Video Frame Encryption Algorithm using AES

Keshav S. Kadam
EXTC Department
SKNCOE Vadgaon(bk) Pune
Maharashtra,India

Prof. A. B. Deshmukh
EXTC Department
SKNCOE Vadgaon(bk) Pune
Maharashtra,India

***Abstract*-The data in some fields may include some sensitive information which should be protected from outside world while transmitting over network. Therefore security & privacy of sensitive data is one of the important issues. Proposed methodology in this paper focuses on the security & privacy of a digital video. The proposed research includes three parts, that is first one is MPEG video compression, second one is video encryption and third one decryption. For encryption we used the AES algorithm.AES algorithm is a block cipher & most used algorithms. Here, encryption of video streams is directly on the compressed domain Thus it preserves the compression & decompression time cycle.**

***Keywords*- AES, MPEG, Video encryption, Video Transmission,**

I INTRODUCTION

A system for encrypting and decrypting information is a cryptosystem. Encryption usually involves an algorithm for combining the original data plaintext with one or more keys numbers or strings of characters known only to the transmitter and/or receiver. The resulting output of encryption is known as cipher text[1]. Cryptographic algorithms play an important role in security and resource conservation of real time applications. Cryptography is science in which information is transmitted over network securely. In the cryptography there is a process in client-server model. At server side encryption is done. Encryption is nothing but conversion of plaintext data into cipher text so that unauthorized user cannot access it. That encrypted data are transmitted over network to the client. At client side decryption is done in which cipher text is converted in to the plain text. To protect data using cryptographic system there are two type of cryptographic algorithm one is symmetric key algorithm and second is asymmetric key algorithm. In symmetric key algorithm same key is used at sender as well as receiver side [2][3].Data Encryption Standard (DES) and Advance Encryption Standard (AES) are the example of symmetric key algorithm. While in asymmetric key algorithm two different key are used such as Rivert Shamir Adleman (RSA). For hardware as well as software implementation and high speed data transmission AES algorithm is more efficient. In wireless video communication system for high security hardware implementation is most useful [4].

MPEG (moving picture expert group) is most usable standard for video processing applications. Such In multimedia application like Video-on- Demand, video broadcast, multimedia mail and video-conferencing. Security of the video depends on the redundancy in the video as low as redundancy the video is more secure, As attacker get less clues about video. MPEG video is composed of a sequence of group of pictures (GOPs). Each GOP is composed of series of I, P, and B frames. I frames are intra-frame coded without any reference to other frames; P frames are predicatively coded using a previous I or P frames; and B frames are bidirectional interpolated from both the previous and following I and/or P frame. [5]. The security of MPEG video transmission can done by using two method by partial encryption or the entire MPEG bit stream. Algorithm which is use whole data is heavy weight algorithm while algorithm which uses partial or selective data is light weight algorithm. These both algorithms involve complex computations. Heavy-weight algorithm displeases the problem and increases the time while light-weight algorithm provides sufficient security level and has an acceptable computation cost to MPEG video applications. Here we presented an efficient MPEG video encryption algorithm for real-time video transmission by AES algorithm. Here we presented light-weight selective encryption scheme for secure MPEG transmission. It is based on Video Encryption Algorithm (VEA) .VEA is light-weight selective encryption algorithm based on DES/IDEA. The security is significantly improved by adopting AES to encrypt data. This algorithm reduce computation time by processing by bounding the maximum number of bits selected [6].

II. RELATED WORK

For secure MPEG video encryption there are several video encryption algorithm is available which based in DES/IDEA. Every algorithm has its of them has its potency and weakness in terms of encryption ratio, security level, speed, and resulting stream size matrices. The well know video encryption algorithms are Naive algorithm, Pure Permutation Algorithm, Video Encryption Algorithm (VEA), Zig-Zag Permutation algorithm, and selective algorithm [7].The most straightforward method is to encrypt the entire MPEG stream by using standard encryption method such as DES or AES, This is called the Naive algorithm. In Naive algorithm MPEG bitstream is nothing but traditional text data and does not make use of the special any structures. This algorithm is the most secure algorithm but it is not applicable for video encryption because of its speed limit and data of video are big in size. as this algorithm is unable to fulfill the real time video encryption requirement so that it is not used for video encryption[8]. There is different method for selective algorithm which uses the features of MPEG layered structures. The basic selective algorithm uses only I frames for encryption as the value of P and B frames are nothing without knowing the corresponding I frames. But great portions of the video could be visible if p frames and b frames are not encrypted because some of the P and B frames may contain intra-coded I blocks which may visible. If only I frames encrypted it save 35-55% of encryption-decryption time. The size of encrypted stream does not change. One method of encryption is encrypt only MPEG headers. But headers contain mostly standard information and a video stream is indexed by frame in order to perform synchronization so that the beginning of each frame is known to attacker and this is not effective method [9].In Zig-Zag-Permutation algorithm encryption is an integral part of the MPEG compression process. In which Instead of mapping 8x8 block to a 1x64 vector in zig-zag order. This compression process uses a random permutation list to map the individual 8x8 block to a 1x64 vector. It cannot resist the known plaintext attack and is also fenceless to the cipher text only attack. The speed of processing is very fast and nearly the same as the MPEG encoding/decoding time .By this algorithm the size of encrypted MPEG stream will increase by a significant factor [10]. Video Encryption Algorithm (VEA) in this algorithm secret key is used to randomly change the sign bits of all DCT coefficients of MPEG video. Propaganda to VEA is Real-time Video Encryption Algorithm (RVEA). For selected sign bit encryption RVEA uses DES and VEA use only XOR operation. The security of RVEA is expressively improved by adopting secret key cryptography algorithms to encrypt the data. RVEA restrict and reduce its computation time by bounding the maximum number of bits selected[11]. In Pure Permutation algorithm scrambling of byte stream is not part of permutation. The cardinality of the permutation key relies on the security level and the application requirement it can be varied as per requirement. The drawback of Pure Permutation algorithm is same as zig-zag permutation algorithm that it is also vulnerable to the known plaintext attack. Pure permutation algorithm doesn’t have problem with speed as permutation is very fast. But Pure Permutation algorithm does not increase the stream size unless we change keys for each frame [12]

A. *Advance Encryption Standard (AES)*

AES is the standard encryption standard adopted by the NIST (National Institute of Standards and Technology) for securing data while communication. AES works on substitution permutation network. AES has a fixed block size of 128 bits and a key size of 128, 192 or 256 bits. The entire algorithm is divided in to two sections, the Key expansion unit and the state processing unit. The number of rounds is 10 in case of 128 bits key (12 when key length is 192 bit and 14 when the key length is 256). For encryption, each round consists of the following four steps: 1) Substitute bytes, 2) Shift rows, 3) Mix columns, and 4) Add round key. The last step consists of XOR operation the output of the previous three steps with four words from the key schedule [13].

Below table give the comparative study of different video encryption algorithms.

TABLE 1.Comparison of different video encryption scheme

Algorithm	Security	Speed	Size	Encryption Ratio
Naïve	High	Slow	No change	100%
Pure Permutation	Low	Super fast	No change	100%
Zig-Zag Permutation	Very Low	Very fast	Big increase	100%
VEA	High	Fast	No change	50%
Selective	Moderate	Fast	Increase	1%-100%

III PROPOSED METHODOLOGY

The block diagram of proposed method of real time video encryption is shown below.

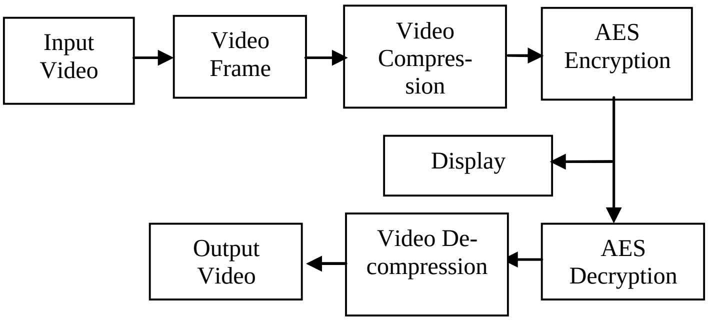

Fig.1. Block diagram for MPEG video encryption-Decryption

As above diagram is includes three part video Compression, AES Encryption and AES Decryption each parts is explained below.

A. *Video compression*

Initially Input video taken from camera with predefined size 256*256 pixels. Sequence of video frame is given to compression. A Frame consist of YUV component where Y represent luminance and UV represent chrominance components.1st this RGB frame convert into gray image. As the gray frame require less bit per pixel .This gray image convert into float image Float image used for DCT. So apply DCT on float image, by applying DCT to the float image get DCT coefficient value. this DCT coefficient value are I frame sign bit .Take sign bit value of DCT coefficient for AES. Apply 128 bit AES algorithm on sign bit value of I frame. From I frame and D frame get motion vectors. Then take out sign value of motion vector.

B. *AES Encryption*

AES is standard chosen by National Institute of standard and Technology(NIST).This algorithm used block cipher of length 128,192 or 256 bits. Here we use 128 bit cipher. The input to the cipher is array of plaintext which is converted as state matrix. For each round, transformation round key is expansion of cipher key and never specified directly. Each round transformation is nothing but four different transformations such as AddRoundKey ByteSub, ShiftRow, and MixColumn,. The repeated application 10 rounds of transformation.

By the video compression we get the sign bit value of I frames and motion vectors this array of sign bit apply to the AES algorithm, Secret key is used to apply encryption. Input for cipher is 4*4 matrix of differential values..After 10 round of AES encryption cipher output is generated which is accessed by person who have secret key.

C. *AES Decryption*

Decryption algorithm is same at encryption and decryption side except at the the decryption time, inverse operations are performed. If user have secret key decryption process carried out. After decryption some of the coefficient are changed which will be propagated by Inverse DCT.

As compare to previous method this proposed method bounding the computation time by limiting maximum number of bit selection. General scheme for the real time video encryption by selective encryption method.

Let P is plain text which produces bit streams C called cipher text , and Tk1 is invertible transformation for video stream. So

Cipher text will get by

$$? \ ? \ ?_{??} ?? ? \tag{1}$$

So the user who Have secret key k2 can only decrypt the video by transformation

$$?_{??} \ ? \ ?_{??}^{??} \tag{2}$$

Decryption process is

$$?_{??} ?? ? ? \quad ?_{??}^{??} ?? ? ? \quad ?_{??}^{??} ??_{??} ?? ?? ? \ \ ? \tag{3}$$

Where k1 is called encryption key while k2 is decryption key.

D. Flow chart of proposed methodology

Proposed methodology can also be explained with help of flow chart given in figure 2. The flow chart show the all steps of systems .

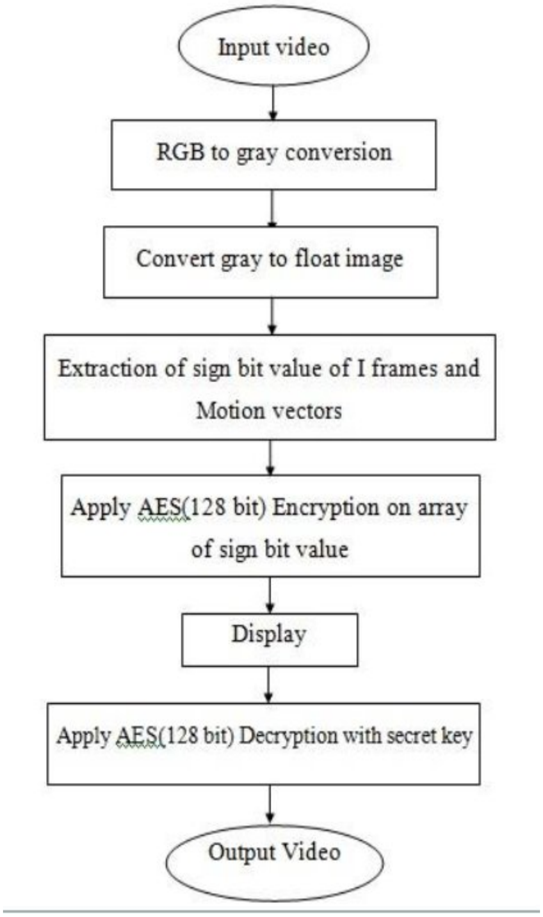
Input video
RGB to gray conversion
Convert gray to float image
Extraction of sign bit value of I frames and Motion vectors
Apply AES(128 bit) Encryption on array of sign bit value
Display
Apply AES(128 bit) Decryption with secret key
Output Video

Fig.2. Flow chart of proposed methodology

IV.EXPERIMENTS

The following experiments were conducted on Real time MPEG video. A secure video communication system is implemented by using Linux platform based Ubuntu operating system . For coding C++ programming language is used. For real-time operation communication encryption is done at the server side while decryption is done at the client side. Here only one system showed that is server side. It is impossible to include all the image frames here. Instead we just show one frame from video sequence to demonstrate our algorithm. The original frame is as shown in Figure 3.

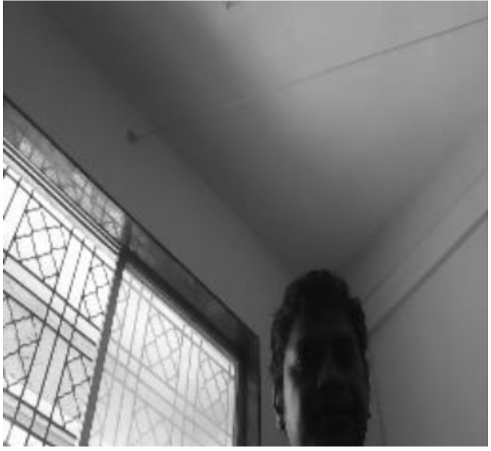

Fig.3. Original frame

By Encrypting sign bits of all DCT coefficients of only I frame: The video image is incomprehensible. This is the medium level of encryption. This is as shown in Figure 4.

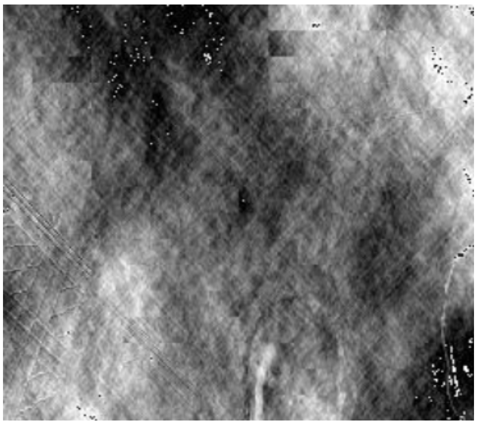

Fig.4. Encryption of sign bit DC and AC coefficients.

Encrypting sign bits motion vector coefficients, the video image is incomprehensible .motion vector taken from I frames and reference frame. Motion vector difference are taken out by motion vectors and P frame. By Appling AES on sign bits of motion vector difference we get higher level of encryption than the previous one. This is shown in Figure 5.

So the figure 2 and 3 are the result of algorithm used for video encryption. Which is sufficient to provide security while real time video transmission. Decryption algorithm is also implemented on given set up and result of the decryption after applying secret key is shown in figure 6.

This result shows that the encryption-decryption of the real time video is possible by using the given algorithm of encryption.

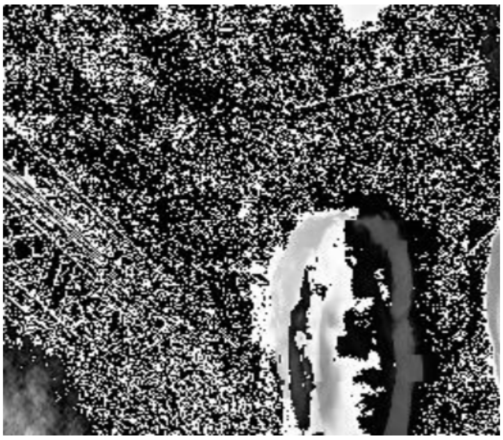

Fig.5. Encryption of sign bits of motion vectors

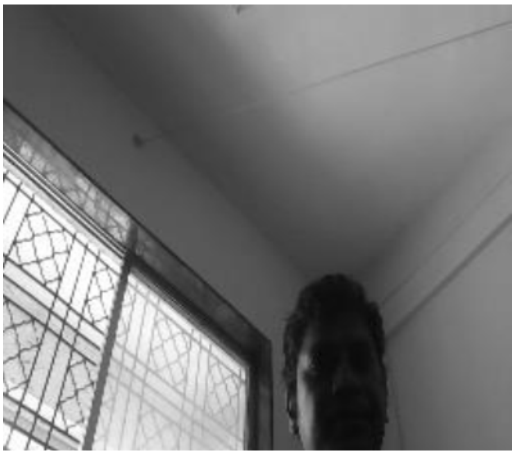

Fig.6.Decrypted video frame

V. CONCLUSION

Selective encryption algorithm selectively encrypts a fraction of the whole video. Which is faster than encrypting the whole video with AES? As studying MPEG frame it s found that in typical MPEG-1 videos sign-bits occupy less than 10% of the entire video bit stream. So that it can save up to 90% of encryption time as compared to the algorithm which encrypts entire video. This algorithm encrypts at most 128 bits, no matter what type of frame is used. This considerably reduces encryption computations achieving satisfactory encryption results. A software implementation is fast enough to meet the real-time requirements of frame decoding. We believe that this can be used for secure real time video transmission applications.

this is software implementation. Farther it will be implemented on Raspberry pi with ARM Processor.

ACKNOWLEDGMENT

Author would like to thanks to Prof. A. B. Deshmukh for his support as a project guide, co-operation and valuable suggestions.

REFERENCES

[1] M. Abomhara, Omar Zakaria, Othman O. Khalifa “An Overview of Video Encryption Techniques”International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010,1793-8201

[2] Ms. Pooja Deshmukh, Ms. Vaishali Kolhe “Modified AES Based Algorithm for MPEG Video Encryption” ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India

[3] Keshav S. Kadam, Prof. A.B. Deshmukh, “A Review on Video Encryption Technologies” International Journal of Advanced Research in Computer and Communication Engineering Vol. 5, Issue 3, March 2016

[4] S.Hemalatha, V.Hemamalini, S.Manimozhi, B. Revathi, S. Sridevi “Improved Crypto Analysis for Scrambling Digital Video Using Secret Key” International Journal of Innovative Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2015

[5] Le Gall, Didier, "MPEG: A Video Compression Standard for Multimedia Applications," Communications of the ACM, vol.34, no.4, pp. 46-58, April 1991.

[6] C. Shi, Sheng-Yih Wang, and Bharat Bhargava,"MPEG Video Encryption in Real-time using secret key cryptography", Proc. Of PDPTA 99, Las Vegas, Nevada 1999.

[7] C. Shi and Bhargava, "A Fast MPEG VideoEncryption Algorithm", Proceedings of 6th ACM International Multimedia Conference ,Bristol, UK, pp. 81-88, September 1998.

[8] S. Lian, Multimedia Content Encryption: Techniques and Applications.CRC, 2008.

[9] I. Agi and L. Gong, "An Empirical Study of MPEG Video Transmission", Proceedings of the Internet Society Symposium on Network and Distributed Systems Security, pp. 137-144. San Diego, CA, Feb. 1996.

[10] Lei Tang, "Methods for Encrypting and Decrypting MPEG Video Data Efficiently", Proceedings of ACM Multimedia 96, pp. 219-229, Boston, MA, November 1996.

[11] L. Qiao and K. Nahrstedt, “A new algorithm for MPEG video encryption,"in Proceedings of The First International Conference on Imaging Science,Systems, and Technology (CISST'97), (Las Vegas, Nevada), pp. 21{29,July 1997.

[12] Adam J. Slagell. Known-Plaintext Attack Against a Permutation Based VideoEncryption Algorithm. Available from http://eprint.iacr.org/2004/011.pdf .(Accessed on March 2, 2009)

[13] Karthik Thiyagarajan “ Low Computational Overhead Video Encryption For Wireless Multimedia Devices”Dalhousie University Halifax, Nova Scotia September 2014