International Research Journal in Global Engineering and Sciences. (IRJGES)
ISSN: 2456-172X | Vol. 1, Issue 2, June 2016 to August 2016 | Pages 128-136

EFFECTIVE SECRET DATA SHARING USING MULTIMEDIA COMPRESSION PARADIGM

M. Revathi[1], S.Jayanthi[2]

Assistant Professor, Department of CSE, Agni College of Technology, Chennai.

Abstract: As the need of multimedia security is increasing more. Here, we propose a new data hiding technique and extraction process directly in the encrypted version of H.264/AVC video stream which includes video encryption, data embedding and data extraction. Even though, there is encryption for videos, only a fraction of video is encrypted. In this paper, encryption is done for three sensitive parts of video i.e. codewords of intra prediction mode, codewords of motion vector differences, codewords of residual data. Encrypted video is split into four parts and data hiding data which is encrypted using standard AES algorithm is split into two parts. Both the encrypted data are embedded and compressed. At the receiver end, Extraction of data can take place in encrypted domain or decrypted domain.

Keywords: Data hiding, encrypted domain, H.264/AVC, codeword substituting, Lossless compression.

I. INTRODUCTION

CLOUD computing has become an important technology trend, which can provide highly efficient computation and large-scale storage solution for video data. Given that cloud services may attract more attacks and are vulnerable to untrustworthy system administrators, it is desired that the video content is accessible in encrypted form. The capability of performing data hiding directly in encrypted H.264/AVC video streams would avoid the leakage of video content, which can help address the security and privacy concerns with cloud computing. In addition to cloud computing, this technology can also be applied to other prominent application scenarios. For example, when medical videos or surveillance videos have been encrypted for protecting the privacy of the people, a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted

domain. Till now, few successful data hiding schemes in the encrypted domain have been reported in the open literature. With the increasing demands of providing video data security and privacy protection, data hiding in encrypted H.264/AVC videos will undoubtedly become popular in the near future.

Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Generally, in Data Hiding, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data Hiding is the art and science of writing hidden messages in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. Generally, in Data Hiding, the actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it.

II. EXISTING SYSTEM

A novel scheme of data hiding in the encrypted version of H.264/AVC videos is presented, which includes three parts, i.e., 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. At the receiver end, the hidden data extraction can be accomplished either in encrypted or in decrypted domain. By analyzing the property of H.264/AVC codec, three sensitive parts (i.e., IPMs, MVDs, and residual coefficients) are encrypted with stream ciphers. A digital watermarking algorithm for copyright protection based on the concept of embed digital watermark and modifying frequency

coefficients in discrete wavelet transform(DWT) domain is presented. We embed the watermark into the detail wavelet coefficients of the original image with the use of a key. This key is randomly generated and is used to select the exact locations in the wavelet domain in which to embed the watermark. Original unmarked image is not required for watermark extraction. The performance of proposed watermarking algorithm is robust to variety of signal distortions and noises. Disadvantages of existing techniques are Watermark images may easily let us know the hidden data. If we use image we cannot embed higher standard to it. If we watermark the image together with data then the actual content of data may vary. Bit rate is also increased.

In the existing systems, two novel solutions for data hiding are obtained. The first approach is hiding the message bits by modulating the quantization scale of a macroblock. The quantization scale is either incremented or decremented based upon the message bit. The macroblock-level feature variables are extracted and a second order regression model is computed, and using this regression model, decoder computes the hidden message bit. In the second approach, message bits are hidden and extracted using flexible macroblock feature of H.264/AVC video. Here macroblocks are assigned according to the content of the message bit. But in existing network, delivery of compressed video, packets may be lost if the channel is unreliable. Such losses may tend to occur in burst. So, a new block shuffling scheme is introduced to isolate erroneous blocks caused by information losses. This proposed solution reduces the information loss during video transmission.

III.PROPOSED SCHEME

In this paper, we introduce split of encrypted data in order to intruder from attacking the data. Even though, intruder decrypts the data, only one packet would be known. The process would be carried as following. Sender sends the information in the form of video using mp4 files to the receiver. Sender also wants to send secret information along with this video source. We encrypt and send the secret information which could be viewed only after decompression. The encrypted video is divided into 4 parts and the encrypted data is split into 2 parts. Data could be hided in any of the two parts. Symmetric Ciphering Algorithm and Data Hiding in Encrypted H.264/AVC Video ,codeword substitution techniques involved together and hide the secret content in this video source. Encoded format of this content is compressed and the compressed source sends to the receiver.

A. Encryption of video content

In this paper, an H.264/AVC video encryption scheme with good performance including security, efficiency, and format compliance is proposed. By analyzing the property of H.264/AVC codec, three sensitive parts (i.e., IPMs, MVDs, and residual coefficients) are encrypted with stream ciphers.

B. Embedding the additional data

As we are embedding the additional data into the encrypted video stream we use code word substitution technique. The codewords substitution should satisfy the following three limitations. First, the bitstream after codeword substituting must remain syntax compliance so that it can be decoded by standard decoder. Second, to keep the bit-rate unchanged, the substituted codeword should have the same size as the original codeword. Third, data hiding does cause visual degradation but the impact should be kept to minimum.

C. Splitting Process

Sender splits the encrypted video stream into four parts using cipher stream splitting. A stream cipher has a sequence or stream of Ciphers are classified as block or stream ciphers. All ciphers split long messages into blocks and encipher each block separately. Block sizes range from one bit to thousands of bits per block. A block cipher enciphers each block with the same key. A stream cipher has keys and enciphers each block with the next key. The key stream may be periodic, as in the Vigenere cipher or a linear feedback shift register, or not periodic, as in a one-time pad. Cipher text is often formed in stream ciphers by exclusive-oring of the plaintext with the key, as in the Vernam cipher. Now we will look at more sophisticated collision resolution techniques which have higher achievable throughput These techniques also maintain stability without a complex estimation procedure like in pseudo-Bayesian slotted Aloha. The way they obtain this is by choosing different retransmission probability for different nodes, at each time slot during collision resolution the nodes are subdivided into two sets.

A preliminary explanation as to how this is possible is to consider an algorithm that will make new arrivals wait until an ongoing collision has been resolved. Assuming a small attempt rate it is most likely to have only two packets colliding. All other nodes will refrain from transmitting until they have observed that those two backlogged packets have been successfully

transmitted. Each of the colliding packets could then be retransmitted with probability 1/2 leading to successful retransmission of one of them with probability 1/2 and the other could then be transmitted in next slot. With probability 1/2 another collision or an idle slot occurs. If so, the two packets would again be retransmitted with probability 1/2 until a successful transmission occurred which would be followed by the transmission of the remaining packet? The probability of two slots for retransmitting the packets is 1/2 since this happens if there is no further collision.

D. Compression of embedded data

Embedded data is compressed using Lossless compression which allows receiver to recompress or retrieve the original data without varying of file size. In this paper, We compress the embedded data using standard Data compression algorithm.

Lossless Compression

Lossy Compression is generally used for image, audio, video; where the compression process neglects some less important data. The exact replica of the original file can't be retrieved from the compressed file. To decompress the compressed data we can get a closer approximation of the original file. The Data Compression (DC) is not only the cost effective technique due to its small size for data storage but it also increases the data transfer rate in data communication. A data compression algorithm should emphasize the originality of the data during compression and decompression process. The components of the algorithm are: source file, filtering unit, syllables unit, compression unit, dictionary file and target file. The method uses variable bit length representation depending on the number of different syllables in the dictionary and performs compression in three steps. The first step is filtering to find non alphabetic characteristics.

X	p(X)
a	0.171
b	0.031
c	0.057
d	0.092
e	0.274
f	0.052
g	0.042
h	0.130
i	0.149
j	0.002

Bit representation for compression

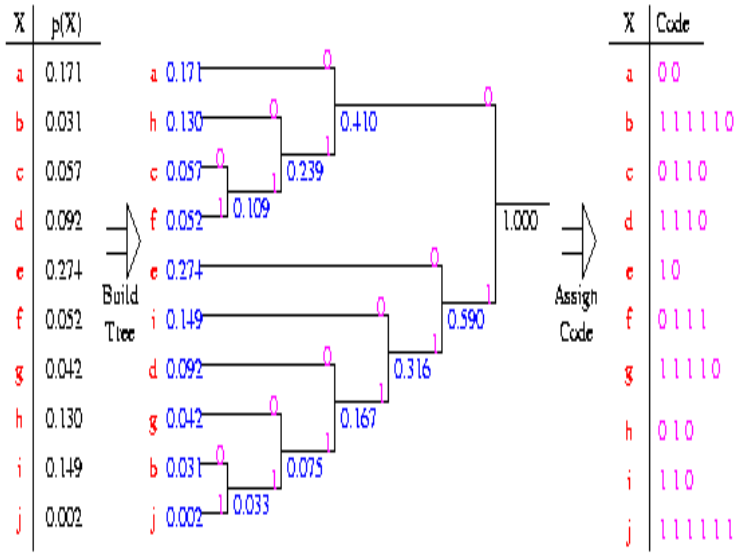
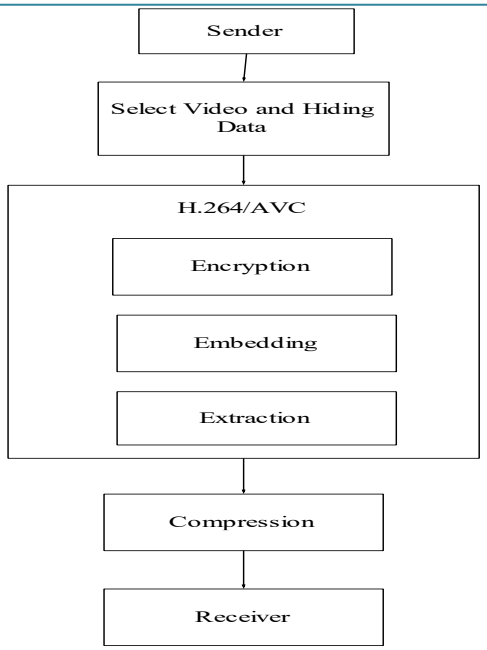


Fig (1) Code Compression

E. Data Extraction

In this scheme, the hidden data can be extracted either in encrypted or decrypted domain, as shown in Fig. 1. Data extraction process is fast and simple. We will first discuss the extraction in encrypted domain followed by decrypted domain. 1) Scheme I: Encrypted Domain Extraction. To protect privacy, a database manager (e.g., cloud server) may only get access to the data hiding key and have to manipulate data in encrypted domain.

Decrypted Domain Extraction. In scheme I, both embedding and extraction of the data are performed in encrypted domain. However, in some cases, users want to decrypt the video first and extract the hidden data from the decrypted video. For example, an authorized user, which owned the encryption key, received the encrypted video with hidden data. The received video can be decrypted using the encryption key. That is, the decrypted video still includes the hidden data, which can be used to trace the source of the data.



Fig(2) VIDEO ENCRYPTION AND DATA HIDING IN H.264/AVC

IV. EXPERIMENTAL RESULTS

When the system is executed, the video is displayed. First select the secret message (Here secret message is a text message) and it is converted into binary stream of bits. Embed the secret message into the video file during the encoding process. There are chances for errors during the embedding process in the video files and during the transmission over the internet. These errors may tend to information loss in the video or packet loss during transmission. This is avoided by lossless compression. During the decoding process, we extract the secret hidden message from the video files and if the errors are also extracted completely from the video, then we can guarantee that there is no information loss in the video. And finally the original hidden message can be extracted without any changes.

VI. CONCLUSION & FUTURE WORK

In this paper, we can enhance our work to robustness of the existing work against information losses in video steganalysis methods. Data hiding in encrypted media is a new topic that has started to draw attention because of the privacy-preserving requirements from cloud data management. The existing systems superior in terms of message payload while causing less distortion and compression overhead and the proposed solution reduces the information loss

during transmission. It can be enhanced in military services, hospitals For example, when medical videos or surveillance videos have been encrypted for protecting the privacy of the people, a database manager may embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain. it can be enhanced by hiding data such as audio and video in future.

References:

[1]. M. Carli, M. Farais, E. D. Gelasca, R. Tedesco, and A. Neri, "Quality assessment using data hiding on perceptually important areas," in Proc. IEEE Int. Conf. Image Processing, ICIP, Sep. 2005, pp. III-1200-3–III-1200-3.

[2]. A. Yilmaz and A. Aydin, "Error detection and concealment for video transmission using information hiding," Signal Processing: Image Communication, vol. 23, no. 4, pp. 298–312, Apr. 2008.

[3]. S. Kapotas and A. Skodras, "A new data hiding scheme for scene change detection in H.264 encoded video sequences," in Proc. IEEE Int. Conf. Multimedia Expo ICME, Jun. 2008, pp. 277–280.

[4]. K. Nakajima, K. Tanaka, T. Matsuoka, and Y. Nakajima, "Rewritable data embedding on MPEG coded data domain," in Proc. IEEE Int. Conf. Multimedia and Expo, ICME, Jul. 2005, pp. 682685.

[5]. Y. Li, H.-X. Chen, and Y. Zhao, "A new method of data hiding based on H.264 encoded video sequences," in Proc. IEEE Int. Conf. Signal Processing, ICSP, Oct. 2010, pp. 1833–1836.

[6]. D.-Y. Fang and L.-W.Chang, "Data hiding for digital video with phase of motion vector," in Proc. IEEE Int. Symp. Circuits Systems, ISCAS, Sep. 2006.

[7]. C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in Proc. Int. Conf. Innovative Computing, Information and Control, ICICIC"06, 2006, vol. II, pp. 803–806.

[8]. K. Wong, K. Tanaka, K. Takagi, and Y.Nakajima, "Complete video quality-preserving data hiding," IEEE Trans. Circuits Syst. Video Technol., vol. 19, no. 10, Oct. 2009.

[9]. K. Solanki, U. Madhow, B. S. Manjunath, S. Chandrasekaran, and I. El-Khalil, ""Print and Scan" resilient data hiding in images," IEEE Trans. Inform. Forensics Security, vol. 1, no. 4, pp. 464–478, Dec.2006.

[10]. X.-P. Zhang, K. Li, and X. Wang, "A novel look-up table design method for data hiding with reduced distortion," IEEE Trans. Circuits Syst. Video Technol., vol. 8, no. 6, pp. 769–776, Jun. 2008.

[11] 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.

[12] B. Zhao, W. D. Kou, and H. Li, "Effective watermarking scheme in the encrypted domain for buyer-seller watermarking protocol," Inf. Sci.,vol. 180, no. 23, pp. 4672–4684, 2010.

[13] P. J. Zheng and J. W. Huang, "Walsh-Hadamard transform in the homomorphic encrypted domain and its application in image watermarking,"in Proc. 14th Inf. Hiding Conf., Berkeley, CA,USA, 2012, pp. 115.

[14] W. Puech, M. Chaumont, and O. Strauss, "A reversible data hiding method for encrypted images," Proc. SPIE, vol. 6819,pp. 68191E-1–68191E-9, Jan. 2008.

[15]. X. P. Zhang, "Reversible data hiding in encrypted image," IEEE Signal Process. Lett., vol.18, no. 4, pp. 255–258, Apr. 2011.

[16]. W. Hong, T. S. Chen, and H. Y. Wu, "An improved reversible data hiding in encrypted images using side match," IEEE Signal Process.Lett., vol.19,no. 4, pp. 199–202, Apr. 2012.

[17] .X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2,pp. 826–832, Apr. 2012.

[18] . K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553–562, Mar. 2013.