens. Cryptographic key is generated from biometric traits of user and the biometrics traits can be fingerprints, iris, retina, palm print, speech, face etc and stored in the database so that it is not possible to reveal the keys without biometric authentication. Since the biometric trait used in key generation must be private; it should not tell anything about the user's biometric data. The biometric trait are fixed in a person and the key that is generated from the biometric trait is also fixed. So, if either the biometric trait or the cryptographic key is compromised anyway, it cannot be reused. Different transformation parameters are used in different applications to generate distinct transformed templates. Thus cancelable biometric can be revoked easily if compromised.

A cancelable template is generated from the original fingerprint template of both the communicating parties and the original template undergoes a one-way transformation so that it is not possible to recover from the cancelable template and the cancelable template is exchanged between them. The opposite communicating party by receiving the encrypted cancelable template from the other side first decrypts it and combined with its own cancelable template in order to generate a master template on both side. Then secret key is generated from master cancelable fingerprint template. Here the generated secret key is not necessary to store anywhere.

2. LITERATURE SURVEY

Various methods are used for generating the cryptographic keys. Some of them are discussed below:

2.1 A matrix formulation for NTRU cryptosystem

Rakesh Nayak et al. [2] suggest a method to generate the keys based on NTRU cryptosystem. In this system a pair of keys i.e both public and private key is generated. NTRU is the first public key cryptosystem that uses lattice-based cryptography to encrypt and decrypt data. NTRU uses truncated polynomials to generate public and private keys based on – Truncated Polynomial Ring Units R=Z[X]/(X^N-1)) and the basic tool is the reduction of polynomials with respect to two relatively prime moduli. First randomly choosing two matrices X and Y, User A creates a public/private key pair and keeps the matrices private, if anyone knows either one of them will be able to decrypt the messages sent to User A. Then computes matrix Xq as inverse of X modulo q and Xp as inverse X modulo p. And then he computes the product H = p* Xq *Y (modulo q) where p and q are the parameters. User A's private key is the pair of matrices X and Xp, and his public key is the matrix H. By using User A's public key H, User B can send a message to User A and for the encryption process User B first puts his message in the form of a binary matrix M, (which is a matrix of order as X and Y).To send a message M, User B chooses a random matrix R (which is of same order as matrix X), and User A's public key H to compute the matrix ,E = R*H + M (modulo q).The matrix E is the encrypted message which User B sends to User A and the decryption is the reverse of encryption process.

2.2 Classifying Iris Image Based on Feature Extraction and Encryption using Bio-Chaotic Algorithm

Rashmi M. Mhatre et al. [3] suggest a method to generate secret key based on iris image feature extraction. Iris image can be classified based on feature extraction algorithms like SIFT i.e Scale-Invariant Feature Transform. Macro features can be retrieved from the iris template using SIFT algorithm. Then the iris images are stored into the database undergoes SIFT feature extraction technique .Here, iris image is used in the form of binary patterns and then this binary data is divided into number of blocks and the Bio-Chaotic Algorithm is applied to that input image.

Firstly image is classified and one block is randomly selected to use as the secret encryption key. This key in return also encrypted using quantum cryptographic algorithm and the whole image is encrypted using the same key. The authorized user only knows about the random block then the encrypted image is send to the receiver through e-mail, so that decryption can be done securely at the receiver side. The bio-chaotic stream cipher is used to encrypt the iris images and store them securely using biometric key and bio-chaotic function. Bio –chaotic algorithm is used to encrypt the iris image. Here, the initial condition is applied to generate the secret key by using the LFSR method. An LFSR of length n over a finite field Pq consist of n stages (an-1, an-2, an-3,……., a0) with ai Є of Pq, and a polynomial.

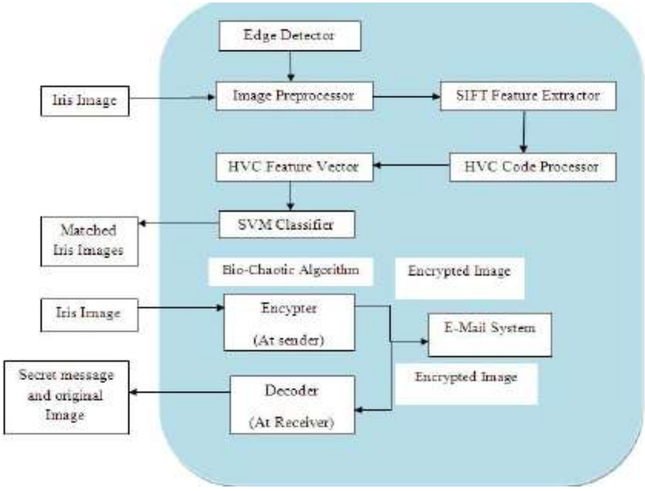

Fig -1: System Architecture

B(x) =1+c1x1+c2x2+…. + cnxn over Pq.

The secret key and iris template is X-ored simultaneously to generate the biometric key.

Biometric key=a1 xor b1, a2 xor b2,……., an xor bn.

And the generated Biometric key is then Xored with the other blocks of the iris template which encrypts the image in a way that no attacker can easily decrypt the image.

2.3 Fingerprint Based Symmetric Cryptography

Subhas Barman et al. [4] suggest a method to maintain the privacy of key by protecting it with users biometric from unauthorized access. In this method, a cryptographic key is combined with users fingerprint data. A string of binary number is extracted from fingerprint template and this binary number as cryptographic key is used to encrypt a message. In the traditional cryptography, key is stored somewhere else with a protection of user specified password. If the password becomes compromised in anyway by the attacker then the key also becomes compromised. For that, Biometrics is combined with traditional cryptography to improve the information security with a stronger cryptosystem, known as crypto-biometric system (CBS). In CBS, either cryptographic key is generated from biometric features of the user or key is protected using biometric data. Here, the key is generated from fingerprint template of user so that the user does not require to store or remember the key. As the key is generated from user's key, it can provide non repudiation to information security.

Fingerprint features are extracted from the fingerprint image of user A using feature extraction algorithm. Minutiae points are detected as features from the fingerprint image. Minutiae points are represented by the triplet of (x_i, y_i, Θ_i) where (x_i, y_i) is the coordinate values used as minutiae points and Θ_i is the alignment angle of minutiae points. The fingerprint template F_{TA} of user A is generated from the minutiae points. At last, fingerprint template F_{TA} is generated with zero and non-zero values and it is used to generate cryptographic key.

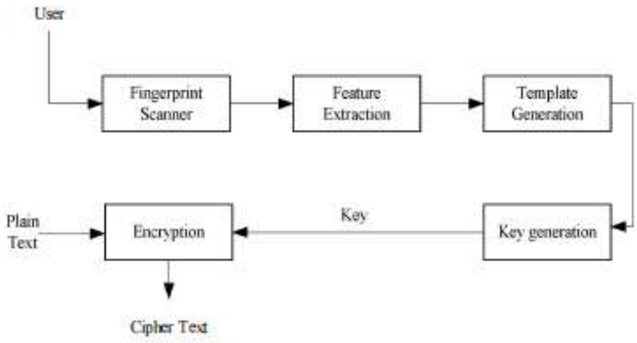

Fig -2: Key generation and message encryption process

The key generation steps are described below:

1. User A generates fingerprint template F_{TA} from fingerprint features.

2. User selects an element F_{TA} [i] of template and puts 0 or 1 in the same location of key (i.e., K[i]).

3. User puts 1 in the first location of key vector K (i.e. K[i] = 1).

4. User puts 0 at K[i] if F_{TA} = 0 (i.e., K[i] = 0) and puts 1 if $F_{TA} \neq 0$ (i.e., K[i] = 1).

This way, cryptographic key K is generated from fingerprint template F_{TA} .

2.4 Biometric Based Cryptographic Key Generation from Faces

B. Chen et al. [5] proposed a method which uses an entropy based feature extraction process and coupled with Reed-Solomon error correcting codes. So that it can generate deterministic bit-sequences from the output of an iterative one-way transform. Iterative, chaotic, and bispectral are the one-way transform employed by the system that accepts a one-dimensional vector input and is used to produce a magnitude and angle pair per iteration. The output can be converted to binary to form a very large bit matrix and these matrices are used to locate feature bits suitable to be used as part of the bio-key (*Borig*) using an entropy based criteria.

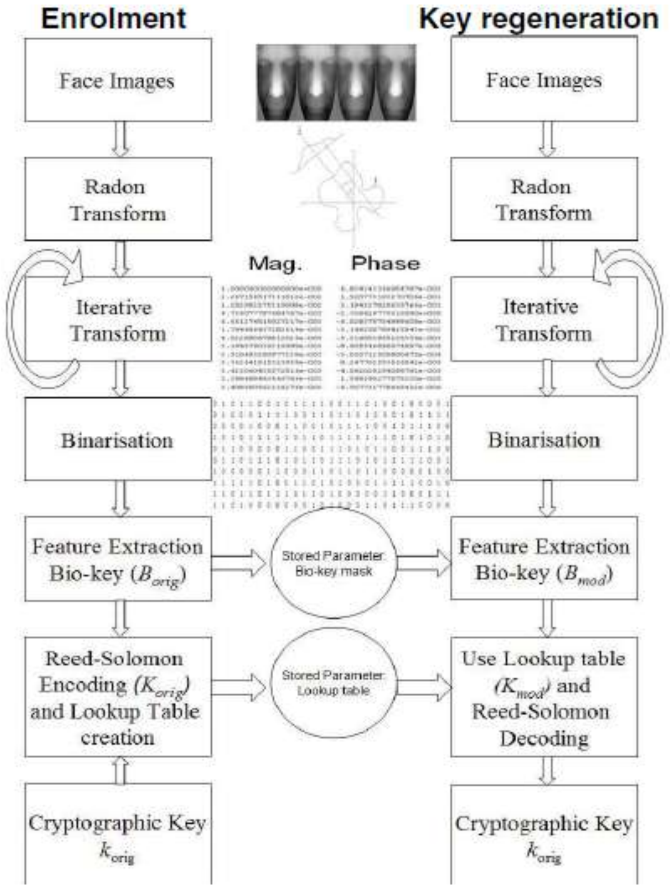
Enrolment
Key regeneration
Face Images
Radon Transform
Iterative Transform
Binarisation
Feature Extraction Bio-key (B_{orig})
Reed-Solomon Encoding (K_{orig}) and Lookup Table creation
Cryptographic Key k_{orig}
Mag.
Phase
Stored Parameter Bio-key mask
Stored Parameter Lookup table
Face Images
Radon Transform
Iterative Transform
Binarisation
Feature Extraction Bio-key (B_{mod})
Use Lookup table (K_{mod}) and Reed-Solomon Decoding
Cryptographic Key k_{orig}

Fig -3: Biometric cryptosystem flowchart

To create a lookup table, these bio-keys are then combined with the Reed-Solomon encoded version (*Korig*) of the protected cryptographic key (korig) and that can be used to regenerate korig given a slightly modified bio-key Bmod presented by the user in future. The technique is evaluated using 3D face data and produce keys of suitable length for 128-bit Advanced Encryption Standard (AES).

2.5 A Novel Algorithm towards Designing the Protocol for Generation of Secret key with Authentication in Collaboration (PGSAC)

Shyamasree Mukherjee et al. [6] proposed an authentication technique for new nodes to an ad-hoc network. Here, the request-reply messages are used to generate a secret key at the two ends. It also estimates the distance of a node from the power loss of a message from node. Based on this distance, both the sender and the receiver separately compute the same secret key. It does not use GPS and identifies location of nodes by distance and direction only.

If a new node S with cryptographic key K want to communicate with an existing node R in an ad hoc network by using this key K node S encrypt message and transmits to node R and the encrypted message by node R decrypted by S Using the same key k. This mechanism consists of two parts key generation and key management.

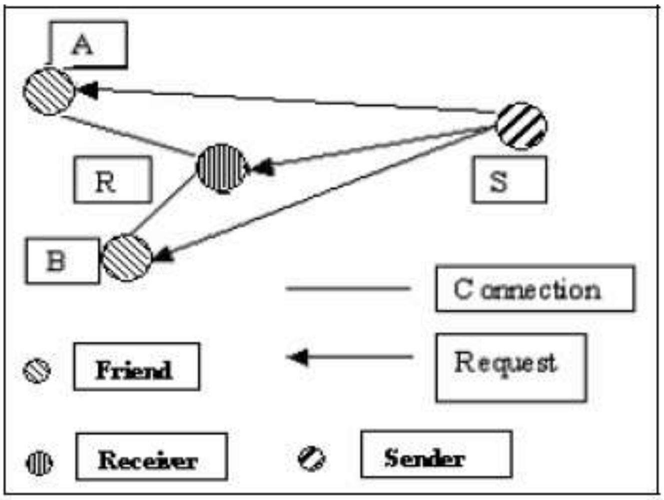

Fig -4: Trust model

Steps for key generation:

Step 1: New node S sends request signal to node R with power of the signal P1 and simultaneously S also sends request signal to friend nodes A and B with power P2 and P3.
Step 2: R can compute the power loss L1 and the distance D1 using the given equation.

$$D = (\lambda \sqrt{L}) / 4\pi$$

Step3: A can compute the power losses L2 and sends to R. Similarly B can compute the power losses L3 and send to R.

Step4: Using L2 and L3 node R computes the distance D2, D3 and arranges the distances in ascending order to have the key k.

Step5: A and B also send the same with power P2 and P3 and S can compute distances D1, D2 and D3 from power losses L1, L2 and L3 and S arranges the distances D1, D2 and D3 in ascending order and makes the same key itself without any key transmission.

2.6 Symmetric Key Algorithm Using Vernam Cipher : VSA

Bhagyashri K. Pawar et al. [7] suggest a method to achieve security measures for data and information. In this, cryptosystem consists of three algorithms: 1) key generation 2) encryption process 3) decryption process. The key generation is dependent on current system time. Different keys are generated at different instances therefore time is a major factor in this system. The key generation is done using public static long currentTimeMillis() method in java which makes the system more secure and at every start of the session the key will be different.

Steps for key generation:
Step1: Take current time in milliseconds.
Step2: Pass this time value to simple random number generator.
Step3: Calculate its absolute value
Step4: Generate Key1.
Step5: Take next instant of system's time
Step6: To generate Key2 follow step2 & 3.

For every message a new pair of keys is generated therefore this system achieves a high level of secrecy as the system is symmetric which makes the proposed cryptosystem more unique.

3. CONCLUSION

The literature survey could fetch a number of different methods to generate the cryptographic key. The limitations of the existing methods are: key is stored somewhere else with a protection of user specified password, if the password becomes compromised in anyway by the attacker then the key also becomes compromised. For that, Biometrics is combined with traditional cryptography to ensure better security systems. Here the cryptographic key is strongly linked with the fingerprint traits of the user and the key is generated using cancelable fingerprint template of both the communicating parties at their sites. This cryptographic key is not required to be remembered and also not required to be stored.

REFERENCES

[1] A. Sarkar and B. K. Singh, "Cancelable biometric based key generation for symmetric cryptography," *2017* International Conference on Inventive Communication and Computational Technologies (ICICCT)*,* Coimbatore, 2017, pp. 404-409.

[2] R. Nayak, C. V. Sastry and J. Pradhan, "A matrix formulation for NTRU cryptosystem," 2008 16th IEEE International Conference on Networks*,* New Delhi*,* 2008*,* pp. 1-5.

[3] R. M. Mhatre and D. Bhardwaj, "Classifying Iris Image Based on Feature Extraction and Encryption Using Bio-Chaotic Algorithm (BCA*),"* 2015 International Conference on Computational Intelligence and Communication Networks (CICN)*,* Jabalpur*,* 2015, pp. 1068-1073.

[4] S. Barman, S. Chattopadhyay and D. Samanta, *"*Fingerprint based symmetric cryptography*,"* 2014 International Conference on High Performance Computing and Applications (ICHPCA), Bhubaneswar, 2014, pp. 1-6.

[5] B. Chen and V. Chandran, "Biometric Based Cryptographic Key Generation from Faces," 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications *(*DICTA 2007*)*, Glenelg, Australia, 2007, pp. 394-401.

[6] S. Mukherjee, S. Choudhury, N. Chaki and D. Mukhopadhyay, "A Novel Algorithm towards Designing the Protocol for Generation of Secret-Key with Authentication in Collaboration (PGSAC)," *2007* International Symposium on Information Technology Convergence (ISITC 2007)*,* Joenju*,* 2007, pp. 353-327*.*

[7] S. S. Hatkar and B. K. Pawar, "Symmetric key algorithm using vernam cipher: VSA*,"* 2016 International Conference on Inventive Computation Technologies (ICICT)*,* Coimbatore*,* 2016*,* pp. 1-5.