International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

An Uncompressed AVI Encryption Based on Haar Wavelet Decomposition of Frames and Audio

Minal C.Toley[1], Mayur S.Burange[2]

[1]Master of Engineering Scholar, Computer Science and Engineering Department, P.R.Pote College of Engg. and Management Amravati, Maharashtra, India
minaltoleypaper@gmail.com

[2]Assistant Professor, Computer Science and Engineering Department,
P.R.Pote College of Engg. and Management ,Amravati, Maharashtra, India
mayurmsb123@gmail.com

Abstract: ***The privacy and security becomes the major issues since the multimedia is transmitted openly over the network. Along with the privacy and security, storage space is also an important point that can't be missed. So it is necessary to provide the privacy and security to the multimedia with help of encryption. This work presents design and implement of an efficient video encryption of uncompressed AVI system, where lossy compression is considered. The AVI (Audio Video Interleaved) file which is uncompressed divided into frames and audio which will be encrypted. Here a new modified International Haar Wavelet is used to encrypt the full video in an efficient secure manner, after encryption the frame and audio will be decomposes and deliver final uncompressed video. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security and efficiency.***

Keywords: Encryption, AVI, Haar wavelet, uncompressed video**.**

1. Introduction

The high growth in the networking technology leads a common culture for interchanging of the digital video very drastically. Hence it is more vulnerable of duplicating of digital video and re-distributed by hackers. Therefore the videos has to be protected while transmitting it, Sensitive information like credit cards, banking transactions and social security numbers need to be protected. For this many encryption techniques are existing which are used to avoid the information theft. In recent days of Internet, the encryption of data plays a major role in securing the data in online transmission focuses mainly on its security across the internet. Different encryption techniques are used to protect the confidential data from unauthorized use [1][2]. With the rapid development of multimedia and network technologies, the security of multimedia becomes more and more important, since multimedia data are transmitted over open networks more and more frequently. Typically, reliable security is necessary to content protection of digital images and videos. Encryption schemes for multimedia data need to be specifically designed to protect multimedia content and fulfill the security requirements for a particular multimedia application. For example, real-time encryption of an entire video stream using classical ciphers requires heavy computation due to the large amounts of data involved, but many multimedia applications require security on a much lower level, this can be achieved using selective encryption that leaves some perceptual information after encryption.

Government, military and private business amass great deal of confidential videos about their patient (in Hospitals), geographical areas (in research), enemy positions (in defence) product, financial-status [3][4].

Most of this information is now collected and stored on electronic computers and transmitted across network to other computer, if these confidential videos about enemy positions ,patient ,and geographical areas fall into the wrong hands, than such a breach of security could lead to lots of war , wrong treatment etc. Protecting confidential video is an ethical and legal requirement [6][7]. We store information in computer system in the form of files. File is considered as a basic entity for keeping the information. Therefore the problem of securing image data or information on computer system can be defined as the problem of securing file data. It is worldwide accepted fact that securing file data is very important, in today's computing environment. Good encryption makes a source look completely random, traditional algorithms are unable to uncompress encrypted data. For this reason, traditional systems make sure to encrypt. We are using the concept of Haar Wavelet Decomposition encryption, for the encryption and decryption of video.

2. Literature Survey

In 2006, *Alexander Wong and William Bishop* has introduces the video encryption algorithm. The theory behind partial video encryption is reviewed and a multi-key video encryption technique for parallel hardware implementation. Encryption algorithm is provided. The parallel architecture for the algorithm and a discussion of the security implications are presented. Video compression algorithms attempt to pack information into as little space as possible. This characteristic can be exploited to reduce the amount of video data that needs to be encrypted while maintaining an acceptable level of security.

Shujun Li, Guanrong Chen [7] has proposed, some existing perceptual encryption algorithms of MPEG videos are reviewed and some problems, especially security defects of two recently proposed MPEG video perceptual encryption schemes, are pointed out in 2007. Then, a simpler and more effective design is suggested, which selectively encrypts fixed-length codeword's (FLC) in MPEG-video bit streams under the control of three perceptibility factors. The proposed design is actually an encryption configuration that can work with any stream cipher or block cipher.

In 2007, *Narsimha Raju C, UmaDevi Ganugula, Kannan Srinathan, C. V. Jawahar has* proposed a secure and computationally feasible video encryption algorithm based on the principle of Secret Sharing. The strength of the DC is distributed among the AC values based on *Shamir's Secret Sharing (SSS) scheme*. The proposed algorithm guarantees security, fastness and error tolerance with a small increase in video size.

In 2008, *Shuguo Yang, Shenghe Sun* [9] has proposed a new and secure video encryption method based on chaotic maps in DCT domain, which is quite in keeping with the common ideas and the frequent practices of video encryption. The I - frames of the video sequence as encryption objects. First, introduce two coupling chaotic maps to scramble the DCT coefficients of every original I-frame, and receive the scrambled I-frame. Second, encrypt the DCT coefficients of the scrambled I-frame using another chaotic map. In the whole process, three chaotic maps and five keys; the I-frame is encrypted twice.

In 2008, *C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar* [10] proposed a computationally efficient and secure video encryption algorithm. It uses RC5 for encryption of the DCT coefficients. This makes secure video encryption feasible for real-time applications without any extra dedicated hardware. Here achieve a 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. On an average, our algorithm takes only 8.32ms of encryption time per frame.

In 2009, *Chunhua Li, Chun Yuan, Yuzhuo Zhong* [11] has proposed a layered selective encryption scheme for Scalable Video Coding (SVC). The main feature of this scheme is making use of the characteristics of SVC. This method fully meets the encryption requirements of SVC and the encryption procedures are carried out at the Network Abstractor Layer (NAL) level. Based on the different structure and importance of base tier and enhancement tiers, different domains are encrypted. For base tier, Intra-Prediction mode (IPM) and residual sign are selected. For enhancement tiers, temporal scalability and spatial/SNR scalability are distinguished. Furthermore, key generation and distribution schemes are presented. Stream cipher—Leak EXtraction (LEX) algorithm is adopted to reduce computational cost. Experiments were performed to verify the proposed method using the joint scalable video model (JSVM**).**

In 2009, *Siu-Kei Au Yeung, Shuyuan Zhu, and Bing Zeng* [8] has proposed a novel video encryption technique that is used to achieve *partial* encryption where an annoying video can still be reconstructed even without the security key. In contrast to where the encryption usually takes place at the entropy-coding stage or the bit-stream level, here proposed scheme embeds the encryption at the *transform* stage during the encoding process. Here, develop a number of new unitary transforms that are demonstrated to be equally efficient as the well-known DCT and thus used as alternates to DCT during the encoding process. Partial encryption is achieved through alternately applying these transforms to individual blocks according to a pre-designed secret key.

In 2010, *Qinchun Qian, Zengqiang Chen and Zhuzhi Yuan,* [13] has proposed schemes out multiple chaotic systems which deal with both video streams being compressed and compressed video streams. The so-called multiple chaotic system actually consists of three chaotic or hyper chaotic maps, namely Logistics Map, 2-D Baker Map and a 4-D hyper chaotic 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.

In 2012, *Mayank Arya Chandra, Ravindra Purwar, Navin Rajpal* [14] has proposed new novel scheme for digital video encryption. A method to generate an encrypted video by encrypted Video-frame. Based on novel secure video scheme, an effective and generalized scheme of video encryption. It is a matrix computation scheme which uses a concept of Video-frame and xor operation.

In 2013, *S.Rajagopal, M.Shenbagavalli* [15] has 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. By rotating the phase angle in the DCT based transformation stage of the input residual video frame, a new class of unitary transforms can be generated. Different rotation angle can be choosen 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.

In 2014, *N. Geetha, K. Mahesh,* has proposed a method for encryption in video is taken place by using the AES Rijndael encryption algorithm. Instead of using the text or the images, the video encoding is taken place here. The video is converted into number of frames, which in turn converted to blocks used for encryption. The division of video resulted in images in turn this image is followed by encryption. The block cipher algorithm is used for converting frames to blocks. The Rijndael algorithm is used, because of its simplicity, efficient working syntax. Since, Rijndael algorithm is specified substitution ciphers were used to encrypt the given frames.

In 2014, *A. Kaja Moideen, K. R. Siva Bharathi* has proposed the concept of separable reversible data hiding technique that is related with internet security. When it is desired to send the confidential/important/secure data over an insecure and bandwidth-constrained channel it is customary to encrypt the cover data and then embed the confidential/important/ secure data into that cover data. With an encrypted image/video containing additional data, if a receiver has the data-hiding key alone, he can extract the additional data but the image/video content is unknown to him. If the receiver has the encryption key, he can decrypt to obtain only an image/video similar to the original one, but the additional data cannot be obtained. If the receiver has both the data hiding key and the encryption key, he can extract both the additional data and recover the original image/video without any error by exploiting the spatial correlation in natural image.

3. Classification of Video Encryptions

a) Fully layered Encryption
In this case the complete content of video is first compressed and then encryption is done with the use of standard algorithms like DES, RSA, AES, etc. This encryption technique is not appropriate in real time video applications because of heavy computation and slow speed.

b) Permutation based Encryption
The different permutation algorithms are used to scramble or encrypt the content of video. The scrambling of each and every byte is not necessary. Some algorithms use permutation list as secret key to encrypt video contents.

c) Selective Encryption
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. Selective encryption is faster as compared to the full encryption of the data [7].

d) Perceptual Encryption
The requirement of the perceptual encryption is that quality of aural/visual data is only degraded by encryption to some extent i.e., the encrypted multimedia data are still partially perceptible after encryption. The quality degradation of aural/visual can be continuously controlled by a factor *p*.

4. Proposed Methodology

In this method, with the help of algorithm the video will be encrypted and decrypted as well. The video is combination of the frames and audio. So here the frame and audio both are encrypted and decrypted separately with help of algorithm. In multimedia, video contains more information than other media, so efficient video compression methods are vital. Existing international video coding standards were created as a result of collaboration between two standardization organizations. Most of the time in the multimedia only the image was encrypted and decrypted as they have to send some sensitive message from one to another. But now a days when sometimes it's very needy to send very confidential video from one to other so, it is very necessary to encrypt and decrypt video with particular method.

Proposed methodology has been divided into 6 phases.
Proposed methodology has been divided into 6 phases.
1) Video Encryption
2) Video Decryption
3) Frame Encryption
4) Frame Decryption
5) Audio Encryption
6) Audio Decryption

Module1: Video Encryption
In this phase, video will be encrypted**.** In the first step an input as uncompressed Audio video Interleaved will be selected. The selected video is split up in to Frames and Video. After splitting the video we get the extracted Frames and Extracted Audio. The extracted frames will be decomposed with help of Haar Wavelet. The key will generated with the help of key generater.After that the visual image cryptography, the decomposed frames will get encrypted. At the same time, at another side the the key is generated for extracted audio with help of key generater.With this the audio will encrypted. Finally with the help of Video Encoder we get the encrypted video**.**

Module2: Video Decryption
Video decryption is the exactly reverse process of that video encryption. In this phase, video will be decrypted**.** In the first step an input as uncompressed Audio video Interleaved will be selected. The selected video is split up in to Frames and Video. After splitting the video we get the extracted Frames and Extracted Audio. The extracted frames will be decomposed with help of Haar Wavelet. The key will generate with the help of key generater.After that the visual image cryptography, the decomposed frames will get decrypted. At the same time, at another side the the key is generated for extracted audio with help of key generater.With this the audio will decrypted. Finally with the help of Video Encoder we get the decrypted video.

Module3: Frame Encryption
In this phase, the video which is divided in to frame and audio. Here first of all the frame will be encrypted with Haar Wavelet.

Module4: Frame Decryption
When the frames get encrypted in that same manner we to decrypt the frame to get the original video with the help of Haar Wavelet.

Module5: Audio Encryption
With help of Haar Wavelet as the video is distributed into frames and audio, so the audio encryption is takes place.

Module5: Audio Decryption
After encryption of the audio to get the original audio, have to decrypt the audio.

5. Conclusion and Future Scope

Although only some of the main video encryption techniques were discussed here, one can see that there exists a large selection of approaches to video encryption in digital media.

All the major video file formats have different methods of video encryption, with different strong and weak points respectively. Where some above technique lacks in the *robustness, High security, Speed*. So, our future study and research includes developing the video encryption methods with high embedding capacity & robustness. This above information might be useful to carry out further work in this research area.

References

[1] Gary J. Sullivan, *Fellow, IEEE*, Jill M. Boyce, *Senior Member, IEEE*, YingChen, *Senior Member, IEEE*, Jens-Rainer Ohm, *Member, IEEE*, C. Andrew Segall, *Member, IEEE*, and Anthony Vetro, *Fellow, IEEE* "Standardized Extensions of High Efficiency Video Coding (HEVC)" *IEEE* journal of selected topics in signal processing, vol. 7, no. 6, december 2013

[2] 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

[3] Shujun Li, Guanrong Chen, *Fellow, IEEE*, Albert Cheung, *Member, IEEE*, Bharat Bhargava, *Fellow, IEEE* and Kwok-Tung Lo, *Member, IEEE* "On the Design of Perceptual MPEG-Video Encryption Algorithms" *IEEE* Transactions On Circuits And Systems For Video Technology, Vol. 17, No. 2, Pages 214-223, February 2007

[4] Saurabh Sharma, Pushpendra Kumar Pateriya, Lakshmi "A Study Based on the Video Encryption Technique" *International Journal of P2P Network Trends and Technology- Volume3Issue1- 2013*

[5] Ajay Kulkarni, Saurabh Kulkarni, Ketki Haridas, 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, March 2013*

[6] Niraj Kumar, Prof. Sanjay Agrawal "Issues and Challenges in Symmetric Key based Cryptographic Algorithm for Videos and Images" International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 5, May 2013

[7] Shujun Li, Guanrong Chen, *Fellow, IEEE*, Albert Cheung, *Member, IEEE*, Bharat Bhargava, *Fellow, IEEE* and Kwok-Tung Lo, *Member, IEEE"* On the Design of Perceptual MPEG-Video Encryption Algorithms" IEEE transactions on circuits and systems for video technology, vol. 17, no. 2, pages 214-223, february 2007

[8] L. S. Choon, A. Samsudin, and R. Budiarto, "Lightweight and cost-effective MPEG video encryption," in *Proc. of Information and Communication Technologies: From Theory to Applications*, 2004.

[9] Shuguo Yang , Shenghe Sun " A video encryption method based on chaotic maps in DCT domain"Science Direct,2008.

[10] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar International Institute of Information Technology, Hyderabad, India-500032." Fast and Secure Real-Time Video Encryption" Sixth Indian Conference on Computer Vision, Graphics & Image Processing, 2008.

[11] Chunhua Li, Chun Yuan, Yuzhuo Zhong" Layered Encryption for Scalable Video Coding" IEEE Region 10 Conference, pp. 1-4, 2009.

[12] Y.G. Won, S.H. Jin, T.M. Bae and Y.M. Ro, "A Selective Video Encryption for the Region of Interest in Scalable Video Coding," IEEE Region 10 Conference, pp. 1-4, 2007.

[13] 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, January 2010.

[14] *Mayank, Arya Chandra, Ravindra Purwar, Navin Rajpal"* A Novel Approach of Digital Video Encryption*" International Journal of Computer Applications (0975 – 8887) Volume 49– No.4, July 2012*

[15] *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) ISSN (Online) 2319-183X, (Print)* 2319-1821 *Volume 2, Issue 6 (June 2013), PP. 54-58.*

[16] *N. Geetha, K. Mahesh*]" A Secure Video Encryption Technique Using Rijndael Algorithm" International Journal of Science and Research (IJSR) Volume 3 Issue 5, May 2014

[17] A. Kaja Moideen1, K. R. Siva Bharathi2" A Novel Method for Data Hiding In Encrypted Image And Video" International Journal of Emerging Technology and Advanced Engineering Volume 4, Issue 2, February 2014.

Author Profile

Ms. Minal C. Toley is a scholar of ME, (Computer Science Engineering), at P .R .Pote COE&M, Amravati, under SGBAU, Maharashtra India.

Prof. Mayur S. Burange is Asst Professor at P.R.Pote College of Engg. & Management Amravati. He did his M.E from Prof. Ram Meghe Institute of Technology & Research, Badnera.