A Survey on Efficient and Secure Video Encryption Techniques

Ashrith K.A

Prajwal S Patil

Raunak Matai

Saurabh Rajpal

Syed Akram

Abstract- Encryption is a widely used technique which offers security for video transmission and therefore many video encryption algorithms are proposed. This study is aimed to give readers a quick overview about various video encryption algorithms. In this paper, the different video encryption algorithms and comparison between encryption methods are presented. With respect to not only their encryption speed but also their security level and streaming size. In this paper video streaming quality and selection of best encryption algorithm is shown.

I. INTRODUCTION

Fast growth in use of multimedia data on the internet needs more security during transmission. The video encryption algorithm is used to transmit the video securely over the network so that no unauthorized user is able to decrypt it. Video encryption has applications in many fields including internet communication, medical system, telemedicine and military Communication and so on.

Encryption is the process of applying algorithms and keys to transform digital message into cipher code and transmitted to the destination and decryption is a process of applying algorithms and keys to get back the original digital message from cipher code. The main goal of information security management is to provide authentication of users, integrity, accuracy and security of data resources. For real-world applications, a video encryption algorithm has to take into account parameters such as efficiency of computation and compression, high security and so on. Efficiency of computation means that the encryption and decryption algorithm should not cause too much time delay, and the requirements of real-time applications are met.

The first kind of algorithm is called symmetric key algorithm in which the same key is used for encryption as well as decryption, Data Encryption Standard is an example of symmetric key algorithm. The second kind of algorithm is asymmetric key cryptography which uses different keys for encrypting and decrypting the data, RSA algorithm is an example of asymmetric key encryption. This paper gives a brief introduction of all the video encryption techniques used in various applications. [1].

II. DIFFERENT VIDEO ENCRYPTION TECHNIQUES

Omar et al. proposed a new system [2] of video encryption technique which aimed to gain a deeper understanding of video data security on multimedia technologies, investigate how encryption and decryption could be implemented for real time video applications, and enhance the selective encryption for H.264/AVC. The system includes two main parts, first is the encryption of video stream in which the input sequence of video is first compressed by the H.264/AVC encoder, and the encoded bit stream is partially encrypted using the AES block cipher, the second function is the decryption of the video by specifying the encrypted stream, decryption of the frames, and decoding with H.264/AVC decoder.

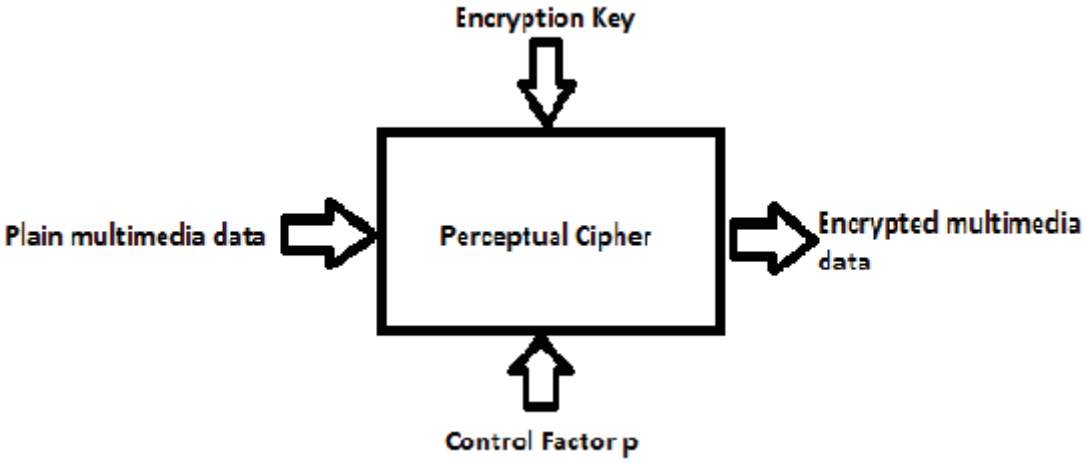
Amit Pande et al. illustrate the technique of joint compression and encryption of videos [3]. This method reduces the computational complexity greatly and also reduces the size of the encrypted video. Joint Video Compression and Encryption (JVCE) has gained increased attention in recent years to provide encryption of multimedia content

delivered over the internet. A JVCE framework based on modified Binary Arithmetic Coding (BAC) is used in which the overall length allocated to each symbol, is preserved, while the choice of map used to encode each symbol is based on a key. The encoder, referred to as Chaotic Binary Arithmetic Coder (CBAC), performs the function of scrambling the intervals without making any changes to the width of interval in which the code word must reside, thereby allowing encryption without sacrificing any coding efficiency. Also, some security enhancement features are presented to show how they can alleviate the limitations of the technique based on BAC-based encryption schemes.

Data Hiding through Video Encryption has been proposed in three Modules. They are H.264/AVC video encryption, data extraction and data embedding [4]. The process in this proposed method is that the H.264/AVC video stream ciphers with the encryption keys and produces an encrypted video stream. The data-hider can then embed the additional data into the encrypted video stream by the use of code-word substituting method without any knowledge of the original video content. At the receiving end, the hidden data extraction is accomplished either in encrypted or in decrypted version. The main advantage here is that the video file is always strictly preserved. According to the proposed system, data hiding is performed in encrypted H.264/AVC video bit stream which can ensure format compliance and preserve file size strictly. Application can be extended to two scenarios, which include extraction of hidden data from encrypted or the decrypted video stream. The proposed system being easy to implement preserves the bit-rate efficiently even after encryption and data embedding and is ideal for real time video applications. Data hiding in the encrypted domain preserves file size and confidentiality efficiently.

The technique of selective encryption [5] saves computational power, overhead, time and provides quick security by encrypting only a selected portion of the bit stream. The focus here is on the selection of the important part of the image that can be efficiently achieved by conceptually selecting the part of the image that is also further used in its normal mode of operation for the process of encryption. Once encryption is completed, the encrypted data is sent along the remaining original part of the message, by ensuring its secured transmission over the public networks. The main idea here is to select the part of the image by arranging the bit stream in grid form and selecting the diagonal grid. Two issues are mainly concentrated on here; the conceptual selection of message as to conserve time for transmission and overhead and the application of encryption algorithm to encrypt the selected part of the message. The solutions for the issue of application of traditional symmetric key algorithm for protection of data in a dynamic environment are proposed, such as MANET, WANET etc.

Bharat Bhargava et al, suggest a simpler and more effective design [6], which selectively encrypts fixed-length code words in MPEG video bit streams under the control of perceptibility factors. The proposed design is an encryption configuration that works with any stream or block cipher. Compared to the previously proposed schemes, the new design has more useful features, such as strict file size preservation, real time encryption. This enables it to support more applications with different requirements. It is desirable that the aural/visual quality degradation can be continuously controlled by a factor (p), denoted as encryption strength in percentage.



In many applications, such as pay-per-view videos and video on demand, the feature called perceptual encryption is advantageous. This feature needs the quality of the visual data is only partially degraded by the encryption process, i.e., the encrypted multimedia data are still partially perceptible after encryption.

Wail S Elkilani et al. describe how the AES encryption algorithm can be used to encrypt MPEG-4 video effectively [7]. Author is trying to implement AES for MPEG-4 in real time secure video transmitting system. It provides sufficient performance to display the received frames on time. The encryption delay overhead using RC-4 (rivert cipher 4 – It is a stream cipher known for simplicity and speed and is vulnerable when beginning of output stream is not discarded) and XOR algorithm is more when compared to AES algorithm encryption delay overhead. It is concluded that, AES algorithm is a feasible solution to speedy and real time video encryption and transmission.

Varalakshmi et al. focus on achieving encryption with low computational time and high data security [8]. The encryption process is achieved by encrypting intra-frames by secret sharing using DCT and DWT with scrambling of motion vectors. The performance comparison is based on secret sharing of DCT and DWT. Here the exploitation for temporal redundancy in the video frames is obtained by transforming each sequence of images to one image eventually with high spatial correlation and then the converted intra frames are scrambled which reduces the computational time effectively. The proposed system uses GF polynomial and increased LSFR key space, making cipher text robust by generating a new seed for every intra frame.

Reddy et al. [9] illustrates the approach of encryption and decryption of the video frames by using chaotic algorithm and also implements it. The chaotic image cryptosystem generally consists of two stages: Confusion and Diffusion. Here the encryption algorithm is applied to encrypt the individual frames with the help of the different dynamic chaotic systems to shuffle the pixel positions and then to change the pixel values to confuse the correlation between the frames of plain image and cipher image. The features of this approach are high security and high feasibility. The experimental results of this technique resulted in high throughput rate which is required for real time data protection.

Rahul Bambodkar et al. discuss an efficient and lightweight video encryption algorithm, which is based on scrambling of the DCT (Discrete Cosine Transformations) coefficients [10]. It is a Compression-Logic based video encryption algorithm. Rather than randomly permuting 8×8 coefficients of one DCT block, the random permutation is employed on to a number of permutation groups. Each permutation group is comprised of the DCT coefficients of the same frequency from every single block of a frame. Since each DCT block has 64 coefficient frequencies so 64 permutation groups can be formed, hence to encrypt a single video frame this technique runs random permutations on each of the groups. The encrypted video data is then compressed by standard Run-Length Encoding. The video

encryption algorithm is format-compliant because the video bit stream generated by this algorithm has the same format as that of bit stream generated by standard MPEG algorithms. Also according to the proposed video encryption algorithm it consumes low computation resource, achieves high scalability and confidentiality.
S.Rajagopal et al. describes a robust Perceptual video encryption technique which is applied by selecting one out of multiple unitary transforms depending upon the encryption key produced from method of random permutation at the transformation stage
[11]. A new class of unitary transforms is achieved when the phase angle is rotated in the DCT based transformation stage of the input residual video frame. A particular rotation angle is selected which gives a number of Unitary Transforms. Partial encryption is obtained by alternately using these transforms based on pre-designed secret key. The encrypted video frames are then quantized and encoded to transmit the encrypted video. Also an adaptive arithmetic encoder is used at the coding stage to overcome the limitations of Huffman coding. Hence, the encrypted bit stream is obtained. The decryption has to be done to obtain the original video. The performance factors are also analyzed depending upon various parameters. This technique will be convenient for video-based services over the networks. Therefore compression and joint encryption are applied in the video encryption for secure and high speed transmission and also their performance is measured by parameters such as Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

Pranali Pasalkar discuss the classification of various existing algorithms [12], its advantages and disadvantages. Security and time efficiency are really important for a video encryption algorithm. Security is an essential requirement, therefore cost of breaking the encryption must be greater than buying the legitimate video. The time efficiency refers to the time taken by encryption and decryption as heavy delay is not acceptable in real time.

There are few parameters to test the quality of video encryption technique given below
Speed: Total time required by an algorithm to encrypt is known as its computational speed.
Encryption ratio: The ratio between the size of encrypted part and the whole data size during an encryption of a video is encryption ratio.
Size: Encryption of video can increase its size, which in turn can increase time required for computation hence the size of video encryption should be as minimal as possible so compression of video is performed.
Security: Video encryption algorithm are assessed mostly on this parameter. It should be able to resist numerous attacks such as brute force attack, plain text attack etc.

The video encryption algorithms are classified into five categories:
Fully layered Encryption: The video content is first compressed to reduce the size of the video and then using standard algorithms like AES and DES encryption is achieved in this method. The disadvantage of this method is that it's not suitable for real-time video encryption because there is heavy computation required and the speed is also slow.
Scrambling based Encryption: The algorithms in this category mainly use different permutation algorithms to scramble and encrypt the contents of video. Scrambling means re-positioning of pixels and not changing its value. In this encryption method, security is low, speed is fast but it is vulnerable to known-plaintext attack.
Selective Encryption: The video encryption algorithms in this kind of encryption selects only the needed bytes in the video frames and then encrypts it. The computational capacity lowers to a great degree because every single byte of video content is not required to be encrypted. Selective encryption algorithm is fast but encryption ratio is low.
Perceptual Encryption: The quality of video is partially degraded in Perceptual Encryption. The low quality video observed in many pirated videos is due to perceptual encryption. Perceptual encryption is not secure against known-chosen plaintext attack.
Chaotic Encryption: Chaos based video encryption is best suited for real-time video encryption because of low computational complexity, format-compliance, invariance of compression ratio, real-time, strong transmission error tolerance, multiple levels of security, and hence, it is superior over other conventional encryption methods.

A perceptual encryption scheme is proposed in which uses four linear transforms and then the cipher video data is handed over to MPEG-2 encoder [13]. 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.

The algorithm produces an arbitrarily degraded view by encrypting it in DCT Domain [14]. 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.

In a perceptual cryptography scheme for 3DSPIHT compressed video is proposed. In this scheme the video is degraded to different degrees by controlling a quality factor [15]. 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 [16]. 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.

III. COMPARISON OF DIFFERENT VIDEO ENCRYPTION TECHNIQUES

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

Observing the table we can infer that the algorithms performing total encryption such as AES although provide high robustness, suffer from visual degradation and slow speed. The algorithms under permutation techniques provide better speed but their robustness and visual degradation suffer. Similar case could be built for selective encryption techniques as they suffer from low robustness and high visual degradation. The perpetual encryption techniques provide a combination of different levels of robustness, speed and visual degradation.

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 Code word Technique	ND	ND	ND	H	General
	LTCE	ND	L	H	H	Wireless devices
	VEA	ND	L	H	H	General

Selective Encryption	MVEA	ND	L	H	H	General
	RVEA	ND	L	H	H	Real time videos
	Compliant Selective	~20%	L	H	H	General
	Secure Advanced Video Coding	L	H	H	ND	Video conferencing
	Roy and Pradhan	ND	L	H	H	Peer to peer, video-on-demand
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

Table 1: Comparison of Video Encryption Algorithms

IV. CONCLUSION

In real time application to maintain the quality of video with Encryption algorithm is a difficult task. There are trades offs when applying different encryption algorithms and its choice depends on the applications. These algorithms suffer from either low security, or low speed, or quality, or stream size increases. Therefore there is a need to propose a new video encryption algorithm which will provide efficient and secure video transmission and reception.

ACKNOWLEDGEMENT

The work reported in this paper is supported by the college through the TECHNICAL EDUCATION QUALITY IMPROVEMENT PROGRAMME [TEQIP-II] of the MHRD, Government of India.

REFERENCES

[1] M. Abomhara, Omar Zakaria, Othman O. Khalifa , “An Overview of Video Encryption Techniques”
[2] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.BZaidan.,”Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard”
[3] Sulochana.P1, M.Santhi Sudha2, D.Krishna,”Joint Video Compression and Encryption using Arithmetic Coding and Chaos”
[4] An Approach for Data Hiding Through Video Encryption 3 M.Tech (CSE) 1, Assistant Professor2, Associate Professor, HOD of CSE Dept3 Jawaharlal Nehru Institute of Technology.
[5] PriyankaAgrawal Department Of Computer Science and Engineering, RCET, Bhilai, ManishaRajpoot Department Of Computer Science and Engineering, RCET, Bhilai,”.A Fast and Secure Selective Encryption Scheme using Grid Division Method”
[6] Shujun Li, Guanrong Chen, Fellow, IEEE, Albert Cheung, Member, IEEE, Bharat Bhargava, Fellow, IEEE and Kwok-Tung Lo, Member, IEEE,”Design of Perceptual MPEG-Video Encryption Algorithms"
[7] Wail S Elkilani, Hatem M Abdul Kader, Faculty of computer and information, MINUFYA University, IEEE 2009,”EVALUATION OF AES ENCRYPTION TECHNIQUE”
[8] VARALAKSHMI LM, Dr. RLORENCE SUDHA G, VIJAYALAKSHMI V, Associate Professors, DEPT. of ECE, Proceeding of 2011 international conference on signal processing communication, computing and network technologies (ICS CCN 2011),”LIGHT WIEGHT VIDEO ENCRYPTION ALGORITHM”

[9] S Raghunath Reddy et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3259 – 3261.
[10] Rahul Bambodkar, Avinash Wadhe“ Fast Encryption Algorithm for Streaming Video over Wireless Networks”, International Journal of Computational Engineering Research,Vol 03,Issue 5.
[11] S.Rajagopal, M.Shenbagavalli,"Partial Video Encryption Using Random Permutation Based on Modification on Dct Based Transformation", International Refereed Journal of Engineering and Science (IRJES), Volume 2, Issue 6, PP. 54-58,June 2013.
[12] Pranali Pasalkar et al. Int. Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 5, Issue 2, (Part -4) February 2015, pp.25-29.
[13] M. Pazarci and V. Dipcin, “A MPEG2-Transparent Scrambling Technique”, IEEE Transactions on Consumer Electronics, Vol. 48, No. 2, 2002, pp. 345-355
[14] 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.
[15] 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.
[16] 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.