International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014)

Detection Through Storage Device: Encryption By AES Algorithm

Shraddha Satish Kashid[1], Prof. Nagnath B. Hulle[2]
[1]Student & G.H.R.C.O.E.&M, Ahmadnagar, Maharashtra, India
[2]Professor & G.H.R.I.E&T, Pune, Maharashtra, India

***Abstract*— With the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. It is essential to protect the confidential data from unauthorized access. In this paper, we analyze the Advanced Encryption Standard (AES). To provide the security of the Military confidential data we use encryption algorithm which take over reward of superior encryption algorithm. The proposed implementation using encryption algorithm was implemented on ARM 7 to encrypt and decrypt the confidential data on data storage devices such as SD card or Pen drive. The main objective of proposed implementation is to provide protection for storage devices. The ARM and encryption algorithm protect the data accessibility, reliability and privacy successfully. Since (AES) Advanced Encryption Standard algorithm is widely used in an embedded system or fixed organization. These AES algorithms are used for proper designs in defense for security. The AES algorithm is a block cipher that can encrypt and decrypt digital information.**

***Keywords*— AES, encryption, decryption, block cipher, storage device.**

I. INTRODUCTION

Advanced Encryption Standard (AES), a Federal Information Processing Standard (FIPS) are categorized as Computer Security Standard. The AES algorithm is a block cipher that can encrypt and decrypt digital information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits. The Rijndael cipher has been selected as the official Advanced Encryption Standard (AES) and it is well suited for hardware. This paper talks of AES 128 bit block and 128 bit cipher key and is implemented on ARM7 using VHDL as the programming language.

To improve the security of the Military information during WAR, and to provide the security of the Military confidential data during WAR an encryption and decryption algorithm, which inherits the advantages of advanced encryption algorithm, is proposed in this work. To encrypt and decrypt the confidential data on storage devices such as SD card or Pen Drive. This proposed work was implemented on ARM 7.

This system aims at reduced hardware structure and high throughput. VB software is used for simulation and optimization of the synthesizable VHDL code.

In this proposed work, we deliberate and implemented an encryption system to encrypt the stored data based on ARM (S3C6410). The PN sequences with good properties are generated from chaotic map and the system provides two kinds of encryption algorithm, one is stream cipher with Xor operation [2], the other is a hybrid algorithm of AES and chaos [3-7]. And we have tried our best to improve the speed of encryption and security.

The main rewards of this encryption scheme are as below:

1) It is extra safe and multifarious than software encryption and security chip;
2) It provides two chaotic systems to generate PN sequence and three algorithms to encrypt source data;
3) The standards of constraint of chaos maps know how to survive input by means of client to assurance the safety of the system.

II. RELATED WORK

Encryption is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication. Many image-protection techniques are using vector quantization (VQ) as encryption technique (Chang et al., 2001; Chen and Chang, 2001). In Chang et al. (2001), VQ decomposes an image into vectors, which are then encoded and decoded vector-by-vector. Alternatively, Chen and Chang (2001) use VQ to divide desired images for encryption into a large number of shadows that are guaranteed undetectable to illegal users. Image and text cryptography has been achieved using chaotic algorithms (Fridrich, 1997; Sobhy and Shehata, 2001, Haojiang, Yisheng, Shuyun and Dequn Li 2005). A symmetric block encryption algorithm creates a chaotic map (Fridrich, 1997) for permuting and diffusing image data.

www.manaraa.com

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014)

For thorough encryption, the chaotic map is applied to the image, iteratively, multiple times. The chaotic algorithm of Sobhy and Shehata (2001) is based on the Lorenz system of equations. Both image and text data are encrypted successfully, but knowledge of the system allows devising an optimization routine that discovers the key by output minimization. Phase encoding techniques exist for encrypting image data (Zhang and Karim, 1999; Park et al., 2001). Color image data is regarded in Zhang and Karim (1999), where a double-phase technique is utilized. Color images are encrypted from an indexed image and thereby decrypted back to its color format.

The work of Wu and Kuo (2001) describes selective encryption based on a digital coefficients table. It was shown its limitation due to a less intelligible recovered image. Color and gray-scale images were considered in Koga and Yamamoto (1998), where a lattice-based extension to Visual Secret Sharing Scheme (VSSS) (Naor and Shamir, 1994) was developed. A hashing approach to image cryptography is taken in Venkatesan et al. (2000); wavelet representations of images are obtained, and a new randomized strategy for hashing is introduced. Several cryptosystems exist like as data encryption, steganography, digital signature (Aloka Sinha, Kehar Singh, 2003) and SCAN (S.S. Maniccama, N.G. Bourbakis 2004) have been proposed to increase the security of secret images. However, one common defect of these techniques is their policy of centralized storage, in that an entire protected image is usually maintained in a single information carrier. If a cracker detects an abnormality in the information carrier in which the protected image resides, he or she may intercept it, attempt to decipher the secret inside or simply ruin the entire information carrier (and once the information carrier is destroyed, the secret image is also lost forever). Another method is to encrypt image data, e.g., using DES (Data Encryption Standard). DES, however, is very complicated and involves large computations.

The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. As AES has been invented according to investigation by Rijndael.

In the literature many researchers used different approaches have been used for the implementation on the basis of different technical acceptations which may be like AES strength execution, AES for efficiency or effectiveness execution, AES by hardware and software implementation and all that.

This section referred to ideal standard identifications on the target for evaluation achievement stages of AES optimization.

Ashruf et al in [10] have implemented AES in Molen hardware like Field Programmable Gate Array (FPGA) and General Purpose Processors (GPP) merging together to form Molen processor. The processor by using Molen hardware implementation architecture gives result as fast as poor FPGA. FPGA has highest velocity and more flexibility. The implementation of Molen hardware is only depends on its size rather than its cost.

The researcher T.Ravichandra Babu [8] implemented AES algorithm onto ARM processor platform. According to this implementation, shift Rows and Substitute byte (sub byte) operations is implemented on software. Wher5eas, on hardware Add Round Key operation and Mix Column operations performed. Therefore, Hardware and Software execution of AES have completed.

K.Atasu et al [11] include memory and speed efficiency optimized AES implementation. They open for us the Mix Column concept by focusing speed optimization on linear integration component. They proposed a new combine approach in this paper. It uses standard approach for the encryption [3] and the transposed approach [8] for decryption.

That gives an excellent performance than the uncontaminated approach of standard and transposed.

III. AES ALGORITHM

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits

www.manaraa.com

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014)

This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection.

Other FIPS-approved cryptographic algorithms may be used in addition to, or in lieu of, this standard. Federal agencies or departments that use cryptographic devices for protecting classified information can use those devices for protecting sensitive (unclassified) information in lieu of this standard.

In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.

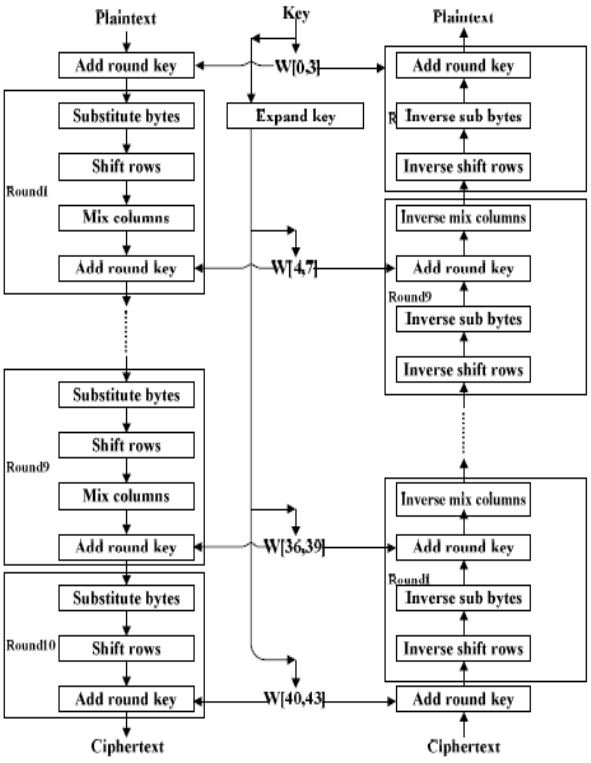

Fig 1: Flow Diagram of AES Algorithm

As the name of the paper suggests we are making an encryption and decryption system for military application.

IV. Proposed Model System

This implementation work mainly has 2 parts:

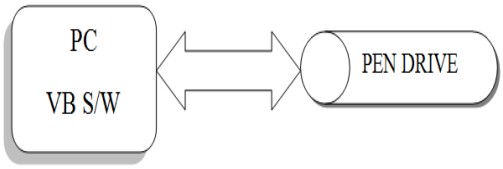

Fig 2: Proposed Model System-Encoder

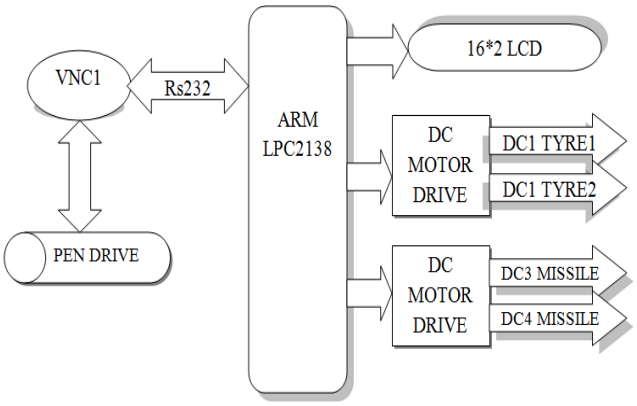

Fig 3: Proposed Model System –Decoder

Encoder unit:

This section consists of a master pc terminal on which we are developing our own vb s/w. The vb s/w is used to encode the frame and send the encoded frame to the master

Microcontroller. The master Microcontroller then stores this encoded frame to the SD card in a text format.

Interfacing of ARM LPC 2148 board and Computer

The RS232 port of computer is connected to RS232 Port0 of ARM LPC2148 boards. The AES encryption and decryption code is dumped onto ARM through RS232 port by using a flash burner called Philips flash utility V2.2.3.

Decoder unit:

In this section the user has to insert the SD card into the SD card slot connected to the Microcontroller. The Microcontroller then reads the encode frames from SD card and decodes the frame by applying the AES algorithm. Then finally the encoded frame is displayed on LCD. The decoder Microcontroller decodes the no of steps the motor is supposed to move after the decoding is over the decoder unit Microcontroller turns the motor based missile model giving us the exact position of missile.

This system basically consists of SD card interface, LCD display and the dc motor for missile navigation.

www.manaraa.com

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014)

V. Application In Text Encryption

In order to present the performance of this encryption system, we take the text encryption based on the system for example. The chaotic sequence used in this experiment is generated from equation (1). The three different encryption algorithms have the same initial conditions. The condition is that a=35, b=3, c=20, d=5, k=5 and x=1.0, y=1.0, z=1.0, u=1.0. Fig. 3 shows the plaintext, and Fig. 4, Fig. 5 and Fig.6 show the cipher text, respectively, encrypted by the above three different algorithms

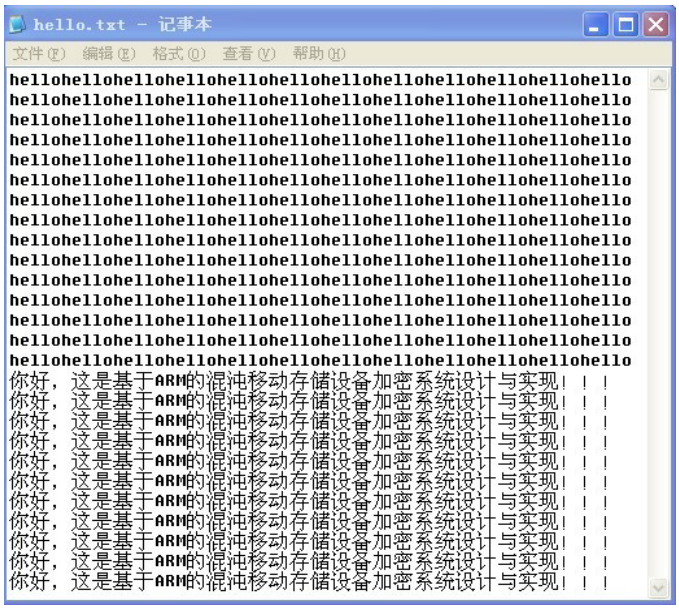

Figure 4: Plaintext

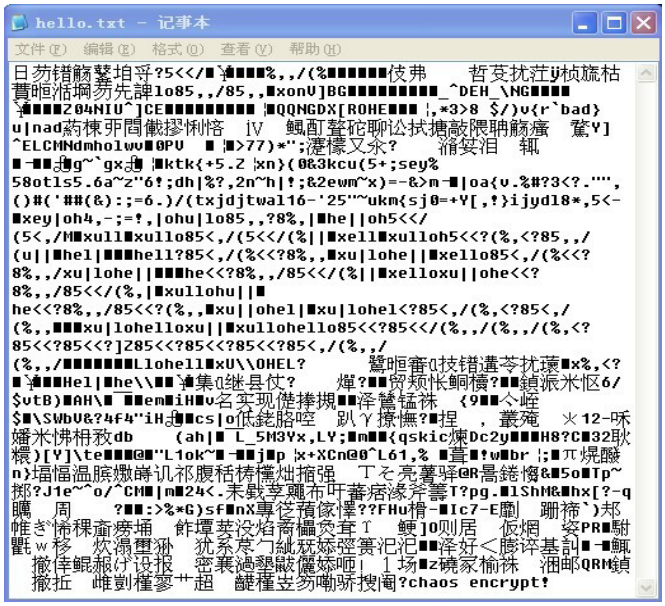

Figure 5: Cipher text of Stream Cipher

Figure 6: Cipher text of using chaotic sequence as the key of AES

www.manaraa.com

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 4, Issue 7, July 2014)

Figure 7: Cipher text of Using chaotic sequence as the expand key of AES.

VI. Performance Analysis Of System

Speed of encryption

An experiment is done to test the speed of encryption. The target to encrypt is a PDF file, whose size is 7.1M. The values given by the Table1 are the average speed of many test results.

Table 1
Test Results

ENCRYPTION ALGORITHM	ENCRYPTION SPEED(M/min)	DECRYPTION SPEED(M/min)
Stream cipher based on chaos	23.72	38.10
Using Chaotic sequence as the key of AES	5.87	5.05
Using Chaotic sequence as the expand key of AES	5.32	5.18

A Security of the encryption system

1) Using the unattached encryption device based on ARM instead of designing software on PC.
2) A login GUI is designed to prevent unauthorized user from invading.
3) Several different chaos maps and encryption algorithms are provided to improve the security of this system.
4) The values of parameters are set by user, which means that the secret keys are only known by the user himself.

VII. Encryption Algorithm Implementation

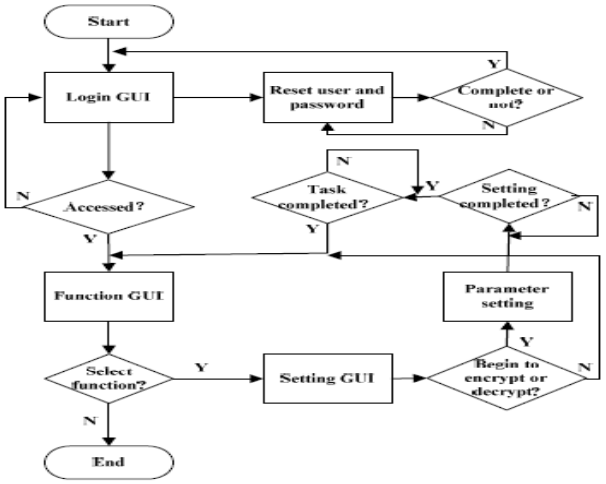

Figure 8: The software procedure.

Here we write the GUI code in visual basic. Which relatively contain two windows namely sending window and receiving window respectively? Above fig.5 shows the data of any kind e.g. „128 AES algorithm" which is send during encryption. After sending this data by the sender at the receiving end this encrypted data is converted through plain text by AES decryption. At sender side the encrypted data LCD shows the cipher text message while at receiver side the LCD shows the plaintext message at the ending.

Algorithm Strengths:

- The difficulty of knowing where any value is in the table.
- The difficulty of knowing which location in the table is used to select each value in the sequence.
- A particular AES Algorithm key can be used only once. Encryption is about 10 times faster than DES.

VIII. Conclusion

Implementation of Detection of storage Device: encryption By AES Algorithm on embedded platform is presented in this paper. According to the previous research work the researcher was used the separate memory for hardware and software. For the implementation of shift rows and substitute byte on software and add round keys and mixed column operations on hardware. But in this proposed work we implemented both on hardware. That increases the speed and effective area and decreases time for implementation. That makes the system more reliable and reducing its cost.

www.manaraa.com

Acknowledgement

I would like to thank all mighty for the successful completion and moreover the teaching staff of the college for their persistence in keeping me on schedule and quality. I am thankful to my seminar guide Prof. Nagnath B.Hulle, for his active involvement and guidance throughout the seminar work. I would like to thank many other individuals from department, including our respected M.E coordinator Prof.Vishal Bhope who contributed greatly to this seminar work and provided us all the proper facilities. I would also like to thank our respected principal sir for providing us good infrastructure and all amenities. Sincere thanks to the management and the lab attendants for their full cooperation throughout the seminar work. Last but not the least my friends and my family for their continuous support and encouragement.

If I forget to give thanks as well as if I forget to mention reference name of anybody in reference list I apologies for that.

REFERENCES

[1] N. Sloss, D. Symes, and C. Wright, ARM System Developer"s Guide,Designing and Optimizing System Software, Morgan Kaufmann, 2004.

[2] Journal of research of the NIST, volume 106, November 3, May-June 2001

[3] NIST, Advanced Encryption Standard (AES), (FIP PUB 197), November 26, 2001.

[4] J. Daemen and V. Rijmen, AES Proposal: Rijndael (Version 2). NIST AE.

[5] UM10120 LPC2131/2/4/6/8 User manual File Format: PDF/Adobe Acrobat Numerous editorial updated throughout the user manual. 02. 2006.09.18. Updated edition of the User Manual covering both LPC213x and LPC213x/01 devices. For www.nxp.com/documents/user manual/UM10120.pdf.

[6] M. McLoone, J. McCanny, "High Performance Single-Chip FPGA Rijndael Algorithm Implementations," Proceedings Cryptographic Hardware and Embedded Systems Workshop, CHES, Paris, May 2001.

[7] B. Gladmans, A specification for Rijndael, the AES Algorithm. Available at http://fp.gladman.plus.com, May 2002.

[8] T.Ravichandra Babu, K.V.V.S.Murthy, G.Sunil , "AES Algorithm Implementation using ARM Processor",2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011.

[9] G. Bertoni, L. Breveglieri, P. Fragneto, M. Macchetti and S. Marchesin, "Efficient Software Implementation of AES on 32-bit Platforms," CHES 2002, LNCS 2523, pp. 159–171, 2003.

[10] R. Ashruf et al, Reconfigurable Implementation for the AES Algorithm, Delft University of Technology, Netherlands, 2005.

[11] K. Atasu et al, Efficient AES Implementation for ARM Based Platforms, ACM, 2004 Philips LPC2131, LPC2132, LPC2134, LPC2136, LPC2138 Data Sheet.

www.manaraa.com