Impact Factor Value: 4.029 ISSN: 2349-7084
International Journal of Computer Engineering In Research Trends
Volume 4, Issue 6, June-2017, pp. 259-262 www.ijcert.org

Biometrics based Cryptographic Key Generation using Finger Print

Mrs. A. Ruba[1] **Dr. G. Rajkumar**[2] **Dr. K. Parimala**[3]
[1 2 3] *Assistant Professor, N.M.S.S.Vellaichamy Nadar College, Madurai – 625019, Tamilnadu, India.*

Abstract :- Accurate and automatic identification and verification of users are essential in all system. Shared secrets like Personal Identification Numbers or Passwords and key devices such as Smart Cards are not presently adequate in few situations. What is necessary is a system that could authenticate that the person is the person. The biometrics is improving the capability to recognize the persons. The usage of biometrics system permits the identification of a living person according to the physiological or behavioral features to be accepted without human involvement. The construction of cryptographic key from biometrics is used to make safe our system. To implement this concept, sender's recent fingerprint would be used to construct key by combining it with the information. For key decryption, the sender's Database fingerprint images, which are previously kept by receiver's end, would be used.

Keywords:- Information Security, Biometrics, Cryptography, Encryption, Decryption, Cryptographic Key Generation

---

1. Introduction

Information security is designed to protect the confidentiality, integrity, and availability of computer system data from those with malicious intentions. There are two most important issues in information security improvement. One is to protect the user possession and control the access to information by authenticating an individual's identity. The other is to ensure the privacy and integrity of information and to secure information communication. Biometrics and Cryptography offer solutions to these two issues from different perspectives. Biometrics offers greater security and convenience than traditional identity authentication systems. Cryptographic techniques have gained its recognition due to its security reason. In this paper, we attempt to present an outline of biometrics and cryptography in security improvement. Given the practical importance of cryptographic keys and biometric templates, our focus will be on methods which search for combinations of biometrics and cryptography to increase the security of these keys and templates.

2. Biometric System

The automated use of physiological or behavioral characteristics to verify identity is called Biometrics. Automated use means with computers or machines, rather than human beings, verify physiological or behavioral characteristics. Physiological characteristics are related to the shape of the body, such as finger-scan, facial-scan, iris-scan, hand-scan, and retina-scan. Behavioral characteristics are related to the pattern of behavior of a person, such as voice-scan and signature-scan. The element of time is essential to behavioral biometrics. Depending on the application context, a biometric system may operate either in verification mode or identification mode. Verification system answers the question: "Am I whom I claim to be?" The answer returned by the system is a match or no match. An identification system answers the question: "Who am I?" The answer returned by the system is an identity such as a name or ID number. A biometric system consists of four main modules. (Figure.1)

1) Sensor module captures the biometric data of a personality. An example is a fingerprint sensor that images the ridge and valley structure of a user's finger.

2) In Feature extraction module, where the captured biometric data is processed to extract a set of most important or discriminatory features.

3) In Matcher module, the features extracted are compared against the stored templates to produce matching scores. It also encapsulates a decision-making module, in which a user's claimed identity is confirmed (verification) or a user's identity is established (identification) based on the matching score.

4) System database module is used by the biometric system to store the biometric templates of the enrolled users.

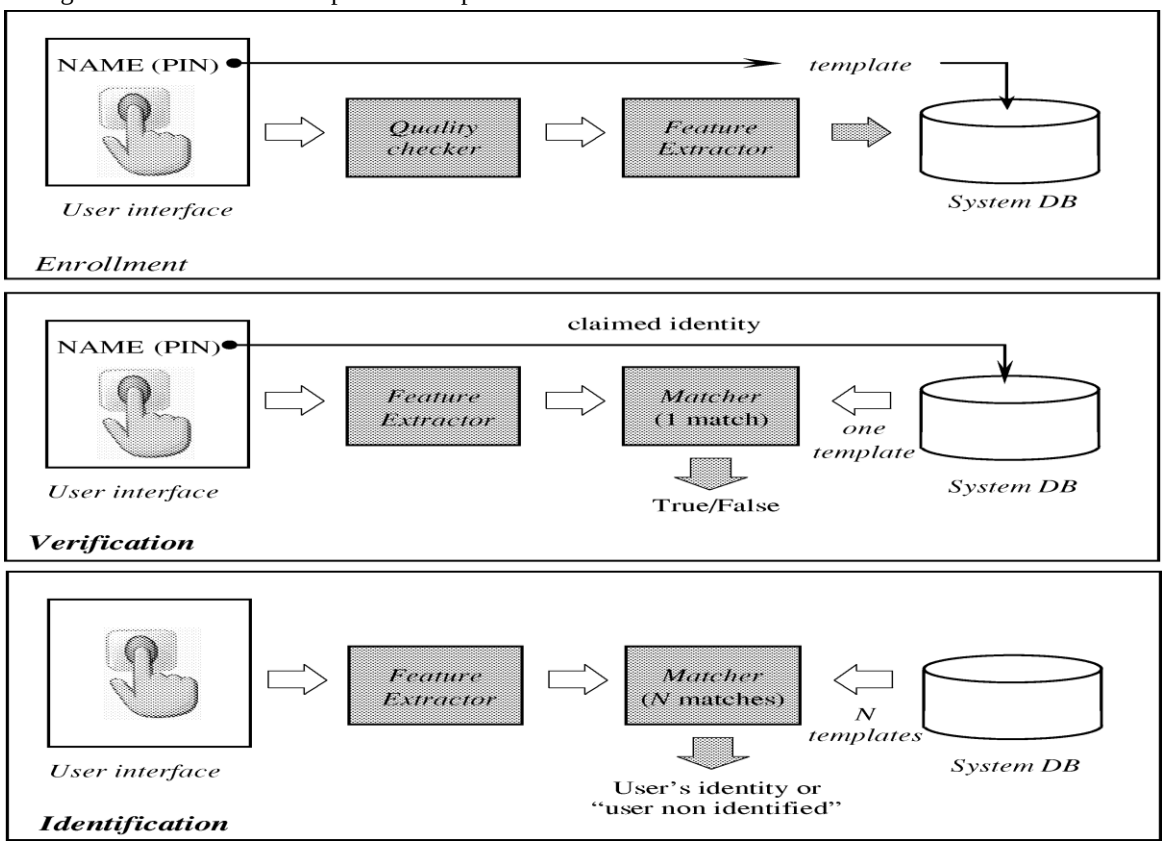

Figure 1: Biometric System

A template is a small file of distinct characteristics that have been extracted from a user's biometric data, used to carry out biometric matches. Biometric data such as finger prints and facial images cannot be reconstructed from biometric templates. Unique templates are generated every time a user presents biometric data.

Fingerprint:

Fingerprint technology uses the unique fingerprint patterns on the human finger to identify or verify the identity of the individual. A finger print is defined by the different ridges and valleys on the surface of each person's finger. Ridges are the upper level of skin, and the valleys are the lower level of the skin. Fingerprint uniqueness comes from the pattern of ridges and valleys. There is nine basic level fingerprint patterns as shown in figure 2.

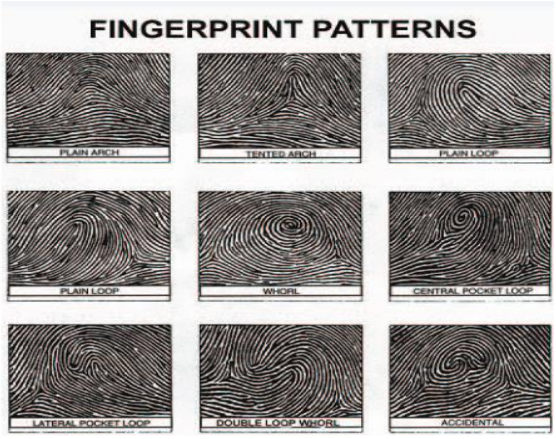

Figure 1: Basic level fingerprint patterns

3. Cryptography

Cryptography means "secret writing." It is used not only to provide confidentiality but also to give solutions for other problems like data integrity, authentication, non-repudiation, Access control and Availability. Plaintext is Original data, which is readable either by a person or by a computer. Whereas the cipher text, which is unreadable, without the proper cipher to decrypt it. The process of encoding the plaintext into cipher text is called Encryption and reverse the process of decoding cipher text to plaintext is called Decryption. They need encryption and decryption algorithm and key. Key plays a vital role in cryptography because the algorithm directly depends on it. Encryption schemes are divided into two groups:

Symmetric Encryption:

In this scheme, the same key is used for encryption and decryption. It is also known as secret key encryption or conventional encryption. One of the main advantages of using the symmetric key encryption is that the computational power of this encryption technique is small. Figure.3 represents the model for conventional encryption.

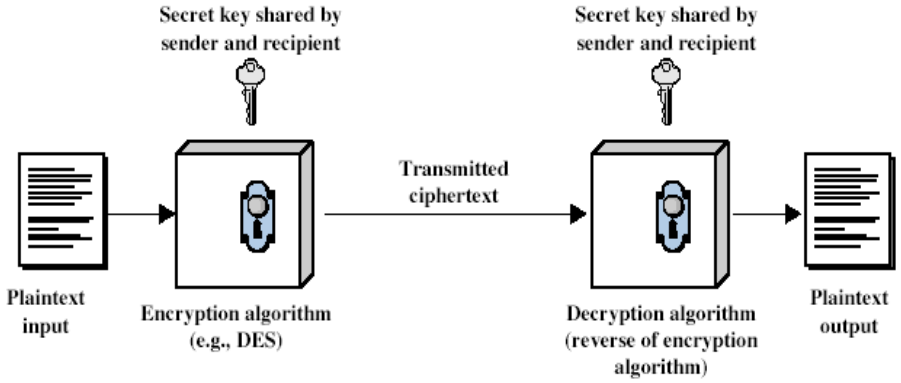

Figure.3 A Model of Conventional Encryption

Asymmetric Encryption:

In this scheme, different keys are used for encryption and decryption. It is also known as public key encryption. They are important because they can be used for transmitting encryption keys or other data securely even when the both users have no opportunity to agree on a secret key in private. They are slow. Figure.4 represents the model for Asymmetric Encryption.

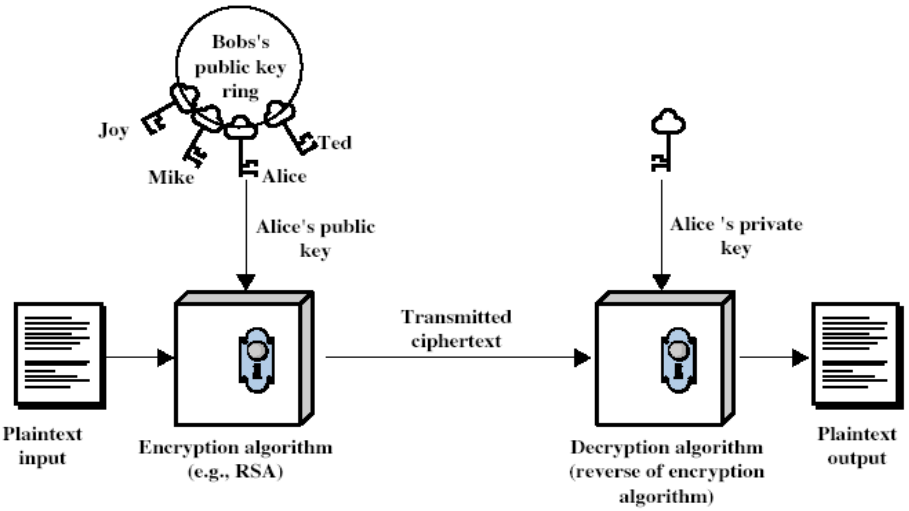

Figure.4 A Model for Asymmetric Encryption

4.Biometrics-Based Cryptographic Key

Many cryptographic algorithms are available for securing information. However, regardless of whether a user deploys a symmetric or a public-key system, the security is dependent on the secrecy of the secret or private key, respectively. The design of combining biometric authentication with cryptography has been developed with the help of fingerprint. Here the total technique is discussed in some individual steps. At first at sender's side and then at receiver's side.

STEPS AT SENDER'S SIDE

At sender's end, the plain text in binary form would be encrypted by the encryption process, from which we will get the encrypted text and some information. The information would be combined with the sender's recent fingerprint template for key generation. Now the encrypted text along with key would be sent to the sender.

STEPS AT RECEIVER'S SIDE

At receiver's end, Cipher text along with key would be accepted by the receiver. Cipher text and the key will be separated. The information would be decrypted with the help of sender's database fingerprint template (which are kept by the receiver) and the fingerprint matching algorithm from the key. If the two images do not match, information cannot be received. With the help of information, the encrypted text would be decrypted into plain text.

5. Conclusion

This paper uses the sender's fingerprint for both encryption and decryption. No other fingerprint can derive the information from the key. Due to symmetric key encryption, the total cryptographic technique is fast and efficient. The key formed by using fingerprint, is more advantageous and can be applied in PC access and internet security (Computer network security, Internet transaction, Laptop Security, Application level security), Physical area security (military, government, banking, voting, prisons) Employee record check, Mobile phones (network access and theft protection) and Mobile financial transaction (Credit cards & ATM cards). My future work will focus on applying other person-dependent biometric features and finding a good approach for biometric authentication.

References

[1] B. Raja Rao, Dr. E.V.V. Krishna Rao et al., "Finger Print Parameter based Cryptographic Key Generation", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 6, Nov – Dec, 2012, pp. 1598 – 1604.

[2] Dr. G. Rajkumar, Dr. K. Parimala and Mrs. A. Ruba, "An Innovative Approach to Genetic Algorithm based Cryptography", International Jouranl of Computer Science, Vol. 5, Issue 1, No 9, 2017, Page No. 1199 – 1202.

[3] N. Ratha and J. Connell et al. Cancelable biometrics: A case study in fingerprints. Intl. Conf. on Pattern Recognition, page 370C373, 2006

[4] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3):614C634, 2001.

[5] Nanavati, S. Thieme, M. and Nanavati, R. *Biometrics: Identity Verification in a Networked World*. Wiley Computer Publishing, New York, 2002

[6] Saad Abuguba, Milan M. Milosavljevic, and Nemanja Macek, "An Efficient Approach to Generating Cryptographic keys from the face and Iris Biometrics fused at the feature level," International Journal of Computer Science and Network Security, Vol. 15, No. 6, June 2015.

[7] Sanjukta Pal, Sucharita Pal, Dr. Pranam Paul "Fingerprint Geometry matching by Divide and Conquer Strategy" accepted and published in International Journal of Advanced Research in Computer Science(IJARCS), ISSN No. 0976-5697, Volume 4, No. 4, March-April 2013.

[8] T. Connie, A. Teoh, M. Goh, and D. Ngo, " Palm hashing: A novel approach for cancellable biometrics," Information processing letters, vol. 93, no. 1, pp. 1-5, 2005

[9] Cryptography and Network Security Principles and Practices by William Stalling, Prentice Hall, 2005.

[10] M.Sathya, & Dr.K.Thangadurai. (2017). Implementation of Optimization Using Eclat and PSO for Efficient Association Rule Mining. International Journal of Computer Engineering In Research Trends, 4(1), 4-8. Retrieved from http://ijcert.org/ems/ijcert_papers/V4I0102.pdf.

