ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(22), DOI: 10.17485/ijst/2016/v9i22/95288, June 2016* ISSN (Online) : 0974-5645

Biometrics as a Cryptographic Method for Network Security

Kumar Ankit and Jayaram Rekha

Department of Information Science and Engineering, Dayananda Sagar College of Engineering, Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru - 560078, Karnataka, India; shah.ankit456@live.com, rekhajayaram20@gmail.com

Abstract

Background: Cryptography is considered as an effective method for secure transmission of data but falls prey to network attacks. The proposed biometrics-based Encryption/Decryption Scheme uses fingerprints to generate a unique key. **Methods:** The presented technique combines portions of fingerprint of the sender and the receiver to generate a random sequence, which is used as a public-key for Encryption as well as Decryption. The key thus generated is distinct as it is watermarked with sender's biometric signature. The encrypted message is then sent to the receiver along with the key. The receiver uses this key to decrypt the message to plain text. **Findings:** This system has a significant advantage as there is no requirement for the asymmetric key to be stored in a protected place, thus reducing the security threats to the minimum. The fingerprint is an inherent trait of every individual and is distinct. Hence billons of unique keys can be created, making it very hard for an attacker to guess the key. **Applications:** The biometric based system significantly increases the power of traditional crypto-systems.

Keywords: Biometrics-based System, Distinct, Encryption, Fingerprint, Network Attacks

1. Introduction

With the exponential increase in information exchange over the past few years, reliable transmission and storage of sensitive data has become a vital aspect of network security. Data as it traverses a network is at its most vulnerable state as it is a very easy target for any attacker present in the network. A passive attack such as Masquerading or sniffing through a network can easily give away critical data being transferred. For Secure transmission of data over an unsecured channel, cryptography is considered as the most effective method. Cryptography has been in existence for thousands of years, from Egyptian hieroglyphics to enigma machine and on to the 21st century. Information sent over any open network must be encrypted in order to make it incomprehensible for everyone else other than the intended receiver, and this is exactly what cryptography does. It is the process of converting plain text i.e. the readable text, into cipher text i.e. unreadable or encrypted text. Cryptography can be used on data that people or organizations want to keep private or data that should be accessible to only certain users. In other words, cryptography is hiding of message content from unintended/unauthorized users. Cryptographic encryption is done on the sender's side when the data is to be sent over the network. At the receiver's end, the process of decryption is initiated as soon as the cipher text is received[1]. But the flaws in algorithmic encryption techniques are a gateway for attackers who can decrypt the data packets traversing a network by the use of automated tools[2]. A cryptographic technique when combined with biometric encryption approach is the new world answer to network and data security problems. Biometrics is the unique characteristics of a person which differentiates him/her from the others. A person's identity can be verified by the use of such techniques.

2. Encryption

Modern cryptographic techniques uses encryption algorithms to encrypt data, banking transactions, online web transactions, wireless communications etc. An

* *Author for correspondence*

encryption algorithm is a combination of a mathematical function and a key. The algorithmic function's strength and the key's secrecy determine how secure the encrypted data is. In most cases, the algorithm isn't the secret; it's known to the public. The secret is the key. Values taken from the allowable keyspace arranged in a random sequence forms the keys for encryption/decryption. The number of randomly sequenced keys that can be derived from a keyspace depends on the size of the keyspace[2,3]. There are two broad categories of such cryptosystems based on the level of security they offer. These are Symmetric and Asymmetric encryption techniques. The following sections explain both of these in details.

A. Symmetric Encryption

The oldest and best-known technique used in cryptography is the Symmetric Encryption technique[4]. Cryptosystems that make use of this technique maintains a single key for both encryption and decryption processes. The sender encrypts the message he/she wants to send with a secret key, and the receiver having a copy of the same key, decrypt the message. The secret key can be anything such as a number, a special character, a word or just a sequence of random characters and is used to change the plaintext, to be sent to the receiver, in a particular way[5]. If the sender wants to encrypt a different message and send it to another receiver, a different secret key must be used. Same way as the number of receivers and messages in the equation increases, so does the number of secret keys, this becomes a big problem for the sender. Another problem with secret keys is how to send one to the receiver decrypting the message[1]. Although the problems stated above are a risk for data security, the symmetric encryption mechanisms are swift and can be used to encrypt large blocks of data. There are two types of symmetric algorithms currently in use: Stream ciphers and block ciphers. Regardless of the algorithms used, symmetric encryption techniques rely on one and the same key to encrypt and decrypt data as represented in figure 1.

B. Asymmetric Encryption

Although offering a high level of security, symmetric encryption fails to provide any secure means of key exchange which has to be done over a network posing a risk of being sniffed while being transferred[5]. One answer to this problem is asymmetric encryption. As represented in figure 2, instead of a single key, asymmetric algorithms use two mathematically related keys, known as a key pair, such that one key is used for encryption and decryption is only possible by applying the second key. The Asymmetric Encryption approach uses a public key, known to everyone, to encrypt the message and a private key, known only to the intended receiver, to decrypt the message. Public key encryption done on a plaintext message or data by the use of an algorithm can only be decrypted by the paired private key known only to the receiver, by applying the same algorithm[4].

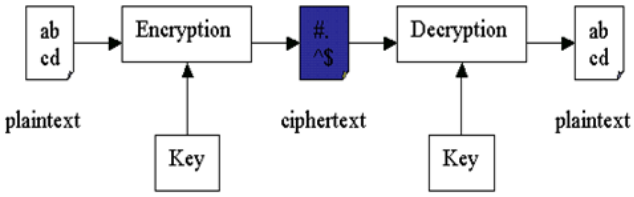

Figure 1. Symmetric Encryption and decryption using a single key[10].

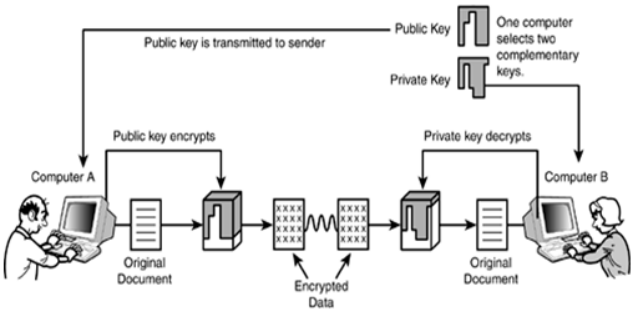

Figure 2. Asymmetric Encryption and decryption scheme[11].

This solves the problem of sharing the key with the receiver as it is supposed to be public. This technique however faces the issue of being slower as compared to symmetric encryption[6,7]. Both the encryption as well as decryption processes require much greater processing power. Some of the asymmetric key algorithms include RSA, Diffie-Hellman, Digital Signature[4].

3. Biometric Crypto Systems

Although effective in secure transmission of data over an insecure channel, Cryptography has significant drawbacks. The encrypted message is based on key rather than user authenticity. For powerful encryption, the length of the keys used for encryption and decryption

becomes quite large. But still these keys can be guessed or cracked by simple dictionary attacks. Moreover, the maintenance and sharing of such lengthy and random keys becomes a critical problem in cryptography systems. These problems are well tackled by using Biometric Cryptosystems[4,8]. The integration of biometrics with cryptographic algorithms yields a much powerful system known biometric cryptosystem. It involves the use of both the fields to strengthen the encryption scheme. Such systems take advantage of cryptographic level of security along with the uniqueness of the biometric traits of the user. Biometrics eliminates the need to remember the key or even its exchange over an open network. In such a system, the key generation process involves the use of a biometric trait of the user (generally fingerprint or iris) and is stored in a database accessible to both the sender and receiver, secured by another level of biometric authentication[5,9]. One of the huge merits, which also is a demerit, of the system is the uniformity of biometric template or data over time. As the biometric traits are inherently unchangeable, when compromised the same is non revocable by the owner making them unusable and potentially threatening. This results in the biometric data to become permanently useless. To revoke the irrevocable biometric template, a cancellable transformation of the same is needed. This would tackle the problem of a compromised template. It also ensures no leakage of information regarding the original template and the privacy of biometric data. The remote usage of the biometric data requires it to be transmitted over an unsecured channel (such as the internet), hence there is a need to generate revocable cryptographic key from the biometrics of two different users[10]. This transform method results in the biometric data that in unrecoverable by any unauthorized user or an attacker.

The focus of this paper is the generation of cryptographic key using fingerprint as the biometric of choice without compromising the privacy and security involved in the key generation process.

4. Fingerprint Analysis

Each finger has a distinct pattern and is different from the rest of the fingers. This is a permanent and unique feature of a person[11]. Although the patterns on each finger looks dissimilar to the naked eye based on the difference in design pattern of the ridges, through intensive researches in the field, Minutia (abnormal points on the ridges as shown in Figure 3) are shown to be the distinguishing factor rather than the ridges and the furrows. Termination, the immediate ending of a ridge[8,12] and bifurcation, the origin points of two branches of the ridge are among the variety of minutia types and the most significant and prominently used. The general shape of the fingerprint is generally used to pre-process the images. These prints are divided into 3 classes i.e. Loop, whorl and arch.

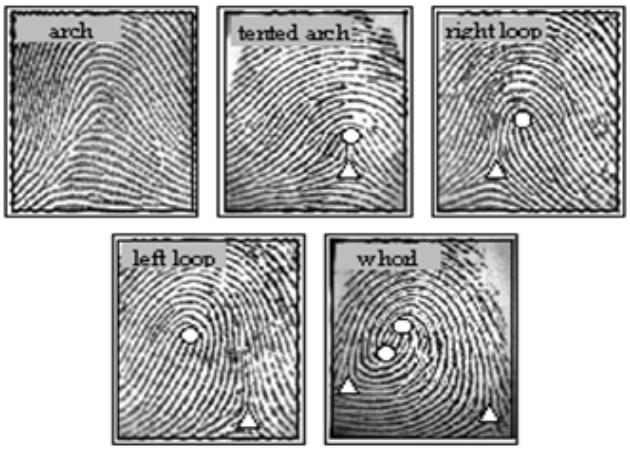

Figure 3. Fingerprint classes.

5. Unique Feature of Fingerprints[11]

- Each fingerprint is unique to individuals i.e. no two fingers have identical ridge characteristics.
- Majority of the population have readable fingerprints hence they are universal in nature.
- They are distinct and hence highly reliable in identifying a person.
- They remain structurally unchanged throughout and individuals lifetime.
- Accuracy in distinguishing people makes fingerprints the most widely used form of biometrics.

6. Cryptographic Key Generation from Biometrics

An irrevocable cryptographic key generation scheme is proposed through the following algorithm. Its efficiency lies in its ability to generate the key from the extracted minutiae points of the fingerprint biometrics[13]. The minutiae point extraction technique makes use of a matrix to represent the scanned image of the fingerprint.

The matrix contains information regarding the number of ridges and furrows; thus each element in the matrix is a set of number of ridges and furrows in a small region of the scanned fingerprint image.

A. Extracting Minutiae Points

This is a three-stage approach as given below[5]:

- Preprocessing – The initial stage of scanning the fingerprints using a fingerprint scanner so as to upload a digital copy of it onto the computer for further processing.
- Minutiae Extraction – The digital copy of the scanned fingerprint is processed to extract the minutiae point. Ridge and Furrows are used in this proposed system because of their distinct characters.
- Post processing – Ridge thinning required for minutiae recognition constitutes the final stage.

B. Binarization of the Scanned Fingerprint

The scanned fingerprint produces an 8-bit grayscale image. This image requires transformation to a 1-bit image for digital processing where the pixel representing a ridge point is assigned 0 and furrow pixels are assigned 1 as shown in Figure 4. The binarization technique transforms the scanned digital image of the fingerprint to machine interpretable values. Such a method checks each pixel value and compares it to the mean intensity value; if found greater, changes the pixel value to 1[5,9].

Figure 4. Fingerprint before and after binarization.

C. Minutiae Points Extraction

Skeletons are the set of connected lines of the ridges having unit width. For the preservation of ridge topology and connectivity, the process of thinning is applied. Ridge thinning process identifies the ridges of pixel width one (skeletons) by repetitive erosion. After the process of binarization and thinning, the minutiae are determined by the use of 3x3 pattern masks. Although the process seems to be simple, there are chances of false detection of minutiae which requires necessary elimination. A successful extraction of minutiae then requires storage which is done in a template. The minutia position, direction (i.e. angle) and type (i.e. bifurcation/ termination) are some of the attributes included in the template[12].

D. Key Generation

In the following section, a key generation system is depicted based on the algorithm using minutiae points[1,14]. Inspired by number of related researches in the field of cryptography and cancellable biometric techniques, the algorithm proposed is represented below. The same is represented in Figure 5.

Algorithm Assumptions:
Mp → Minutae point set
Kl → Key Length
Np → Size of minutae point set
S → Seed value
Sl → Seed limit
M → (x, y) coordinate of a minutae point
Kv → Key vector

Steps involved:
Step 1: Representation of the minutiae points extracted:

$$Mp\ \{mi\}i = 1.....Np \quad (1)$$

Step 2: Definition of the key vector (initial):
Kv = {xi : p(xi)} where, i = 1 ... Kl

$$p(x) = Mp[I\ \%\ Np] + Mp[(i + 1)\ \%\ Np] + S \quad (2)$$

Step 3: The changing values of S is given as follows where the initial value equals the number of minutiae points:

$$S = Kv(i)\ \%\ S1,\ -1 < i < Kl \quad (3)$$

Step 4: Conversion of the key vector (Kv) to a matrix Km of size $\frac{Kl}{2} * \frac{Kl}{2}$ as follows:

$$Km = \frac{(aij)Kl}{2} * \frac{Kl}{2} \quad (4)$$

Step 5: Generation of the key vector (intermediate):
KIV = {Ki : (m(K_i)} where, i = 1.... .....Kl,

m(k) = |Aij|, Aij = Km i, j : i + sizw, j + siz _,

$$-1 < i < \frac{Kl}{2} \quad (5)$$

Note: The submatrix Aij is generated from the key matrix

Step 6: Generation of the private key (final key vector):

Kv = 1, if KIV[i] > mean (KIV), else 0 (6)

Although no two fingerprints are similar, there are chances of having the number of ridges equal to the number of furrows. Hence a NXN matrix is used that precisely stores each furrows and ridges marking in the byte pattern accordingly to the scanned image. This distinctly identifies individual fingerprints as the data in the matrix form will have different patterns of data set[5,15].

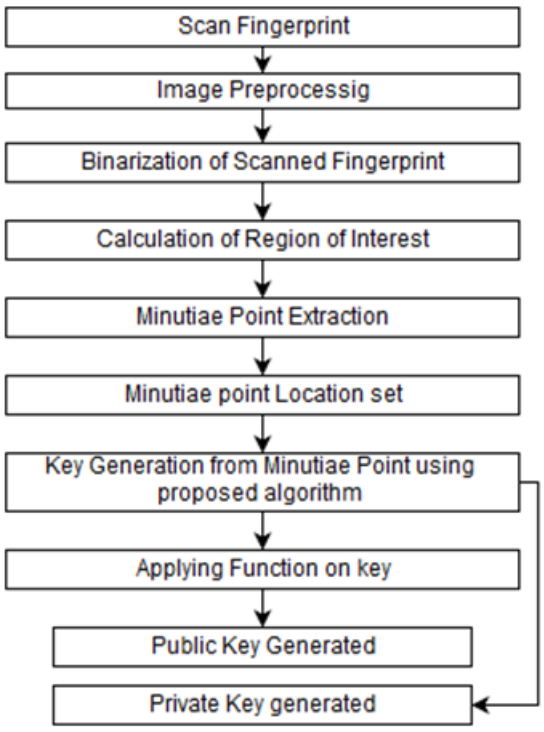

Figure 5. Key generation process.

Hence the public key is calculated based on the data set as shown below:

Assumptions:
d → the total number of 1's (furrows)
in the submatrix A_{ij},
e → the total number of 0's (ridges)
in the submatrix A_{ij},
i,j → 1, 2.....Np

s = (d - e) (7)

Pb = Kv * (mod(s)) * e (8)

e → Public key vector

Thus the key generated using the above mentioned algorithm generates both public and private key using minutiae points of an individual's fingerprints. Further, a technique similar to that of RSA algorithm can be incorporated that uses the key-pair generated rather than the traditional approach based completely on the algorithm to compute the key-pair.

On the basis of the experimental results, it may be inferred that an attacker, in case of a biometric cryptosystem, will be unable to generate a similar but fake key without having the complete knowledge of the algorithm generating the key and the fingerprints of both the sender and the receiver[10].

7. Results

The operations Time in secs for the algorithm proposed here is as given:
Feature extraction of biometric template took about **0.05** seconds.
Generation of a template from the extracted biometric took **0.002** seconds
Encoding and decoding of the template into a function that is used for key generation used **0.15** seconds
The Cryptographic public/private key generation - **0.002** seconds
Resulting in the total time required for the entire operation of **0.204** seconds.

8. Future Work

With the increasing need for secure transmissions over unsecured channels, the real world application of biometric cryptosystem or the integration of biometrics into traditional/legacy cryptographic systems has become crucial. The use of such a system which is a combination of biometrics and cryptographic algorithms provides much better security and privacy over traditional systems.

The soft biometrics uses behavioural characteristics of a user which cannot be replicated by attackers[5]. Future enhancements of such a biometric cryptosystem concentrate on the economic development of the system that ensures security over any network or communication medium.

9. Conclusion

A biometric cryptosystem is proposed in this paper which is more powerful and provides a better secures approach to encryption and decryption methodologies by using a key-pair generated from fingerprint impressions. The Encryption scheme that may be further adopted can be the RSA encryption algorithm because of the similarities in the key-pair application towards encryption and decryption[6,14]. The uniqueness of the proposed system lies in the distinctiveness of the generated keys that are completely based on the fact that human biometric traits are individually distinct and thus provide a much better approach towards securing the message passed over an unsecured or open transmission.

10. References

1. Chandra Sayani, Paul Sayan, Saha Bidyutmala, Mitra Sourish - Generate an Encryption Key by using Biometric Cryptosystems to secure transferring of Data over a Network. IOSR Journal of Computer Engineering.
2. Michael T Simpson. Hands-on ethical hacking and network security. India: Cengage Learning Publications. 2012.
3. Cryptography in VB.NET.. Date accessed: 10/09/2015: Available from: http://www.c-sharpcorner.com/cryptography-in-VB-Net-part-1.
4. Encryption key generation. Date accessed: 05/08/2015: Available from: http://www.slidesearch.org/slide/d01211622 .
5. Biometric Cryptosystem. Date accessed: 12/08/2015: Available from: http://www.academia.edu/4814389/D01211622.
6. Barman Subhas, Samanta Debasis and Chattopadhyay Samiran. Fingerprint-based crypto-biometric system for network security EURASIP. Journal on Information Security. 2015 April; Doi: 10.1186/s13635-015-0020-1.
7. Processing Standards Publication: Announcing the ADVANCED ENCRYPTION STANDARD (AES) – Federal Information. 2001 November 26; 197.
8. Soutar Colin, Roberge Danny, Stoianov Alex, Gilroy Rene and Vijaya Kumar BVK. Biometric Encryption™. McGraw-Hill publications: In: ICSA Guide to Cryptography. 1999; Ch-22.
9. Mahalakshmi U, Shankar Sriram VS. An ECC Based Multibiometric System for Enhancing Security. Indian Journal of Science and Technology. 2013 Apr; 6(4). Doi: 10.17485/ijst/2013/v6i4/31857.
10. Fingerprint-based crypto-biometric system. Date accessed: 06/08/2015: Available from: http://www.jis.eurasipjournals.com/content/2015/1/3.
11. Nagati Khaled. LAP Lambert Academic Publication: Contribution to the Solution of Fingerprint Identification Problem: 2012 April.
12. Understanding Biometrics. Date accessed: 12/09/2015: Available from: http://www.griaulebiometrics.com/en-us/book/understanding-biometrics/types/feature-extractio/minutiae.
13. Ratha NK, Chikkerur S, Connell JH, Bolle RM. Generating Cancellable Fingerprint Templates. IEEE Trans. Pattern Anal. Mach. Intell. 2007; 29(4):561–72.
14. Balakumar P and Venkatesan R. Secure Biometric Key Generation Scheme for Cryptography. International Journal on Computer Science and Engineering. 2010; 02(06):1992-95.
15. TCP/IP tutorial. Date accessed: 07/10/2015: Available from: http://www.yaldex.com/tcp_ip/0672325659_ch20lev1sec1.html.
16. Fingerprint Verification Competition FVC2002. [Online] Available from: http://bias.csr.unibo.it/fvc2002.