A Comprehensive Survey of Video Encryption Algorithms

Darshana Hooda
System Analyst &
Head Computer Centre
DCRUST, Murthal

Parvinder Singh, PhD.
Associate Professor
Computer Science & Engg.
DCRUST, Murthal

ABSTRACT

Encryption is the widely used technique to offer security for video communication and considerable numbers of video encryption algorithms have been proposed. The paper explores the literature for already proposed video encryption algorithms with the focus on the working principle of already proposed video encryption schemes. This study is aimed to give readers a quick overview about various video encryption algorithms proposed so far.

General Terms

Encryption, video security, video encryption metric, compression, decompression.

Keywords

Video encryption, video security requirements, video encryption evaluation metric, self adjustable encryption, codec independent.

1. INTRODUCTION

Recent advances in multimedia compression, communication technologies and abundant availability of low cost constrained display devices, have led to phenomenal growth of digital multimedia services and applications video chat, video conferencing, telemedicine & variety of entertainment services. These services are widely used over open network, so security of multimedia applications are on stake. For the digital video data, the major security threats are unauthorized play, forging, and distortion of video by eavesdropper. Early methods available for video data security were concerned to user's identity authentication and access control, while video content were not encrypted. These security concerns are not sufficient when video is distributed over open network as it makes stealing, decoding, playing and broadcasting of transmission relatively easy process. One more recent arising requirement is to ensure the video content privacy against unwelcome third parties. Video consumption by constrained devices add one more precaution in designing of security techniques that they must meet to the real time operation constraint at receiver device, which means that techniques must be compact(code size) and simple and should have low processing complexity taking care of limited capability of receiver in terms of limited memory, processing speed and power. Encryption is widely established technique to address all these security needs of video applications. Conventional approach like AES, DES called naïve algorithm approach in video encryption is straight approach to encrypt whole video data. These cryptographic algorithms are highly secure but not well suited for video encryption as they cannot process the bulky volume of video data in real time. The video consumption by constrained devices and rich diversity of video services pose special requirements in the context of security. Conventional cryptographic techniques are not adaptable to meet newly seen peculiar security requirements of commonly used video services. So the demand for cryptographic components that can be efficiently implemented is strong and growing. For such implementations, generic term lightweight cryptography is used. Lightweight cryptographic techniques are designed to cope with the trade-offs between performance, security and cost . It is generally simple to optimize any two of the design goals, security & cost, security & performance or cost & performance; but, very difficult to optimize all three design goals at once.[1] Since the mid-1990 research efforts have been directed towards the development of specific video encryption algorithms to address specific need of video applications.

The main purpose of this study is to explore working principle of various available encryption techniques proposed so far and intends to motivate the scholars/researchers towards the development on new video encryption techniques to address newly seen challenges in the area. A strong belief emerges from current scenario, that there is need of encryption algorithm to encrypt the video data as per constrained receiver's computing resources and security requirement of video service so decryption may take place on consumer's constrained device without worrying about computational resources, platform, video application and data pipe, in real time.

2. SECURITY ISSUES IN VIDEO TRANSMISSION

The goals of secure video transmission are: confidentiality, conditional access, authentication, copy control, content tracking. Different video application requires different level of security. Above mentioned security needs further may be classified in to two categories: Entertainment applications like VoD and pay TV. Personalised video applications are like business meetings, diplomat dialogues, and telemedicine etc. Both categories need different kind of security. Entertainment applications have loose security needs while personalized video services require high degree of security. The value of video data in entertainment application is associated with video quality and timeliness. In entertainment industry high quality video is priced and requires an authorized access , while low quality versions may free , to stimulate the user to purchase high quality version[2]. The verification of source and receiver identities is needed for entertainment applications as well as personalized video applications and this is achieved using digital signatures or certificates.

Copy control is necessary security measure for entertainment applications because it is possible to reproduce a digital video without any loss or degradation, leads to illegal copying of video streams [3]. For video transmission applications copy control involves identifying protected video streams, defining conditions for which a legal copy of a video stream can be made and ensuring that the video stream is accessed only through the use of compliant receivers. Watermarks and side information written in video header are generally used for this purpose.

Content tracking is the embedding of identification information to video, to create unique copy of video stream for each user or group of user. Robust watermarking is used for content tracking as they cannot be easily removed from the video stream. Watermarking has been proposed to carry copyright, authentication and content tracking information.

Personalized video applications are sensitive applications and usually have strict security requirements equal to those demanded for text encryption. The encryption algorithms for personalised video services have to withstand not only classical cryptanalytic attacks but also the perceptual attack[4,5] in order to ensure that no visible information related to the sensitive communication is disclosed.

The methods/techniques that are used for secure video transmission include cryptography, digital signature and video watermarking. It is generally accepted that no single technology can provide a complete solution for securing video transmission and that cryptography, digital signatures and watermarking each has a role in security applications.[6] Encryption algorithms used in entertainment applications are considered secure and valuable if the two conditions firstly if the cost to break the algorithm is higher than the license fee for the video content and secondly if the time required to break the algorithm is longer than the time that the encrypted video .Perceptual attack in most cases are able to reconstruct just low-quality video whose perceptual value is not comparable to the original video. Therefore perceptual attack do not pose a great threat to entertainment applications[2].

It is observed that cryptographic techniques plays vital role in providing security to video applications. The advantages of using cryptography is that the encrypted video stream can not be viewed nor interpreted unless the receiver knows the decryption key however security of encryption solely depending on protection of decryption key. The recent flourish of devices processing the video data however having limited resources in terms of memory, computational capability and power , rapid growth in enabling technologies & rich diversity of video services arises the need, to evolve lightweight cryptographic technique in such a way that one technique may used for different security needs of video transmission.

3. VIDEO ENCRYPTION EVALUATION METRIC

For quantitative analysis of video encryption techniques, there is a need to define a set of performance parameter considered as Video encryption metric. This metric helps the user to evaluate the performance of video encryption algorithm.

Computational Efficiency: It may be defined in terms of space complexity and time complexity of encryption algorithms. Space complexity of encryption is determined by memory requirement for code and data while time complexity measures the time requirement for encryption/decryption. Software and hardware implementation of cryptographic algorithms exits in plenty and both have different and sometimes contrary characteristics. For software implementation RAM and ROM requirements and required number of clock cycles, plays vital role in determining performance of algorithm. Situation becomes more critical in today’s scenario when video data is displayed on constrained devices i. e. display devices with limited computing resources like memory, processing speed and power. It ignite the need of small size encryption and decryption algorithms code as well as fast enough to meet real time requirement of video applications. Here we will restrict our discussion to software implementation of video encryption techniques.

Security Offered: Emerging video applications like VoD, Videoconferencing, telemedicine etc, and each needs different level/type of security. VoD requires loose security needs with perceptual degradation only while video conferencing may require totally closed communication for all others out of communication group.

Compression efficiency: Video data is generally very large so usually compressed to reduce storage space and to save bandwidth. Encryption algorithm may work before the encryption after the encryption or during the compression. During the design of encryption algorithm it is major concern that the size of compressed video should not be increased by the encryption.

Codec Portability: It is recommended that an encryption algorithm should work in compliance to video codec and does not require a modification of the underlying video codec/implied framework.

Transcodability: A video stream compressed with a codec contains syntax structure respective to codec, to help the decoder to properly interpret the video stream. It is recommended that an encryption algorithm is able to preserve the syntax structure for the encrypted video stream so that it is decidable at the receiver side without decryption.

Visual Degradation: This is required to measure perceptual distortion of video stream. For sensitive video applications like video conferencing for business meetings needs high degree of visual degradation to make it totally incomprehensible for third parties other than communicators while for entertainment applications low visual degradation is needed to keep it comprehensible to user to stimulate for purchase of high quality video.

Error Tolerance: A highly desirable feature of encryption algorithm especially critical when data travelled through error prone networks. Some of encryption techniques have strong avalanche effect(error in one encrypted bit results in more erroneous bits during decryption) hence causes distortion and in some cases lost of important information, which is critically intolerable for some of video application like medical imaging. There is strong need to device error tolerant encryption techniques.

Lossless Visual Quality: Highly desirable feature for entertainment applications. The encryption should produce same visual quality as original video when decrypted legally.

4. VIDEO ENCRYPTION TECHNIQUES

Since the mid 1990s many research efforts have been made to the development of specific video encryption algorithm. Fuhrt and Kirovski(2004) has given detailed overview of early video encryption algorithms. 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 algorithms. They also evaluated performance of video encryption taking in to consideration various performance parameters like: encryption efficiency, compression efficiency, security offered, video codec compliance etc. Aim of this study is to give readers a quick overview about various video encryption algorithms proposed so far.

In Naïve Approach whole video data is encrypted using a symmetric key cryptosystem. However, even the fastest modern symmetric schemes such as DES or AES are computationally very expensive so not well suited for video data encryption, due to need of processing, large volume of data in real time. However these techniques offer highest level of security.

Video Scrambling techniques offer fast yet very insecure distortion of the video data. This technique was evolved due to industrial need of protecting the viewers from free viewing of paid cable channel. The work known on signal scrambling was based on using an analog device to permute the signal in the time domain or distort the signal in the frequency domain by applying filter banks or frequency converters[7]. However, these schemes are easy to break.

Specific Video Encryption techniques evolved as pre compression, in compression and after compression. Meyer and Gadegast(1995) introduced the Secure MPEG(SECMPEG) proposed a selective video encryption after the compression. The after compression algorithms takes specific properties of the compressed video video stream into account. They generally select a partial video stream for encryption or whole video stream using light weight cryptographic algorithm. SECMPEG encrypts important part of video using conventional encryption algorithm. Four levels of security may be achieved by selecting different parts of compressed video stream. In first level security headers from the sequence layer to slice layer are encrypted however motion vector and DCT blocks remain unencrypted. In second layer security, additional to above, most relevant parts of I blocks are also encrypted. In third level security all I frames and I blocks are encrypted. Fourth level security offers highest security and here whole MPEG video stream is encrypted using any standard symmetric encryption. This approach does not achieve a significant computational reduction with respect to total encryption overhead and defines new syntax which is incompatible to the MPEG syntax.[8] A similar approach to secure MPEG-I & MPEG-2 video stream was proposed by Maples and Spanos, 1995 called Aegis, In this all I frames in MPEG video stream are encrypted, while P- and B- frames are left unencrypted. In addition, MPEG video sequence header, that contains important information for decoding process, also encrypted. ISO end code, last 32 bit of the video stream is also encrypted. Agi and Gong criticized encrypting only I-frames Aegis and SECMPEG and presented results to show that partial leakage from the I blocks in P and B frames renders AEGIS unsuitable for applications like military where each and every part of the video data is important[10]

Choon(2004) proposed a light weight and cost effective encryption algorithm based on Shanon principle of diffusion and confusion. These principles can be achieved by permutation of macroblock followed by XOR operation on the permuted macro block[11]. Choo(2007) introduced one another leight weight encryption algorithm on the uncompressed raw MPEG data named Secure Real Time Media Transmission(SRMT), which uses two block transpositions and a XOR operation[12]. However survey of various lightweight cryptographic implementation are given by Eisenbarth(2007)[23].

Quio and Nahrstedt (1998) proposed video encryption algorithm based on statistical analysis. This algorithm works on compressed video stream. The basic idea of VEA is byte scrambling algorithm on output video data stream. It handles I frames at slice level and process them bitwise. the data is divided into two byte stream as odd and even numbered bytes and two streams are XORed forming the first part of the cipher. The second part of cipher is constructed by performing DES over the even numbered byte streams[13].

Tang(1996) offered Zigzag permutation algorithm based on embedding the encryption into the MPEG compression process. In this algorithm ordering transformation coefficients is modified by using a random permutation matrix that act as secret key. In this scheme I- frames of MPEG video undergo zigzag reordering of 8X8 block to 1X64 vector. This technique works in three stages: In first stage list of 64 permutation is generated. Next splitting of 8X8 block is carried out by splitting the DC coefficient(8 bits) in to two equal halves, 4 most significant bits are placed in DC coefficient and least significant bits as the last AC coefficient, then random permutation is applied to the split block. [14]

Alattar, AI-Regib and Al-Semari, 1999 proposed three methods for selective video encryption of MPEG-I video sequence, based on DES Cryptosystem. In first method every n^{th} I – macroblock is encrypted. In second method headers of all the predicated macroblocks and nth macroblock data is encrypted. Third method encrypts n^{th} macroblock aswell as header of every n^{th} predicate macroblock. This scheme works during compression. [15]

Shi, Wang and Bhargava, 1999 & 2004 proposed four different video encryption algorithms: Algorithm I, Algorithm II(VEA), Algorithm III(MVEA), Algorithm IV(RVEA). These techniques were based on selective encryption selective coefficients in the JPEG/MPEG schemes. Algorithm I uses the permutation of Huffman codewords in the I- frames during compression. This permutation serve as secret key. Algorithm uses the observation uses the observation that encryption of sign bits of DCT coefficient in MPEG video stream is significant, therefore in VEA signbit of DCT coefficient is XORed with a secret m bit binary key. Syncronization pointes over the stream are created to help in recovering of corrupted data parts in case of error, noise or loss during the transmission. They discussed that key has to be long enough and frequently changed. An additional point stressed is not to encrypt predictable header information. MVEA is actually improvement on VEA by changing the sign bits of both DC coefficients of I block and motion vectors of B and P frames. Each GOP begins with new synchronization point. They conclude that because of the differential coding of motion vectors, sign bit change affects the vector's magnitude as well as its direction, hence encrypting the motion vector ensures satisfying privacy so that encrypting B and P frame's DCT coefficient becomes useless. The main difference between MVEA and VEA is that MVEA encrypts only DC coefficients of I blocks. This is because DC coefficients are reported to be more influential on video data than AC coefficient. They also claim that DC coefficients may be obtained using ACs and recommends encryption of first few AC coefficients for more important videos. To eliminate the weakness against plaintext attack, improved version of MVEA is proposed. B. Bhargava proposes DES encryption of the above mentioned coefficients in an importance order. Next REVA was proposed with the basic idea that only a fraction of the DCT coefficients is selected for the encryption to reduce the computational burden[16,17]. REVA can resist against known plaintext attack, but is vulnerable to perceptual attack reported by Wu, Kuo(2005), therefore not suitable for perceptual encryption[18].

Recently Li S et. al(2007), proposed a perceptual MPEG-video encryption algorithm called PEVA, based on VEA rather than REVA. PEVA selectively encrypts fixed length code(FLC) words in video bit stream under three control factors: intra DC coefficients, sign bits of non intra DC coefficients and AC coefficients and third sign bits and residuals of motion vectors, to produce different levels of visual qualities: Low-resolution, Rough view, The high resolution details and The motions.[19]

In 2000, Cheng and Li initially offered partial encryption schemes for still images and further extended to the video. This Partial encryption schemes works with quadtree compression algorithms and wavelet compression algorithm based on zerotrees for the video stream I-frame, motion compensation and residual error coding. This scheme works for the video stream based on Set Partitioning In Hierarchical Trees image compression algorithm. Therefore, proposed methods are not suitable for JPEG images hence not applicable MPEG video compression standard. Proposed partial encryption encrypts the I-frames, motion vectors and residual error code of video stream.[20]

Wen et al.(2002) they generalized the ideas of selective encryption encryption into format-compliant method called format Compliant Configurable encryption. In this scheme data is grouped in to information carrying and not information carrying parts then only information carrying fields are encrypted. These information field can be fixed length code(FLC) codewords or variable length code(VLC) codewords. For format compliance bits for encryption chosen and after encrypting with DES placed back to its original bit position in video stream[21].

Zeng and Lei(2002) proposed the frequency domain scrambling algorithm. The general scheme of scrambling is based on some or all of the following three operations: Selective bit scrambling, block shuffling and block rotation. As most of the video compression uses Wavelet Transform or Discrete Cosine Transform, therefore proposed encryption is designed for these transforms.[22]

Wu and Kuo,(2000,2005) proposed two selective encryption algorithms for MPEG video, MHT(Multiple Huffman Tables)-encryption scheme and MSI(Multiple State Indices)-coder. Basic principle of this scheme is encryption during entropy coding. During entropy coding stage, symbols in video stream transformed in to binary sequences in accordance to predefined Huffman table, to integrate encryption with entropy coding. Wu and Kuo proposed adaptive entropy coder based on multiple Huffman table encryption scheme. The basic MHT encryption work as: firstly, 2^k Huffman tables generated and numbered 0 to 2^k-1 then random vector P of n numbers generated, where each number is k bit number in the range 0 to 2^k-1. For encoding of i^{th} symbol in video stream, table p is used. The basic building block of this algorithm is that it converts entropy coders into encryption ciphers[23,18]. Later in 2005, Enhanced MHT Encryption were proposed, in this a one way hash function to imitate a key hopper by first giving some seed value s is used and then producing the output values applying hash function on the seed value and further values generated from seed value like(s+1, s+2..and so on). But there are a number of cryptanalysis studies which prove that basic and enhanced MHT methods are vulnerable under chosen and known plaintext attacks[24,25]. The video encrypted with MHT scheme is completely incomprehensible, so it cannot be used for perceptual encryption. One more scheme based on encryption within entropy coding is randomized entropy coding and rotation in partitioned bit stream(REC/RPB) proposed by Xie and Kuo[26].

Pazarci and Dipcin, 2002 proposed compression independent perceptual encryption method that encrypts the video in the RGB colour space using four secret linear transformations before video compression by MPEG-2 encoder. In this scheme each frame (in RGB- format) is divided into MXN scrambling blocks, consisting of multiple macroblock of size 16X16. Four linear transformation are defined to encrypt the video pixels . It can keep the compression efficiency of the video codec[27]. But Li et all (2007) shows that the scheme is not secure enough against brute force attacks because its key space is not sufficiently large. It is also vulnerable to the known plain text attacks also[19]. One more compression independent encryption algorithm correlation-preserving video encryption was proposed by Socek et all. The basic idea of this algorithm is the design of a sorting permutation that has a correlation-preserving property. The scheme encrypts the raw video before compression by using the sorting permutation to keep the compression efficiency. The scheme is not secure enough against known-plaintext attacks. The computational complexity for the decryption is very low, but is very high for the encryption[28].

Liu and Koeing proposed Puzzle encryption algorithm for compressed video stream , based on children's game puzzle. This puzzeling algorithm works in two steps:(1) Puzzling the compressed video data of each frame and(2) Obscuring the puzzled video data. Puzzle algorithm dramatically reduce the computational cost for video encryption. It achieves a sufficiently fast encryption speed to meet the real time requirements of mostly used multimedia applications, especially for high resolution video games[29,30].

Daniel et. all(2007) proposed a novel video encryption algorithm specially designed for both lossless and lossy low motion spatial only video codecs. This algorithm works before the compression and at receiver side after decompression, a unique feature and often desirable feature. But, it works only for certain class of video sequence and codec[31]. Working principle of this scheme is based on canonical sorting permutation σ_i of frame V_i. In the approach, canonical sorting permutation σ_1 computed for V1 (first frame of video sequence($V=V_1,V_2....V_n$)) and after compression ($C(V_1)$) transmitted through secure channel without encryption. This first frame works as secret key for encryption/Decryption process. Each subsequent frames V_i encrypted by applying canonical sorting permutation $\sigma_{i-1}(V_i)$. Receiver computes sorting permutation for received frame and use it to recover next frames from encrypted frames.

The encryption algorithms which works after compression destroys the syntax structure of of the compressed video stream. Ordinary video players that have no tolerance to the syntax errors would crash when directly playing encrypted video stream although today robust system available which have tolerance for it. To address this weakness, Wen et all proposed the format –compliant configurable encryption framework for the access conrol to video stream. The basic fundamental behind this algorithm is that the syntax of the video stream is left unencrypted, while the the information carrying fields, such as fixed-length code(FLC) or variable-length codeword(VLC) are selectively encrypted according to the security requirement[21].They claims that the security level of the scheme is sufficient for entertainment applications because the encrypted parts cannot be recovered in the reconstructed video by attackers. The scheme is well suited for perceptual encryption due to its format compliance. However this scheme requires fairly deep parsing in to bitstream to identify the parts of bit stream to identify the parts of bit streams to be encrypted. This incurs a significant processing overhead. Zhu et all, states that the naïve algorithm is much faster than this scheme. Compression efficiency is also decreased in this scheme[32].

Bergeron and Lamy-Bergot(2005) proposed a syntax compliant encryption algorithm for H.264/AVC. Encryption inserted within the encoder. In this scheme encryption takes place after entropy coding on selected bits.To achieve syntax compliance selected compliant codewords are randomly permuted with other codewords[33]

Grangetto, Magli, Olmo(2006), proposed encryption in compression based on randomization of the arithmetic coder. This is achieved by randomly swapping the most probable symbol and least probable symbol intervals. Since only the interval magnitude is important for encoding the compression efficiency remains unchanged. This may work as whole or selective encryption based on the layers or resolution levels to encrypt[34].

Siu-Kei, Au Yeung, Shuyuan Zhu, Bing Zeng proposed encryption technique during transform encoding phase. They have proposed MTT based technique in which a transform is selected from various unitary transforms based on the key and the order in which the transform is applied is kept secret. This scheme does not offer higher security as it is used only for the encryption of residual frames without encrypting I frames and motion vectors but has a low cost. It also result in low speed[35].

Narsimha Raju et. al.(2008) proposed technique based on frequently occurring patterns in the DCT coefficients of the video and they state that computational complexity of the encryption proportional to the influence of the DCT coefficient on the visual data. Further they reported that the average encryption time taken by the algorithm is 8.32 ms per frame [36].

Fuwen liu , Hartmut Koenig states that all the video encryption algorithms have a relatively low security level although they meet better the specific requirement of video encryption than the naïve algorithm except for the security strength[2].

5. DISCUSSION AND FUTURE DIRECTION

Efficient compression is critical requirement of video communication and to provide secure video communication, encryption is the widely used technique. Encryption of video streams can either occur along the compression or before the compression or after the compression. Before compression encryption is format compliance but sometimes increases the size of data. Joint compression and encryption techniques are codec dependent and further, combine compression and encryption reduces the overall processing time but generally is either less secure or computationally expensive one. Post compression techniques are inherently not format compliant. Integration of encryption algorithm on video codec make their domain limited so it is inferred that there is need to evolve codec/compression independent video encryption techniques, which work before compression at the sender side and after decompression at receiver side.

The video consumption by constrained devices and rich diversity of video services pose special requirements in the context of security and till date no single technology/technique is capable to provide a complete solution for different security needs of commonly used video services. Therefore there is need to device a complete security solution capable to address various security requirements of video services, as single solution.

Video consumption by constrained devices arise need of self adjustable & fast encryption algorithm as per receiver device resources , so that decryption may take place on consumer’s constrained device without worrying about computational resources, video codecs and data pipe, in real time.

6. REFERENCES

[1]. Thomas Eisenbarth, Christof Paar and Axel Poschmann,Sandeep Kumar,Leif Ushadel.A survey of Lightweight-Cryptography Implementations. Design and test of ICs for Secure Embedded Computing(IEEE Design & Test of Computers)(2007)

[2]. Fuwen Liu, Hartmut Koenig. A survey of video encryption algorithms. Computer & Security 29(2010) ;3-15;

[3]. A.M. Eskicioglu and E.J. Delp. An overview of multimedia content protection in consumer electronics devices. Proceedings of SPIE Vol. 3971; Security and Water Marking of Multimedia contents II, 246-263, San Jose, California, Jan. 24-26,2000

[4]. A. Uhl and a. Pommer. Image and video encryption: from digital rights management to secured personal communication, Advances in Information Security, vol 15, Boston, USA: Springer Science+ business Media, Inc., 2005.

[5]. C.P. Wu and C. C. j. Kuo. Design of integrated multimedia compression and encryption systems. IEEE transaction on multimedia(7)(5):828-839; October 2005

[6]. Eugene T. Lin, Gregory W. Cook, Paul Salama and Edward J. Delp, “An over view of Security Issues in Streaming Video”, work supported by grant CERIAS,2001, IEEE Xplore

[7]. C.P. Wu and C. C.,j. Kuo, “Efficient multimedia encryption via entopy codec design, in: proceedings of SPIE Security and Watermarking of multimedia Content III, Volume 4314, San Jose, CA, January 2001.

[8]. MeyerJ, Gadegast F. Security mechanism for multimedia data with the example MPEG-1 video, project description of SECMPEG. Technical University of Berlin;1995.

[9]. T.B. Maples, G.A. Spanos . Performance study of a selective encryption scheme for the security of networked real time video. In: Proceedings of the 4th international Conference on computer and communication, Las Vegas,NV;1995.

[10]. L. Agi, L.Gong, An empirical study of MPEG video transmission, in:Proceedings of the Internet Society Symposium on Network and Distributed system security, san Diego, CA, 1996,137-144 .

[11]. Choon, L.S. Lightweight and cost-effective MPEG video encryption. International Conference on Information and Communication Technologies: From Theory to Application 2004:525-526

[12]. Euijin Choo, Jehyun Lee, Heeio Lee, Giwon Nam, “SRMT: A Lightweight Encryption Scheme for Secure Real-time Multimedia Transmission, International Conference on Multimedia and Ubiquitous Engineering (MUE’07), 2007.

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

[14]. L. Tang. Methods for encrypting and decrypting MPEG video data efficiently. In: proceedings of the ACM International Multimedia Conference, Boston,MA,1996

[15]. A.M. Alattar,G.I. Al-Regib,S.A. Al-Semari, Improved selective encryption techniques for secure transmission on MPEg video bitstreams, in:Proceedings of the international Conference on Image Processing(ICIP’99)

[16]. C.Shi,S.Y. Wang,B. Bhargava,” MPEG video encryption in real time using secret key cryptograpgy,” in : proceedings of the international conference on parallel and distributed processing techniques and applications(PDPTA99), Las Vegas, Nevada,USA,99

[17]. B. Bhargava , C.Shi, S.Y. Wang, “ MPEG Video Encryption algorithms”, Multimedia tools and applications 24(1)(2004),57-79

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

[19]. Li S, Chen G, Cheung A, Bargava B, Lo KT. On the design of perceptual MPEG-video encryption algorithms. IEEE transactions on Circuits and Systems for video technology 2007;17(2):214-23

[20]. H. Cheng, X. Li. Partial encryption of compressed images and video. IEEE Transaction on Signal Processing,48(8):2439-2451;2000

[21]. Wen J. Severa M, Zeng W, Luttrell MH,Jin W. A format-compliant configurable encryption framework for access control of video. IEEE Transaction on Circuits and Systems for Video Technology (12)(6):545-57;June 2002

[22]. W. Zeng ,S.Lei. efficient frequency domain selective scrambling of digital video. IEEE transaction on Multimedia(5)(1):118-219;March 2002

[23]. Eisenbarth, T. A survey of lightweight cryptography implementation. IEEE Design and Test of Computers,2007(24)(6):522-533.

[24]. Z. Zhou,Z. Liang, Y. Chen, O.C.Au., Security analysis of Multimedia encryption schemes based on Multiple Hauffman table, IEEE Signal processing letters 14(3)(2007);

[25]. G. Jakimoski, K.P. Subbalakshmi, Cryptanalysis of some multimedia encryption schemes, IEEE transactions on multimedia 10(3)(2008)

[26]. Xie D, Kuo C-Cj Multimedia encryption with joint randomized entropy coding and rotation in partitioned bitstream. EURASIP journal on information Security,January 2007(6)(1):118-29

[27]. Pazarci M, Dipcin V, A MPEG-2 transparent scrambling technique, IEEE transaction on Consumer Electronics 2002,48(2):345-55

[28]. Socek D, Magliveras S, Culibrk D, Marques O, Kalva H, Furt B. Digital video encryption algorithms based on corealation preserving permutations. EURASIP journal on Information Security January 2007;2007(1)

[29]. Liu F, Koenig H. Anovel video encryption algorithm for high resolution video.Stevenson,WA,USA. In: Proceeding of ACM NOSSDAV’05. New York:ACM Press;June 2005;69-74

[30]. Liu F, Koenig H.Puzzel- a novel video encryption algorithm. IFIPCMS 2005 LNCS 3677. Salzburg,Austeria:Springer; Set. 2005;88-97

[31]. Daniel Socek, Hari Kalra, Spyros S., Mogliveras, Oge Marques, Dubravko C., Borko F. New approach to encryption and staganography for digital video. Multimedia Systems,Springer-Verlog,2007

[32]. Zhu BB,Yuan C, Wang Y, Li S. Scalable protection for MPEG-4 fine granularity scalability. IEEE transaction on Multimedia 2005;7(2):222-33

[33]. C. Bergeron, C. Lamy Bergot, compliant selective encryption for H.264/AVC video streams, in:proceeding of 7th IEEE workshop on multimedia Signal processing, Shanghai, China, October 2005:1-4

[34]. M. Grangetto, E. Magli, G.Olmo, Multmedia selective encryption bi means of randomized airthmatic coding. IEEE transaction on multimedia(8)(5):905-907,2006

[35]. Siu-Kei, Au Yeung, Shuyuan Zhu, Bing Zeng. Partial video encryption based on alternating transform. IEEE Signal Processing Letters(6)(10):893-896; October 2009

[36]. C. Narsimha Raju, Ganugula, Umadevi, Kannan Srinathan, C.V. Jawaha, “Fast and Secure Real-Time Video Encryption”.in: Sixth Indian Conference on Computer Vision, Graphics & Image Processing 2008:257-264