Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 9, September 2015, pg.101 – 104

SURVEY ARTICLE

Biometric System Using Cryptography: A Survey

Anupam Baruah[1], Prof. (Dr.) Lakshmi Prasad Saikia[2]

[1]Research Scholar, Dept. Of Computer Sc. & Engg, Assam downtown University, India

[2]Professor, Dept. Of Computer Sc. & Engg, Assam downtown University, India

[1] anupambaruah04@gmail.com; [2] lp_saikia@yahoo.co.in

Abstract—In this paper, the biometric recognition for verification identification process and various cryptographic techniques for authentication purpose are discussed along with detailed review of literature. the main objective of this approach is to combine both cryptographic and biometric recognition to a system to provide high degree of security with protection against various attackers.

Keywords— Biometrics, Cryptography, symmetric key encryption, asymmetric key encryption

I. INTRODUCTION

Today internet is one of the most important parts of our daily life. Using internet, we can do large no of things, so it is very important. People use internet to get information, share information worldwide. User can share or access any data or information at any time, because there is no global time for internet. User can use internet any time. It is very important to keep personal information or confidential information from hackers. So authentication is most important at this stage. Traditionally password and other authentication methods to protect their confidential information. But these techniques provide low security mechanism. Because sometimes user cannot remember password, which can result in user error or password can be stolen by hacker or unauthorized persons. Today Biometric recognition and cryptography techniques are used together. Some of the biometric techniques commonly use are image recognition, fingerprint , iris recognitions and commonly used cryptographic techniques are symmetric key cryptography and asymmetric key cryptography.Biometrics technology has been proposed to strengthen authentication mechanism in general by matching a stored biometric template to a live biometric template. Cryptography provides the necessary tools for accomplishing secure and authenticated transactions. It not only protects the data from theft or alteration, but also can be used for user authentication [9]. Crypto-biometric system, however, has some issues. Any biometric system needs to provide biometric tem-plate protection which confirms the privacy and security of biometric data [11]

A. MEANING OF BIOMETRICS:

Biometrics refers to metric related to human characteristics. It deals with automated methods of identifying a person or verifying the identity of a person based on physiological and behavioural characteristics. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are categorized as physiological and behavioural. Physiological characteristics are related to shape of body. Example includes finger print, face recognition, DNA, palm print, hand geometry, iris recognition, retina recognition etc. Behavioural characteristics are related to the pattern of behaviour of a person like voice, typing rhythm etc.

1) Image Processing: In contrast to feature-based biometric systems, the Biometric Encryption algorithm processes the entire fingerprint image. The mechanism of correlation is used as the basis for the algorithm. A general overview of correlation, as it relates to Biometric Encryption, is given in the following section. More detailed discussions of correlation and its applications are given in the references by Goodman, Steward and Wanderlust [12].

B. MEANING OF CRYPTOGRAPHY :

Cryptography refers to encryption ,which is the process of converting text(plain text) to unreadable text called cipher text.Decription is reverse , moving from cipher text to plain text. A cipher is a pair of algorithm that generates the encryption and reversing decryption. Cryptographic techniques fall into two major categories:-Symmetric key encryption and public key encryption. These two techniques require the use of a "key" or a set of numbers used in combination with a formula to encode and decode a message into an unreadable format.

1) Symmetric key encryption: This technique employs the same key to encrypt and decrypt the message. DES, Triple DES, AES, RC5, etc may be the example of such encryption.

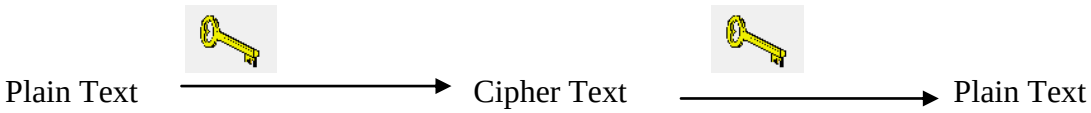

Fig1: Symmetric key algorithm

*(2)Public key cryptography***:** this technique requires a pair of different keys known as public and private key. Public key need to be kept secret. On the other hand private key is only known to the owner of the key. RSA, Elliptic Curve, etc may be the examples of such Encryption.

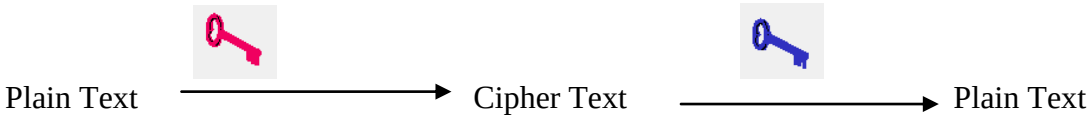

Fig2: Asymmetric key algorithm

II. RELATED WORKS

In 1986 M. Kirby and L. Sirovich introduced a method characterization of human faces using low dimensional procedure [1].

In 2011 K Hemanth , Srinivasulu Asadi , Dabbu Murali , N Karimulla and M Aswin have proposed A Secure Crypto Biometric protocol for Authentication. The proposed blind authentication is extremely secure under a variety of attacks and can be used with a wide variety of biometric traits. Protocols are designed to keep the interaction between the user and the server to a minimum with no resort to computationally expensive protocols such as secure multiparty computation (SMC)[10].

In 2012 A.O. Afolabi, Adigun A.A developed a secured e-banking system using encryption and face recognition asthe two levels of security mechanism since the username and passwordsecurity mechanism are easily breached . ThisE-banking system was designed using MATLAB as well as face recognition and encryption.[9]

In 2004 Umut Uludag , Sharath Pankanti ,Salil Pravakar proposed a system Biometric Cryptosystems .This technique combines cryptosystem with biometric recognitions.

In 1999 P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss proposed an algorithm for face recognition. The primary objectives of his algorithm was (a) assess the state of the art, (b) identify future areas of research, and (c) measure algorithm performance [5].

In 1996 Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone proposed some methods for cryptography technique. It is a rigorous encyclopedia of known techniques, with an emphasis on those that are both (believed to be) secure and practically useful. The topics covered range from low-level considerations such as random-number generation and efficient modular exponentiation algorithms and medium-level items such as publickey signature techniques, to higher-level topics such as zero-knowledge protocols [6].

Thambiraja et al. showed that AES consumes highest processing power among DES, 3DES, BLOWFISH. AES is better than RC4 for smaller packets also it is better for live video streaming transmission compared to RC4 and XOR. Time taken by RSA is much higher than that of AES and DES. Memory usage of RSA is high compared to AES, DES. Output byte in RSA is less as compared to AES and DES.RC4 is fast and energy efficient than AES for larger packets[7].

By Hernando & Neito ,"E-Banking Management –Issues, Solution & Strategies "[13] Overall, e-banking seems to serve as a complementary means of interacting with customers rather than a substitute for other channels such as physical branches. Despite the large investment in the Internet as a distribution channel, the branch network remains an important channel for retail banking products.

In 1985, Miller [14] and Koblitz [15] proposed a public key cryptographic scheme called ellipticcurve cryptography (ECC). The ECC has a smaller key size which offers the same security strength as the RSA

III. CONCLUSIONS

We have studied different techniques used in crypto-biometric systems where both biometric recognition and various cryptographic techniques applied. All confidential or important information send on internet, so it is very important to keep records secure. Both biometric recognition and cryptographic techniques can be applied separately .But both techniques does not fulfill all requirement for security purpose when applied separately. If we combine both techniques then as a whole the system can provide greater improvement over security threads.

REFERENCES

[1] M. Kirby and L. Sirovich, "Low-Dimentional Procedure for the Characterization of Human Faces", Optical Society of America A-Optics, Image Science and Vision, Vol.4, No.3, march 1987, pp.519-524.

[2] Donald E. Knuth, The art of computer programming;volume2:seminumerical Algorithm,3rd ed,.Addison-Wesley,1998.

[3] Umut Uludag , Sharath Pankanti ,Salil Pravakar , Anil K Jain "Biometric Cryptosystems Issues and Challenges" proceedings of IEEE 2004.

[4] Journal of Internet Banking and Commerce -- Arraydev.com/commerce/jibc.

[5] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET Evaluation Methodology for Face-Recognition Algorithms," IEEE Transactions on PAMI, 2000, Vol. 22, No. 10: 1090-1104.

[6] A. J. Menezes; P. C. van Oorschot; S. A. Vanstone (1997). Handbook of Applied Cryptography. ISBN 0-8493-8523-7.

[7] E. Thambiraja, G. Ramesh and Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 7, July 2012 ISSN: 2277 128X.

[8] http://www.webopedia.com/TERM/N/network_security.html

[9] A.O. Afolabi and Adigun A.A, "Development of Crypto-Biometric E-Banking System", International Journal of Engineering andTechnology Volume 2 No. 11, November, 2012.

[10] K Hemanth, Srinivasulu Asadi, Dabbu Murali, N Karimulla and M Aswin,"High Secure Crypto Biometric Authentication Protocol", International Journal of Computer Science and Information Technologies, Vol. 2 (6) , 2011, 2496-2502.

[11] AK Jain, K Nandakumar, A Nagar, inSecurity and privacy in biometrics.Fingerprint Template Protection: From Theory to Practice (SpringerLondon, 2013), pp. 187–214

[12] Colin Soutar, Danny Roberge, Alex Stoianov, Rene Gilroy, and B.V.K. Vijaya Kumar ," Biometric Encryption™", ICSA chapter 22.

[13] Hernando & Neito ,"E-Banking Management –Issues, Solution & Strategies " , Information Science Reference Hushey, Newyork 2007.

[14] Koblitz N. Elliptic curve cryptosystems,Mathematics of Computation 48, 1987; 203--209.

[15] MillerV.Use of elliptic curves in cryptography,CRYPTO 85, 1985.

