ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Improved Crypto Analysis for Scrambling Digital Video Using Secret Key

S.Hemalatha[1], V.Hemamalini[2], S.Manimozhi[3], B. Revathi[4], S. Sridevi[5]

Assistant Professor, Department of ECE, New Prince Shri Bhavani College of Engg. & Tech., Chennai, India [1&2]

Department of ECE, New Prince Shri Bhavani College of Engg. & Tech., Chennai, India [3,4&5]

ABSTRACT: In the modern technology world, information security is very essential to communicate the confidential data between the networks. The cryptography is used to data transmission, information storage and also useful for system communication. for that, we implemented a high speed AES algorithm in order to provide the high security, reliability, safety for the transmitted data. The video is converted to image frames, then is converted to the VHDL codes in the MATLAB 2014a.The AES algorithm is used for transmitting the text, images, videos with available key values of the 128,198,256 bits. But, here the security is implemented with 128 key values of the AES algorithm for video cryptography in the VHDL implementation. The proposed system of the algorithm provides the high processing speed in the order of ps(>6800ps). The algorithm is implemented in ModelSim-Altera 6.3g_p1 (Quartus II 8.1) Web Edition. The video cartography is processed in video size of 8Mbps. The encryption and decryption is processed in VHDL with the digital output.Finally, the video is viewed by the single board computer Raspberry pi.

KEYWORDS: AES, VHDL, encryption, decryption and block cipher.

I. INTRODUCTION]

Cryptography is the science of information and communication security. Cryptography is the science of learning secret codes which provides the confidentiality communication through an unsecured channel. (i.e) It protects the information against unauthorized parties by preventing secret keys for users. Mostly Cryptography is used to Scramble the Plaintext into other form. To protect the data transmission from unsecured channels, two types of cryptographic systems are used: Symmetric and Asymmetric cryptosystems. Symmetric cryptosystems such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) uses an identical key for the sender and receiver; both to encrypt the message text and decrypt the cipher text. Asymmetric cryptosystems such as Rivest-Shamir-Adleman (RSA) &Elliptic Curve Cryptosystem (ECC) uses different keys for encryption and decryption. Symmetric cryptosystem is more suitable to encrypt large amount of data with high speed. AES encryption is an efficient scheme for both hardware and software implementation. Due to Hardware implementation we get high security and speed compared to software implementation. In wireless Communication Hardware Implementation are mostly useful with high security like military communication and mobile telephony where there is a greater emphasis on the speed of communication. AES algorithm is widely applied in the financial field or domestic, such as ATM, Intelligence Card in that it is useful to realize the encryption.

II.BACKGROUND

A MPEG (Moving Picture Expert Group) [13] video is composed of sequence of group pictures(Gops).I,P and B.I called intra coded frames are the types of GOP and are compressed without reference too any other frames.

Choosen [7], proposed a fully layered scheme, in which the full content is compressed. Then the compressed bit stream is entirely encrypted using AES or DES algorithm. This principles can be achieved by permutation of macroblocks both by XOR operation on permutted block .Although the full content of the video is not encrypted only certain or selective part of the video is encrypted in the form [1,8] using text based algorithm which limits the encryption time of the frame..

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

The [5] proposed another selective video encryption algorithm (VEA). The encryption is done using XOR, (example bit of I frame, video motion). The VEA is faster than selective algorithm. In this the frame is divided in to two halves .The both are stored in one half .It provide good security and reduces the number of XOR operations.
Another category of algorithm is based on scramble (permutation), once the DCT Coefficients are permutted, the computation efficiency leads to security cost .The trade off security is the drawback of this method .For complete and protable security of video data, the entire video needs to be encrypted, however a naiie encryption of the complete stram is infeasible.

In this paper the video are encrypted using a standard algorithm called AES (Advanced encryption standard). The AES algorithm is the advanced version of RC5 algorithm. This method is supposed to be most secure for transmission of video for real time application. The input video is get through by Matlab software. Then the videos are divided into n number of frames. The encryption and decryption are carried out by AES algorithm in matlab which is converted into verilog HDL by fdatool and simulated using modelsim PE. The Raspberry pi used which for displaying the decrypted video. The long distance transmission of video or data can be possible by using Raspberry pi by knowing the IP address for both source and destination in the real time application. The proposed algorithm (i.e.) Advance Encryption Standard algorithm using modelsim software takes less time for the encrypting the video frame and the clarity of video is maintained significantly.

II. THE AES ALGORITHM

The AES is a substitution permutation network (SPN) developed by Joan Daemen and Vincent Rijmen Andthis SPN was approved by the U. S. National Institute of Standards and Technology (NIST) which consider as the new Advanced EncryptionStandard (AES). It became official in October 2000, replacing DES (FIPS 197, 2001). (AES, Rijndael)algorithm is a symmetric block cipher that processes data block of 128, 192 and 256 bits using, respectively,keys of the same length. In this paper, only the 128 bit encryption version (AES-128) is considered. Rijndaeloperates on a state that is initialized with a plaintext block, and after encryption this contains the cipher text.

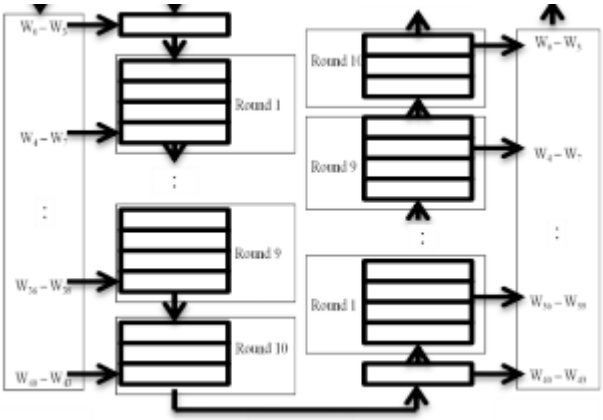

Fig.1. Encryption and decryption process of AES algorithm

1. AES encryption

The AES algorithm operates on a 128-bit block of data.128,192 and 256 are the key length used. The pre-round and last rounds differ from other rounds, there is an Add Round Key transformation in pre-round and no Mix Columns transformation is performed in the last round as shown in fig. 1. In this paper, we use the key length of 128 bits as a model for general explanation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

1.1 Sub Bytes Transformation

The Sub Bytes transformation includes non-linear byte substitution, it operates on each state bytes independently. This is done by using a previously calculated substitution table called S-box. S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values. Advantage of performing the S-box computation in a single clock cycle, reducing the latency and avoids complexity of hardware implementation.

1.2 Shift Rows Transformation

Shift Rows transformation includes, the rows are shifted in cyclic manner. Row 0 remain unchanged ; row 1 does shift of one byte to the left; row 2 does shift of two bytes to the left and row 3 does shift of three bytes to the left.

1.3 MixColumns Transformation

Mix Columns transformation includes, the columns are considered as polynomials in states and multiplied with fixed polynomial by modulo x4+1,given by: c(x)={03}x3 + {01}x2 + {01}x + {02}.

1.4 Add Round Key Transformation

Add Round Key transformation includes, a Round Key is added to the State - resulted from the operation of the Mix Columns transformation - by a simple bitwise XOR operation. The Round Key for each round is derived fromthe main key using the Key Expansion algorithm. The encryption/ decryption algorithm needs eleven 128-bit Round Key, which are denoted by Round Key[0] to Round Key[10].

2. AES decryption

Reverse of encryption which inverses round transformations to compute the original plaintext from cipher-text in reverse order called as decryption. Therounds of transformation of decryption use the functions Add Round Key(ARK), Inv Mix Columns(ICM), Inv Shift Rows(ISR), and Inv Sub Bytes(ISB) successively as shown in fig. 1.

2.1 Add Round Key

Add Round Key is its own inverse function because the XOR function is its own inverse. Here cipher text state XOR with round key . The round keys obtained from key expansion algorithm selected in reverse order.

2.2 Inv Shift Rows Transformation

Inv Shift Rows functions in the same way as the Shift Rows, only in the opposite direction. The first row is not shifted, Shifting of 2nd ,3rd and 4th row with right by one step, two and three bytes respectively.

2.3 Inv Sub Bytes transformation

From once-pre calculated substitution table called Inv S box, Inv Sub Bytes transformation is done. Inv S-box table contains 256 numbers (from 0 to 255) and their corresponding values.

2.4 Inv Mix Columns Transformation

Inv Mix Columns transformation includes, ,polynomials of degree less than 4 over GF (28) which coefficients are the elements in the columns are multiplied with modulo (x4 + 1) by a fixed polynomial d(x) = {0B}x+{0D}x2 + {09}x + {0E}, where {0B}, {0D}; {09}, {0E} denote hexadecimal values.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

IV. THE PROPOSED ARCHITECTURE

There are many techniques to design AES architecture to yield optimized implementation. Basic architecturein which each round manipulates 128 bit together and encrypts them by one clock cycle. Proposed architecture is implementing 128 bits data-path or both cipher key and plaintext. Thedeveloped architecture combines basic architecture with one round and chopping technique to compromise the area with speed.

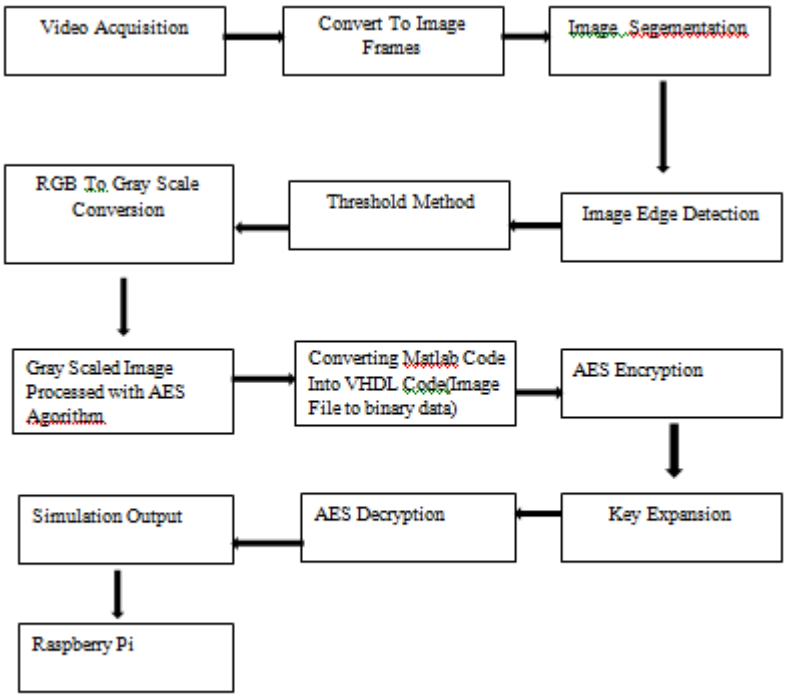

Fig.2. Proposed Architecture

The code of the proposed design is implemented in VHDL code. Since the main point of the proposed architecture is to compromise the data rate and speed.

V. SIMULATION RESULTS

decryption The design has been coded by Verilog HDL. the results of all encryption and process are synthesized and simulated based on the Model SimPE 10.4. The results of simulating theencryption/decryption algorithm from the ModelSim simulator are shown in Fig3 and Fig4.

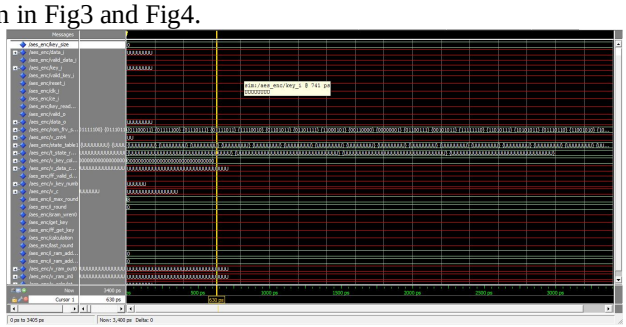

Fig 3 Timing simulation of AES encryption algorithm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

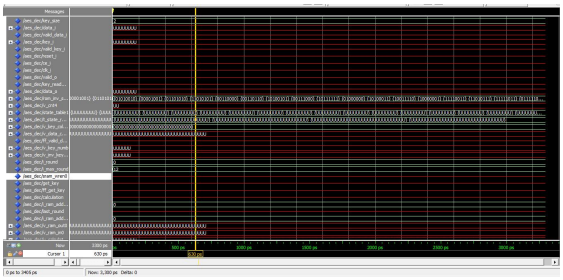

Fig 4. Timing simulation of AES decryption algorithm

Hence, the encryption decryption method are analysed by practical result . To test the system, a test bench is used. The test benchshows encryption/decryption input pulse triggering . The output result of the encryption and decryption was founded accurately.

VI. COMPARISIONS

In this section, the results are obtained and compared our result with existing paper and other equivalentimplementations is given. Proposed system design of AES 128-bit encryption/decryption algorithm wassynthesized, implemented by Raspberry Pi. Therefore it allows us toprocess data in communication applications requiring a high security communication.

VII. RESULTS

The paper proposes AES design combines key schedule and cipher block. Pre computation key is considered in this algorithm. A Matlab file is to get the input video and converted into VHDL using fda tool command. The proposed AES architecture which is described by VHDL is simulated using ModelSim to verify the functionality as a primer verification tool.

VIII. CONCLUSION

The Advanced Encryption Standard algorithm is asymmetric block cipher that can process data blocks of 128bits through the use of cipher keys with lengths of 128, 192, and 256 bits. In our project, we are going to improve processing speed and maintaining clarity of video which is viewed in Raspberry pi implementation. Also, improvement in modelsim which resist various kinds of password attack on AES algorithm plain text data. The Advanced Encryption Technique was implemented successfully using ‘VHDL’ language. Various data messages were encrypted using different keys and variable key size. The original data was properly received via decryption of the ciphered video. The modifications in the code was tested and proved to be accurately encrypting and decrypting the data messages with even higher security and immunity against the unauthorized users.

IX. FUTURE WORK

This Implementation of 128 bit AES algorithm in modelsim, and the same can be extended to encrypt 192 and 256 bits of plain text data with proper key length, which makes even tougher to decrypt the original data form an unauthorized receivers.

REFERENCES

[1] P. N. Tudor. MPEG-2 video compression.In Electronics and Communication Engineering Journal, December - 1995.
[2] T. B. Maples and G. A. Spanos. Performance Study of a Selective Encryption Scheme for the Security of Networked, Real-Time Video.In Proc. of Fourth International Work-shop on Multimedia Software Development ’96), 1995.
[3] E. Choo, L. Jehyun, L. Heejo, and N. Giwon. SRMT: A lightweight encryption scheme for secure real time multimedia transmission. In Multimedia and Ubiquitous Engineering, p60–65, 2007.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

[4] I. Agi and L. Gong. An empirical study of MPEG video transmission.In Proc. of the Internet Society Symposium on Network and Distributed Systems Security, p137–144, 1996.
[5] A. Biryukov and E. Kushilevitz. From differential cryptanalysis to ciphertext-only attacks. Lecture Notes in Computer Science, Advances in Cryptology – Proceedings of CRYPTO'98, 1462:72–88, 1998.
[6] A. Biryukov and E. Kushilevitz.Improved cryptanalysis of RC5. Lecture Notes in Computer Science,1403:85–100, 1998.
[7] Z. Chen, Z. Xiong, and L. Tang.A novel scrambling scheme for digital video encryption. In Proc. of Pacific-Rim Symposium on Image and Video Technology (PSIVT), p997–1006, 2006.
[8] L. S. Choon, A. Samsudin, and R. Budiarto.Lightweight and cost-effective MPEG video encryption. In Proc. of Information and Communication Technologies: From Theory to Applications, p525–526, 2004.
[9] L. Qiao and K. Nahrstedt.A new algorithm for MPEG video encryption.In Proc. of First International Conference on Imaging Science System and Technology, p21–29, 1997.
[10] R. L. Rivest. The RC5 encryption algorithm.In Proc. of the Second International Workshop on Fast Software Encryption (FSE), p86–96, 1994.
[11] B. Schneier. Applied Cryptography Second Edition Protocols Algorithms and Source Codes in C, 1996.
[12] L. Tang. Methods for encrypting and decrypting MPEG video data efficiently.In Proc. of ACM Multimedia, p219–229, 1996.
[13] W. Tsang, B. Smith, S. Mukhopadhyay, H. H. Chan, S. Weiss, M. Chiu, and J. Song. The DALI multimedia software library.In IEEE 2nd Workshop on Multimedia Signal Processing, 1999.
[14] T. Uehara and R. Safavi-Naini.Recovering DC coefficients in block-based DCT.In Proc. of IEEE Transactions on Image Processing, volume II, p3592–3596, 2006.
[15] W. Zeng and S. Lei.Efficient frequency domain selective scrambling of digital video.In Proc. of the IEEE Transactions on Multimedia, p118–129, 2002.