IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

NCAIT 2017

JSS Academy of Technical Education

Vol. 4, Special Issue 8, May 2017

Application of Biometrics and Fingerprint Analysis in Cryptography

Shobitha Kudva[1], Vidya Ratan[1], Dr. D.V.Ashoka[2]

UG Student, Department of Information Science and Engineering, JSSATE, Bengaluru, India[1]

Professor, Department of Information Science and Engineering, JSSATE, Bengaluru, India[2]

Abstract: When we think of secure transmission of information, the term Cryptography comes to our mind. By using various encryption algorithm, decryption algorithm, key generation algorithm and key matching algorithm cryptography ensures secure transaction of information between the sender and the receiver without the intrusion of an attacker. In this paper primarily cryptography is merged with fingerprint recognition technology which is one of the main forms of Biometrics. Here an inherent biometric characteristic like fingerprints are used to generate the key. So it is more secure compared to symmetric encryption where a lot of care has to be taken in storing the key in a secure place. To put this concept into effect, we use the sender's fingerprint geometry for the generation of the key. On the receiver's side, database of the sender's fingerprint images will be present through which the decryption process takes place using fingerprint matching algorithms. This algorithm is applied on the binary conversion of the fingerprint images and this whole method is applicable on the binary form.

Index Terms: Cryptography, Encryption, Decryption, Key generation, Biometrics, Fingerprint geometry.

INTRODUCTION

Cryptography is the method of introducing secrecy in information security by concealing the messages such that only the intended recipient gets the information. [1] With the exponential rise in information exchange from the past few years there is a vital need for the use of cryptography. The art of Cryptography is considered to be born along with the art of writing. [1] It has been in existence since the Roman and Egyptian civilizations that used techniques like Hieroglyph which used a secret code to send the messages. Nowadays information sent on the internet is vulnerable to intrusions. So in Cryptography, for data transfer the plain text is encrypted into a cipher text using encryption process. Then using the key or information the receiver would decrypt the cipher text back into plain text. People or organizations can use this technique to keep the information private and to be accessible by only the intended/authorized users. But if there are flaws in the algorithmic encryptions or if the key is obtained by the attackers then the private information is easily decrypted and misused. The integration of biometrics with cryptographic algorithms yields a much powerful system. Biometric technology uses a physical or psychological trait for identification and authentication. [2]

TRADITIONAL ENCRYPTION

Encryption is the most effective way to achieve data security. To read an encrypted file, there must be access to a secret key or password that enables us to decrypt it. Unencrypted data is the plain text and encrypted data is referred to as cipher text. On the sender's side encryption is done when the data is sent over the network and on the receiver's side decryption is done on the received cipher text. Fundamentally, there are two types of cryptosystems based on the manner in which the encryption-decryption is carried out in the system. [1]

- Symmetric Key Encryption
- Asymmetric Key Encryption

The main distinction between these cryptosystems is the connection between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is almost impossible to decrypt the cipher text with the key that is not linked to the encryption key.

Symmetric Key Encryption

This is the encryption process where same keys are used for both encrypting and decrypting the information. The features of this type of encryption is that both the sender and the receiver share a common key prior to information exchange and a robust mechanism needs to be present to exchange the key between the communicating parties as the keys are required to be changed frequently.

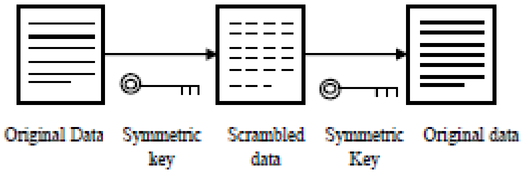

Figure 1: Symmetric Key Encryption

Length of the key is smaller hence and therefore encryption-decryption processes are faster and the processing power of the system required to run the symmetric algorithm is less. But before initiating communication key establishment must be done where both the parties agree upon a secret key. And since this secret key vital in the encryption-decryption process a mechanism must be present for secure key establishment. [1]

Symmetric Key Encryption

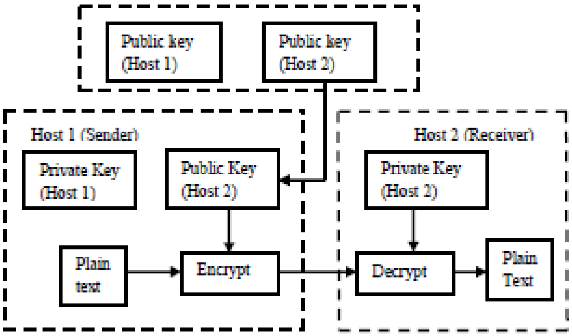

Figure 2: Asymmetric Key Encryption

Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. In this system every user has a pair of dissimilar keys called the private key and the public key. These keys are mathematically related − when one key is used for encryption, the other can decrypt the cipher text back to the original plaintext. It requires putting the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called Public Key Encryption. Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is strength of this scheme. When Host1 needs to send data to Host2, he obtains the public key of Host2 from repository, encrypts the data, and transmits. Host2 uses his private key to extract the plaintext. [1]

BIOMETRIC CRYPTO SYSTEMS

Although Cryptography is useful in transmitting data over an insecure channel it has certain drawbacks. The main drawback is that the privacy of the data transmission depends only on the secrecy of a key. Thus if the key is revealed the data is compromised. Also the length of the keys being shared and maintenance of the keys becomes a critical problem in cryptography systems. All these problems can be efficiently solved by using Biometric Cryptosystems. [11] Here the field of Biometrics and Cryptography are combined to profit from the strength of both fields. In these systems while cryptography provides high security levels, biometric brings in non repudiation and eliminates the need to remember passwords.[3] Instead of storing cryptographic keys, keys will be generated dynamically with the help of biometrics to secure the template and biometric system.[3] Biometric authentication offers new mechanism for key security and acts as a better alternative for password protection by using a biometric to protect the cryptographic key. Instead of entering a password to access the cryptographic key, the use of this key is guarded by biometric authentication. When a user wishes to access a secured key, he or she will be prompted to allow for the capture of biometric sample. . If this verification sample matches the enrollment template, then the key is released and can be used to encrypt or decrypt the desired data. Thus, biometric authentication can replace the use of passwords to secure a key. This offers convenience, as the user no longer has to remember a password and secure identity confirmation, since only the valid user can release the key. [3] Biometric cryptosystems (BCSs) are designed to securely bind a digital key to a biometric or generate a digital key from a biometric. [4]

FINGERPRINT BIOMETRICS

A fingerprint is the pattern of ridges and valleys on the surface of a fingertip. [5] Each person has a unique fingerprint. A fingerprint is made of a number of ridges and valleys on the surface of the finger. Minutiae-based representation has become extensively used fingerprint representation scheme due to its distinctiveness, compactness, and compatibility with features used by human fingerprint experts. The uniqueness of a fingerprint is entirely determined by the local ridge characteristics and their relationships. The ridges and valleys in a fingerprint alternate, flowing in a local constant direction. The two most prominent local ridge characteristics are: 1) ridge ending and, 2) ridge bifurcation. A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. Collectively, these features are called minutiae. [5]

PROPOSED METHODOLOGY

Cryptography with biometric authentication is capable of managing any type of failure handling, enhances the speed limit and false reading handling. The whole cryptographic technique (Encryption process as well as decryption process) has been developed with the help of fingerprint geometry, the current forerunner of biometric authentication. The entire process has been examined in the following steps, starting from sender's side encryption process to receiver's side decryption.

Steps at Sender's side

Step 1**:** At sender's end, the binary format of the normal text is taken as plain text.

Step 2**:** The plain text is encrypted by encryption process, from which we will get the encrypted text and some information.

Step 3: This information is combined with the binary form of sender's recent fingerprint geometry for key generation.

Step 4**:** The encrypted text along with the key generated is sent by the sender to the receiver side. [6]

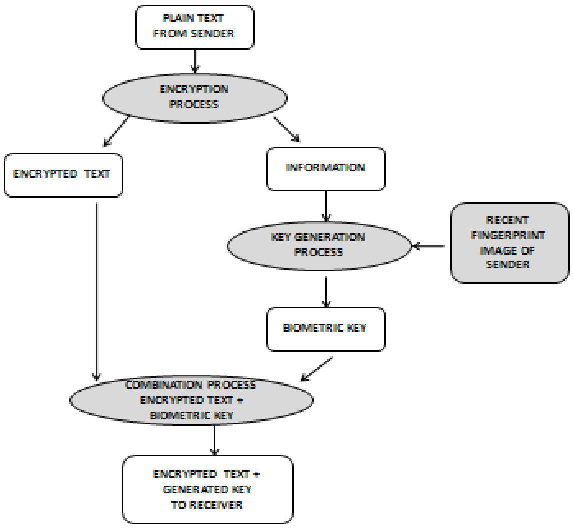
PLAIN TEXT FROM SENDER
ENCRYPTION PROCESS
ENCRYPTED TEXT
INFORMATION
KEY GENERATION PROCESS
RECENT FINGERPRINT IMAGE OF SENDER
BIOMETRIC KEY
COMBINATION PROCESS ENCRYPTED TEXT + BIOMETRIC KEY
ENCRYPTED TEXT + GENERATED KEY TO RECEIVER

Figure 3: At Sender's Side

Steps at Receiver's side

Step 1: At receiver's end, the encrypted text along with the key is accepted by the receiver.

Step 2: The encrypted text and the key are separated.

Step 3: Using the sender's database fingerprint geometry (which is maintained by the receiver) and the fingerprint geometry matching algorithm, the information is abstracted from key. If the two images do not match, the information cannot be received.

Step 4: With the help of the information, the encrypted text is decrypted into plain text or in the original binary form of the plain text or normal text. [6]

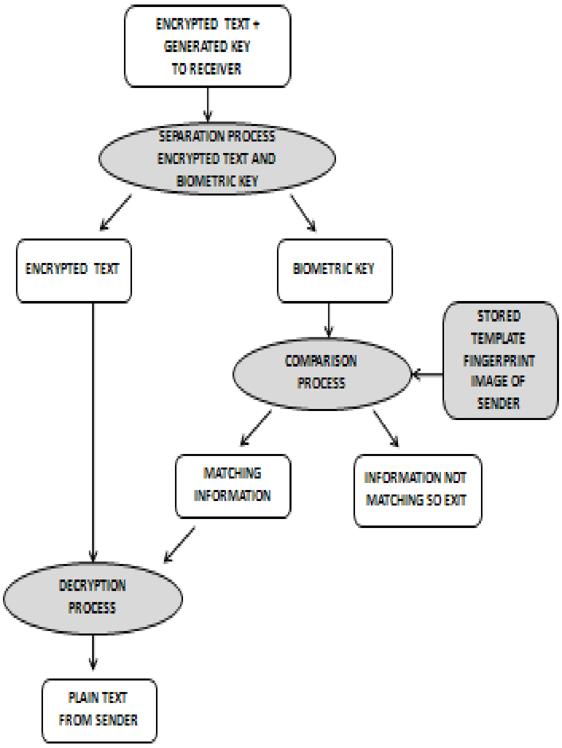
ENCRYPTED TEXT + GENERATED KEY TO RECEIVER
SEPARATION PROCESS ENCRYPTED TEXT AND BIOMETRIC KEY
ENCRYPTED TEXT
BIOMETRIC KEY
COMPARISON PROCESS
STORED TEMPLATE FINGERPRINT IMAGE OF SENDER
MATCHING INFORMATION
INFORMATION NOT MATCHING SO EXIT
DECRYPTION PROCESS
PLAIN TEXT FROM SENDER

Figure 4: At Receiver's side

Cryptographic key generation

The biometrics feature for cryptographic key generation selected is fingerprint. Minutiae points from the fingerprint are extracted and that point set is used for generating cryptographic key.

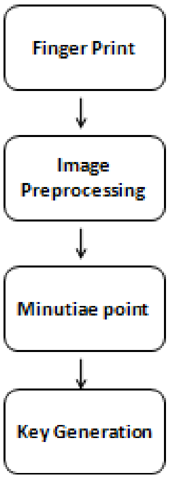

Figure 5: Steps in Key generation

Image preprocessing

For image preprocessing, first, Histogram Equalization and Filters are used to enhance the image. Then Binarization is applied on fingerprint image. Finally, Morphological operation is used to extract Region of Interest.

Histogram equalization

Histogram equalization is a technique for adjusting image intensities to enhance contrast. [9] It boosts the contrast of images, especially when usable data of the image is represented by close contrast values. It allows pixel value to expand with pixel intensities ranging from 0 to 255 which will enhance visualization effect.

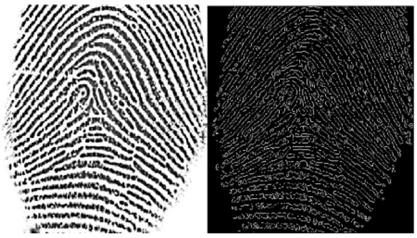

Figure 6: Sample Finger Print before and After Histogram Equalization

Region of Interest

The steps involved in Region of Interest are Binarization and Morphological operation.

Binarization

There are only two levels of interest that all minutiae extraction algorithms function on binary images: the black pixels which represent ridges, and the white pixels which represent valleys. Binarization is the process that translates a grey level image i.e., a pixel image into a binary image. This intensifies the contrast between the ridges and valleys in a fingerprint image, and accordingly makes the extraction of minutiae feasible. Hence, Binarization process involves analyzing grey level values of each pixel, where a global threshold is chosen by classifying all pixels with values above this threshold as white, and all other pixels as black. [10] If the values are greater than the global threshold, set binary value as 1 else 0.

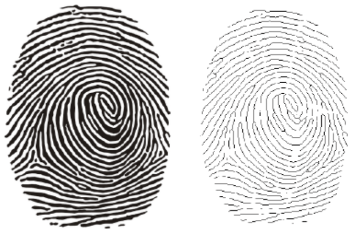

Figure 7: Finger print before and after binarization

Morphological Operation

Morphological operations are used to understand the structure or form of an image by identifying objects or boundaries within an image. They are performed on binary images where the pixel values are either 0 or 1, where a value of zero is black and a value of 1 is white. While most morphological operations focus on binary images, the result of this approach is tightly bounded region just containing the bounded inner area. Binary morphological operators are applied on binarized fingerprint image. The unnecessary spurs, bridges, line breaks are removed by these operators. Thinning process is performed to reduce thickness of lines. [8]

Minutiae Points Extraction

Thinning removes the redundant pixels of ridges till the ridges are just one pixel wide. Ridge thinning algorithm is applied and in each scan of full fingerprint image, the algorithm marks down unnecessary pixels in each small window and finally eliminates all those marked pixels after numerous scans. After fingerprint ridge thinning minutiae points are marked easily.

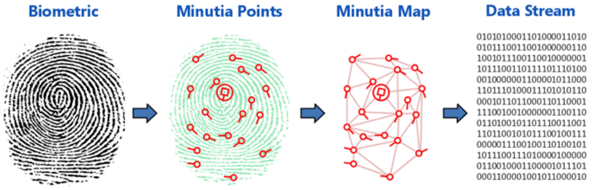

Figure 8: Minutiae Points Extraction

Matrix & key generation:

The key generation algorithm is as follows Extracted minutiae points co-ordinates are maintained in a vector

M_p- Minutiae points set
S_p - Size of M_p
KL - Key length
K_v - Key vector
L_k - Length of key vector
Z - (X, Y) co-ordinate of a minutiae point

```
Step1: Read the Minutiae points
Step2: Find the point H with highest x+y
Step3: Draw a line from origin (0, 0) to the H and call it as L
Step4: Sort the Minutiae points and Store in an array A
Step5: value= KL / $M_p$
 Vector=KL % $M_p$
 Step6: For i=1 to value
 For j=1 to $S_p$
 Read point X from Array A and Check the point whether it is above or below the line L.
 If it is above the line or on the line put value as ‘0’ else value is ‘1’.Store them in array K.
Final key = Append the key vector of length vector to value of K. [8]
```

FUTURE DEVELOPMENTS

The idea of incorporating a biometric system with cryptography is not only for enhancing the security but also for better implementation and technical simplicity.
The development of a new technology was announced by Fujitsu Laboratories Ltd. recently. When traveling across a network, it converts biometric data into a cryptographic key to ensure that personal data is protected. This newly developed technology boosts the security of the encryption method and protects confidential data, such as IDs and passwords.

For example, for private data managed in a cloud service, it would be necessary to send the biometric data through the network, increasing issues in network security. Now, Fujitsu Laboratories has developed a technology that uses randomized numbers, each different, to convert biometric data into a cryptographic key for use in encryption and decryption. This makes it possible to easily and securely handle an individual's confidential data using biometric data, while restricting the unconverted biometric data from passing through the network. Biometric authentication is made simpler and more convenient to carry out the verification of the identity of a person procuring personal data managed on the Internet.

The technology uses different randomized numbers that turns the biometric information, such as the veins in the palm of the hand, into a cryptographic key for encrypting and decrypting confidential data on each side of the communication. [7]

A user’s randomized code which is a representation of their biometrics is compared with the number generated at the start so as to verify the person at the end of the data transfer. This would eliminate the need for handling encryption keys for accessing your encrypted data.

Fujitsu also added that it used error-correction codes to compensate for any minor errors, such as slight movements of the hand, during transmission of data. This will be a more effective way of protecting private information as there is a decreased chance of the biometric data being intercepted on a network and it could broaden the use of biometrics to cloud services in a more secure way.

Generally, biometric information is used only for accessing local devices because the data might be intercepted in transit over a network. Fujitsu's technology could bring this form of login to cloud storage, social networks, and other online services.

The company says it is currently working on improving the time it takes for data decryption and is intending to commercialize the system by 2017. [7]

CONCLUSION

In this paper, incorporation of Biometrics with Cryptography has been proposed as it provides security to the data through Cryptography and Biometric authentication avoids the overhead of storing and remembering long cryptographic keys. Here, we have proposed a method for generation of Cryptographic key using fingerprint patterns which is stable throughout a person's lifetime. This system is unique because of 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 open transmission.

REFERENCES

[1] https://www.tutorialspoint.com/cryptography/
[2] Biometrics, definition http://searchsecurity.techtarget.com/definition/biometrics
[3] "A review on Biometric Cryptosystems" by Jisha Nair B.J RanjithaKumari S, International Journal of latest trends in Engineering and Technology. http://www.ijltet.org/wp-content/uploads/2015/09/8.pdf
[4] "A survey on biometric cryptosystems and cancelable biometrics", Christian Rathgeb and Andreas Uhl, EURASIP Journal on Information and Security. https://jis-eurasipjournals.springeropen.com/articles/10.1186/1687-417X-2011-3
[5] "Minutiae-based Fingerprint Extraction and recognition", By NaserZaeri, https://www.intechopen.com/books/biometrics minutiae-based-fingerprint-extraction-and-recognition.
[6] Sanjukta Pal, Prof (Dr) Pranam Paul "Cryptographic Technique Using Biometric Authentication" in International Journal of Innovative Research in Computer and Communication Engineering.https://www.ijircce.com/upload/2014/september/10_Cryptographic.pdf
[7] Johnathan Keane "Fujitsu develops Tech that turns Biometric data into a Cryptographic Key" https://www.digitaltrends.com/computing/fujitsu-developing-tech-that-turns-biometric-data-into-a-cryptographic-key/
[8] Dr.R.Seshadri, T.Raghu Trivedi "Efficient Cryptographic Key Generation using Biometrics" http://www.ijcta.com/documents/volumes/vol2issue1/ijcta2011020116.pdf
[9] https://www.math.uci.edu/icamp/courses/math77c/demos/hist_eq.pdf
[10] https://www.research.ibm.com/haifa/projects/image/glt/binar.html
[11] "Biometrics as a Cryptographic Method for network security." By Kumar Ankit and JayaramRekha, Indian Journal of science and technology.