ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

IRIS BASED CRYPTOGRAPHY

Sruthi B. Asok[1], P. Karthigaikumar[2], Sandhya R[3], Naveen Jarold K[4], Siva Mangai[5]

PG Scholar, Electronics and Communication Engineering, Karunya University, Coimbatore, India[1]

Associate Professor, Electronics and Communication Engineering, Karunya University, Coimbatore, India[2]

PG Scholar, Electronics and Communication Engineering, Karunya University, Coimbatore, India[3]

PG Scholar, Electronics and Communication Engineering, Karunya University, Coimbatore, India[4]

Associate Professor, Electronics and Communication Engineering, Karunya University, Coimbatore, India[5]

ABSTRACT - **Cryptography is a technique which uses mathematics to encrypt and decrypt data. Using cryptography information can be transmitted through insecure channel so that only the intended recipient can access .the secret key is extracted from the iris image so that security improves. This key is used to encrypt the data to be sent. Different tests are conducted to check the randomness of the key.**

Keywords: Cryptography, IRIS, Biometric Cryptography.

I.INTRODUCTION

Cryptography means secret writing. It forms the basis for many technological solutions in computer and communication systems. The original message to be encrypted is called plaintext and the encrypted message is called cipher text. In order to get the original data back decryption is done.

A key is a value which works with cryptographic algorithm to produce specific cipher text. In different algorithms different keys can be used. For Advanced encryption standard key lengths used are 128,256 and 192. In AES, both encryption and decryption have ten rounds. Four different transformations are used, one of permutation and three of substitution. The main problem of conventional cryptography is that it cannot authenticate genuine users. Conventional systems are based on the possession of token or knowledge based. They can be cracked. Identification of human iris provides a unique structure suitable for non invasive biometric assessment.

Software based cryptography uses encryption key which are long bit strings. They are very hard to memorize such a long random numbers. Also it can be easily attacked by brute search or technique. Biometric e.g. fingerprint, iris, face, voice etc uniquely identifies a person and a secure method for stream cipher, because Biometric characteristics are ever living and unstable in nature.

Biometric cryptography is a method using biometric features to encrypt original data. This method can improve the security of the encrypted data .. Biometric key is generated reliably from genuine iris codes. This key is used to encrypt the data and is sent through a secure channel. At the decryption phase same key is used to generate the original data.

II.RELATED WORKS

Kai xi and jiankun Hu [20] introduced in his paper about the problems of traditional cryptography. Symmetric key cryptography, data encryption standard, advanced encryption standard etc are also discussed which are different techniques in cryptography. This paper also discussed how to integrate biometrics with cryptography.

Abdullah Sharaf Alghamdi, Hanif Ullah, Maqsood Mahmud, Muhammad Khurram Khan [3] stated that image encryption cannot be used for large amount of data and high resolution images. In order to overcome the problems some chaios based cryptosystems are used.

FengHao,RossAnderson,John Daugman[13] presented a secure way to integrate iris biometric with cryptography. Biometric key is generated from iris code. Proposed a feature level fusion network based on fuzzy vault and fuzzy commitment scheme. Alisher Kholmatov and Berrin

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

Yanikoglu[5] presented the benefits of biocryptography. The online signature of a person is a behavioural biometric. Online signature is widely accepted as the formal way of approving documents, bank transactions, etc.minute points are extracted from signatures and used in fuzzy vault schemes. Jing Huang et.al [15] described about the segmentation process for iris feature extraction. It uses canny edge detection method to extract features. Image acquisition ,feature matching and normalization are other processes discussed. A. Jagadeesan et.al [7] proposed methods for extracting features from iris. Iris is unique even for identical twins. It is the part between pupil and white colour part.Doughman rubber sheet model is used for normalization process. 128 bit secret key is used for encryption and decryption. Advanced encryption standard is the algorithm used.1t uses 128 bit key and data. It is a symmetric key cryptography because same key is used at both the encryption and decryption phase[20].

III.DESIGN METHODOLOGY

Images taken from cassia iris database are used for feature extraction. From iris image 128 bit secret key is selected. This key is used to encrypt the data. The information that is to be sent to the channel is encrypted using this key. At the decryption phase original data is retrieved back. Randomness check is conducted for the key. Working model is shown in fig.1

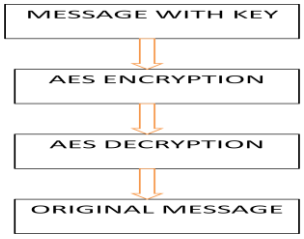

Fig.1 working model

IV KEY GENERATION

Iris feature extraction consists of different steps. They are image acquisition, processing and converting in to binary values. processing consists of segmentation and normalization. Edge maps of the images are generated after these processes. From the normalized image key is generated.

A. Segmentation

Segmentation divides the whole image in to different segments. The main aim of segmentation is to convert the image to something which can be easily analyzed. It consists of estimation boundary and noise removal.

B.Normalization

Normalization changes the range of pixel intensity values. It is a method of contrast stretching. Dogman's Rubber Sheet Model is utilized for the transformation Process, in which iris image is converted to rectangular image. It consists of two resolutions namely radial and angular resolution.

C.128 bit key

Blocks of 128 bits should be generated. From these only one block of 12 bit is selected as the key. Randomness checking is done for that.

D .Tests conducted to check the randomness of key

Five tests are conducted to check the randomness. They are

- The Frequency (Monobit) Test,
- Frequency Test within a Block,
- The Runs Test,
- Tests for the Longest-Run-of-Ones in a Block,
- Non overlapping template match test.

In frequency monobit test proportion of zeros and ones are checked. It should be equal for the sequence to be random In frequency test within a block proportion of zeros and ones is checked within a block. The purpose of runs test is to determine whether the number of runs of ones which means checking the occurrence of continuous zeros or ones of various lengths. The purpose of longest runs of ones in a block test is to determine whether the occurrence of continuous zeros or ones of various lengths within a block. The purpose of Non overlapping template match test is to detect generators that produce too many occurrences of a given non-periodic pattern.

V. RESULTS AND DISCUSSION

A. Key generation

Iris image for experiments are taken from cassia iris data base. The input image is shown in figure 2(a).the centre of image is calculated for extraction.

It is shown in figure 2(b).after segmentation inner and outer circle boundary of iris is calculated. These image are

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

shown in figure 2(c) and 2(d).the image then undergo radial edge suppression for extraction.Radially suppressed image is shown in figure 2(e). The final image is obtained after normalization in figure 2(f).From this key is generated

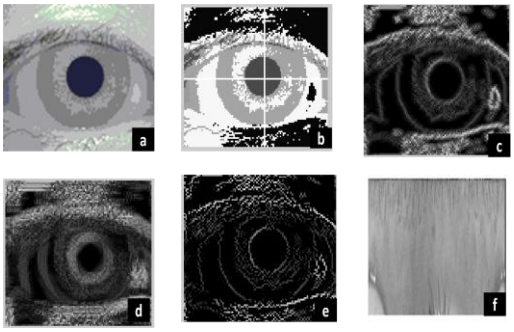

Fig. 2 (a) Input image (b) Calculation of centre (c) Calculation of inner circle (d) Calculation of outer circle (e) Radially suppressed image (f) Output image

B. Advanced encryption

This 128 bit, extracted from iris image is used as the key in AES encryption.AES is a symmetric block cipher so same key is used at both encryption and decryption side. Encryption consists of transformations like add round key, shift rows,subbytes,mix columns, key expansion etc.Expanded key is used as the key in all the rounds expect the initial round.

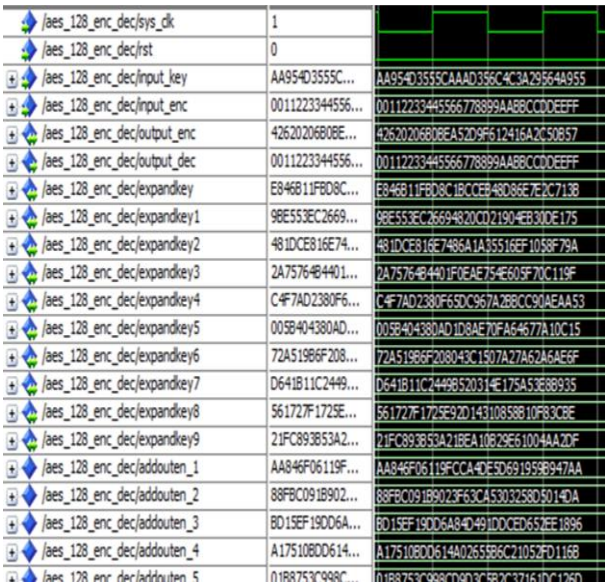

Fig.3 AES encryption and decryption

VI.CONCLUSION

Iris based cryptography is implemented in this paper. Secret key is generated from iris image. Randomness check is conducted for the key sequence. In AES information is encrypted and decrypted using the key.

REFERENCES

[1].A.Senthil Arumugam,. Dr.N.Krishnan, " Biometric encryption and bio-fusion authentication using combined arnold transition and permutation matrices", International Journal of Engineering Science and Technology,Vol. 2(10), pp-5357-5369, 2010.

[2].A. Menezes, P. van Oorschot, and S. Vanstone, " Handbook of Applied Cryptography", CRC Press, New York, pp 81-83, 1997.

[3].Abdullah Sharaf Alghamdi, Hanif Ullah, Maqsood Mahmud, Muhammad Khurram Khan, "Bio-chaotic stream cipher-based iris image encryption". International Conference on Computational Science & Engineering, vol 2, pp 739-744, 2009.

[4].Ann Cavoukian and Alex Stoianov, **"** Biometric encryption chapter from the encyclopedia of biometrics". Springer of encyclopedia, pp 1-14 ,2009.

[5].Alisher Kholmatov and Berrin Yanikoglu, " Biometric cryptosystem using online signatures". International conference on computer & information sciences,volume 4263 , pp 981-990,2006 .

[6].AndrewRukhin,JuanSoto,JamesNechvatal, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications" , , pp 1-131,2010.

[7].A.Nagar and A. K. Jain, "Multibiometric cryptosystems based on feature level fusion". IEEE transaction on information forencis and security, , ,volume 7 ,issue 1, pp 255-268,2012 .

[8].B. Fang, Y.Y. Tang, "Elastic registration for retinal images based on reconstructed vascular trees", IEEE Transactions on Biomedical Engineering,pp 1183–1187. ,2006.

[9].C. Rathgeb A. Uhl," Context-based biometric key generation for iris". The Institution of Engineering and Technology, Volume 5, issue 6,pp 389-397,2011.

[10].Christian Rathgeb and Andreas Uhl, **"** A survey on biometric cryptosystems and cancellable biometrics". EURASIP Journal on Information Security,pp 1-25, 2011 .

[11].C.E. Shannon, "Communication theory of secrecy system", Bell syst Tech, ,pp 656-715, 1949 .

[12].Daemen J. and Rijmen V, " The design of Rijndael: AES – The Advanced Encryption Standard, Springer-Verlag, ISBN 3, pp 540-650.

[13].Feng Hao, Ross Anderson, John Daugman. " Combining cryptography with biometrics effectively", IEEE transaction,volume 55,issue 9,pp 1081- 1088,2006 .

[14].Gustafson et al., "A computer package for measuring strength of encryption algorithms," Journal of Computers & Security. Vol. 13, pp 687-697, 1994.

[15].J. Huang et al. "A novel iris segmentation using radial-suppression edge detection". Elsevier Signal Processing ,pp 2630–2643,2009.

[16].J.G. Daugman, "The importance of being random: statistical principles of iris recognition", Pattern Recognition,pp 279–291,2003.

[17].J. Daemen and V. Rijmen, " The block cipher Rijndael, Smart Card research and Applications", LNCS 1820, Springer-Verlag, pp. 288-296.

[18].J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Image and Text Cryptography", International Journal of Imaging Systems and Technology, pp. 178-188 , 2005.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

[19].K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, H. Nakajima, "An effective approach for iris recognition using phase-based image matching", IEEE Transactions on Pattern Analysis and Machine Intelligence, pp 1741–1756,2008 .
[20].Kai xi and jiankun Hu , " Bio-cryptography", hand book of information and communication security, Springer,pp 129-157 ,2010.
[21].L. Shiguo, S. Jinsheny, W. Zhiquan, "A block cipher based a suitable of the chaotic standard map", chaos, solutions and fractals,pp117-129,2005 .
[22].L. Shujun, Z. Xuan, M. Xuanqin, C. Yuanlong, "Chaotic encryption scheme for real time digital video", SPIE vol.4666,pp 149-160.
[23].M. Mclone, J.V. McCanny, "Rijindael FPGA implementations utilizing look-up tables", *J.VLSI* signal process,pp 261-275, 2003 .
[24].Pareschi F., Rovatti R., Setti G, " Second-level NIST Randomness Tests for Improving Test Reliability, IEEE International Symposium on Circuits and Systems, New Orleans, pp 1437–1440, 2007 .
[25].R. Ursulean. " Reconsidering the Generalized Logistic Map asa Pseudo Random Bit Generator ", Electronics and Electrical Engineering, pp 10–13, 2004 .
[26].R. C.-W. Phan, "Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)", Information processing letters pp 33-38,2004 .
[27] R. Bremananth, and A. Chitra, " An efficient biometric cryptosystem using autocorrelations", International Journal of Information and Communication Engineering, pp 158-164, 2006 .
[28].U. Maurer, "A Universal Statistical Test for Random Bit Generators," Journal of Cryptology. Vol. 5, pp 89-105 , 1992
[29].W. Cao, R. Che, D. Ye, "An illumination-independent edge detection and fuzzy enhancement algorithm based on wavelet transform for non-uniform weak illumination images", Pattern Recognition Letters,pp 192–199,2008,.
[30].X. He, P. Shi, "A new segmentation approach for iris recognition based on hand-held capture device", Pattern Recognition,pp 1326–1333,2007.