Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.270 – 274

SURVEY ARTICLE

A Survey Report on Video Encryption and Decryption Techniques

Saraswati Singh[1], Nilmani Verma[2], Vinay Kumar[3]

[1]M.Tech. Scholar, CSE Department, School of Engineering & IT, MATS University, Raipur (C.G.), India
[2]Head, CSE Departments, School of Engineering & IT, MATS University, Raipur (C.G.), India
[3]Assistant Professor, ET&T Department, Bhilai Institute of Technology, Raipur (C.G.), India
[1] saraswatipatel13@gmail.com; [2] nilmaniv@matsuniversity.ac.in; [3] vinaypatel.elex@bitraipur.ac.in

Abstract— With the increase in the development of multimedia technologies, the multimedia data are transmitted in the various fields like commercial, video conferencing, medical and military fields, which generally include some sensitive data. Hence there is a great demand for transmission technique. Cryptography is becoming most popular for communication any type of sensitive data. There are various encryption algorithms have been proposed for the video transmission and reception which are discovered from time to time to encrypt the video data to make more secure and in addition focuses on compression efficiency. This paper shows a study report on various video encryption algorithms and presents a survey of over 15 research papers dealing with video encryption and decryption techniques.

Keywords— Encryption, Decryption, Cipher, Decipher, Compression

I. INTRODUCTION

Fast growing the use of multimedia data in internet need more security during transmission, hence security is an important issue in communication and storage of video data. The video encryption algorithm is to transmit the video securely over the network so that no unauthorized user can able to decrypt the video. Video encryption has applications in many fields including the internet communication, medical system, telemedicine and military Communication, etc. The video data have special properties such as bulk capability, high redundancy and high correlation among the pixels. Encryption is the process of applying special mathematical algorithms and keys to transform digital data into cipher code before they are transmitted and decryption involves the application of mathematical algorithms and keys to get back the original data from cipher code. The encryption can be performed either using Symmetric key cryptography or by using Asymmetric key cryptography. If same key is used for encryption and decryption then it is called as Symmetric key cryptography and if the different key is used for encryption and decryption then it is called as Asymmetric key cryptography. Image compression algorithms are used use to reduce the amount of data required to represent a digital image and the basis of the reduction process is the removal of spatial redundancies. Two types of compression are lossless compression and lossy compression. If same image can be generated from the compressed image then it is Lossless compression otherwise it is lossy compression.

The main goal of security management is to provide authentication of users, integrity, accuracy and safety of data resources. For real-world applications, a video encryption algorithm has to take into account various parameters like high security, computational efficiency, compression efficiency and so on. High level of security is required to completely prevent unauthorized access. Computational efficiency means that the encryption or decryption algorithm should not cause too much time delay, so that the requirements of real-time applications are met. Video compression is employed to reduce the storage space and save bandwidth, so that the encryption process should have the least impact on the compression efficiency.

II. LITERATURE REVIEW

Various algorithms have been proposed in the near future. Some look very effective but lack efficiency. In the literature survey it has been seen that the dual approach of image compression & encryption is carried out in any one of the following ways based on the order of these two processes.

1. Individual or independent compression and encryption

i) Compression followed by Encryption (CE): In this sequence, an intruder has less cleave to access images but encryption may again increase the size.

ii) Encryption followed by Compression (EC): In this sequence, size is not again increased but an intruder may have more clues to access the images.

2. Joint Compression and Encryption (JCE): This approach is recently used which may be fast as compared to CE and EC but procedure is complicated.

Listed below are a few video encryption algorithms.

1. MPEG Video Encryption in Real-time using Secret Key Cryptography [2]:

C. Shi, S. Y.Wang and B. Bhargava have presented an algorithm for a real time video encryption (RVE) using secret key. It encrypts selected sign bits of the DC coefficients and/or sign bits of motion vectors using DES or IDEA. It selects at most 64 sign bits from each macro block. RVEA achieves the goal of reducing and bounding its computation time by limiting the maximum number of bits selected. The differential encoding of DC coefficients and motion vectors in MPEG compression increases difficulty of breaking RVEA encrypted videos. If the initial guess of a DC coefficient wrong, it is very difficult to guess the following DC values correctly.

2. Perceptual Cryptography on SPIHT Compressed Images and Videos [3]:

S. Lian, J. Sun and Z. Wang have presented an algorithm for 3D-SPIHT compressed videos. In this scheme different number of wavelet coefficients encrypts different number of coefficients signs and data cubes. Videos can be degraded to different degrees under the control of quality factor. Its encryption strength can be adjusted according to certain quality factor. It is not secure against known chosen plaintext attack.

3. Compliant Selective Encryption for H.264/AVC Video Streams [5]:

C. Bergeron and C. Lamy-Bergot proposed a new algorithm a syntax based encryption for H.264 videos. Encryption is done in the encoder. The proposed method inserts the encryption mechanism within the video encoder, providing secure transmission which does not hamper the transmission process. The bits selected for encryption are chosen with respect to the considered video standard according to the following rule: each of the encrypted configurations gives a synchronized and a standard compliant bit stream. This can in particular be done by encrypting only parts of the bit stream which have no or a negligible impact in evolution of the decoding process, and whose impact is consequently purely a visual one.

4. Secure Advanced Video Coding Based on Selective Encryption Algorithms [6]:

Shiguo Lian, Zhongxuan Liu, Zhen Ren and Haila Wang proposed an algorithm based on Advanced Video Coding **(**AVC). During AVC encoding sensitive data such as intra prediction mode, residue data and motion vector are encrypted partially. DCs are encrypted based on context based adaptive variable length coding. The encryption scheme is of high key sensitivity, which means that slight difference in the key causes great differences in encrypted video and makes statistical attack difficult. It is difficult to apply known plaintext attack. In this encryption scheme, each slice is encrypted under the control of a 128 bit sub-key. Thus, for each slice, the brute force space is 2^128. This brute force space is too large for attackers to break the cryptosystem. According to the encryption scheme proposed here, both the texture information and the motion information are encrypted, which make it difficult to recognize the texture and motion information in the video frames.

5. On the Design of Perceptual MPEG Video Encryption Algorithm [7]:

Shunjun Li, Guanrong Chen, Albert Cheung, Bharat Bhargava, and Kwok-Tung Lo made an algorithm based on a generalized version for perceptual encryption, by selectively encrypting FLC data elements in the video stream. Apparently, encrypting FLC data elements is the most natural and perhaps the simplest way to maintain all needed features, especially those needed for strict size preservation. To maintain format compliance, only

last four FLC data elements are considered, which are divided into three categories; i) intra DC coefficient ii) sign bits of non intra DC coefficients and AC coefficients iii) sign bits and residuals of motion vectors.

6. Fast and Secure Real-Time Video Encryption [9]:
C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar proposed Data Encryption Standard (DES) algorithm for encrypting and decrypting unclassified data of the same length by using a symmetric key to make secure video encryption feasible for real-time applications without any extra dedicated hardware. This algorithm achieves computational efficiency by exploiting the frequently occurring patterns in the DCT coefficients of the video data. Computational complexity of the encryption is made proportional to the influence of the DCT coefficients on the visual content.

7. Joint Video Compression and Encryption using Arithmetic Coding and Chaos [10]:
Amit Pande, Joseph Zambreno & Prasant Mohapatra proposed chaos-based for Joint Video Compression and Encryption (JVCE) to reduce the computational complexity of video compression, as well as provide encryption of multimedia content for web services. In this paper a JVCE framework based on Binary Arithmetic Coding (BAC). It first present an interpretation of BAC in terms of a skewed binary map and then describe 7 other possible chaotic maps which give similar Shannon optimal performance as BAC and then it modified BAC in which the overall length within the range [0, 1] allocated to each symbol that is preserved, but the choice of map used to encode each symbol is based on a key. A JVCE scheme reduces the computational cost involved with traditional approach of encryption after compression. The CBAC scheme uses an interpretation of Arithmetic Coding using chaotic camps. The compressed data itself is not encrypted, making it easier to preserve properties of video data for indexing, search, network communications and other operations. The proposed security enhancements allow us to build a video encryption scheme resistant to known attacks.

8. Video Compression and Encryption Based-On Multiple Chaotic Systems [11]:
Qinchun Qian, Zengqiang Chen and Zhuzhi Yuan made a new algorithm based on multiple chaotic systems which deal with both video streams being compressed and compressed video streams. The so-called multiple chaotic systems actually consists of three chaotic or hyperchaotic maps, namely Logistics Map, 2-D Baker Map and a 4-D hyperchaotic Map. The three secret key functions are carried out as partial encryption when compressing the video data, as block permutation and confusion after the video compression respectively. This scheme provides high security and small size preservation.

9. Partial Video Encryption Using Random Permutation Based on Modification on DCT Based Transformation [12]:
S.Rajagopal and M.Shenbagavalli proposed a robust Perceptual video encryption technique is applied by selecting one out of multiple unitary transforms according to the encryption key generated from random permutation method at the transformation stage. A new class of unitary transforms is generated by rotating the phase angle in the DCT based transformation stage of the input residual video frame. Different rotation angle is chosen which provides number of Unitary Transforms. By alternately applying these transforms based on pre-designed secret key, partial encryption is achieved. For the transmission of encrypted video, the encrypted video frames are quantized and encoded. To overcome the drawbacks of Huffman coding, adaptive arithmetic encoder is used at the coding stage. Thus the encrypted bit stream is obtained. Thus the decryption is done to obtain the original video. Also the performance factors under various parameters are analyzed. This methodology will be useful for video-based services over networks. Thus joint encryption and compression are applied in the video encryption for high speed and secure transmission also their performance is measured by means of parameters such as MSE & PSNR.

10. Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study [13]:
Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas and Aniket More made a safely exchange confidential videos by an innovative encryption algorithm for compressed videos using H.264. It shuffles the video frames along with the audio to maintain a balance between security and computational time and then AES is used to selectively encrypt the sensitive video codewords. A comparative study of with other existing algorithms has been put forward in this paper to prove the effectiveness. This algorithm compared with the currently known methods of cryptography, where two different types of the encryption methods (Symmetric key encryption and Asymmetric key encryption) are highlighted and evaluated with respect to their security level and encryption speed. Also, various existing algorithms are explained where Simple Permutation algorithm and the proposed video encryption algorithm are the most secure algorithms, whereas crisscross permutation algorithm [8] has a serious security flaw; it does not immune to the known-plaintext-attack. With respect to encryption speed, the proposed encryption algorithm and crisscross permutation algorithm [1] are fast, Simple Permutation [3][8] is

very slow while applying DES on entire video stream. Hence a need of trade-off to be maintained in video encryption algorithms and its choice depends on the applications.

11. A Permutation-based Correlation- Preserving Encryption Method for Digital Videos [14]:
D. Socek, H. Kalva, S. S. Magliveras, O. Marques, D. Culibrk and B. Furht made a new highly optimized algorithm using permutation. Most encryption algorithms have a randomization effect on the source data, and cannot be effectively applied before compression stage. This method using correlation preserving permutation which performs encryption prior to video encoding. There is no secret key on which a permutation is generated. This method relies on the sorting permutation of previous frame, and thus, a key is directly dependent on the plaintext. Under a chosen plaintext attack, the adversary can compute the sorting permutation for the chosen frame, but this gives no information about the sorting permutations for the unknown frames. Some algorithms use permutation list as secret key to encrypt video contents.The limited known-plaintext attack is applicable to this method.

12. Selective encryption of MPEG-2 video [15]:
T. Lookabaugh et al made an algorithm using Selective encryption schemes but most of them have proven to be weak against [16]. The aim of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security. The video frames are encrypted with use of selective encryption algorithm in which not each and every byte of the video is encrypted. Selective encryption is a technique to save computational power, overhead, speed, time. . This scheme is unsuitable in real time application due to high delay and computation complexity.

13. A Light-Weight Encrypting For Real Time Video Transmission [17]:
Salah Aly made an algorithm for light weight encryption. The most straight-forward method to encrypt every byte in the whole Moving Picture Experts Group (MPEG) stream using standard encryption schemes such as DES or AES. The idea of Naïve algorithm to treat the MPEG bit-stream as text data and does not use any of the special structure. Naïve algorithm ensures the security level to the entire MPEG stream by standard encryption. This algorithm not applicable solution for big video, because it is very slow especially when we use triple DES.

14. Design of secure computer systems on the advanced encryption standard (AES) [18][19]:
Jean-Yves chouinard made an algorithm for advanced encryption standard **(**AES). In 1997, the NIST called for submissions for a new standard to replace the aging DES. AES cryptosystem operates on 128-bit blocks, arranged as 4 × 4 matrices with 8-bit entries. The algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits and blocks of length 128, 192, or 256 bits . The security of AES uses types of transformation. Substitution permutation network is used, mixing of column and adding key, each round of AES except the last round uses the four transformations. It is also complex but more secure using symmetric key.

15. Introduction to the analysis of the Data Encryption Standard (DES) [20][21]:
Wayne G. Barker proposed for Data Encryption Standard. DES is one of the most important examples of a block cipher which operates on blocks of 64 bits at a time, with an input key of 64 bits. DES was the result of a contest set by the U.S. National Bureau of Standards (now called the NIST) in 1973, and adopted as standard applications in 1977. DES is having 16-round series of substitution and permutation. The data and key bits are shifted, then permutated, after the permutation the bits are XORed, and sent through, 8 s-boxes in each round. Decryption is the reverse process of the same. The DES is widely used for encryption of PIN numbers, bank transactions, and the like. It is very complex and less secure .

III. CONCLUSION

In this paper, we summarize some researches about the application in the field of cryptography. This paper focuses survey report on the various techniques for video Encryption. We have studied and analyzed, each technique is unique in its own way, which might be suitable for different applications. Encryption algorithm is difficult to perform in real-time applications without harming the quality of video in some way. 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.

REFERENCES

[1] L. Tang, "For encrypting and decrypting MPEG video data efficiently", in Proceedings of The Fourth ACM Intl. Multimedia Conference (ACM Multimedia), (Boston, MA), pp. 219-230, November 1996.

[2] 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 ,pp. 191–201, 1999.

[3] 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, pp. 57-60,2004.

[4] 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

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

[6] Shiguo Lian, Zhongxuan Liu, Zhen Ren and Haila Wang, "Secure Advanced Video Coding Based on Selective Encryption Algorithms", IEEE Transaction on Consumer Electronics, Vol. 52, No. 2, pp. 621-629,2006.

[7] 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, pp. 214-223, 2007.

[8] Shiguo lian, Multimedia Content Encryption: Algorithms and Application, CRC Press, 2008.

[9] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar ,"Fast and Secure Real-Time Video Encryption" , Sixth Indian Conference on Computer Vision, Graphics & Image Processing , pp.257-264, year-2008.

[10] Amit Pande, Joseph Zambreno & Prasant Mohapatra, "Joint Video Compression and Encryption using Arithmetic Coding and Chaos", IEEE Intl. Conf. on Internet Multimedia Systems Architecture and Application, 2010.

[11] Qinchun Qian, Zengqiang Chen and Zhuzhi Yuan , "Video Compression and Encryption Based-On Multiple Chaotic Systems", International Journal of Innovative Computing, Information and Control Volume 6, Number 1, pp.315-322,January 2010

[12] 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.

[13] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas and Aniket More, "Proposed Video Encryption Algorithm v/s Other Existing Algorithms: A Comparative Study", International Journal of Computer Applications (0975 – 8887) Volume 65– No.1, pp.1-5, March 2013.

[14] D. Socek, H. Kalva, S. S. Magliveras, O. Marques, D. Culibrk, and B. Furht, "A Permutation-based Correlation- Preserving Encryption Method for Digital Videos", in International Conference on Image Analysis and Recognition,LNCS 4141,pp. 547-558, 2006.

[15] T. Lookabaugh et al., "Selective encryption of MPEG-2 video", in Proceedings of the SPIE Multimedia Systems and Applications VI, (Orlando, FL), September 2003.

[16] T. Lookabaugh and D. C. Sicker, "Selective encryption for consumer applications", IEEE Communications Magazine, pp. 124-129, May 2004 .

[17] Salah Aly, "A Light-Weight Encrypting For Real Time Video Transmission". Available from http://www.cdm.depaul.edu/research/Documents/TechnicalReports/2004/TR04-002.pdf. (Accessed on March 2, 2009).

[18] Jean-Yves chouinard, "Design of secure computer systems on the advanced encryption standard (AES)". Available from http://www.site.uottawa.ca/~chouinar/Handout_CSI4138_AES_200.pdf. (Accessed February 15, 2009).

[19] Shon Harris, SICCP Exam Guide, fourth edition, McGraw-Hall (2007).

[20] Wayne G. Barker, "Introduction to the analysis of the Data Encryption Standard (DES)", A cryptograph-ic series, Vol. 55, p. viii + 190, Aegean Park Press, 1991.

[21] Kofahi, N.A., TurkiAl-Somani and KhalidAl-Zamil, "Performance evaluation of three encryption/decryption algorithms" 2005 IEEE International Symposium on Micro-NanoMechatronics and Human Science, Volume: 2, pp 790-793, 2003.

[22] 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 .

