International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 6, June 2015)

RFID Fusion Based Enhanced Encryption of Audio Signals using 128 Bit Advanced Encryption Scheme

Anusha A M
Dept. of Electronics and Communication Engineering
P A College of Engineering, Mangalore
anushaniji@gmail.com

Prof. Shamna N V
Dept. of Electronics and Communication Engineering
P A College of Engineering, Mangalore
shamnanv@gmail.com

Dr. Jose Alex Mathew
Director/HOD
Dept. of Electronics and Communication Engineering
P A College of Engineering, Mangalore
ayamanamkuzhy@gmail.com

***Abstract*- Cryptography is the backbone of modern security systems. The conventional problem of such systems is that they cannot authenticate genuine users. So a new scheme based on RFID is introduced such that it has benefits of both systems i.e. security and genuine user authentication. Here AES algorithm is used for encryption and decryption. The secret key is extracted from iris feature, and is used to encrypt and decrypt audio signals. Audio signals are processed in real time. Security of audio signals is achieved through the use of encryption; this information can be securely transmitted and stored for the access of only the proper Individual. The audio signals taken in real time are converted to binary form. So these bits are taken as the plaintext in encryption. After encryption and decryption same signals are reconstructed. The secret key is extracted from a novel fusion technique introduced in this project. This increases the randomness of the key so that security will increase. The security system will be modelled in Verilog and simulated for functional correctness. Sufficient effort will also be put in-order to optimize power, area and delay constraints of the implemented system.**

***Index Terms*—AES, Audio Signals,**

I. INTRODUCTION

Cryptography is the practice and study of protecting information by data encoding and transformation techniques. The original message called plain text is transformed to cipher text using some encryption algorithm. In decryption algorithm same data can be recovered using the secret key. Advanced encryption standard was announced by the National Institute of Standards and Technology (NIST) as the new encryption standard. AES has a block length of 128 bit, and key lengths of 128, 192, or 256 bit. All operations in AES are byte oriented operations. The block size is 16. AES operates on a 4*4 array called a state. A byte is represented by two hexadecimal digits. In AES, both encryption and decryption have ten rounds. Four different transformations are used, one of permutation and three of substitution.

Biometric cryptography is a method using biometric features to encrypt original data. This method can improve the security of the encrypted data. The most accurate feature iris is used. Iris image is converted to binary code to form the secret key. This key is used to encrypt the data which are audio signals. At the decryption phase same key is used to generate the original data.

The audio signals taken in real time are converted to binary form. So these bits are taken as the plaintext in encryption. After encryption and decryption same signals are reconstructed. The secret key is extracted from iris image. Key generation algorithm is designed and used to produce a key from RFID system.

II. LITERATURE SURVEY

The following is the base paper for the project work:

[IEEE 2013] A SECURE CRYPTOGRAPHIC SCHEME FOR AUDIO SIGNALS
Sruthi B. Asok , P. Karthigaikumar, Sandhya R, Naveen Jarold K, N.M Siva Mangai

[IEEE 2010] THE FIVE MODES AES APPLICATIONS IN SOUNDS AND IMAGES Chi-Wu Huang, Chien-Lun Yen, Che-Hao Chiang, Kuo-Huang Chang and Chi-Jeng Chang, Department of Industrial Education Institute of Applied Electronics Technology National Taiwan Normal University Taipei, Taiwan

Kai xi and jiankun Hu [20] made a survey for the cryptography algorithms. The different algorithms used are DES,3 DES,AES,public key cryptography etc.DES is vulnerable to attacks and 3 DES is slower in performance. So AES is the best for encryption and decryption. They also surveyed on biometrics and bio cryptography.

A.Senthil Arumugam,. Dr.N.Krishnan [1] proposed abiometric encryption method based on pseudorandom numbers and permutation matrices.Henon map is used to generate pseudo random numbers. Encryption of biometric trait pixel is done step by step using permutation matrices.

Abdullah Sharaf Alghamdi, Hanif Ullah, Maqsood Mahmud, Muhammad Khurram Khan et.al [3] introduced bio chaotic function which encrypt images. Here secret keysare different at different sections.L.Rosa method is used toextract the

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 6, June 2015)

images. Here a biometric key is generated to encrypt and decrypt the key.

Ann Cavoukian and Alex Stoianov [4] proposed the ideaof biometric encryption. BE is a technology that bind a digital key to a biometric . It also generate a digital key from the biometric so no biometric image is stored. The stored data is called helper data. Digital key is r correct biometric sample is presented for verification.

Alisher Kholmatov and Berrin[5]proposed Yanikoglu Biometric cryptosystem using online signa fuzzy vault scheme. Fuzzy vault scpreviously stored key when biometric data verification matches previously stored tem signature of a person is a behavioural trai transaction, approving documents etc. Epoints from online signatures and use duri unlocking phase .

C. Rathgeb A. Uhl [9] introduced a m distinct bits in iris codes exhibit higher others. This fact is utilised to detect the m within iris codes out of which biome constructed. Error correction is applied to remaining variance between biometric measurements.

III. BLOCK DIAGRAM

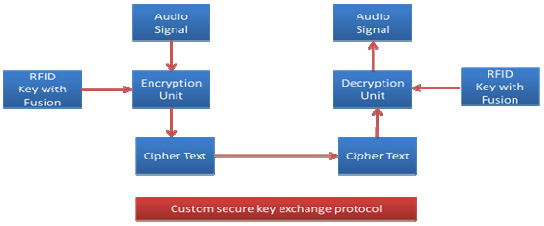


Fig 1: Block diagram of the entire system

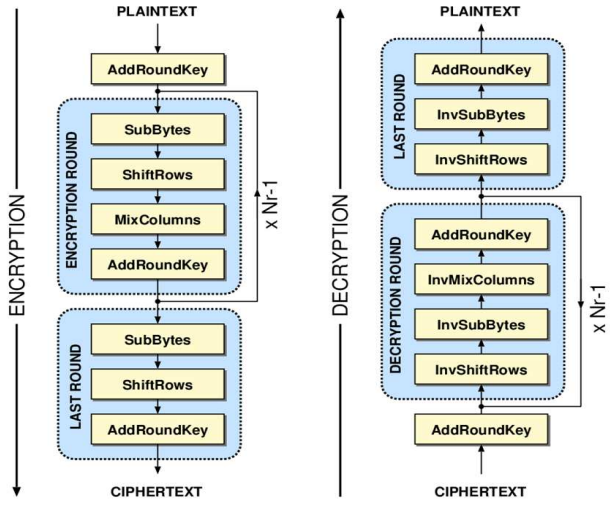


Fig 2: AES encryption and decryption scheme

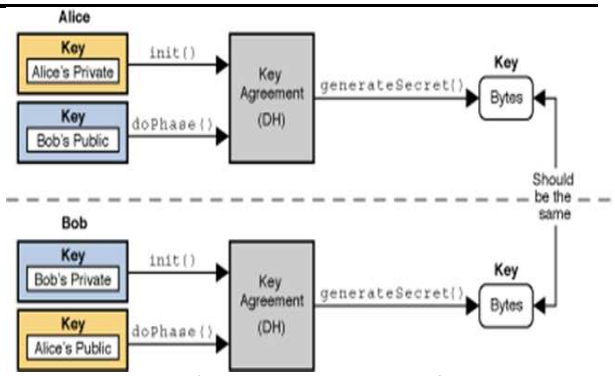


Fig 3: Basic scheme of key exchange which will be further improvised

IV. OBJECTIVES

1. Realize a MATLAB model of audio encryption scheme
2. RTL design and verification of the proposed scheme
3. Analyze various security parameters
4. Implement the design on FPGA

V. PROPOSED SYSTEM

The base paper proposes a scheme based on iris scanning. Generating key from this method can be error prone and building a highly reliable system using this technique is very tedious, prone to errors and requires more investment. In this project, the key derivation is done using a unique RFID code instead of generating a random key or reading from a bio metric sensor. A fusion technique is designed to implement a randomly generated code to modify the RFID data to make it more secure. We will also design a key exchange method based on a secure public and private key exchange method after analyzing various security factors such as identity of the person initiating the key exchange.

VI. METHADOLOGY

The project will be carried out in the following stages:

1. Further literature survey has to carried out to extract more ideas
2. A design plan should be created with an application
3. MATLAB modeling should be done
4. RTL Design of the proposed design should made
5. RTL verification should be done to make sure the design is working as decided
6. Next, speed, area, power and other parameters should be observed and tabulated.
7. Analysis and comparison of the parameters should be done
8. A demonstration should be and this can be done using the application decided

International Journal of Ethics in Engineering & Management Education
Website: www.ijeee.in (ISSN: 2348-4748, Volume 2, Issue 6, June 2015)

9. Thesis/dissertation should be written.

Applications:

1. Hybrid firmware encryption
2. Wireless sensor networks
3. Challenge response protocols
4. Key-establishment protocols
5. Military

Hardware:

1. Xilinx FPGA Kit
2. PC
3. USB-Serial cables
4. ZigBee Modules
5. Other application related hardware

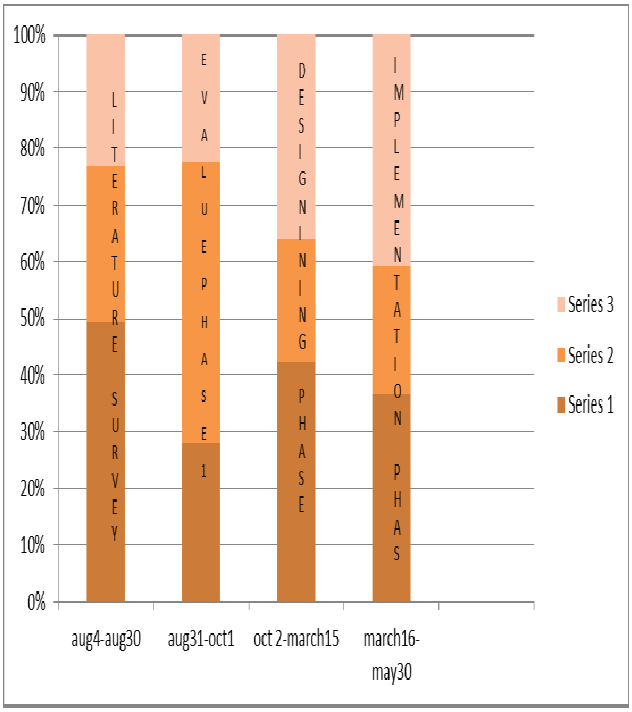
Software:

1. Xilinx Vivado Design Suite
2. ISIM simulator
3. MATLAB
4. TMFT

EXPECTED OUTCOME

A fully realized audio encryption system based on RFID fusion based key generation.

TIME CHART



CONCLUSION

A secure cryptographic scheme for audio signals is presented in this paper. Key with more randomness is selected to improve the network security. Different tests are conducted to check the randomness of the generated keys. Using this key original data that is audio signals are encrypted and decrypted in real time.

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 .