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 10, October 2015**

# A Survey of Video Encryption Methodologies

Madhvi Soni[1] , Sapna Chaudhary[2]

M.Tech student, Dept. of Computer Science & Engineering, Shri Ram Group of Institutions, Jabalpur, India.[1]
Professor, Dept. of Computer Science & Engineering, Shri Ram Group of Institutions, Jabalpur, India[2]

**ABSTRACT:** Security and privacy has become an important issue in the world of digital multimedia services and applications. Encryption seems to be the most efficient way for achieving multimedia data security. The encryption algorithms developed to secure text data are not suitable for video content due to particular requirements and special properties of video data. This paper, presents a classification scheme and description of various video encryption methodologies proposed so far along with their performance evaluation.

**KEYWORDS:** Video data, Cryptography, Video encryption, Selective encryption, Evaluation metrics.

## I. INTRODUCTION

A video is an audio visual content. The dictionary definition says that a video is the recording, reproducing, or broadcasting of "moving visual images". Thus we can imagine a video as actually a sequence of image frames displaying at a high rate along with motion information. They may also contain the sound element. Cryptography[1] is the art and science of protecting information from unauthorized people by converting it into unreadable format. The translation of data into a secret code is called encryption.
Encryption is the most effective way for achieving data security. In order to read an encrypted file, one should have an access to a password to decrypt the file. Unencrypted data is called as plaintext; encrypted data is called as ciphertext; password is called as secret key.

Various encryption algorithms have been proposed so far like DES, RSA, IDEA, AES etc. most of which are used for text and binary data. These algorithms are highly secure but are not suitable to directly encrypt video content since a video file is huge in size; coding structure of video content is different from text or binary content and also due to constraints of real time operation at receiver device such as limited memory or processing power. Moreover various video applications like pay TV, Video chat, telemedicine, personalized business videos need different level of security. For example, for VoD or pay TV, low security will be fine but for military training videos, high level of security is required. This has led to the demand for designing new and efficient video encryption methodologies to meet the specific requirements of a particular application.

The rest of the paper is organised as follows: In section 2, various performance evaluation metrics of video encryption algorithms are defined. In section 3, a possible classification scheme is given. Section 4 provides a literature review of previous work carried on this area and finally conclusion is drawn in section 5.

## II. PERFORMANCE EVALUATION METRICS

Performance evaluation metrics are used for quantitative analysis of video encryption methodologies. These are:

*Encryption Ratio*: It is the ratio of encrypted video size to the size of original video. It has been found that lesser the ER, more is the computational efficiency of the algorithm.

*Security:* The algorithm should meet the required security level of a given application and should be resistant to specified attacks.

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 10, October 2015**

*Compression efficiency:* Video data is generally very large so it is compressed to save storage space and to save bandwidth while transmission. The ease of encryption depends on the data compression efficiency. Therefore, the size of compressed video should not be increased by encryption.

*Codec Portability*: A compressed video stream contains syntax structure respective to codec. The encryption algorithm must be able to preserve the syntax structure. It is required that an encryption algorithm should work in compliance to video codec and does not result in a need to modify the underlying video codec.

*Speed:* For real-time applications the encryption and decryption algorithms should be fast enough to meet the real time requirements.

*Visual Degradation*: This is required to measure visual distortion of video stream. Sensitive video applications need high degree of visual degradation to make it totally non-understandable to an attacker while other videos may be kept as partially perceptible.

*Error Tolerance:* It is a critical feature when data travelled through error prone networks. Error in encrypted bits results in more erroneous bits during decryption hence causes loss of important information. So we need to design error tolerant encryption algorithms.

*Lossless Visual Quality:* It is the most significant feature of entertainment applications like VoD, payTV. The encryption should produce same video quality as original video when decrypted legally.

## III. CLASSIFICATION OF VIDEO ENCRYPTION METHODOLOGIES

Since the mid 1990s many research efforts have been made to the development of specific video encryption algorithm. Fuhrt & Kirovski (2004) has given detailed overview of early video encryption methodologies. Later Fuwen Liu and Harmut (2010) classified encryption algorithms according to their association with video compression as compression independent encryption and joint compression and encryption methodologies.

### *A. Independent encryption:*

Encryption of video streams can occur before the compression or after the compression. This method 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.

### *B. Joint compression and encryption:*

Encryption can also occur along with compression. This method is codec dependent and reduces overall processing time but it is less secure and may be computationally expensive.

Video encryption methodologies can be classified into four categories.

### *A. Full encryption (Naïve approach):*

The naïve approach is the most straight forward method where whole video data is encrypted. The video stream (bit sequence) is treated as text data, and every byte is encrypted using standard encryption algorithms like DES, RC5 or AES etc. This approach is supposedly the most secure as it is hard to break classical algorithms like 3DES or AES. This method is not suitable in real time video application since standard algorithms needs heavy computation; also, encrypting each and every byte will be a slow and expensive operation.

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 10, October 2015**

*B. Selective encryption:*

It is also called as partial encryption. It provides faster security because it encrypts only a selected portion of a bit stream. In this 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.

*C. Permutation based encryption:*

The methods falling in this category use different permutation algorithms to scramble or encrypt the content of video. The bytes within a frame are scrambled and permuted. For example in Zig-zag permutation [7], instead of mapping an 8X8 block to 1X64 vector in Zig-Zag order, it maps individual 8X8 block to 1X64 vector by using random permutation. The scrambling of each and every byte is not necessary. Permutation list can be a secret key to encrypt video contents. Scrambling offers fast distortion of video but is not considered as secure since all frames could be easily decrypted once the permutation list is figured out.

*D. Perceptual encryption:*

The requirement of the perceptual encryption is that quality of video is degraded by encryption to some extent i.e., the encrypted multimedia data 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.

*Table1. Classification of video encryption methodologies*

| Full encryption | Selective encryption | Permutation based | Perceptual encryption |
|---|---|---|---|
| Uses standard algorithms to encrypt every byte | Only selected bytes are encrypted | Permutation of DCT coefficients | Quality of video is degraded |
| Highly secure | Moderately Secure | Not secure | Not secure |
| Needs heavy computation | Needs less computation | Needs less computation | Computations can be controlled |
| Slow | Fast | Very fast | Speed can be controlled |

## IV. LITERATURE REVIEW

*A. Methodology proposed by Maples and Spanos (1995): AEGIS:*

Maples and Spanos in [2] have shown that full encryption creates bottleneck in high bitrate distributed video applications. Thus they introduced a new method called AEGIS to securely encrypt the MPEG video stream based on selective scheme. An MPEG video consists of I, P and B-frames. Aegis encrypts only I-frames using DES in CBC mode, while P & B-frames left unencrypted. To improve the security level, video stream header and the ISO 32 bits end code was also encrypted. Later, Agi and Gong [3] experimented with aegis and explained that the partial information leakage from the I-blocks in P and B frames causes some scenes predictable. Thus AEGIS is unsuitable for applications like military where each and every part of the video data is important.

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 10, October 2015**

*B. Methodology proposed by Meyer and Gadegast (1995) : SEC-MPEG:*

Secure MPEG is an after compression algorithm. They generally select important parts of video stream and encrypt them using RSA or DES in CBC mode. SECMPEG encrypts important part of video. Four levels of security may be achieved by selecting different parts of video for encryption.

- Level1- encrypts all headers.
- Level2- encrypts all headers and also DC, lower AC coefficients of I blocks.
- Level3- encrypts I-frames and I-blocks of P, B-frames.
- Level4- encrypts all bit streams.

As we move from level1 to level4, security increases but speed decreases making it computationally inefficient. Also the proposed special encoder was not MPEG compliant. [4]

*C. Methodology proposed by Qiao and Nahrstedt (1998): Scrambling:*

This methodology is based on statistical analysis of compressed MPEG video stream. The basic idea is scrambling of bytes. Scrambling allows unauthorized users to have an arbitrarily degraded view of current video. In this method, the data is divided into two streams as odd and even numbered bytes and two streams are XORed forming the first part of the cipher. To construct the second part of the cipher, DES is performed over the even numbered byte streams. This method reduces the amount of data to be encrypted and is immune from known-plaintext attacks. [5]

*D. Methodology proposed by Tang (1996): Zigzag permutation:*

Tang embedded the encryption into the MPEG compression process. The ordering transformation coefficients are modified by using a random permutation matrix that act as secret key. In this method, I-frames of MPEG video undergo "Zig-Zag" reordering of 8X8 block to 1X64 vector. This method works in three main steps:

- Step1 generates a list of 64 permutation.
- Step2 splits 8X8 block by splitting the DC coefficient (8 bits) into two equal halves, 4 most significant bits are placed in DC coefficient and least significant bits as the last AC coefficient.
- Step3 applies random permutation to the split block.

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

*E. Methodology proposed by Shi, Wang & Bhargava (1999 & 2004): VEA:*

They proposed four different video encryption algorithms:

1) *Algorithm I:* In this Algorithm [7] the Huffman codeword in I-frames are permuted during compression. This permutation serves as secret key. The compression ratio can be saved when the permutation p must be such that it only permutes the code words with similar number of bits. *Algorithm I is* vulnerable to both cipher text only attack and known plaintext attack. If some of video frames are known in advance then by comparing the known frames with the encrypted frames the opponent can simply figure out and reconstruct the secret permutation p.

2) *Algorithm II (VEA):* Video Encryption Algorithm encrypts only the sign bits of DC coefficients in the I-frame blocks by XORing the sign bits of DC coefficients using a secret key. The security of *Algorithm II* depends on the length of the key. If the size of the key is short, then the system can be easily broken and if the size of the key is too long system may be infeasible.[8]

3) *Algorithm III (MVEA):* Moving VEA [9] was an enhancement to VEA with reduced computational complexity. Instead of encrypting the sign bits in I-frame block, the sign bits of differential values of DC coefficient and motion vectors in P and B-frames are encrypted by XORing them with the secret key. This made the video more random and more non viewable. The MVEA also relies on the secret key size.

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 10, October 2015**

4) *Algorithm IV (RVEA):* Real Time Video Encryption Algorithm [10] uses a symmetric key cryptography to encrypt the sign bits of DCT coefficient and the sign bits of motion vectors. From each macro block it selects atmost 64 sign bits. By encrypting only signbits in MPEG stream, it speeds up the encryption. Therefore, it is most secure than the previous three algorithms.

*F. Methodology proposed by Wu and Kuo: 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. First scheme encodes the input datastream using multiple Huffman tables. The table content and the order in which tables are used is 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 pitfalls of this methodology are:

- Decoding a Huffman coded bit stream without any knowledge about the Huffman coding tables would be very difficult.
- The basic MHT is vulnerable to known and chosen plaintext 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.

*G. Methodology proposed by Narsimha Raju et. al.(2008):*

The authors in [12] proposed technique based on statistical analysis of frequently occurring patterns in the DCT coefficients of the video stating that the computational complexity of encryption is proportional to the influence of the DCT coefficient on the visual data. The average encryption time taken by their methodology is 8.32 ms per frame.

## V. CONCLUSION

In this paper a survey of various video encryption methodologies were presented. Four types of video encryption techniques were highlighted. From table1 we found that Naïve algorithm provides highest level of security but it is very slow and cannot be used in real time applications. Permutation based algorithms are generally faster but they do not provide sufficient level of security. A selective encryption algorithm reduces computational complexity by selecting only a minimal set of data to encrypt. Perceptual encryption algorithms are suitable for low security applications like pay per view TV, video on demand where potential users like to see low quality video before buying them. So, selection of encryption algorithm always depends on requirements of application in use. Also, it will be a challenge for researchers to design an encryption algorithm which maintains a balance between all performance evaluation metrics of a video encryption methodology.

## REFERENCES

[1] Atul Kahate, Cryptography and Network Security, (Second Edition 2008)
[2] G.A. Spanos and T.B. Maples, "Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications," in Conference on Computers and Communications, 1996, pp. 72-78.
[3] I. Agi and L. Gong, "An empirical study of MPEG video transmissions," in Proceedings of The Internet Society Symposium on Network and Distributed System Security, (San Diego, CA), pp. 137-144, Febuary 1996.
[4] J. Meyer and F. Gadegast, "Security Mechanisms for Multimedia Data with the Example MPEG-1 video," Project Description of SECMPEG, Technical University of Berlin. 1995
[5] Qiao L, Nahrstedt K., Comparison of MPEG encryption algorithms, International Journal of Computer and Graphics,1998;22(4);437-48
[6] L.Tang, "For Encrypting and Decrypting MPEG Video Data Efficiently", in Proceedings of the Forth ACM International Multimedia Conference, 1996, pp. 219-230.
[7] B. Bhargava, C.Shi, S.Y. Wang, " MPEG Video Encryption algorithms", Multimedia tools and applications 24(1)(2004)
[8] C. Shi and B. Bhargava, "A Fast MPEG Video Encryption Algorithm," in Proceedings of the 6th ACM International Conference on Multimedia, 1998, pp. 81–88
[9] C. Shi and B. Bhargava, "An efficient MPEG video encryption algorithm," in Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems 1998, pp.381–386.

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 10, October 2015**

[10] C. Shi, S. Y.Wang, and B. Bhargava, "MPEG Video Encryption in Real-time using Secret Key Cryptography," in Proceedings of the International Conference on Parallel and Distributed Processing Algorithms and Applications,1999
[11] Wu C-P, Kuo C-CJ, "Design of integrated multimedia compression and encryption systems". IEEE transaction on Multimedia( 7)(5):828-39 ; October 2005
[12] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan, C.V. Jawahar, "Fast and Secure Real-Time Video Encryption" in Sixth Indian Conference on Computer Vision, Graphics & Image Processing 2008:257-264