Implementation of Cryptography Algorithm for Video on FPGA

Mr.VEDPRAKASH SHARMA[1], Ms. Nabila Shaikh[2]
[1] PG Student, Department of master of Engineering, LJ Institute of Engineering and Technology, Gujarat,, India
[2] Assistant Professor, Department of master of Engineering, LJ Institute of Engineering and Technology, Gujarat, India

ABSTRACT

Advances in digital media content transmission have increased in the past few years. Security of multimedia data is an imperative issue because of fast improvement of digital data exchanges over an unsecured network. Multimedia data security is achieved by methods of cryptography, which deals with encryption of data. Standard symmetric encryption algorithms provide better security for the multimedia data, but applying symmetric key encryption algorithm on more complex multimedia data we face computational problem. Over the last few years, several encryption algorithms have applied to secure video transmission. While a large number of multimedia encryption schemes have been proposed in the literature and some have been used in real time applications, cryptanalytic work has shown the existence of security problems and other weaknesses in most of the proposed multimedia encryption schemes. Encryption is a common technique to uphold multimedia security. MPEG video stream is quite different from traditional textual data because inter frame dependencies exist in MPEG video. Special MPEG video encryption algorithms are required because of their special characteristics, such as coding structure, large amount of data and real-time constraints. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, and military communication. The Advanced Encryption Standard (AES) algorithm is used and modified it, to reduce the calculation of the algorithm and for improving the encryption performance.

Keyword: MAES, AES, RSA, VIDEO, 3DES, FPGA, SYMMATRIC CRYPTOGRAPHY, RTL

1. INTRODUCTION

Encryption is the process of encoding information so it cannot be read by hackers. The information is encrypted using AES algorithm and is converted into a form unreadable, which is called a cipher text. The authorized person will decode the information using decryption algorithms. The cryptography algorithms are of three types symmetric cryptography (using 1 key), asymmetric cryptography (using 2 different keys), and cryptographic hash functions using no keys. Symmetric algorithms are faster than asymmetric algorithms since the CPU cycles needed for symmetric encryption are fewer than for asymmetric encryption. Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple DES, Rivest Cipher (RC2), Rivest Cipher (RC6), and Blowfish are some of the symmetric algorithms. Users are eager to not only enjoy the convenience of real-time video streaming also share various media information in a rather cheap way without awareness of possibly violating copyrights. In view of these, encryption and watermarking technologies have been recognized as a helpful way in dealing with the copyright protection problem in the past decade. Encryption allows secure end–end communication of data while digital watermarking allowing still faces some challenging difficulties for practical uses; there are no other techniques that are ready to substitute it. Within the signal processing and multimedia communities, many schemes have been proposed for protecting sensitive information while allowing certain legitimate operations to be performed. These schemes typically lack a rigorous model of privacy, and their protection becomes questionable when scaled to large datasets. The cryptography community has long developed rigorous privacy models and provably secure procedures for data manipulations. However, these

procedures are primarily designed for generic data. As a result, they usually lead to a blow up in computational costs and overheads when applied to real-life multimedia applications. In a real time, the transmitted frames are sent within a minimum delay. Also, video frames need to be displayed at a certain rate; therefore, sending and receiving encrypted data must be sent at a certain amount of time so as to utilize the acceptable delay such as Video on-Demand requires that the video stream needs to be played whenever the receiver asks. So, there are no buffer or playback concepts for the video stream (i.e. it runs in real time). The size of a two - hour MPEG video is about 1 GB. Performance of processing multimedia streams should be acceptable. The encryption techniques should be fast enough and require a small overhead in comparison to compression techniques. The security of video data is needed for many applications such as Computer forensics and Distance education. Computer forensics require secured good quality video for presenting digital evidence in the courtroom, and Distant education and training needs encryption for no alteration of information.

2. PROPOSED BLOCK DIAGRAM

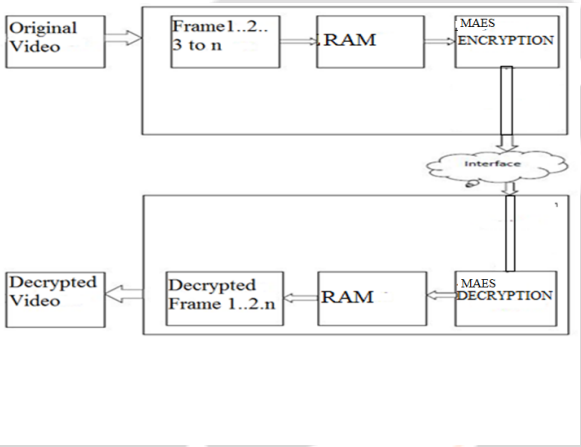

Fig.1 Proposed Block Diagram [2]

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. Three types of algorithms that will be discussed here.

1. Symmetric Key Cryptography (Secret Key Cryptography)
2. Asymmetric Key Cryptography (Public Key Cryptography)
3. Hash Function

1. Symmetric Key Cryptography (Secret Key Cryptography)

a) Same Key is used by both parties
b) Simpler and Faster

2. Asymmetric Key Cryptography (Public Key Cryptography**)**
a) Two different keys are used Users get the Key from a Certificate Authority**.**

b) Authentication in asymmetric cryptography is more secured but the process is relatively more complex as the certificate has to be obtained from certification authority

In the following proposed block diagram we convert our original video in to number of Frames then it is store in to the RAM and then after MAES Encryption and Decryption we get our Decrypted video (original video).

Modern cryptography concerns itself with the following four objectives:

1) Confidentiality (the information cannot be understood by anyone for whom it was unintended)

2) Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)

3) Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)

4) Authentication (the sender and receiver can confirm each other's identity and the origin/destination of the information)

2.1 Comparison between Different Algorithms:

Factors	RSA	DES	3DES	AES	MAES
Created by	Ron Rivest,Adi Shamir, Leonard Adelman in 1978	IBM in 1975	IBM in 1978	Vincent Rijman, Jon Doorman in 2001	-
Key length	Depends on the number of bits in the module, n=p*q	56 Bits	168 bits(k1,k2 and k3) 112 bits(k1 and k2)	128,192,256 Bits	512,768,1024 Bits
Round(s)	1	16	48	10-128 bits,12-192 bits,14-256 bits	10
Block type	Variable	64 Bits	64 Bits	128 Bits	128 Bits
Cipher type	Asymmetric	Symmetric	Symmetric	Symmetric	Symmetric
Speed	Slowest	Slow	Very slow	Fast	Very Fast
security	Least secure	Not secure enough	Adequate security	Excellent security	Most secure among them

Table 2.1 Comparison between Different Algorithms [2]

2.2 MAES (Modified Advanced Encryption Standard) Algorithm:

This standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 384, 512, 768 and 1024 bits. Rijndael was designed to handle additional block sizes and key lengths. AES used with the key length of 128,192 and 256 bits. The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "MAES-384", "MAES-512" and "MAES-768" "MAES-1024". But MAES algorithm can be used with more number of bits.

There are 10 rounds for full encryption. The four different stages that we use for Modified-AES Algorithm are:

- Substitution bytes
- Shift Rows
- Permutation
- AddRoundKey

Substitution Bytes, Shift Rows and AddRoundKey remain unaffected as it is in the AES. Here the important function is Permutation which is used instead of Mix column. These rounds are managed by the IP table. Permutation is widely used in cryptographic algorithms. Permutation operations are interesting and important from both cryptographic and architectural points of view. The DES algorithm will provide us permutation tables. The inputs to the IP table consist of 128 bits. Modified-AES algorithm takes 128 bits as input. The functions Substitution Bytes and Shift Rows are also interpreted as 128 bits whereas the Permutation function also takes 128 bits. In the permutation table each entry

indicates a specific position of a numbered input bit may also consist of 256 bits in the output. While reading the table from left to right and then from top to bottom, we observe that the 242th bit of the 256-bit block is in first position, second position and so forth. After applying permutation on 128 bits we again complete set of 128 bits and then perform next remaining functions of algorithm. If we take the inverse permutation it gives again the original bits, the output result is a 128-bit cipher text. For the full decryption of Modified-AES algorithm the transformation processes are, Inv-Bytesub, Inv-Shiftrows, Inv-Permutation, and the Addroundkey, which are performed in 10 rounds as it is in the encryption process.

3. Simulation Result :

By applying modified advanced encryption on HD video we get these type of encrypted image frame of video,

Image 1 **Final Encrypted Image**

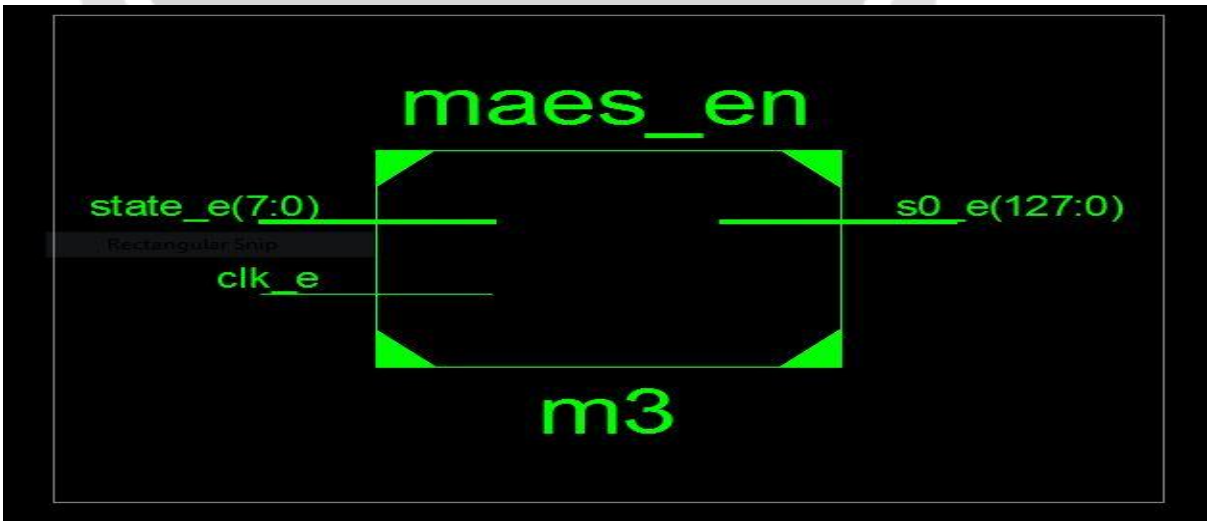

Fig 3.1 RTL Schematic of MAES Encryption

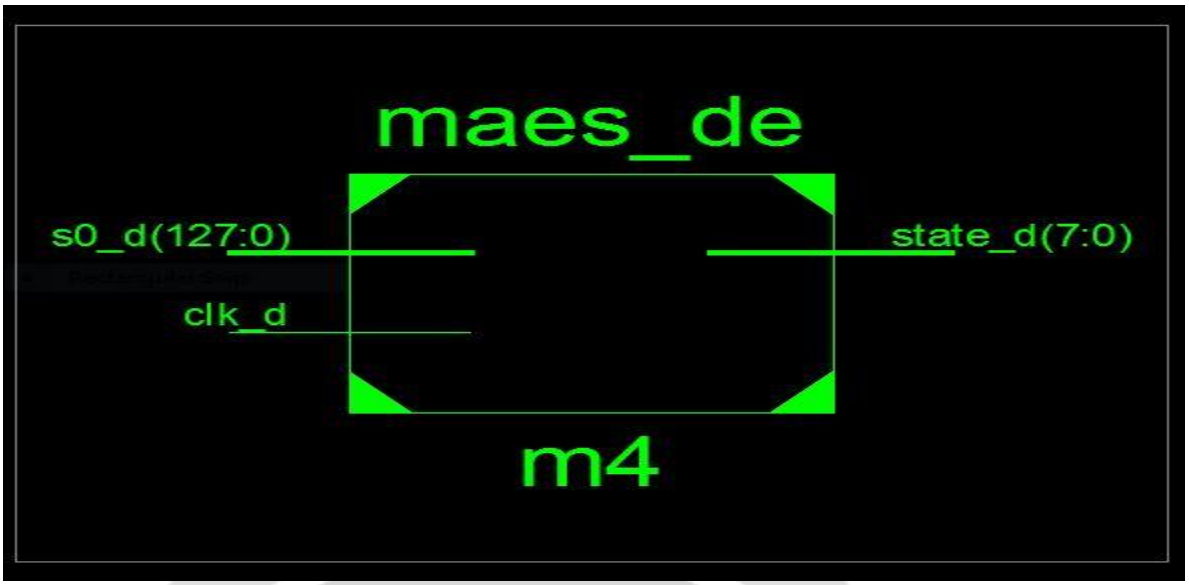

Fig 3.2 RTL Schematic of MAES Decryption

3.1 FPGA Implementation

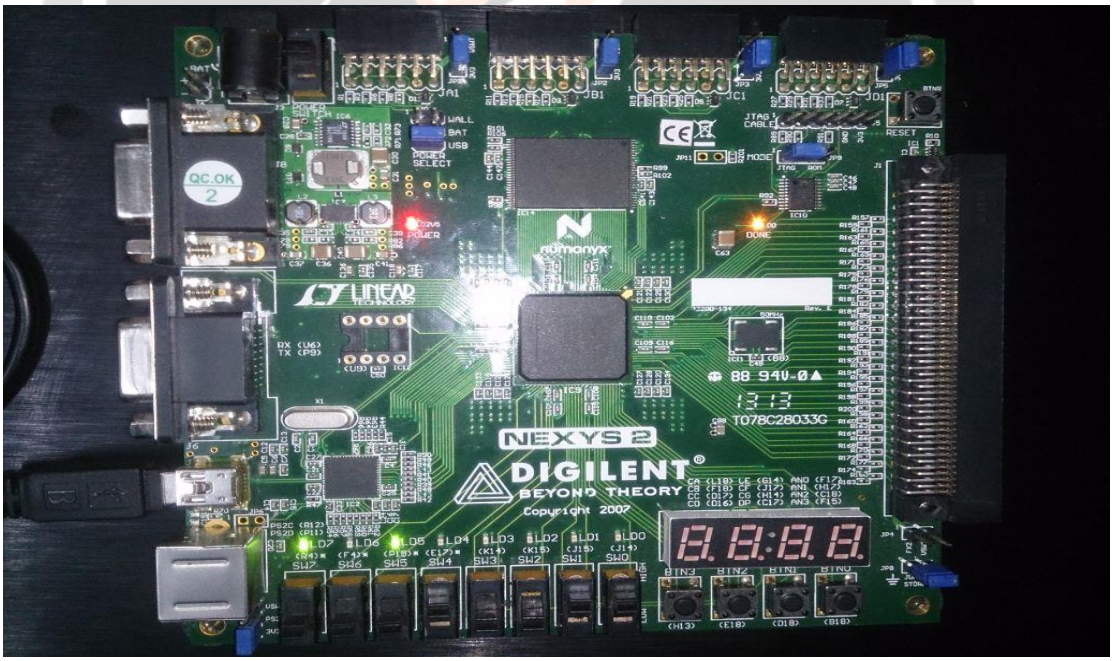

Fig 3.3 SPARTAN 3E- 500

4. CONCLUSIONS

Many Encryption Application made earlier which is only for data Encryption. From study of IEEE Paper we conclude that video encryption system is made but there is not reliable means there is some problems occur in this system. So here by using an MAES algorithm we develop a new application which is real video encryption system by which we can secure video and make video security stronger compared to recent security system.MAES uses more number of bits then other algorithm which is advantage of it.

5. REFERENCES

[1] Dhananjay M. Dumbere, Nitin j janwae "Video Encryption Using AES Algorithm" 2nd International Conference on Current Trends in Engineering and Technology, ICCTET'14 © IEEE 2014 IEEE Conference Number - 33344 July 8, 2014, Coimbatore, India.
[2] Ms. Pooja Deshmukh ,Ms.vaishali khole "Modified AES Based Algorithm for MPEG Video Encryption" ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India. ISBN No.978-1-4799-3834-6/14/$31.00©2014 IEEE
[3] S.Sridevi sathya Priya,P.Karthigai Kumar, N.M. SivaMangai, V.Rejula "FPGA Implementation of Efficient AES Encryption "IEEE Sponsored 2nd International Conference on Innovations in Information Embedded and Communication Systems ICIIECS'15 978-1-4799-6818-3/15/$31.00 © 2015 IEEE
[4] JG pandey, S gurunarayan "Architectures and Algorithms for Image and Video Processing using FPGA-based Platform "978-1-4799-4006-6/14/$31.00 ©2014 IEEE
[5] Vakkayil Megha Gopinath "MAES Base Data Encryption and Description Using VHDL" © 2015 IJEDR | Volume 3, Issue 2 | ISSN: 2321-9939
[6] Pravin Kawle, Avinash Hiwase, Gautam Bagde, Ekant Tekam, Rahul Kalbande "Modified Advanced Encryption Standard" ISSN: 2231-2307, Volume-4, Issue-1, March 2014
[7] Gurupeet singh and supriya "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security" International Journal of Computer Applications (0975 – 8887) Volume 67– No.19, April 2013
[8] Shraddha Soni, Himani Agrawal, Dr. (Mrs.) Monisha Sharma "Analysis and Comparison between AES and DES Cryptographic Algorithm" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012 ISSN: 2277-3754
[9] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona "ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES" DOI : 10.5121/ijnsa.2014.6404
[10] A.Romeo, G.Romdotti, M.Mattavelli and D.Mlynek."Cryptosystem Architecture for Very High Throughput Multimedia Encryption: The PRK Solution.The 6th IEEE International Conference on Electronic,Circuit and System,September 5-8.Procedding of ICECS 99,Vol .1, 261- 264
[11] Ranjeet Masram, Vivek Shahare, Jibi Abraham, Rajni Moona "ANALYSIS AND COMPARISON OF SYMMETRIC KEY CRYPTOGRAPHIC ALGORITHMS BASED ON VARIOUS FILE FEATURES" DOI : 10.5121/ijnsa.2014.6404
[12] A.Romeo, G.Romdotti, M.Mattavelli and D.Mlynek."Cryptosystem Architecture for Very High Throughput Multimedia Encryption: The PRK Solution.The 6th IEEE International Conference on Electronic,Circuit and System,September 5-8.Procedding of ICECS 99,Vol .1, 261- 264

BOOKS:

[1] Data communication And Networking by BEHROUZ a FOROUZAN

WEBSITES:

[1] http://www.cryptographyworld.com/algo.htm
[2]http://stackoverflow.com/questions/5554526/comparison-of-des-triple-des-aes-blowfish-en and http://www.scenesavers.com/grfx/SD_HD_UHD.pdf