A Secure Data Transmission in MPEG Format by using AES Video Data Encryption Technique

R.Hariprakash Reddy[1] Dr. K. Venkataramana[2]
[1]Student [2]Assistant Professor
[1,2]Department of Computer Applications
[1,2]KMM Institute of PG Studies, Tirupati, India

Abstract— MPEG video stream is kind of totally different from ancient matter knowledge as a result of interface dependencies exist in MPEG video. Special MPEG video encoding algorithms square measure needed attributable to their special characteristics, like cryptography structure, great amount of information and period of time constraints. We gift a period of time MPEG video encoding algorithmic program supported AES that is quick enough to satisfy the period of time necessities.

Key words: AES, MPEG1 Video Encrypt, Decrypt, Cipher-Text

I. INTRODUCTION

A. Network security

Network security may be a branch of engineering science that involves in securing a electronic network and network infrastructure devices to stop unauthorized access, data theft, network misuse, device and knowledge modification. Another operate of network security is in preventing dos (denial of service) attacks and reassuring continuous service for legitimate network users. Network security involves proactive defence ways and mechanisms to guard knowledge, network and network devices from external and internal threats.

Data is the most precious factor of today's businesses. Top business organizations spend billions of dollars every year to secure their computer networks and to keep their business data safe. Imagine the loss of all necessary analysis knowledge on that the corporate has endowed several dollars and dealing for years!!!

We square measure captivated with computers these days for dominant massive cash transfers between banks, insurance, markets, telecommunication, electrical power distribution, health and medical fields, nuclear power plants, space research and satellites. We cannot negotiate security in these critical areas.

B. MPEG

MPEG is AN industrial normal for video process. Multimedia system applications like Video on-Demand, video broadcast, multimedia system mail and video-conferencing should be supplied with secure transmission. Secure video transmission may be a technique during which video may be sent to a receiver with the reassurance that any unapproved eavesdroppers on the approach won't be able to get any info from video i.e. it's fascinating that solely people who have got the services will read their videos or movies. The high quantity of redundancy within the video offers AN aggressor a lot of clues to reconstruct the first video. Traditional information, like program code or text, has a lot of less redundancy in its structure. These factors build providing secure MPEG video a challenge. Adding security to MPEG transmission sometimes involves encrypting elements or the whole MPEG bit stream.

II. LIST OF MPEG STANDARDS

A. MPEG-1

In its day MPEG-1 represented a remarkable technical achievement. It was designed to com- press image streams with SIF picture size, 352x288 (25fps PAL) or 352x240 (30fps NTSC), and associated audio, to approximately 1.5 Mbps total compressed data rate. This rate is suitable for transport over T1 data circuits and for replay from CD-ROM, and corresponds approximately to the resolution of a consumer video recorder. A measure of this achievement may be seen by comparing the numbers for an audio CD. A normal audio CD, carrying two-channel audio, at 16-bit resolution with a sampling rate of 44.1 kHz, has a data transfer rate of up to 1.5 Mbps. MPEG-1 succeeds in compressing video and audio so that both may be transmitted within the same data rate!.

B. MPEG-2

MPEG-1 was frozen (i.e., subsequent changes were allowed to be editorial only) in 1991. Within the same year the MPEG-2 method was started, and MPEG-2 eventually became a regular in 1994. The initial goals were simple; there was a requirement for a regular that will accommodate broad- solid quality video dimension. This required the committal to writing of "full size" normal definition pictures (704x480 at twenty nine.97 fps, and 704x576 at twenty five fps), and also the ability to code lattice like video efficiently. In some ways, MPEG-2 represents the "coming of age" of MPEG. The bigger flexibility of MPEG-2, combined with the in- wrinkled availableness of large-scale integrated circuits, meant that MPEG-2 may well be employed in an enormous range of applications. The success of MPEG-2 is best highlighted by the dying of MPEG-3, in- tended for high-definition television. MPEG-3 was presently abandoned once it became clear that MPEG-2 might accommodate this application with ease. MPEG-2 is, of course, the premise for each the ATSC and DVB broadcast standards, and also the compression sys- tem utilized by optical disc. MPEG-2 was conjointly permissible to be a moving target. By the employment of profiles and levels, mentioned below, it absolutely was doable to complete the quality for one application, then again to manoeuvre on to accommodate a lot of tightened applications in AN evolutionary manner. Work on ex- tending MPEG-2 continues.

C. MPEG-4

International standardization may be a slow method, and technological advances usually occur that can be incorporated into a developing normal. Often this is desirable, but

All rights reserved by www.ijsrd.com

continual improvement can mean that the standard never becomes final and usable. To en- sure that a standard is eventually achieved there are strict rules that prohibit substantive change after a certain point in the standardisation process. So, by the time a typical is formally adopted there's usually a backlog of desired enhancements and extensions. So it was with MPEG-2. As mentioned higher than, MPEG-3 had been started and abandoned, so the next project became MPEG-4.Two versions of MPEG-4 are already complete and work is continuing on further extensions. At first the most focus of MPEG-4 was the secret writing of video and audio at terribly low rates.

D. MPEG-7

Because MPEG-3 was off, the sequence of actual standards was MPEG-1, MPEG-2, and MPEG-4. Some committee participants needed subsequent customary to be MPEG-5; others were attracted by the binary nature of the sequence and most well-liked MPEG-8. Finally, it absolutely was finished that any straightforward sequence would fail to signal the elemental distinction from the work of MPEG-1 through MPEG-4, and MPEG-7 was chosen. MPEG-7 isn't regarding compression; it's regarding information, also known as the "bits about the bits." Metadata is digital information that de- scribes the content of other digital data. In modern parlance, the program material or content, the actual image, video, audio or data objects that convey the information are known as data essence. The information tells the planet all it must realize what's within the essence. Anyone who has been involved with the storage of information, be it videotapes, books, music, whatever, knows the importance and the difficulty of accurate cataloguing and indexing. Stored in- formation is useful only if its existence is known, and if it can be retrieved in a timely manner when needed. This drawback has forever been with US, and is addressed in the analogue domain by a combination of labels, catalogues, card indexes, etc. More recently, the computer industry has given us efficient, cost- effective, relational databases that permit powerful search engines to access stored information in remarkable ways. Provided, that is, the knowledge is gift in a very kind that the computer program will use.

E. MPEG-21

MPEG-21 again differs in kind from the earlier work of the committee. The basic idea is fairly easy – although wide reaching. MPEG-21 seeks to create a complete structure for the management and use of digital assets, including all the infrastructure support for the commercial trans- actions and rights management that must accompany this structure. The vision statement is "to change clear and augmented use of transmission re- sources across a good vary of networks and devices."

III. PROPOSED MODEL

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).

The basic AES 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 .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.

IV. PROCESS AES-VIDEOS ENCRYPTION TECHNIQUE

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.

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

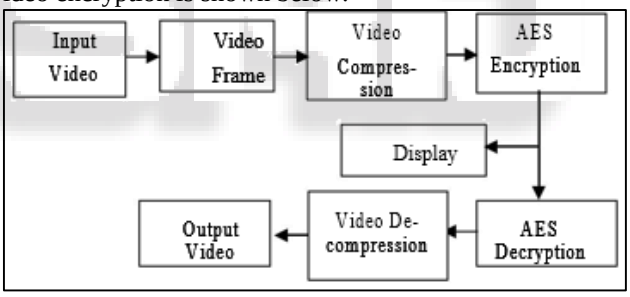

Fig. 1: Block diagram for MPEG video encryption-Decryption

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 compo- nents.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 co- efficient value. This DCT coefficient value is 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.

All rights reserved by www.ijsrd.com

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 Add Round Key Byte Sub, Shift Row, and Mix Column. The repeated application 10 rounds of transformations.

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 ac-cessed by person who have secret key.

C. AES Decryption

Decryption algorithm is same at encryption and decryption side except at 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.

D. Result

This Chapter shows the implementation results of the dissertation work. There are different figures that show how the video is processed and how the system tools works in MATLAB. In this we upload the digital video.

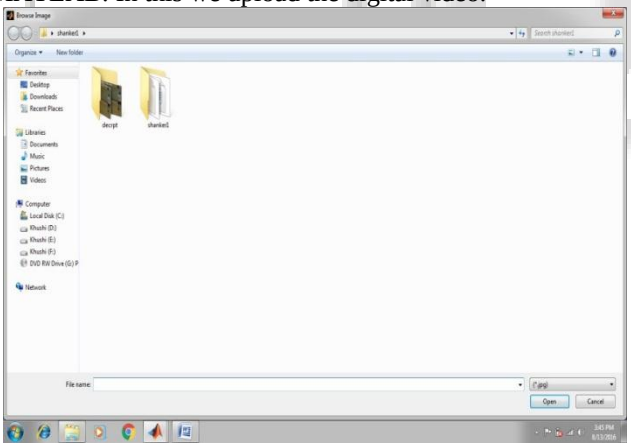

Fig. 1: Browsing the Input video

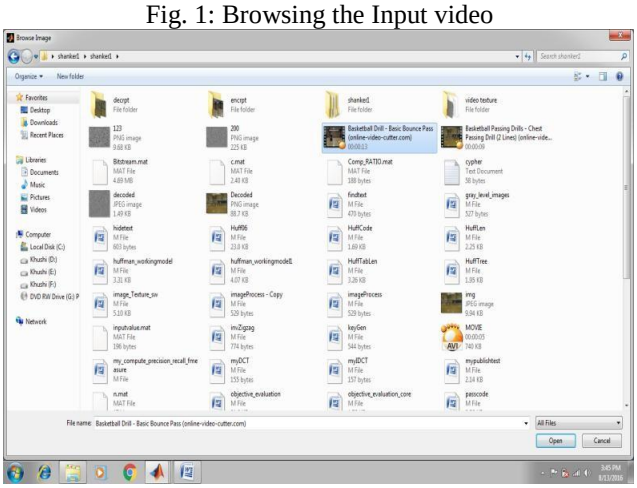

Fig. 2: Input Video Browsing

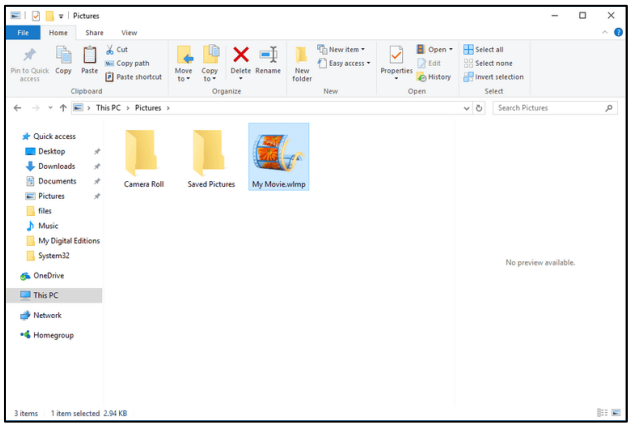

Fig. 3: Encoded Video

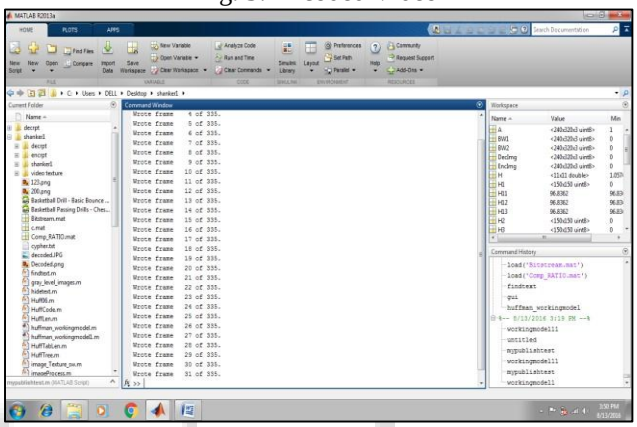

Fig. 4: Video Frame Processing

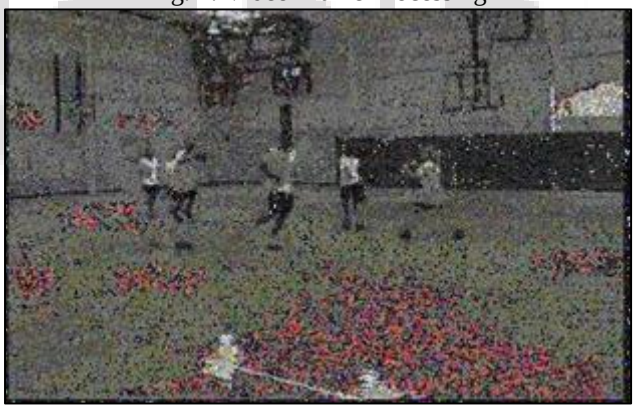

Fig. 5: Decrypted Frame with DCT

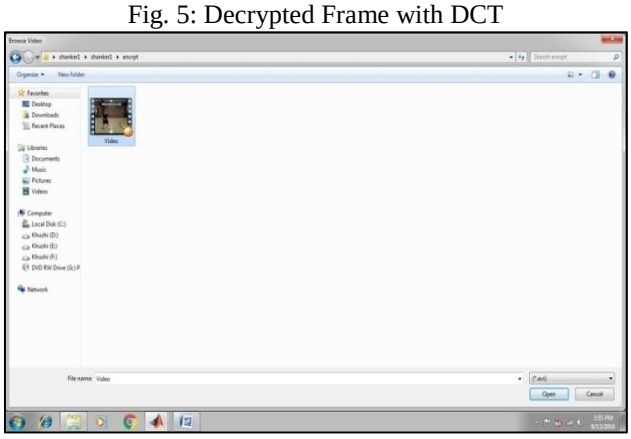

Fig. 6: Original video at receiver side

All rights reserved by *www.ijsrd.com*

V. CONCLUSION

Our process selectively encrypts a fraction of the whole video. It is quicker than encrypting the complete video with AES. We found that in typical MPEG-1 videos sign-bits occupy but 100% of the complete video bit stream. Therefore it will lay aside to ninetieth of encoding time compared to the algorithmic program that encrypts the complete video. It encrypts at most 128 bits, no matter what type of frame is used. This significantly reduces encoding computations achieving satisfactory encoding results. A code implementation is quick enough to satisfy the time period necessities of MPEG-1 cryptography. We believe that this will be used for secure video-on-demand applications and pay-per-view programs.

REFERENCES

[1] Le Gall, Didier, "MPEG: A Video Compression Standard for Multimedia Applications," Communications of the ACM, vol.34, no.4, pp. 46-58, April 1991.
[2] C. Shi and Bhargava, "A Fast MPEG Video Encryption Algorithm", Proceedings of ACM International Multimedia Conference, Bristol, UK, pp. 81-88, September 1998.
[3] Lei Tang, "Methods for Encrypting and De- crypting MPEG Video Data Efficiently", Pro- ceedings of ACM Multimedia 96, pp. 219- 229, Boston, MA, November 1996.
[4] T.Sikora, "MPEG Digital Video Coding Standards",In Digital Electronics Consumer Handbook, McGraw Hill Company, Ed. R.Jurgens, to be published 1997.
[5] Meyer, J., - Gadegast., F.: "Security mechanisms for multimedia-data with the example MPEG-1-video". Proj. Description of SECMPEG, Te ch. Univ.of Berlin, Germany, 1995.
[6] Jayshri Nehet K. Bhagyalakshmi, M. B. Manjunath, Shashikant Chaudhari, T . R. Ramamohan, "A Real-time MPEG Video Encryption Algorithm using AES".
[7] D.L. Gall, "MPEG: A video compression standard for multimedia applications," Communications of the ACM, Vol. 34, No. 4, pp. 46–58, 1991.
[8] Jolly shah and Dr. Vikas Saxena, "Video Encryption: A Survey", in International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011, pp:- 525 – 534.

All rights reserved by *www.ijsrd.com*