A Comparative Study of Video Encryption Schemes

Jitendra Rajpurohit
Amity University Rajasthan
Jaipur, India

Shweta Sharma
Amity University Rajasthan
Jaipur, India

Bhagyashri Naruka
Amity University Rajasthan
Jaipur, India

ABSTRACT

A method to protect video contents from unauthorized access is known as a video encryption scheme. This paper first surveys the literature to identify most desired features of an encryption algorithm. Then a classification has been drawn according to their characteristics. After that, some of the algorithms are discussed and their working has been explained briefly. At the end a comparison has been shown displaying their performance on a few chosen parameters.

KEYWORDS

Video encryption, selective encryption, perceptual encryption

1. INTRODUCTION

A large amount of information is being communicated in the form of video in the present era of time. As the communication channels are advancing and becoming more able to transfer large amounts of data, this amount of video is going to further increase. At the same time videos are becoming more susceptible to various types of security attacks over the communication channel. A video encryption scheme is a method to encrypt video before transmission over the network and decrypt it at the receiving end. Encryption is sometimes required to hide a part of the video sequence that is important enough to disclose sensitive information. In some cases, aim of the encryption scheme is not to hide the whole content but to convert it in a degraded view, high quality view is available only after proper decryption. Large size of video data makes it different from the encryption of ordinary data. To reduce the size videos are stored and transmitted in compressed form using standard compression methods like MPEG-1/2/4 [1][2][3], H.263, H.264/AVC[4][3]. An encryption scheme should not affect the compression efficiency of the video. The general sequence of steps in video processing is shown in Figure 1, but the exact order varies in different algorithms. A few algorithms suggest embedding the encoding and encryption processes while all of them support some of the standard encoding methods. A variety of video encryption schemes are found in the literature. In this survey, first the main features of a good algorithm are identified, then various existing algorithms are discussed with their major features and a comparison is figured out.

2. MAJOR FEATURES OF A SECURITY ALGORITHM

Of course, the most desired feature of an encryption algorithm is to provide resistance against an attack, but the large amount of data associated with video, requires that these algorithms be more flexible for some of the other factors also. Ref. [5] identifies fidelity, robustness, use of the key, speed capacity, statistical imperceptibility, low error probability and real time detector complexity as the major requirements of a security algorithm. In [6], authors first present a scenario which includes preprocessing and encryption and then try to work out problems, they identify security, performance and complexity as the major parameters for an algorithm. In [7], authors identify "three major security technologies to protect video contents:

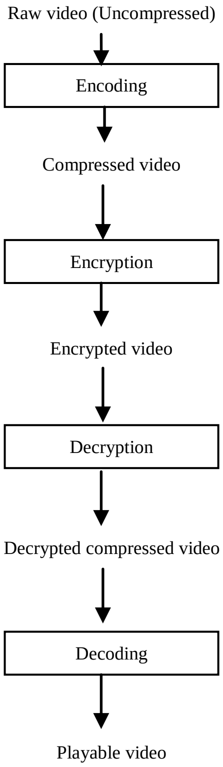


Figure 1: Sequence of steps in secure video processing

1) To provide end-to-end security using encryption technology at the distributing video over internet or other public communication channel.

2) To achieve copyright protection with water marking, ownership trace and authentication

3) To prevent unauthorized access using access control technology."

We conclude following as the most desired features of a video security algorithm:

2.1 Encryption ratio

Encryption ratio can be understood as

Encryption ratio=(size of encrypted data)/(size of actual data)

As the video application always has to deal with large amounts of data so this ratio should be minimum. The encrypted video data will have to travel over the network, so minimum bytes of data are always desired for better performance of the network.

2.2 Robustness

Robustness is the most desired feature of a security algorithm. It reflects the capability of encrypted data to survive major types of attacks. A complete robust algorithm is able to survive all attacks. While, there are many algorithms which are robust to only a certain category of attacks.

2.3 Visual Degradation

Visual degradation refers to the low quality video content provided in the form of encrypted data. For most of the security algorithms, high degree of degradation is desired but some algorithms as we will see later, control the degradation and provide a controlled quality video.

2.4 Speed

For applications like live streaming of videos and on the fly encryption it is desirable that the algorithm encrypts and decrypts fast enough. Slow encryption or decryption can result in undesired delays. In other applications also, good speed is always desired to minimize time complexity of the algorithm.

2.5 Application areas

This feature describes the specific application areas for which the algorithms are designed. It is essential that each algorithm has its own application areas, most of the algorithms provide security independent of the application. But, some of them are designed keeping in mind their implementation for a special purpose. Algorithms supporting real time videos, network transmission, streaming, video conferencing etc. are some examples.

3. CLASSIFICATION OF THE ALGORITHMS

There are a number of ways to classify these algorithms. We have tried to keep it simple and not to create more categories and to concentrate on the features provided by them. Broadly, we use the following classification:

3.1 Total Encryption

In this category, also known as heavy weight encryption, the whole video data is treated as normal data composed of bytes and then any conventional encryption algorithm like AES[8] or DES[9] is used to encrypt it. As the video data is treated as simple bytes this method is fairly simple and is compatible with all the compression formats. Conventional encryption algorithms like triple DES and AES are still to be broken so these methods are fully secure. But this scheme encrypts each and every byte of the video so it is not so good as far as complexity and memory requirements are concerned. These algorithms also introduce some overload. Common procedure for such encryptions is illustrated in figure 2.

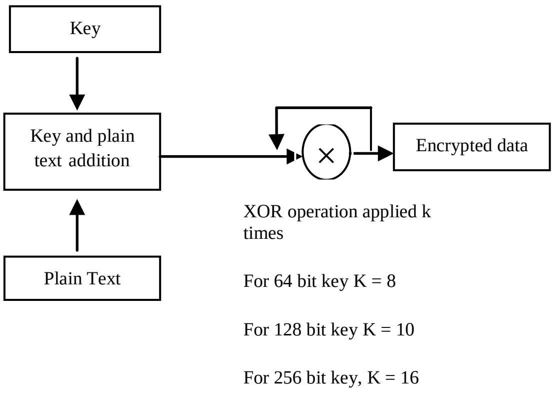


Figure 2: Sequence of steps in total encryption

Ref. [10] proposes such an algorithm called Fast Random Bit Encryption Technique (RBET). First, lossless compression is applied on the video. Compression before encryption is considered better as it shows high efficiency. Care should be taken as the compression may affect the video quality. Encryption algorithm used is AES, key is divided into four parts and encrypted with a random number. Padding is done to increase the key strength. Key management issue can be avoided if both the sender and receiver are bound to use same random number generator. A single bit 1 and an arbitrary number of 0s is padded to generate an arbitrary sized encrypted data, then a fixed length hashed data is generated using hash function. Salt algorithm is used to create a salt from this hash value. The DES encrypted byte data must be converted in the form of frames before applying the salt algorithm. FileInputStream and FileOutputStream are used for this conversion. Password based key derivation function is used to generate a key from this salt. This key is divided into four parts and each part is XORed with a random number and encrypted. Public key standard (PKCS7) padding is applied to the key now.

3.2 Permutation Techniques

Permutation means to simply interchange bytes with each other. In this technique the video becomes a low quality version of the original one as only a few bytes are interchanged. There are a number of permutation techniques found in literature:

3.2.1 Simple permutation

The bytes are simply permutated within a frame. This technique is not strong against the known plain-text attack. If a permutated frame is compared with a known frame the permutation sequence can be figured out and then all the frames can be decrypted [11].

3.2.2 Huffman codeword technique

Introduced in [12], this technique combines the encryption method with the MPEG compression to reduce the encryption and compression time taken together. More, Huffman codeword list is used to take encryption keys. The compression time depends upon the key selected so only standard Huffman codes are used which makes it difficult to identify the key used.

3.2.3 Compression logic random permutation technique (CLRP)

The Compression Logic based Video Encryption Algorithm [13] applies random permutation to a number of permutation groups instead of a single DCT block. Each permutation group is formed in such a way that it consists of DCT coefficients of same frequency from each block of frame. Each permutation group is then encrypted using random permutation and then it is compressed.

3.3 Selective Encryption

As the video data is generally of large volume so to encrypt the whole data is quite time consuming and requires a lot of computation. Light weight encryption or selective encryption encrypts only some selected portions of the data and thus makes it secure and at the same time reduces the amount of calculation and time required. These algorithms are no way more secure than the total encryption techniques referred above, but they try to place a trade-off between the level of security provided and the complexity of the algorithm. Some of the popular selective encryption algorithms are discussed here:

3.3.1 Video Encryption Algorithm (VEA)

Shi and Bhargava proposed this algorithm [14]. The algorithm performs XOR operation between sign bits of the DC coefficients of the I-frames and the bits of a key. Maximum 64 XOR operations are required per frame. Video is degraded highly but one pair of known plain text and cipher text leads to disclosure of secret key and thus all the frames may be decrypted. Strength of the algorithm depends upon the length of the secret key.

3.3.2 MVEA

It was an improved version of VEA algorithm [15]. In this method sign bits of the DC coefficients of Y, Cb, Cr blocks of I-frames and the sign bits of the motion vector in B and P frames are encrypted using a key. This improvement makes the video more degraded as the motion vectors are included. The basic operation remains the XOR. Key is similarly vital and the method still remains vulnerable to known plain-text cipher-text pair attack.

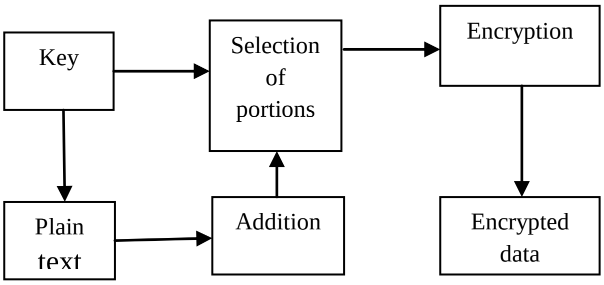


Figure 3: Sequence of steps in Selective encryption

3.3.3 RVEA

Real Time Video Encryption Algorithm [16] further improves the security features of [14] and [15]. In this method sign bits of DC coefficient and/or sign bits of motion vectors are encrypted through DES or IDEA. Good thing is that at most 64 bits are selected per frame so, the maximum computation time is limited. Inclusion of motion vectors increases the visual degradation. But encrypting only 64 bits per macroblock is still not a very large amount of encryption and is yet vulnerable in case of high resolution videos.

3.3.4 Compliant Selective Encryption

In [17] authors propose a frame work for encryption that is compatible with the video standard. Any standard codec will be able to decode the encrypted video, so the scheme is compatible with all the video encoding schemes. This scheme proposes to attach the encryption process within the encoder. The rule to select the bits for encryption is: Each of their encrypted configurations gives a non-desynchronized and fully standard compliant bit stream. In other words the bits selected should have no or negligible effect on the decoding process and only visual alterations are the result. The method is applied on H.264/AVC for an example. In this example the codeword providing the Mb_QP_Delta is selected for encryption as it does not have any impact on rest of the decoding process. This method leads to encryption of about 25% of I-slices and about 10-15% of P-slices. The compatibility of the algorithm with H.264 is proved and with other standards is a matter of research. The PSNR of 25 to 30 db is achievable which is sufficient to make the video unrecognizable.

3.3.5 LTCE Algorithm

A lightweight scheme Luminance Transform Coefficient Encryption [18] explores the special features of H.264 standard. It is designed to provide security in wireless environments with limited power, processing and bandwidth capabilities. The luminance transform coefficients of residual data are partially encrypted by stream cipher. The algorithm only encrypts luminance transform coefficient because the luminance factor (DC LTC) has a greater effect on visibility than the chrominance factor. Traditional encryption algorithms are used to ensure security. Stream ciphers are given priority over block ciphers because of their property of not propagating errors. The experimental results by the authors show that the bit-rate is increased a little but is adjustable by smartly selecting the parameters in practical.

3.3.6 Proposal of Zhang, Wu and Zhao

Another encryption scheme for video conferencing is proposed in [19]. There are three schemes proposed using permutation code and DES algorithm for H.264 standard. Finally one of the schemes is suggested as the most useful, this scheme involves encryption of parts of motion vector codewords, DCT coefficients of luminance residuals, DC coefficients of chrominance residual and intra-prediction mode codeword. Encrypting intra-prediction mode codeword creates confusion because of the inter frame correlation between I and P frames. It has also been shown that encryption before and after entropy encoding affects the compression rate.

3.3.7 Model-based Multimedia Encryption Scheme for Real Time Videos

Another H.264 standard based algorithm is proposed which does not introduce any overhead [20]. It is secure against cipher-text only and known plain-text attack. Secret sharing provides error tolerance. DCs are distributed among the ACs and DCs themselves. This distribution is controlled by a variable k. The objects are not recognizable but the motion of the objects can be identified. The I-blocks of P and B frames leak some information. This leakage can be countered by encrypting these I-blocks also. But the encryption of I-blocks of P and B frames cause encrypting time to be out of tolerating limit. That is why the algorithm is not suggested for extremely sensitive video.

3.3.8 Schemes proposed by Varalaxmi et al.

Three new encryption schemes were proposed for real time videos [21]. In the first scheme video is converted into DCT coefficients, these coefficients are then encrypted using secret sharing. The use of secret sharing assures that there is no combination of members of group which can discover the secret. Then the motion vectors are scrambled using a pseudo random number generator. In the second proposal, instead of DCT, secret sharing is done among discrete wavelet transform. As DWT is frame based and results in better compression ratio.

Intra fame encryption is performed by secret sharing of DWT coefficients using a PRNG. Rest of the process is similar to first proposal. In the third scheme spatial correlation of frames has been exploited using an algorithm ACCordin, it is an algorithm which transforms a group of pictures into a single picture using inter frame spatial redundancies. The schemes are robust against cipher-text only and known plain-text attacks.

3.3.9 Method proposed by Roy and Pradhan

An improvement was proposed over the RVEA algorithm in [22]. The authors proposed an algorithm which addresses both the high resolution and normal videos. AES is used instead of DES in RVEA for its ability to support more key strength and thus improving the security feature. The method gives priority to the lower frequency coefficients and encrypts 128 bits at a time. Authors also claim that the increased computational overhead by the use of AES is not a hurdle for modern day fast computers. Authors believe that the algorithm is suited for peer-to-peer and video-on-demand applications.

3.3.10 Scalable Secure MJPEG Video Streaming (SSMVS)

This algorithm [23] is applicable to MJPEG format only as it does not use inter-frame correlation. Authors propose four categories of encryption according to the amount of encryption done. This scalability in the amount of encryption is better suited in resource constrained environment such as mobile devices. The method utilizes the property of JPEG encoding that separately scans Y (luminance component), Cr and Cb (both chrominance components). Algorithm exploits the fact that change in luminance is more effective for human eyes and thus emphasizes on encrypting more of the Y component. There are four encryption schemes suggested. All of them apply AES as the encrypting algorithm on a part or the whole of the video stream. The schemes are as follows:

a) 100% Encryption

This scheme encrypts the whole video stream. So, it may also be put in the category of total encryption. It is suitable only for the devices having continuous power and good computing abilities. Mobile devices with limited power backup and limited computing resources may not use this scheme.

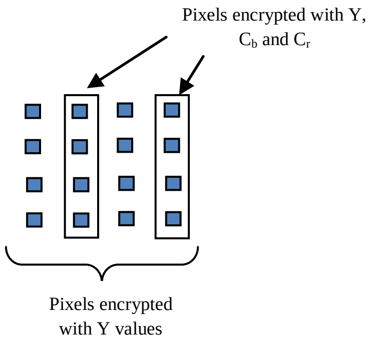
b) 50% Encryption

To make encrypted data more degraded with minimum computation, the Y, Cb and Cr components are selected in the ratio of 4:2:2 respectively. In other words Y component is encrypted for all the pixels while Cb and Cr components are encrypted for only half of the pixels. This selection between the components reduces the computation by 50%. c) Even Less Encryption

Here authors suggest a variable amount of encryption according to the computing capability of the device. In

order of the number of AC coefficients selected for

encryption, the encryption range varies from 15% (only DC and first AC coefficients) to 50% (all AC coefficients). Greater number of AC coefficient selected will make video more degraded.


Pixels encrypted with Y, C_b and C_r
Pixels encrypted with Y values

Figrue 4: Y, C_b and C_r encyption in 4:2:2 ratio

d) Minimum Encryption

This mode is suggested for only extremely power constrained conditions. Here, only the DC coefficients of the first block of the image and the differences of the remaining blocks are encrypted. This leads to hiding of the basic tone of the image while sharp edges, small objects and high contrast areas are still viewable.

3.3.11 Layered video encryption

Layered video encryption [24] utilized the error propagation property of H.264/AVC to distort frames. The proposed framework allows different levels of speed and security, and three layers for encryption namely base layer, middle layer and enhancement layer. Each layer has different complexity as different number and positions of MBs are encrypted. In the base layer encoding only a few MBs of the upper left corner of the Intra coded frame are encrypted and the distortion propagates towards the bottom right in the following Intra coded frames because of the predictions. About 16% MBs of I frames are encrypted.

The middle layer concentrates on encrypting sensitive portion of the frames which generally lies in the middle of the frame. For I frames, MBs of base layer and center part are encrypted, while for inter coded frame only the center part is encrypted. Encryption overhead is higher than the base layer.

The enhancement layer encrypts the entire frame for both intra and inter coded frames. Encryption of this layer provides highest security but involves high amount of computations thus, is recommended for extremely sensitive video information.

3.4 Perceptual Encryption

In this encryption scheme video encryption does not aim to make the contents fully un-viewable. But they allow a low quality version to be available even after encryption. The scheme is convenient for applications like pay-per-video and video on demand where a low quality version is available and the users need to pay for the high quality version. A control factor p should be there which controls the quality of the video by controlling the percentage of encryption [25].

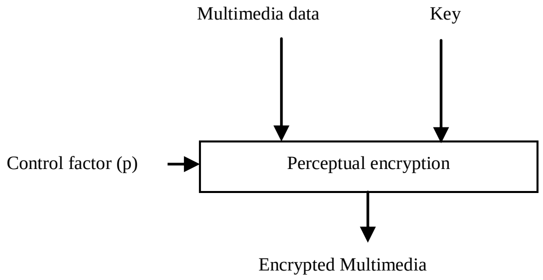


Figure 5: Perceptual encryption

Following points are mentioned regarding the control factor (p):

a) The control factor represents a rough measure of degradation

b) Degradation for different frames may be different so the control factor represents only an average degradation for all the videos

c) The control factor helps in implementation of any perceptual encryption scheme, but higher values of it should always mean higher degradation

d) Control factor is algorithm specific. Its highest value (p = 1) for the specific algorithm means the algorithm has achieved its highest degradation but it does not mean that any other algorithm cannot degrade video more than this.

3.4.1 MPEG-2 Transparent Scrambling Technique

A perceptual encryption scheme is proposed in [26] which uses four linear transforms and then the cipher video data is handed over to MPEG-2 encoder. Unauthorized users are allowed to watch the degraded video. The main advantage of the scheme is that the encryption module may be added to the encoding module without any modification to the MPEG-2 process. Some limitations for this algorithm also exist. The danger of Unrecoverable video quality loss is always there. The reason for this is the fact that the corresponding SBs may be encrypted using different parameters. To reduce this possibility the encrypted parameters of the SBs should be carefully selected. This careful selection may affect security and encryption performance adversely. The scheme is also not very secure against a brute force attack and the known plain text attack.

3.4.2 DCT Based MPEG-2 Transparent Scrambling Algorithm

This scrambling algorithm produces an arbitrarily degraded view by encrypting it in DCT domain [27]. Scheme is suitable for transmission systems which uses MPEG-2 encoding standard. The scrambler can be adjusted with the MPEG-2 encoder. First the DCT transformation and quantization is done and then the coefficients are sent to the scrambler. The values of elements are transformed only in INTRA macro-blocks. The scrambled coefficients are then passed through VLC encoding and prepare transport stream. The scheme scrambles only I-frames as the recovery of P and B frames depends upon last recovered I frame in MPEG-2 encoding, this leads to a low complex method. Scrambling effects can be controlled by a scrambling parameter β and the scrambling.

3.4.3 Scheme proposed by Lian, Sun and Wang

In [28] and [29] a perceptual cryptography scheme for 3D-SPIHT compressed video is proposed. In this scheme the video is degraded to different degrees by controlling a quality factor. The algorithm uses confusion of different number of wavelet transforms, encryption of different number of coefficients' signs and confusion of positions of different data cubes. It supports direct bit control and is not sensitive to transmission errors. Encryption process is also of low cost. The same scheme is extended to JPEG2000 encoding [30] for both images and videos. Encryption process includes four steps i.e. (1) Encryption strength computing, (2) sign encryption, (3) bit-plane permutation and (4) inter-block permutation. The brute force space increases with the decrease of quality factor q. At the values of q lower than 50, the brute force space is larger than 1.0 × 1050000. Further decrease in q can lead to higher amount of security. Pseudo random chaotic binary sequence is used to encrypt the sign sequence which effects have a linear tendency in the range of values of β. The scheme also has very little effect of output bit rate. develops random-similarity in encrypted sign sequences and makes the algorithm secure against statistical or differential attacks.

3.4.4 PVEA

Ref. [25] proposes a framework with exploiting the features like on-the-fly encryption and multidimensional perceptibility. The proposed design is a generalized version of VEA [14]. The algorithm encrypts only FLC data elements as it leads to maintaining of various properties like format compliance, strict size-preservation and fast simultaneous encryption. Encryption of FLC elements also fulfills the requirements of major applications of perceptual encryption. Three control factors Psr, Psd and Pmv are used to control the visual degradation in three different dimensions i.e. the low resolution rough view, the high resolution details and the motions. The encryption process is as follows:

a) Encryption of intra DC coefficients with probability Psr

b) Encryption of sign bits of DCT coefficients other than the DC coefficients and escape DCT coefficients with probability Psd

c) Encryption of sign bits and residuals of motion vectors with probability Pmv

A stream cipher or a block cipher may be used for encryption of FLC components. Suitable values of control factors for various types of attacks are defined.

4. COMPARISON OF THE ALGORITHMS

In this section all the above explained algorithms are compared respective to the features described in section 2. Table 1 shows comparison. The symbols used have the following meanings:

H = High

L = Low

V = Variable

ND = Not Defined

5. CONCLUSION

In this literature survey first the need and functions of a video encryption algorithm are identified. Then various features are found out. Then a categorization is presented and various algorithms are divided into these categories. These categories are Total Encryption, Permutation Techniques, Selective Encryption and Perceptual Encryption. Category wise all these algorithms are discussed with an overview of the working of each of them. At the end a tabular comparison is presented. We can conclude that all these algorithms apply new techniques and most of them are good to be used in the specific area that they are meant for. As far as video piracy measures are concerned none of the above algorithms addresses the issues. In all the algorithms, once the video is received at the destination and is decrypted, the receiver can always redistribute it or create several copies of it.

6. REFERENCES

[1] ISO/IEC 13818:1996, Coding of Moving Pictures and Associated Audio (MPEG-2); Part 1: systems, Part2 : video

[2] Mitchell J. L., Pennebaker W.B., fogg C.E. and LeGall D.J., MPEG Video Compression Standard, Chapman & Hall, 1996.

[3] ITU-T Rec. H.264/ISO/IEC 11496-10. Advanced Video Coding. Final Committee draft, Document JVT-E022, 2002.

[4] Iain E G Richardson. H.264/MPEG Part10, 2002. Available: http://www.vcodex.com.

[5] Hamid Shojanazeri, Wan Azizun Wan Adnan, Sharifah Mumtadzah Syed Ahmad,, M. Iqbal Saripan, "Analysis of Watermarking Techniques in Video". In the proceeding of 11th International conference on Hybrid Intelligent Systems (HIS), 2011, pp. 486-292.

Table 1: Comparison of video encryption algorithms

Category	Algorithm/Author	Encryption Ratio	Robustness	Visual Degradation	Speed	Applications
Total Encryption	AES/ DES and RBET	100 %	H	H	L	General
Permutation Techniques	Simple Permutation	100 %	L	H	L	General
	Huffman Codeword Technique	ND	ND	ND	H	General
	LTCE	ND	L	H	H	Wireless devices
Selective Encryption	VEA	ND	L	H	H	General
	MVEA	ND	L	H	H	General
	RVEA	ND	L	H	H	Real time videos
	Compliant Selective	~20%	L	H	H	General
	Zhang, Wu and Zhao	L	H	H	ND	Video conferencing
	CLRP	V	V	V	H	General
	Varalaxmi et al.	V	H	H	H	Real time videos
	Roy and Pradhan	ND	L	H	H	Peer to peer, video-on-demand
	SSMVS	15-100%	L	H	V	Mobile devices
	Layered Encryption	V	V	V	H	General
Perceptual Encryption	MPEG-2 Transparent Scrambling	ND	L	L	H	Quality degrading
	Model-based Multimedia Encryption	L	L	L	H	Real time videos
	Lian, Sun and Wang	V	H	H	H	3D SPIHT video and JPEG2000 images
	DCT Based MPEG-2 Transparent Scrambling	L	H	H	H	Quality degrading
	PVEA	V	V	V	H	On the fly encryption

[6] Wenjun Lu, Avinash Varna, and Min Wu, “SECURE VIDEO PROCESSING: PROBLEMS AND CHALLENGES”. In the proceedings of the IEEE International conference on Acoustics, Speech and signal Processing (ICASSP), 2011, pp. 5856-5859

[7] R. R. Igorevich, H. Yong, D.Min, E. Choi “A study on multimedia security systems in video encryption,” in proceeding of IEEE 6th International Conference on Network Computing. 2010, pp. 1-5

[8] NIST: Advanced Encryption Standard, FIPS 197, 2001.

[9] NIST: Data Encryption Standard, FIPS 46-3, 1999.

[10] K. John Singh, R. Manimegalai, “Fast Random Bit Encryption Technique for Video Data”, European Journal of Scientific Research, Vol.64, No.3, 2011, pp. 437-445

[11] Adam J. Slaggel. “Known-Plaintext Attack Against a Permutation Based Video Encryption Algorithm” . Available at http://eprint.iacr.org/2004/011.pdf

[12] C. Shi and B. Bhargava, “Light Weight MPEG video Encryption Algorithm”, in Proceeding of the International Conference on Multimedia, 1998,pp. 55-61

[13] Hao Wang and Chong-wei Xu, “A New Lightweight and Scalable Encryption Algorithm for Streaming Video over Wireless Networks”, International Conference on Wireless Network, 2007, pp. 180-185.

[14] C. Shi and B. Bhargava, “A fast MPEG video encryption algorithm,” In the Proceedings of the sixth ACM international conference on Multimedia, New York, USA, 1998, pp. 81-88

[15] B. Bhargava and C Shi, “An efficient MPEG video encryption algorithm,” In the proceedings of the 17th IEEE Symposium on Reliable Distributed Systems, 1998, pp. 381-386

[16] C. Shi, S. Y. Wang and B. Bhargava, “MPEG video encryption in real-time using secret key cryptography,” International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA ‘99), Las Vegas, 1999

[17] C. Bergeron and C. Lamy-Bergot, “Compliant Selective Encryption for H.264/AVC Video Streams,” in the Proceedings of the 7th IEEE Workshop on Multimedia Signal Processing ,2005, pp. 1–4

[18] WANG Li-feng, NIU Jian-wei, MA Jian, WANG Wen-dong, XIAO Chen, “A Lightweight Video Encryption Algorithm for Wireless Application”, Fifth IEEE International Symposium on Embedded Computing, 2008

[19] Zhang Qian, Wu Jin-mu, Zhao Hai-xia, “Efficiency Video Encryption Scheme Based on H.264 Coding Standard and Permutation Code Algorithm”, IEEE World Congress on Computer Science and Information Engineering, 2009, pp. 674-678

[20] T. Vino1, E. Logashanmugam, “A Model-based Multimedia Encryption Scheme for Real Time Videos”, IEEE International Conference on Recent Advances Space Technology Services and Climate Change, 2010, pp. 171-173

[21] Varalakshmi. L. M., Dr. Florence Sudha. G., Vijayalakshmi. V., “Enhanced Encryption schemes of video for real time”, In the proceedings of the International Conference on Signal Processing, Communication, Computing and Networking Technologies, 2011 , pp. 408-413

[22] Mukut Roy, Chittaranjan Pradhan, “Secured Selective Encryption Algorithm for MPEG-2 Video”, In the proceedings of the 3rd International Conference on Electronics Computer Technology (ICECT), 2011, pp. 420-423

[23] Lei Chen, Narasimha Shashidhar, Qingzhong Liu, “Scalable Secure MJPEG Video Streaming”, In the proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops, 2012, pp. 111-115

[24] Lingling Tong, Gang Cao, Jintao Li., “Layered Video Encryption Utilizing Error Propagation in H.264/AVC”, In the proceeding of the IEEE Symposium on Electrical & Electronics Engineering, 2012, pp. 182-187

[25] [25] Shunjun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo, “On the Design of Perceptual MPEG Video Encryption Algorithm”, IEEE Transactions on Circuits and Systems for Video Technology, vol. 17, No. 2, 2007, pp. 214-223

[26] M. Pazarci and V. Dipcin, “A MPEG2-Transparent Scrambling Technique”, IEEE Transactions on Consumer Electronics, Vol. 48, No. 2, 2002, pp. 345-355

[27] C. Wang, H.-B Yu, and M. Zheng, “A DCT based MPEG-2 Transparent Scrambling Algorithm”, IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, 2003,pp. 1208-1213.

[28] S. Lian, X. Wang, J. Sun, and Z. Wang, “Perceptual Cryptography on Wavelet Transform Encoded Videos, “in the Proceedings of IEEE International. Symposium on Intelligent Multimedia, Video and Speech Processing, 2004, pp. 57-60.

[29] S. Lian, J. Sun, and Z. Wang, “Perceptual Cryptography on SPIHT Compressed Images and Videos, “in Proceedings of IEEE International Conference on Multimedia and Expo, Vol. 3, 2004, pp. 57-60.

[30] S. Lian, “Perceptual Cryptography on JPEG2000 Compressed Images or Videos, “ in Proceedings of International Conference on Computer and Information Technology, IEEE Consumer Society, 2004, pp. 78-83