ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

A Method for Information Hiding in Encrypted Video Streams

Dhanya M, Supriya L. P

Post Graduate Student, Dept. of CSE, Sree Buddha College of Engineering for Women, Elavumthitta, Athanamthitta, Kerala, India

Assistant Professor, Dept. of CSE, Sree Buddha College of Engineering for Women, Elavumthitta, Pathanamthitta, Kerala, India

ABSTRACT: With high development of computer technology and internet technology, multimedia service has become a new area in internet services today. It has problems like huge amount of data, high speed play, bandwidth limitations etc. Enhancing its security and speed has become an assurance of the video service. With the increase in the development of multimedia technologies, the multimedia data are transmitted in the various fields like commercial, medical and military fields, which generally include some sensitive data. Protecting the video information by encrypting selective data is the crucial element. There are lots of encryption algorithms proposed for the video transmission. Information hiding refers to the process of inserting information into a host to serve specific purposes. Information hiding in encrypted video streams is a new method for data protection during transmission. It can transmit encrypted secret information which is embedded in an encrypted video stream. Video and information are encrypted by using RC4 symmetric encryption algorithm. This method consists of three phases i.e., video encryption, information hiding and video and/or information extraction. At the receiver side, the user can extract only information or extract only video or extract both video and information.

KEYWORDS: Exp-Golomb coding, information hiding, RC4 encryption, information embedding, prediction modes.

I. INTRODUCTION

Multimedia services are more prominent in day to day lives. More and more people use mobile handheld devices for transferring sensitive information and also to perform commercial transactions. Multimedia information such as graphics, images, audio and video have been widely used in the portal mobile devices. Security in video conference, video surveillance, pay-TV, etc., becomes a challenging task in video communication especially for wireless mobile device. So an efficient encryption algorithm for multimedia data will become increasingly important. Video compression (or video coding) is an essential technology for applications such as digital television, DVD-Video, mobile TV, video conferencing and internet video streaming. Standardising video compression makes it possible for products from different manufacturers (e.g. encoders, decoders and storage media) to inter-operate. H.264 is an industry standard for video compression, the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. An encoder converts video into a compressed format and a decoder converts compressed video back into an uncompressed format.

There are two types of video compression which are lossless and lossy compression. Lossless video compression, as its name suggests, is the compression that no video data is lost. The original video and the corresponding decompressed video are exactly the same. Compressed data exactly denotes the original video within a smaller space; therefore offers the best quality image possible. The disadvantage of lossless compression is the larger data size compared to lossy compression. In lossy compression, a video is compressed with data loss. Generally, the lost data are the unimportant or unperceivable parts of the image. Due to this flexibility, lossy compression offers higher compression ratio in exchange of video quality. The lossy compression is optimized according the perception capabilities of human eyes. When the multimedia industry is investigated, it is seen that lossy video compression is much more widely used than lossless

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

video compression. Lossy video compression is very common on internet and other multimedia areas; however, lossless video compression is limited to the video editing and biomedical area where data loss in unacceptable [1].
Information sent or transmitted over the public networks must have reliable protection. The protection for video streaming can be achieved by using cryptography. Cryptography can protect video streaming in different ways. The video is subjected to encryption and decryption so that it can be read only by authorized receivers. The use of cryptography also ensures that the video reaches its destination without change (not tempered with). It verifies the identity of the communicating parties, and ensures that none of them can deny that he/she has sent or received a specific video (non-repudiation). In order to overcome the problem of processing overhead and to meet the security requirements for real-time video applications with high quality video compression, several encryption algorithms to secure video streaming have been proposed. Most of these algorithms attempt to optimize the encryption process with respect to the encryption speed, and the display process [2]. Video Security (Encryption) has been a serious issue for real time or on demand video services especially in this modern era of high bandwidth data connectivity and Ubiquitous devices with high storage capacity. Video Encryption has evolved from conventional cryptographic techniques using symmetric key or asymmetric key cryptography to now a day's popular selective video encryption. All of them are more or less dependent on key sharing amongst end user and their encryption quality varies with the length of the key used. All these video encryption techniques especially selective video encryption though provide good encryption but at the same time they involve high cost of key sharing and encryption time. Contributions of this paper are: (1) To reduce the time taken for encrypting video streams, only partial frames from the frame list are taken for encryption, (2) Information can be embedded into frames selectively.

The remainder of the paper is organized as follows; section II gives the survey on various methods for data embedding and video encryption. Section III explains the implementation details of proposed method and section IV gives the results and comparisons of this method. Conclusion and future research for this proposed method is discussed in section V.

II. RELATED WORK

Data hiding in encrypted H.264/AVC video [1] is a novel scheme for data hiding. This scheme includes H.264/AVC video encryption, data embedding and data extraction. The sender encrypts the original video stream using encryption keys to produce an encrypted video stream. The data hider can embed the data to the encrypted video stream by using codeword substitution method. At the receiver side the hidden data can be extracted either in encrypted or in decrypted version. Encryption of video streams is done by encrypting the sensitive parts of the video. IPM, MVD, and Residual coefficients are the three main sensitive parts of the video. The codewords of IPMs, the codewords of MVDs and the codewords of residual coefficients are encrypted during video encryption. Intra_4X4 and Intra_16X16 coding types are chosen to encrypt. The macroblock type fields specify the other parameters about this block. This field value is encoded with Exp-Golomb code. To protect both texture information and motion information motion vectors should be encrypted. Exp-Golomb entropy coding is used to encode the MVD. To keep security residual data in frames should be encrypted. Data hiding is performed directly in encrypted bit stream. Data can be extracted either in encrypted or decrypted domain. In encrypted domain scheme, the encrypted video with hidden data is directly sent to the data extraction module. In decrypted domain scheme, encrypted video with hidden data is first pass through the decryption module and the hidden data is extracted from the decrypted video.

In the video domain, the application of information hiding (also referred to as data embedding) can be coarsely categorized as watermarking, steganography, error recovery (resilient) and general data embedding. In the case of watermarking, information is inserted into video to visibly or invisibly render the ownership information [3]. The inserted watermark information is retrieved from the content to prove ownership during a dispute, to detect any attempt in destroying the inserted watermark, or to detect act of tampering the content. On the other hand, steganography is the art and science of concealing the existence of the secret (external) information inserted into a cover such as image, video, audio, text, etc., [4]. The existence of the embedded information should be undetectable, that is, the modified content should be perceptually and statistically (with respect to certain features) similar to its original unaltered counterpart. Furthermore, information hiding is also utilized to realize error recovery (also referred to as error concealment). Here, the important components of the compressed video (e.g., motion vectors, prediction modes) are embedded into the video itself [5]. When error occurs during transmission, the important components can be extracted

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

to patch the lost or corrupted parts at reasonable perceptual quality. Lastly, general data embedding refers to the principle idea of inserting information into a host for specific purpose.

III. PROPOSED ALGORITHM

In this section, a novel scheme of information hiding in the encrypted version of video streams is presented. It consists of three parts, i.e., video encryption, data embedding and data and video extraction. The content owner encrypts the original video stream using standard stream ciphers with encryption keys to produce an encrypted video stream. Then, the data-hider can embed the additional data into the encrypted video stream, without knowing the original video content. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted version. The diagram of the proposed framework is shown in Fig. 3.1.

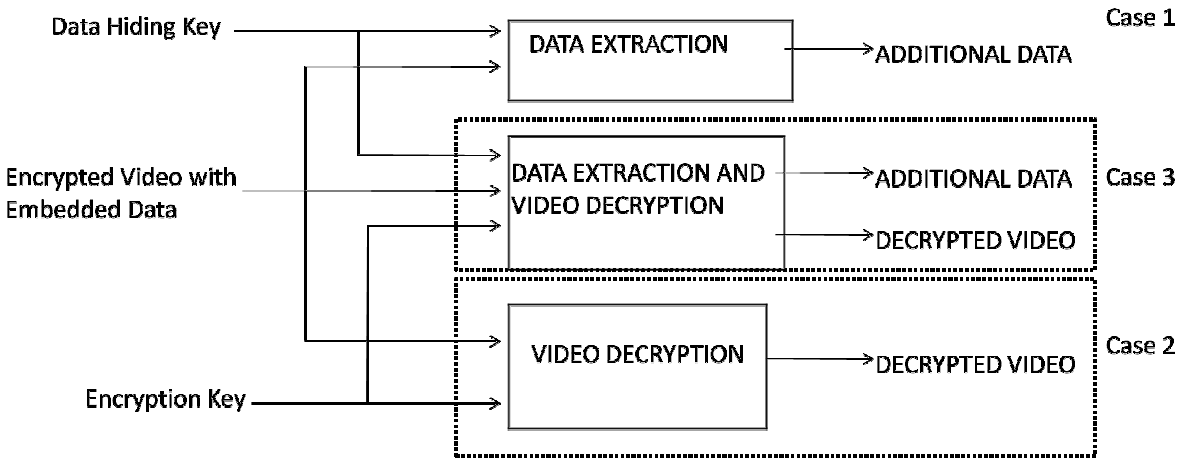

Fig. 3.1. Video encryption and data embedding

A. *Video Encryption:*

Video encryption often requires that the scheme be time efficient to meet the requirement of real time and format compliance. It is not practical to encrypt the whole compressed video bitstream like what the traditional ciphers do because of the following two constraints, i.e., format compliance and computational cost. Alternatively, only a fraction of video data is encrypted to improve the efficiency while still achieving adequate security. The key issue is then how to select the sensitive data to encrypt. Three sensitive parts (i.e., IPMs, MVDs, and residual coefficients) are encrypted with stream ciphers. For video encryption first step is to split the video into number of frames. For this purpose here using the ffmpeg tool. ffmpeg is a free software project that produces libraries and programs for handling multimedia data. ffmpeg is a command-line tool that converts audio or video formats. It can also grab and encode in real-time from various sources such as a TV card etc. ffmpeg reads from an arbitrary number of input "files", specified by the "–i" option, and writes to an arbitrary number of output "files", which are specified by a plain output filename. The created frames are listed and select one frame from this. Some information's about the selected frame can be displayed in view section. The number of frames to be created can be decided by the sender. Next step is to create the key for video encryption. For generating the IPM, MVD and residual values are used. The Exp-Golomb code for these are concatenated together and assigned as the key for encryption.

- Intra prediction mode encryption.

Mainly four types of intra coding are supported, which are denoted as Intra_4X 4, Intra_16X16, Intra_chroma, and I_PCM [6]. Here, IPMs in the Intra_4X4 and Intra_16X16 blocks are chosen to encrypt. Four intra prediction modes (IPMs) are available in the Intra_16X16. The IPM for Intra_16X16 block is specified in the mb_type (macro block type) field which also specifies other parameters about this block such as coded block pattern (CBP). Table 3.1 is the list of mb_type values with their meanings which are taken from the standard. The mb_type is encoded with the Exp-Golomb code. Specifically, there are nine prediction modes (0-8) for Intra_4X4 luminance blocks. From these modes the mode which represents least sum of average difference is taken as the prediction mode. Luma and chroma values

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

are calculated from the number of non-zero coefficients. If the number of non-zero coefficients are greater than one the luma or chroma value will be represented as one otherwise it will be zero.

Table 3.1: IPM Values and codewords

mb_type	Name of mb_type	Intra PredMode	Chroma CBP	Luma CBP	Codeword
1	IntraPred0111111	0	11	1111	010
2	IntraPred0111111	0	11	1111	011
3	IntraPred0111111	0	11	1111	00100
4	IntraPred1111111	1	11	1111	00101
5	IntraPred0111111	0	11	1111	00110

- Motion Vector Difference encryption.

Motion compensation exploits the fact that, often, for many frames of a movie, the only difference between one frame and another is the result of either the camera moving or an object in the frame moving. In reference to a video file, this means much of the information that represents one frame will be the same as the information used in the next frame. Several methods are available for calculating motion vector difference. Motion estimation block exploits the temporal redundancies through the prediction of current frames using the stored information of the past frames. The video captured is converted into frames and stored in the memory. The frame to macro block unit of motion estimation accesses each of the frame and considers frame at time instant "t" as "current frame" while at time instant "t-1" as "reference frame". One may consider a pixel belonging to the current frame, in association with its neighborhood as the candidates and then determine its best matching position in the reference frame. The difference in position between the candidates and its match in the reference frame is defined as the displacement Vector or Motion Vector. Here the exhaustive search method is used to determine the mvd values and these values are coded by using Exp-Golomb coding. In this algorithm in order to find the best matching block, it exhaustively searches all the macro blocks with in the search window to find the best match. The first frame is taken as reference frame after which few of the remaining frames are considered as current frame where current frames are compared with the reference frames to exploit the redundancy that exists between the frames. Then a macro block from current frame, considered as candidate block is taken and compared with the macro block of reference frame to determine the motion, in case of backward motion estimation while a macro block from a reference frame is considered as candidate block and compared with the macro block of current frame to determine the motion, in case of forward motion estimation. Let $X_{i,j}$ be the NxN pixel reference block located at coordinates (i, j) , $Y_{i+k,j+1}$ be the NxN pixel candidate block at coordinates (i+k,j+1) and p be the maximum displacement. The search area is therefore, of the size (n+2p)2. The current frame (t) is divided into overlapping reference blocks. Each reference block in frame (t) is compared with the candidate blocks with in a search area in the previous frame (t-1) in order to obtain the best match. Table 3.2 represents the mvd values and their codeword.

Table 3.2: MVD Values and codeword

Frame Number	X Coordinate	Y Coordinate	MVD Value	Codeword
1	2	1	2	011
2	2	1	2	011
3	2	1	2	011

- Residual Data encryption.

The dc coefficient leftover bits are taken as the residual data values and these values are coded using Exp-Golomb coding. Table 3.3 represents the codeword for residual values.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

Table 3.3: Residual data codeword

Number	Residual Bits	Residual Data	Codeword
1	0	0	01
2	0	0	01
3	0	0	01
4	0	0	01
5	11	11	00100

B. *Data Embedding:*
After encrypting the video streams the encrypted data or message is embedded in this. The message to be sent is encrypted using RC4 encryption method. This encrypted message is embedded in the encrypted video frames and these frames are merged to form the video streams. The message is embedded in a particular location agreed upon by both the sender and receiver.

C. *Data Extraction:*
At the receiver side, only data can be extracted by using the key for data encryption or only video can be extracted by using the key for video encryption or both video and data can be extracted by using both keys. In the first case, the receiver can only view the data.

IV. SIMULATION RESULTS

During video encryption, the selected video is divided into number of frames. Two cases are proposed for frame encryption. First case is to encrypt all the frames from the frame list and data embed into it and then send. Second case is to encrypt only the selected frames. Here the frames are selected with small size. These selected frames are then encrypted and data embed into it for sending. Fig4.1 shows the time difference for both cases for same videos. In each trial it is clear that selected frame encryption is less time consuming than whole Frame encryption.

During data embedding, data can be placed in all the frames or it can be placed in selected frames only. Here the first case represents the data embedding in all the frames from the frame list. Time taken for this process is stored. Second case is to embed the messages in selected frames. Here the frames are selected with small size. Time taken for this process is also taken. From these experiments it is to be proven that selected frame data embedding takes less time than all frame encryption. Fig 4.2 shows the time taken for both cases.

Table 4.1 PSNR for video

Number	PSNR Value	Total PSNR Value
0	10.68974129440...	10.68974129440...
1	10.67586067812...	21.36560197252...
2	10.66348637558...	32.02908834811...
	PSNR for Video	10.67636278270...

Table 4.1 shows the PSNR value for the video. PSNR value for a video means the average of PSNR value for the individual frames from the video. Here also there are a set of frames. PSNR value for each frame is calculated by using the equation. PSNR is defined as 10*log10 of the ratio of the peak signal energy to the MSE observed between the processed video signal and the original video signal. So PSNR can be easily defined via the mean squared error (MSE). MSE can be defined as:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

The PSNR is defined as:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

$$PSNR = 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) = 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE)$$

Here MAX_I is the maximum possible pixel value of the image. For 8 bits per sample this is 255. For colour images with three RGB values per pixel, MSE is the sum over all squared value differences divided by image size and by three. Typical values for the PSNR in lossy image and video compression are between 30 and 50 db, where higher is better.

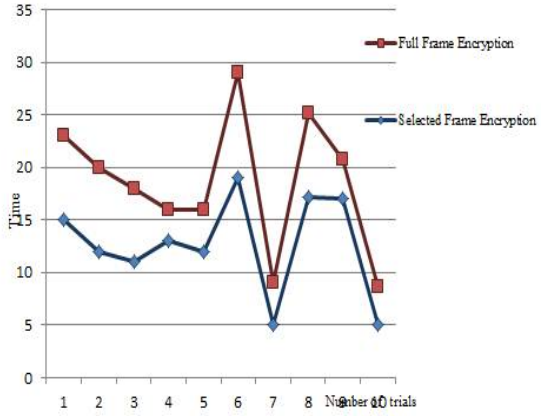

Fig. 4.1. Comparison of Selected and Full frame encryption from frames list

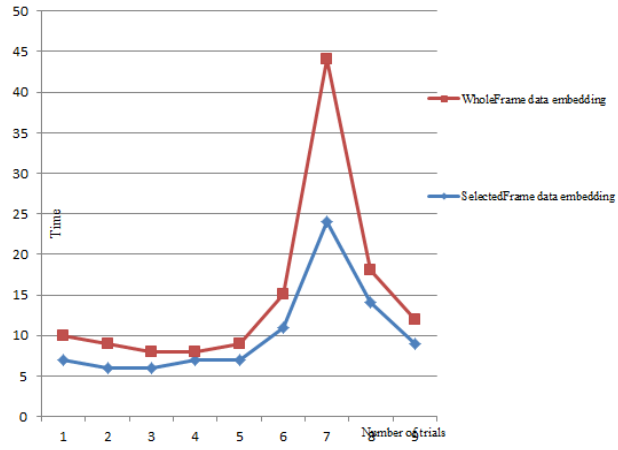

Fig 4.2 Comparison for data embedding.

V. Conclusion and Future Work

Information hiding in encrypted video streams is a method for protecting data during transmission. In this method the sender can transmit his secret data by encrypting it and embedding it into the encrypted video streams. The IPM, MVD, and residual values are used for video encryption. At the receiver side, receiver can extract the data and video. If the receiver knows the key for data he can only view the data. Similarly if he has the key for video, he can only view the video. If both key are known he can extract both. From the experimental results it is clear that selected frame encryption and selected for data embedding is best for processing. In future, best selection methods for frames improve the performance more.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 1, January 2016

REFERENCES

1. Dawen Xu, Rangding Wang, and Yun Q Shi Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution, "IEEE Transaction On Information Forensics And Security", 2014.
2. Dinesh Goyal, and Naveen Hemrajani, Novel Selective Video Encryption for H.264 Video, "International Journal of Information Security Science", 2007.
3. T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, Overview of the H.264/AVC Video Coding Standard, "IEEE Trans. Circuits Syst. Video Technol", 2003.
4. Khan, S.Malik, Ali, R. Chamlawi, M. Hussain, M. T. Mahmood, and I. Usman, Intelligent Reversible Watermarking and Authentication: Hiding Depth map Information for 3D Cameras, "Inform. Sci.", 2012.
5. A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, Digital Image Steganography: Survey and Analysis of Current Methods, "Signal Process", 2010.
6. Shiguo Lian, Dimitris Kanellopoulos, and Giancarlo Ruffo, Recent Advances in Multimedia Information System Security, "International Journal of Computing and Informatics", 2009.

BIOGRAPHY

Dhanya M is a Post Graduate student in Department of Computer Science & Engineering, Sree Buddha College of Engineering for Women, Mahatma Gandhi University. She received Bachelor of Technology (B.Tech) degree in 2009 from Calicut University. Her research interests are networking, image processing etc.