International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

An Efficient and Secure Video Encryption Technique for Real Time Systems

Pradeep kumar.M [1], Kishore.O [2]
[1] PG scholar, Dept. of ECE, GMR Institute of Technology
[2]Assisant Professor, Dept. of ECE, GMR Institute of Technology

---

Abstract: *A number of encryption techniques for video are purposed to encrypt the videos and used for obtaining highly secured encrypted videos. In this paper, an enhanced method for encrypt the videos is proposed by using the Huffmann encryption algorithm. Instead of using the text or the images, the video encoding is taken place here. The video is converted into a series of frames, which are again converted to blocks to encrypt the video. The division of video converted into images in turn these images are followed by encryption. In order to convert frames into blocks the block cipher algorithm is used. Because of its efficient working syntax and simplicity, The DCT algorithm is used.*

Keywords: **Huffman encryption algorithm, I-frames, Video encryption.**

I. INTRODUCTION

Because of quick improvement of different media advancements, more sight and sound information are created and transmitted in the restorative, business, and military fields, which might incorporate some delicate data which ought not to be gotten to by or must be halfway presented to the un authentication clients. In this manner, security and protection has turned into a critical. The fundamental objective of cryptography is keeping information secure structure unapproved aggressors. In this manner information is scrambled through procedure of Encryption. The opposite of information encryption is information unscrambling. With advanced video transmission, encryption innovations are required that can shield computerized video from assaults amid transmission. Because of the enormous size of advanced recordings, they are generally transmitted in compacted organizations, for example, MPEG, or H.264/AVC (standard utilized for video pressure). Encryption of pictures and recordings are essential because of taking after reasons:

1. For averting undesirable survey of transmitted video, for instance from law authorization video observation being transferred back to a focal review focus.

2. To ensure the private multimedia messages that is traded over the remote or wired systems.

3. Video Encryption is useful in securing recordings utilized as a part of administrations such as video on interest (VOD), Video conferencing learning

4. For ensuring medicinal recordings which might contain private data of a patient from unapproved access by vindictive clients.

This study depends on video encryption taking into account investigation of Deformation/Formation Algorithm which is valuable in securing different restorative recordings that contain private data of patients and requires sharing among different specialists that has a place with various department of hospital. The encryption and unscrambling of a plain video content should be possible in two ways:

2. SINGLE SECRET KEY ENCRYPTION METHOD:

In this method, a single secret key can be used to encrypt and decrypt the video stream content. This key holds at both sender and receiver ends only.

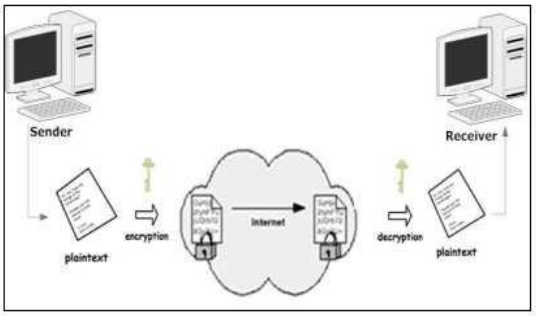

Fig.1 Symmetric key Algorithm

The level of security of the single secure key encryption method is unanimously depends on how well the users keep the single secure key protected. If this key is revealed to an intruder, then all encrypted data can be decrypted. Data Encryption Standard (DES), Triple DES, and Advance

Encryption are some of the generally used video encryption algorithms.

3. PUBLIC KEY ENCRYPTION METHOD:

In this method, there will be two crucial keys, one for encryption and the other one for decryption. The public key is used for encryption, which is known for all senders. Meanwhile the private key is used for decryption, which is owned only by the receivers. [Ref. 2]. It is based on a two-key encryption-decryption system in which two parties(sender and receiver) can securely communicate over a non-secure communications channel without sharing a secret key and solves the problem of secret key distribution by using two keys instead of a single key.

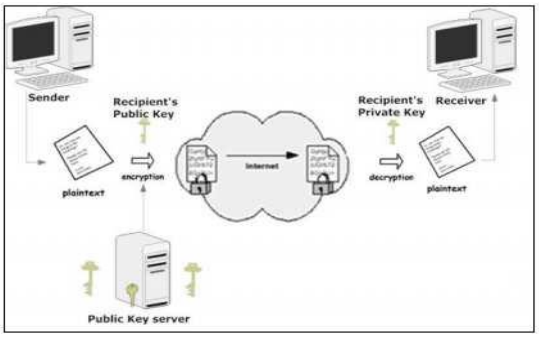

Fig.2 Asymmetric key Algorithm

4.VIDEO ENCRYPTION METHOD CLASSIFICATION

Since the mid-1990s many researchers have been worked to make the development of specific video encryption algorithm. Initially (in 2004) Fuhrt & Kirov ski has given detailed overview of early video encryption methodologies. Later on (2010) Fuwen Liu and Harmut classified encryption algorithms depending on their association with video compression. They are namely compression independent encryption method and joint compression and encryption method.

4.1. Independent Encryption Method:

Encryption of video streams can be done in two ways i.e., before the compression or after the compression. But this has codec portability issue. When video is encrypted before compression, it is codec portable but increases the data size. When video is encrypted after compression it is inherently not codec portable but size of the data can be reduced.

4.2. Joint Compression and Encryption Method:

Encryption can also occur along with compression. This method has codec dependent issue and reduces overall processing time but it is less secure and may be computationally expensive. Video encryption methodologies are classified into four categories.

4.2.1. Full Encryption (Naïve Approach) Method:

The naïve approach is a direct method where whole video data is encrypted. The video stream (bit sequence) is treated as text, and every byte of the data is encrypted using standard encryption algorithms such as DES, RC5 or AES etc. This approach is supposedly the most secure as it is impossible to access classical algorithms like 3DES or AES. However, this method is not suitable for real time video application since standard algorithms needs heavy computation time as encrypting each and every byte of data, so computation time will be slow and expensive operation.

4.2.2 Selective Encryption Method:

It is also called as partial encryption method. It provides faster security because it encrypts only a selected portion of a bit stream which part of the video stream to be encrypted. In this method, we will selectively encrypt the bytes within video frames that may contain sensitive information. This methodology is not encrypting each and every byte of video, thus, reduces computational power, produces less overhead and is much faster than full encryption.

4.2.3. Permutation Based Encryption Method:

Encryption of the content of video use different permutation algorithms to fall in category of this type of method. Every byte within a frame are encrypted and permuted. For example in Zig-zag permutation method [7], , it maps individual 8X8 block to 1X64 vector by using random permutation, instead of mapping an 8X8 block to 1X64 vector in Zig-Zag order. Hence it is not necessary to encrypt the each and every byte there by reducing computational time. Secure key can be used as permutation list to encrypt the content of the video. Scrambling offers fast distortion of video but is not to consider as secure since all frames could be easily decrypted once the permutation list is known.

4.2.4. Perceptual Encryption Method:

The necessity of the perceptual encryption is that quality of video is degraded by encryption to some extent i.e., the encrypted video content are still partially perceptible after encryption. This method may find its application in entertainment industry where high quality of video is priced and will require an authorized access whereas low quality

versions may be free to stimulate user to buy high quality version. The quality degradation of audio/visual content can be continuously controlled by a factor p.

5. LITERATURE SURVEY :

5.1. Qiao And Nahrstedt Proposed Method:

This method is based on statistical analysis of compressed MPEG video stream. The fundamental idea is scrambling of bytes. Scrambling allows unauthorized users to have an arbitrarily degraded view of current video. The video content is divided into two streams namely odd and even numbered bytes and the first part of cipher is formed by XORing the two streams of the video content. Then after, DES is performed over the even numbered byte streams to form second part of the cipher. This method reduces the size of data to be encrypted and is immune from known-plaintext attacks. [5]

5.2. Tang Proposed Method (1996): Zigzag Permutation:

Tang embedded the encryption into the MPEG compression process. A random permutation matrix modifies the ordering transformation coefficients that act as secret key. In this method, I-frames of MPEG video undergo "Zig-Zag" reordering of 8x8 block to 1x64 vectors. This method works in three main steps:

Step1: generates a list of 64 permutations.
Step2: splits 8X8 block by splitting into two halves, 4 most significant bits are placed in DC coefficient and least significant bits as the last AC coefficient.
Step3: apply random permutation to the splitted block.

This method is very fast but compromised at security issue as it is vulnerable to known plaintext attack. Also, Zig-Zag permutation drastically increases the stream size. [6]

5.3.Wu And Kuo Proposed Method: MHT Based Algorithm.

They reconstructed the semantic content of image by fixing DC values at a fixed value and recovering AC coefficients. They proposed two schemes: Multiple Huffman Tables (MHTs) for the Huffman coder and Multiple State Index (MSI) for the QM arithmetic coder. huffman tables are used to encode the input data stream. The table content and the order in which tables are used are used as secret key. Second scheme uses the idea to select 4 initial state indices and to use them in a secret and random order [11]. Major drawbacks of this method are:

It is very difficult to Decode a Huffman coded bit stream without any knowledge about the Huffman coding tables
The MHT is vulnerable to known and chosen plain-text attacks.
For MSI, It is very difficult to decode the bit stream without the knowledge of the state index used to initialize the QM coder.

6. PROPOSED SYSTEM:

6.1. Huffman full encryption Method:

It is a straight forward mpeg video encryption which incorporates encryption along with MPEG compression within a single step [12]. The main aim of this method is to reduce the computation time by taking the advantage of simulating MPEG compression as well as data encryption simultaneously at the same time and also avoid decreasing video compression rate. Huffman word list is used as a secret key in this permutation. During MPEG encoding, the encoder uses the secret key rather than standard Huffman word list. The usage of Huffman word list to encode the MPEG video reduces the compression rate as compression rate is highly depends on the Huffman codeword list.

It limits the permutation of Huffman word list (secret key) to those codewords which have the same length as the standard Huffman word to avoid compression rate. Secondly, it seems that all of permutations of the Huffman word list cannot be used as an encryption secure keys. This makes key generation difficult since a generated key has to be investigated for validity before using.

6.2. Selectively Encryption Method:

This method is Compression logic based video encryption type method [13]. The random permutation is applied to a number of permutation groups. Each permutation group contains the DCT coefficients of same frequency from every single block of a frame, regardless of I,P or B frame. Obviously, since each DCT block has 64 coefficients frequencies so that 64 permutation groups can be formed, the proposed algorithm runs random permutations on each of the permutation groups to encrypt a single video frame. After the random permutation, the encrypted video data is compressed by standard RLE. It is also a adequate algorithm since only a small number of permutation group can be encrypted based on the requirements of confidentiality of

the video content. It is reliable against force attacks due to a very large key space. It is secure against DCT vulnerability.

6.2.1. Proposed Deformation Algorithm:

1) A video V_i is splitted into I_1, I_2...I_n (where n=1, 2.....n) video frames such as frames are collected then take frame one after another.
2) Select two secure key Images namely K1, K2 as key frames for encryption and decryption process, so this key images can be send through secure channel to receiver.
3) Each frame has dimension of "w* h".
4) Let αi denotes any sorting permutation like quick sort, heap sort of Ii & α(Ii) is image with sorted pixels from 'Ii'.
5) Video stream is a group of still images & these images are referred as I-frames.
6) First frame is transferred without any encryption to the secured channel.
7) Second frame is XORred with second key image, K2.Again the output is XORed with sorted value of first frame.
8) The procedure is cumulated for all frames until encrypted video sequences E1,E2....En are generated.

6.2.2. Formation Algorithm:

The following steps has to be followed to decrypting the obtained sequence of encrypted video

1) Collect all frames of videos along with key images :K1,K2.
2) Each frame E_n is xored with first key image & again the output is xored with its previous frame E_{n-1}.
3) The output is xored with key image K2 to obtain first I-frame of video.
4) These steps are cumulated for all the encrypted frames E1,E2....En (where n = 1,2.....n.).
5) Finally construct the final video (consisting of I1,I2.....In frames) by collecting all the frames.

7. RESULTS

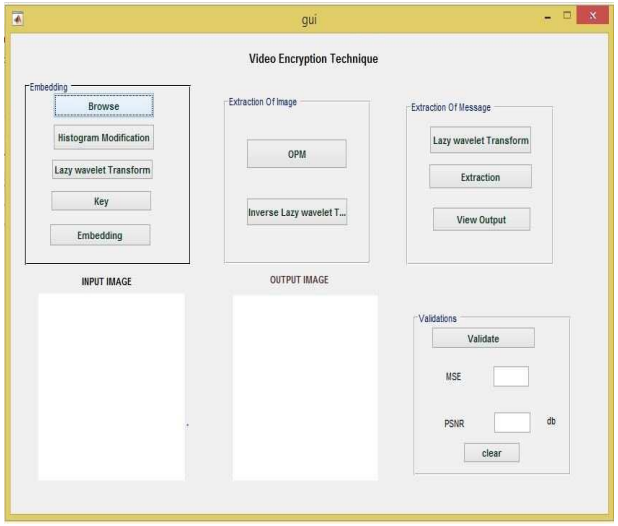

Fig.3. GUI Frame Work

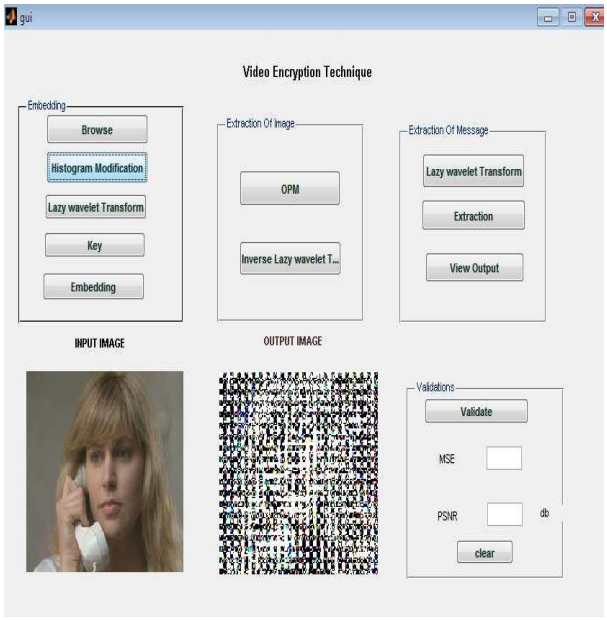

Fig.4. Video Encryption

Fig.5. Video Decryption

S.N	Parameter	Suzie	Hall	New Manu
1	MSE	**31.2159**	**148.51**	**19.5714**
2	PSNR(dB)	**33.187**	**26.4132**	**35.2146**

Fig.6. Experimental Results

7. CONCLUSION

In this internet world nowadays, the security for the digital images has become highly important since the communicating by transmitting of digital products over the broad channel occur very frequently. From the above analysis. Amongst the two approaches: selective encryption takes less computational time as compared to full encryption. An video encryption algorithm which maintains tradeoff among all parameters like visual degradation, speed, encoding/decoding time, compression friendliness, format compliance and cryptographic security and obtained good PSNR, MSE values.

REFERENCES

[1] Mohammed A. Saleh, Nooritawati Md. Tahir, Ezril Hisham & Habibah Hashim "An Analysis and Comparison for Popular Video Encryption Algorithms" IEEE conference 978-1-4799-8969-0/15

[2] 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.

[3] Jolly shah and Dr. Vikas Saxena," Video Encryption: A Survey", International Journal of Recent Trends in Engineering, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814.

[4] Daniel Socek, Spyros Magliveras,Dubravko Culibrk,Oge Marques, Hari Kalva, and Borko Furht, "Digital Video Encryption Algorithms Based on Correlation-Preserving Permutations", in EURASIP Journal on Information Security , Volume 2007,pp: 1-15.

5] D.L. Gall, "MPEG: A video compression standard for multimedia applications," Communications of the ACM, Vol. 34, No. 4, pp. 46–58, 1991.

[6] Qiao L, Nahrstedt K., Comparison of MPEG encryption algorithms, International Journal of Computer and Graphics,1998;22(4);437-48.

[7] L.Tang, "For Encrypting and Decrypting MPEG Video Data Efficiently", in Proceedings of the Forth ACM International Multimedia Conference, 1996, pp. 219-230.

[8] Fadi Almasalha,Ashfaq Khokkar,Rogelio Hasimoto beltran, "Scalable Encryption of variable length Coded video Bit Streams",35th Annual IEEE conference on Local Com.

[9] Daniel Soek, Hari Kalva,Syyros S. Magliveras,"New Approaches to encryption and steganography for digital videos", MultimediaSystems,01 1007/s00530-007-0083- ,@Springer-Verlag 2007.

[10] Knuth, D.E.: The art of computer programming, 2nd edn., vol. 3: Sorting and Searching, pp. 113–122. Addison–Wesley, Reading, MA (1998).

[11] S., Chen, G., Zheng, X.: Multimedia security handbook. Internet and Communications Series, vol. 4, chap. Chaos-Based Encryption for Digital Images and Videos, pp. 133–167. CRC Press, West Palm Beach (2004).

[12] Wu C-P, Kuo C-CJ, "Design of integrated multimedia compression and encryption systems". IEEE transaction on Multimedia (7)(5):828-39 ; October 2005