A Survey on Data Hiding and Encryption Techniques of Videos

Jithya.J.Prakash, Hemand E.P

Abstract— **Data hiding techniques are usually used in image processing . It is used to embed a secret message into a image for ensuring privacy. Data hiding can also be applied to videos. So the confidentiality of the image, video and embedded data is maintained. Sometimes digital video needs to be processed in an encrypted format to maintain security and privacy. For the purpose of content notation and/or tampering detection it is necessary to perform data hiding in these encrypted videos. There are different techniques are present for hiding private data in videos. Several data hiding techniques in videos have been proposed and few of which have been summarized below. H.264/AVC is newest video coding standard. The data is embedded by using codeword substitution method. This method preserve the exact file size and the degradation in video quality caused by data hiding is very small.**

Index Terms—**Codeword Substitution, Data Hiding, H.264/AVC, Tampering Detection**

I. INTRODUCTION

Image Processing is the Processing of images using mathematical operations by using any form of signal processing. An image is an array, or a matrix, of square pixels arranged in columns and rows. A pixel is the smallest unit of an image. The informations like video, audio, images, and other multimedia, are being transmitted through the network. But there may occur privacy problems in the network. So data hiding techniques are usually used in image processing . Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data hiding can be done through different methods. Encryption is also an important part that provides security to confidential data. So, stegenography and cryptography are major areas which provide secure data transmission over internet. Stegenography provide more security compared to cryptography. Cryptography provide security only when the data transmitting. In the time of decryption there is no more protection left.

Cloud computing has become a popular technology, which can provide highly potent computation and huge storage solution for video data. The capability of performing data hiding is done in encrypted H.264/AVC video bitstreams[1] which would avoid the leakage of video information also can help to maintain security and privacy concerns with cloud computing.H.264/AVC video streams would avoid leakage of video content which can help address the security and privacy concerns with cloud computing.

The increasing demands of video data security and privacy protection ,data hiding in encrypted H.264/AVC videos will become popular. H.264/AVC video stream consist three parts. H.264/AVC video encryption, data embedding, and data extraction. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce an encrypted video stream. Then, the data hider (e.g., a cloud server) can embed the additional data into the encrypted video stream by using codeword substituting method, without knowing the original video content. Hidden data can be extracted in two ways at the receiver end. It can be extracted either in encrypted or in decrypted domain. H.264/AVC video encryption scheme provide security, efficiency, and format compliance. It encrypt the codeword of IPMs, the codeword of MVDs, and the codeword of residual coefficients[2] for the encryption of video. The method ensures the strict preservation of the exact file size and degradation in video quality caused by data hiding is also quite small.

II. LITERATURE SURVEY

Data hiding techniques and video encryption can be done in several ways. Some of them are summarized here.

KokSheik Wong [3] proposes a novel data hiding method in the compressed video domain that safeguards the quality of the image of the host video whereas inlaying information into it. Mquant and quantized discrete cosine transform coefficients, are the significant parts of MPEG and H.26x based compression standards and then information is embedded into a compressed video by simultaneously wielding Mquant and quantized discrete cosine transform coefficients .This is a reversible method, where the original video is obtained by omitting the embedded information. Reverse Zerorun Length (RZL) is a new data representation scheme . It is proposed to exploit the statistics of macroblock inorder to attain high embedding efficiency. Two independent solutions are proposed to suppress the bitstream size increment which is a problem caused by data embedding .An average increase of four bits in the video bitstream size is observed for every message bit embedded.

Here data hiding in compressed video domain mainly focuses on complete image quality preservation, reversibility, and efficient data representation scheme. Generally data hiding methods produce image/video of high quality but even then the image quality of the modified video is always lower than that of the original video. To solve this major drawback, novel data hiding method in the compressed video domain is proposed and it preserves the image quality. Video

Manuscript received Dec, 2015.

Jithya.J.Prakash *Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University Calicut, India*

Hemand E.P *,Department of Computer Science and Engineering, Calicut University, Calicut, India.*

ISSN: 2278 – 7798

annotation is an important applications of this method where high image quality and reversibility are greatly desired. Along with high quality video , advanced special functions for searching, playback control, and/or hyper linking with other media are provided.

Xinpeng Zhang [4] proposed a scheme which focus on reversible data hiding technique in encrypted image**.** This include the following phases. Image encryption data embedding and data extraction/image recovery. the original image is encrypted by the content owner using an encryption key, and by using a data hiding key a data hider embeds additional data into the encrypted image ,yet he does not know the original content. This is send to the receiver. It provide security to the image content. Receiver receives an encrypted image containing additional data, and may first decrypt it according to the encryption key, and then extract the embedded data and recover the original image according to the data hiding key , with the aid of spatial correlation in natural image. The data hider segments the encrypted image into a number of non overlapping blocks and each block will be used to carry one additional bit. The least significant bits are used to carry the embedded data. The receiver may segment the decrypted image into blocks and divide the pixels in each block into two sets in a same way.

In this method even someone known the encryption key and can obtain a decrypted image and also detect the presence of hidden data, it is impossible to extract the additional data. That is this activity of data extraction is not separable from the activity of content decryption

Shiguo Lian present[5] a video encryption and watermarking scheme based on H.264/AVC codec, it gives a remedy to the commutation of encryption and watermarking. This method embeds the watermark without exposing video content's confidentiality, Here the encryption and watermarking operations are commutative, there for the watermark can be extracted from the encrypted videos, and the encrypted videos can be re watermarked**.** In this scheme, whereas the amplitude of dc or ac is watermarked ,the parameters like IPM, MVD and residue coefficient's sign are encrypted. the selected parameters are encrypted partially for reducing the computational cost. Here traditional watermark embedding method is modified. So the sign encryption and amplitude watermarking independent

This method have several components. They are the compression component, it includes intra prediction, inter prediction, variable length coding (VLC), etc. the encryption component includes IPM encryption, MVD encryption and residue encryption, and the watermarking component refers to residue watermarking. The independent keys are used to control the encryption process and watermarking process. The coefficients are selected carefully according to macro block type to provide robustness and imperceptibility. This method provides a secure video transmission or distribution between sender and receiver.

Xianfeng Zhao [6] proposed a method in which it reserving room before encryption with a traditional RDH algorithm.This helps the data hider to reversibly embed data in the encrypted image. The method provides real reversibility. This make data extraction and image recovery are free from error. The existing RDH techniques do not give real reversibility. In reversible data hiding method ,the original content can be losslessly recovered after the embedded message is extracted. we can increase the rate of data to be hidden. This is useful in the way that these method recovers the image with its original quality with improved PSNR ratio. Some of the previous methods may subject to some errors in data extraction and image recovery. And also the hackers can recover the embedded data from the original image easily because data is placed in particular bit position after image encryption. But the proposed RDH technique can take the advantage of all the traditional techniques.

Here the content owner first reserves sufficient space on original image and then by using the encryption key converts the image into its encrypted form. Now, the data embedding process in encrypted images is inherently reversible for the data hider only needs to accommodate data into the spare space previous emptied out. It separates data extraction from image decryption The data extraction and image recovery are identical to that of Framework VRAE. These techniques can only achieve small payloads or generate marked image with poor quality for large payload. To separate the data extraction from image decryption, he emptied out space for data embedding by compressing encrypted images. This technique is widely used in medical imagery, military imagery and law forensics, where no distortion of the original cover is allowed.

Wei Liu[7] propose an efficient way to compress encrypted images through resolution progressive compression (RPC). which compresses an encrypted image progressively in resolution. This enables the decoder to observe a low resolution version of the image, study local statistics based on it, and use the statistics to decode the next resolution level. With the help of progressive decomposition and rate compatible punctured turbo codes, this technique provide a lossless compression method for encrypted gray image, which is achieved through Slepian Wolf coding. Resolution progressive compression, shows better coding efficiency and less computational complexity than existing techniques. At first encoder send a down sampled version of the ciphertext. The corresponding low resolution image is decoded and decrypted at the decoder and a higher resolution image is obtained by intraframe prediction. To decode the next resolution level the predicted image and the secret encryption key, is used as the side information (SI).This process is repeated until the whole image is decoded .The task of de correlating the pixels is not possible for the encoder,So by doing so it is shifted to the decoder side.

Changyong Xu [8] Presented a steganographic algorithm in MPEG compressed video stream. The main purpose of steganography is to convey data secretly by concealing the very existence of communication. Image, text, audio and video are the carrier for steganography. Steganography in video can be divided into two main classes. One is embedding data in uncompressed raw video, which is compressed later. The other, embed data directly in compressed video stream .A steganographic algorithm for compressed video is introduced here which operates directly in compressed bit stream. The problem of the first main class of Steganography is how to make the embedded message resist video compression. The research of the latter is more significant because the video basically exists in the format of compression.

ISSN: 2278 – 7798

Control information is embedded in I frame in a GOP. For the purpose of resisting video processing ,in P frames and B frames, the data are repeatedly embedded in motion vectors of macro blocks. Head information, DCT encoded data stream and motion vector data stream are mainly composed in MPEG data stream.DCT encoded data stream is produced by intra encoding to I frames, encoding P frames and B frames using motion compensation prediction technique produced motion vector data stream. Each macro block in P frames has one motion vector, whereas in B frames each has two motion vectors. All motion vectors are times of half pixel. Steganographic algorithm should be designed based on these characteristics.

Mehmet Utku Celik[9] proposed a lossless data embedding technique, which provide the exact recovery of the original host signal upon extraction of the embedded information. It is also reversible method.T his technique include a generalization of least significant bit (LSB) embedding method. The unaltered portions of the host signal utilized by a prediction based conditional entropy coder as a side information, improves the compression efficiency and lossless data embedding capacity. The lossless embedding step takes the host signal and the message data and produces a watermarked signal in which the message data is embedded. The recovery process reconstruct the original host signal with no distortion and keep the embedding distortion. Here the difference between the host and watermarked signal is minimum.

Lossless data embedding techniques employ additive spread spectrum techniques, in which the spread spectrum signal corresponding to the information payload is superimposed on the host in the embedding phase. That is here use a Type I algorithm. It's spread spectrum nature make it robust. The capacity of the scheme depends on the statistics of the host image. The scheme offers adequate capacity to typical images. The proposed algorithm perform bit plane compression and RS embedding methods, especially at moderate to high distortion regions.

Wenjun Lu[10] proposed a scheme which focus on the challenges in secure video processing. Video is different from text due to its large data volume and rich content diversity. A sequence of images possibly accompanied by audio information is generally considered as a video. The rich information contained in video and its temporal nature bring unique challenges in secure video processing This paper include video search, classification, and summarization User need to search his/her private database using video queries by keeping the query and database content secret from the server. To encrypt visual features or search indexes from images in a distance preserving fashion. It allows the server to compare the similarity between encrypted images and encrypted database without additional communication with the user. This can be effectively applied for video retrieval. Privacy preserving video classification and annotation make the better organization and presentation the private video collection for the users. Video summarization is the process of extracting a set of salient images called key frames to represent the video content.

Mark Johnson [11]proposed a novelty of reversing the order of these steps. That is it first encrypt and then compress. In traditional method the redundant data transmit over an insecure and bandwidth constrained channel, it is first compress the data and then encrypt it. The compressed source is encrypted using one of the widely available encryption technologies. At the receiver, decryption is performed first, followed by decompression. Here the compressor does not have access to the cryptographic key, so without any knowledge of the original source, it must be able to compress the encrypted data. A significant compression ratio can be achieved for both lossless and lossy compression, if compression is performed after encryption. In certain scenarios this scheme requires no more randomness in the encryption key than the conventional system where compression precedes encryption. The encrypted data can be compressed using distributed source coding principles, because the key will be available at the decoder. They showed that in some situations the encrypted data can be compressed to the same rate as the original, unencrypted data could have been compressed.

Udit Budhia[12] investigated a effective steganalysis techniques for digital video sequences. It is based on interframe collusion that exploits the temporal statistical visibility of a hidden message. Steganalysis is the process of detecting, the presence of covert data in multimedia with high probability. There are number of image steganalysis algorithms are present. Whereas applying these algorithms directly to video sequences on a frame by frame basis , it lead to suboptimality. This paper present a methods that overcome this limitation. It is done by by using redundant information in the temporal domain for detecting covert messages, which is embedded via spread spectrum steganography.

Hidden watermarks bearing low energy with high accuracy are successfully detecting by proposed steganalysis methods. this paper evaluate the importance of exploiting temporal correlations for video steganalysis and to develop a proactive steganalysis framework that applies to steganography algorithms or cover media and which exploits the actively evolving field of digital watermarking attacks. The simple linear collusion is that it has low complexity and is suitable for real time applications. The steganalytic detection rate increases with an increase in the watermark embedding strength suggesting that robustness increases the chances of detection. Employing such low embedding strengths makes steganography susceptible to active wardens .Which can easily omit the watermark and, thus, prevent covert communications without employing steganalysis.

Dawen Xu [13]proposed a method in which data hiding done directly in the encrypted version of H.264/AVC video stream. It consists of video encryption, data embedding and data extraction phases. The algorithm can preserve the bit rate exactly even after encryption and data embedding. That is the scheme can ensure both the format compliance and the strict file size preservation. It is simple to implement as it is directly performed in the compressed and encrypted domain. It does not requires partial decompression of the video stream thus making it ideal for real time video applications. It preserve the confidentiality of the content completely. Here extracting the hidden data either from the encrypted video stream or from the decrypted video stream. degradation in video quality caused by data hiding is also very small. So this technique is more efficient than other related techniques.

ISSN: 2278 – 7798

III. DATA HIDING IN ENCRYPTED H.264/AVC VIDEO STREAMS BY CODEWORD SUBSTITUTION

When a data is send from a source to destination there is a prone to lose the confidentiality of the data. There are number of data hiding mechanisms to solve this problem. The capability of performing data hiding is done in encrypted H.264/AVC video bitstreams which would avoid the leakage of video information also can help to maintain security and privacy.It avoid content notation and tampering detection. This method embed additional data in encrypted H.264/AVC bit streams,that include video encryption, data embedding and data extraction phases. data hider can embed the additional data into the encrypted video stream by using codeword substituting method, without knowing the original video content The technique can preserve the bit rate exactly even after encryption and data embedding. It is directly performed in the compressed and encrypted domain and is simple to implement It preserve the confidentiality of the content completely.This method consist of following stages.

- Encryption of H.264/AVC Video Stream
- Data Embedding
- Data Extraction

A. *Encryption of H.264/AVC Video Stream*

Here, to achieve the efficiency and security only a fraction of video data is encrypted .Due to the format compliance and computational cost it is not practical to encrypt the whole compressed video bitstream. The sensitive part are only encrypted. The spatial information (IPM and residual data) and motion information (MVD) are encrypted here. So the video file size is strictly preserved. The Intra Prediction Mode (IPM) and Motion Vector Difference (MVD) are encrypted by perform a bitwise XOR operation between the last bit of the codewords and a bit of the pseudo random sequence. The pseudo random sequence is generated using RC4 algorithm. CAVLC [14] entropy coding is used to encode the residual block.

B. *Data Embedding*

Without knowing the original video content data hider can embed the additional data into the encrypted video stream by using codeword substituting method. Code words divided into two opposite code spaces C0&C1 .Codeword assigned in C0&C1 are associated with binary values .Here first select the data to be embedded and check each bit of data with codespace .By using a data hiding key data is embed to the video.

C. *Data Extraction*

In this method, the hidden data can be extracted either in encrypted or decrypted domain. It is simple process. In Encrypted Domain Extraction , it first extract the embedded data and then decrypt video .In Decrypted domain extraction first decrypt the video and then extract the embedded data. This methods guarantees the feasibility

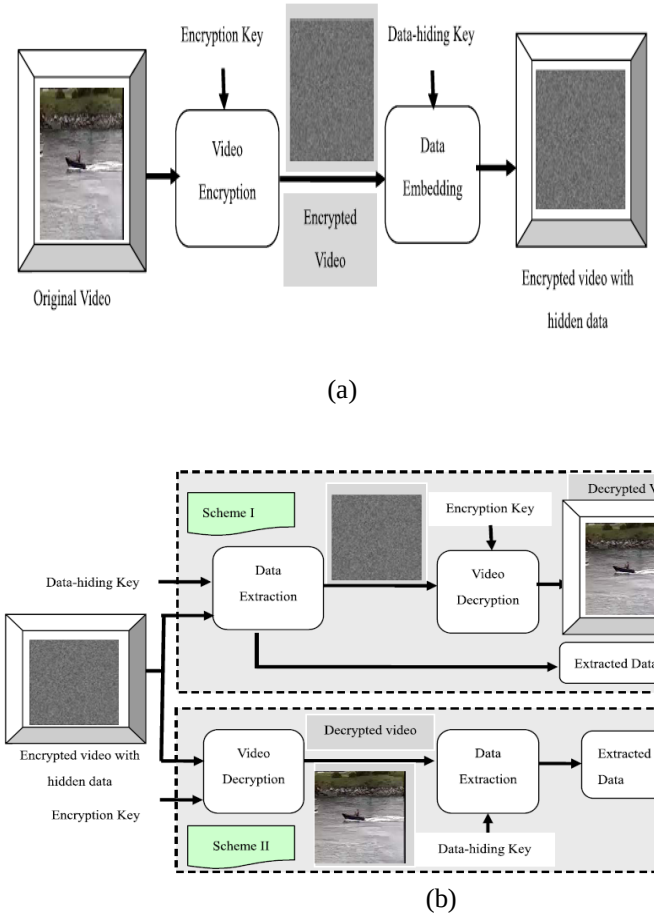

Fig 1.(a) Video encryption and data embedding at the sender end. (b) Data extraction and video display at the receiver end in two scenarios

IV. CONCLUSION

In this paper various data hiding and video encryption methods were analyzed . most of them provides low distortion. In many cases there is a chance of increasing file size when embedding a data to it. The codeword substitution method preserve the file size exactly after decryption . The degradation in video quality caused by data hiding is also quite small. Only the sensitive part are encrypted . As a future work, an error correction and detection method is proposed in the transmission channel and by using orthogonal frequency division multiplexing improve the data rate.

ACKNOWLEDGMENT

I am grateful to my project guide Prof. Hemand E.P and Head of the Department Prof. Mary Linda P.A for their remarks, suggestions and for providing all the necessary facilities like providing the Internet access and appropriate references. We are also thankful to all the staff members of the Department of Information Technology and Computer

ISSN: 2278 – 7798

Science & Engineering of KMCT College of Engineering and Technology, Calicut.

REFERENCES

[1] 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., vol. 13, no. 7, pp. 560–576, Jul. 2003.

[2] S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang, "Secure advanced video coding based on selective encryption algorithms," IEEE Trans. Consumer Electron., vol. 52, no. 2, pp. 621–629, May 2006.

[3] KokSheik Wong, Kiyoshi Tanaka, Koichi Takagi, and Yasuyuki Nakajima, "Complete Video Quality-Preserving Data Hiding, IEEE Ttanscations on circuits and system for video technology, Vol. 19, NO. 10, October 2009

[4] X. Zhang, "Reversible data hiding in encrypted images," IEEE Signal Process. Lett., vol. 18, no. 4, pp. 255258, Apr. 2011.

[5] S. G. Lian, Z. X. Liu, and Z. Ren, "Commutative encryption and watermarking in video compression," IEEE Trans. Circuits Syst. Video Technol., vol. 17, no. 6, pp. 774–778, Jun. 2007

[6] Kede Ma, Wei. Zhang, Xianfeng Zhao, "Reversible data Hiding in Encrypted Images by reserving Room before encryption", IEEE trans. On information forensics and security, vol,8 No.3 , march 2013.

[7] Wei Liu,, Wenjun Zeng, Lina Dong, and Qiuming Yao, "Efficient Compression of Encrypted Grayscale Images", IEEE Ttanscations on image processing, Vol. 19, NO. 4, APRIL 2010

[8] Changyong Xu, Xijian Ping and Tao Zhang, "Steganography in Compressed Video Stream",2006

[9] Mehmet Utku Celik,,Sharma and Ahmet Murat Tekalp, "Lossless Generalized-LSB Data Embedding" IEEE Ttanscations on image processing, Vol.14 , NO. 2,February 2005

[10] W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[11] Mark Johnson, Prakash Ishwar, and Daniel Schonberg, "On Compressing Encrypted Data", IEEE Ttanscations on signal processing,Vol 52,NO 10,October 2004

[12] Udit Budhia, Deepa Kundur, and Takis Zourntos, " Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain". IEEE Ttanscations on information forensics and security,Vol 1,NO 4,December 2006

[13] Dawen Xu, Rangding Wang, and Yun Q. Shi, Fellow, IEEE "Data Hiding in Encrypted H.264/AVC Video Streams by Codeword Substitution",Vol. 9, No. 4, April 2014.

[14] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 5, pp. 565–576, May 2011.

Jithya.J.Prakash is pursuing her M.Tech degree in Computer Science and Engineering from KMCT College of Engineering, Calicut University. She completed her B.Tech Degree in Information Technology from Cochin University College of Engineering,Kuttanad ,in 2014

Hemand E.P is Assistant Professor, Department of Computer Science and Engineering, KMCT College of Engineering, Calicut University. He. Completed his B.Tech degree in Computer Science & Engineering from Government College of Engineering ,Kannur in 2008..he obtained his M.Tech degree in Computer Network Engineering from RV College of Engineering, Banglore in 2012.

ISSN: 2278 – 7798