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 2, February 2016

A Survey on Secure Hiding of Data in Compressed Video

Gayatri Mungse, Yogesh Patil, Mayuri Rathod, Ajit Naikude

B.E Students, dept. of I.T, DYPIET, Pimpri, Pune, Maharashtra, India

ABSTRACT: To preserve the privacy as well as maintain security of data it needs to be stored in an encrypted format. For preventing eavesdropping and transaction tracking we use information hiding techniques that can be achieved by embedding a data into a video bit stream. In this paper hiding information directly in the encrypted version of H.264/AVC video stream is proposed. The proposed scheme contains the three main parts, i.e. encryption of video, embedding secret message and extraction of secret message and video.

Here hiding information directly in the encrypted version of H.264/AVC video stream is studied, it includes the three main parts, i.e. encryption of video, embedding and extraction of data. After analyzing the H.264/AVC codec property, the code words of intra prediction modes **(**IPM), the code words of motion vector differences (MVD), and the code words of residual coefficients are encrypted. The data hider embeds additional data in the encrypted domain, the code word substitution technique is used. The code word substitution technique gives information without knowing the original video content. The extraction of data can be done either in the encrypted or in the decrypted domain.

I. INTRODUCTION

Information hiding in compressed H.264/AVC can be useful in various sectors , such as organizations to send confidential data ,banks to send the secret messages or passwords, secured transmission of private data maintaining its confidentiality and integrity .This project discusses the information hiding in compressed H.264/AVC video .The implementation is done by combining various techniques, such as Intra-Prediction Mode (IPM) Encryption, Motion Vector Difference (MVD) Encryption, Residual Data Encryption techniques. Various challenges in maintaining the privacy and security of data i.e. secured transmission is caused by various types of attacks and variations in the attack .The proposed system that transfers the data securely comprises of three steps. The first step is to encrypt the video. The different parameters of the video such as texture information, motion information, and residual data have to be considered. The next stage is embedding data in the encrypted video. The third stage is to transfer the embedded video. And the final stage is to extract the embedded data from the video.

II. LITERATURE SURVEY

From past few years, there has been an increasing interest among researchers in the problem related to secure data transfer. Intensive research has been carried out in this area, which is evident from large number of technical papers. One such application is information hiding in compressed video for secure transmission of data. The information related to algorithms used or implementation methods is studied by following papers.

A)H.264/AVC video coding standards

H.264/AVC is the newest international video coding standard. By the time of this publication, it is expected to have been approved by ITU-T as Recommendation H.264 and by ISO/IEC as International Standard 14496–10 (MPEG-4 part 10) Advanced Video Coding (AVC). The MPEG-2 video coding standard (also known as ITU-T H.262) , which was developed about ten years ago primarily as an extension of prior MPEG-1 video capability with support of interlaced video coding, was an enabling technology for digital television systems worldwide. It is widely used for the transmission of standard definition (SD) and high definition (HD) TV signals over satellite, cable, and terrestrial emission and the storage of high-quality SD video signals onto DVDs. However, an increasing number of services and growing popularity of high definition TV are creating greater needs for higher coding efficiency. Moreover, other transmission media such as Cable Modem, xDSL, or UMTS offer much lower data rates than broadcast channels, and enhanced coding efficiency can enable the transmission of more video channels or higher quality video representations within existing digital transmission capacities. Video coding for telecommunication applications has evolved through the development of the ITU-T H.261, H.262 (MPEG-2), and H.263 video coding standards (and later enhancements of H.263 known as and), and has diversified from ISDN and T1/E1 service to embrace PSTN, mobile wireless networks, and LAN/Internet network delivery. Throughout this evolution, continued efforts have been made to maximize coding efficiency while dealing with the diversification of network types and their characteristic formatting and loss/error robustness requirements. Recently the MPEG-4 Visual (MPEG-4 part 2) standard has also begun to emerge in use in some application domains of the prior coding standards. It has provided video shape coding capability, and has similarly worked toward broadening the range of environments for digital video use. In early 1998, the Video Coding Experts Group (VCEG) ITU-T SG16 Q.6 issued a call for proposals on a project called H.26L, with the target to double the coding efficiency (which means halving the bit rate necessary for a given level of fidelity) in comparison to any other existing video coding standards for a broad variety of applications. The first draft design for that new standard was adopted in October of 1999. In December of 2001, VCEG and the Moving Picture Experts Group (MPEG) ISO/IEC JTC 1/SC 29/WG 11 formed a Joint Video Team (JVT), with the charter to finalize the draft new video coding standard for formal approval submission as H.264/AVC in March 2003. The scope of the standardization is illustrated in Fig. 1, which shows the typical video coding/decoding chain (excluding the transport or storage of the video signal). As has been the case for all ITU-T and ISO/IEC video coding standards, only the central decoder is standardized, by imposing restrictions on the bitstream and syntax, and defining the decoding process of the syntax elements such that every decoder conforming to the standard will produce similar output when given an encoded bitstream that conforms to the constraints of the standard.This limitation of the scope of the standard permits maximal freedom to optimize implementations in a manner appropriate to specific applications (balancing compression quality, implementation cost, time to market, etc.). However, it provides no guarantees of end-to-end reproduction quality, as it allows even crude encoding techniques to be considered conforming.

B) Separable Reversible Data Hiding in Encrypted Image

In recent years, signal processing in the encrypted domain has attracted considerable research interest. As an effective and popular means for privacy protection, encryption converts the ordinary signal into unintelligible data, so that the traditional signal processing usually takes place before encryption or after decryption. However, in some scenarios that a content owner does not trust the processing service provider, the ability to manipulate the encrypted data when keeping the plain content unrevealed is desired. For instance, when the secret data to be transmitted are encrypted, a channel provider without any knowledge of the cryptographic key may tend to compress the encrypted data due to the limited channel resource. While an encrypted binary image can be compressed with a lossless manner by finding the syndromes of low-density parity-check codes , a lossless compression method for encrypted gray image using progressive decomposition and rate-compatible punctured turbo codes is developed. With the lossy compression method , an encrypted gray image can be efficiently compressed by discarding the excessively rough and fine information of coefficients generated from orthogonal transform. When having the compressed data, a receiver may reconstruct the principal content of original image by retrieving the values of coefficients. The computation of transform in the encrypted domain has also been studied. Based on the homomorphic properties of the underlying cryptosystem, the discrete Fourier transform in the encrypted domain can be implemented. A composite signal representation method packing together a number of signal samples and processing them as a unique sample is used to reduce the complexity of computation and the size of encrypted data.

C) Commutative Encryption and Watermarking in Video Compression

With the rapid development of Internet technology, such media data as images, audios or videos are used more and more widely in human’s daily life. This makes media data not only easy to be transmitted, but also easy to be copied and spread out. Thus, the legal issue rises that some media data should be protected against unauthorized users or operations. To protect media data, two means have been proposed and highlighted since the past decade, i.e., media encryption and media watermarking. Media encryption encrypts media data into unintelligible ones with ciphers, which protects media content’s confidentiality. Taking video encryption for example, the encrypted videos are often difficult to be understood. Different from text/binary data encryption , video encryption often requires the scheme be time

efficient and format complaint in order to meet real time applications. It is not practical to encrypt video data completely with traditional ciphers , This work was supported in part by France Telecom R&D Beijing, Beijing, China, under Grant PEK06-ILAB-008. This paper was recommended by Associate Editor Q. Sun. such as data encryption standard (DES) or advanced encryption standard (AES), because of high computational cost. Alternatively, partial encryption encrypts only a fraction of video data and improves the efficiency. For example, some schemes have been proposed to encrypt the videos encoded with advanced video coding (H.264/AVC) .Also a scheme proposed encrypts videos by scrambling the intra-prediction mode (IPM) of intra-macro-blocks. Its security is analyzed followed with an improved scheme that encrypts not only IPM but also the motion vector difference (MVD). Another scheme encrypts some parameters of video stream including picture parameter, intra-coded frame, slice header and macro-block header of P-slice, and dc's. Compared with media encryption, media watermarking embeds some information into media data perceptibly or imperceptibly, which protects media data's ownership or identification. For invisible video watermarking imperceptibility and robustness are often required. The imperceptibility means that the watermarked video is perceptually same to the original video, and the robustness means that the watermark survives such operations as recompression or signal
processing. Taking the algorithms robust against H.264/AVC compression for example, they can be classified into three types: raw video watermarking, compression domain watermarking and compressed data watermarking. The first type of algorithm embeds watermarks into videos before video compression. For example, the dc's in each 8 X 8 discrete cosine transform (DCT) block are transformed with 1-D DCT and then watermarked]. The second type of algorithm embeds watermarks into DCT coefficients during H.264/AVC encoding . The third type of algorithm embeds watermarks into the compressed data stream. For example, the watermark is
embedded into the skipped macro-blocks]. Generally, the first type of algorithm is robust against recompression or signal processing operations, but has high computational cost. The second one is time efficient, can be combined with compression process, but is only robust against recompression or few signal processing operations. The third one is time efficient, but not robust against recompression or signal processing operations. For video encryption and video watermarking realize different functionalities, they can be combined together to protect both the confidentiality and the ownership/identification. Generally, it is implemented according to two steps . Firstly, media data are watermarked. Secondly, the watermarked media data are encrypted. In this case, if the encryption process and watermarking process cannot be commutated, media data must be decrypted before the watermark can be detected or another watermark can be embedded.

D) A Survey of H.264 AVC/SVC Encryption

H.264 is the most widely-deployed video compression system and has gained a dominance comparable only to JPEG for image compression. The H.264 standard has also been extended to allow scalable video coding with a backwards compatible nonscalable base layer. This extension enables the implementation of advanced application scenarios with H.264, such as scalable streaming and universal multimedia access. Given the dominant application of H.264 as video compression system, the necessity of practical security tools for H.264 is unquestionable. In this survey an overview, classification and evaluation of the stateof- the-art of H.264 encryption, a topic to which numerous proposals that have been made are presented. The survey focuses solely on H.264 AVC/SVC encryption and intends to give researchers a brief, yet comprehensive survey and to aid practitioners in the selection of H.264 encryption algorithms for their specific application context. Furthermore, the survey identifies the most relevant research questions in the area of video encryption, that still need to be answered in order to leverage the deployment of H.264 encryption.A secure approach to encrypt H.264, also referred to as “naive” encryption approach, is to encrypt the entire compressed H.264 bitstream with a secure cipher, e.g., AES, in a secure mode, e.g., cipher block chaining (CBC) mode. There are well-founded reasons not to stick to this approach, but to apply specifically designed encryption routines.1) The implementation of advanced application scenarios, such as secure adaptation, transparent/perceptual encryption and privacy preserving encryption. 2) The preservation of properties and functionalities of the bit-stream, such as format-compliance, scalability, streaming/packetization , fast forward, extraction of subsequences, transcodability, watermarking, and error resilience. 3) The reduction of computational complexity. Secure adaptation requires a scalable bit stream and specific encryption routines that preserve the scalability in the encrypted domain . Secure adaptation is the basis for secure scalable streaming , where secure adaptation is employed in a multimedia streaming scenario. A secure stream for a mobile phone (low bandwidth, low resolution display, low computing power) and a personal computer (high bandwidth, high resolution display, high computing power) can be generated from the same secure source stream (by secure adaptation) without the necessity of the secret key, thus enabling creator-to-consumer security. Transparent encryption denotes encryption schemes where a low quality can be decoded from the ciphertext; this functionality can be implemented with scalable bit-streams by encryption of the enhancement layers.

E) Data Hiding in MPEG Video Files Using Multivariate Regression and Flexible Macro-block Ordering

Data hiding techniques can be used to embed a secret message into a compressed video bit stream for copyright protection, access control, content annotation and transaction tracking. Such data hiding techniques can also be used for other purposes. For instance, used data hiding techniques to assess the quality of compressed video in the absence of the original reference. The quality is estimated based on computing the degradations of the extracted hidden message. The authors of used data hiding technique to enable real time scene change detection in compressed video. The information is hidden using the motion compensation block sizes of an H.264/AVC video. Data hiding is also used for error detection and concealment in applications of video transmission. Edge orientation information and number of bits of a block are hidden in the bit stream for that purpose. In general, the existing solutions rely on hiding message bits in discrete cosine transform (DCT) coefficients, motion vectors (MVs), quantization scale or prediction modes. Examples of data hiding using DCT coefficients include the use the parity of the quantized coefficients to hide a message. Additionally, utilized zero-length codes to insert a dummy value at certain locations to indicate message bits. Examples of using MVs for data hiding include , where phase angles of MVs are used to hide messages. The candidate motion vectors are selected based on the prediction error of the underlying macro-block. MVs associated with high prediction errors are chosen. A prediction error threshold is computed per frame and transmitted in the video bit stream to guide the decoder in recognizing the MVs that carry bits of the secret message. The quantization scale is also used for data hiding. The factor is multiplied by all ac coefficients in the corresponding macro-block. The procedure is referred to as promoting and exiting a macro-block. If a message bit to hide is equal to zero, then such a procedure is followed, otherwise no action is taken. From a syntax viewpoint, since a relatively large number of prediction modes and block sizes are available in H.264/AVC, it has been proposed to use these variants to hide message bits. It was shown that 1 bit can be hidden in each candidate 4 4 intrablock. Additionally,the block types and modes of intracoded blocks of H.264/AVC to hide message bits. Data hiding can also be applied prior to compression. It is also possible to hide data in the wavelet domain. In such an approach, significant wavelet coefficients are identified and used for embedding a message payload. Lastly, hiding of data can also be applied in the compressed domain. For example, hiding messages in the compressed H.264/AVC I-frames without the introduction of drift distortion. Steganalysis, on the other hand, is the process of detecting the presence of hidden messages in multimedia. Steganalysis can be applied to digital images and to digital video. Existing work on video-based steganography takes such analysis into account and tries to maintain the statistics of carrier before and after message hiding. In this paper, we propose two novel solutions for data hiding. In the first solution, the message bits are hidden by modifying the quantization scale of MPEG video coded with constant bit rates. Features are extracted from individual macro-blocks and a second-order regression model is computed. The decoder uses the regression model to predict the content of the hidden message based on macro-block-level feature variables. In the second solution, both constant and variable bit rate coding are supported. The solution utilizes the flexible macro-block ordering (FMO) feature of H.264/AVC video for message hiding and extraction

III. ADVANTAGES

1. The data hiding is performed directly in encrypted H.264/AVC video bitstream.
2. The scheme can ensure both the format compliance and the strict file size preservation.
3. The scheme can be applied to two different application scenarios by extracting the hidden data either from the encrypted video stream or from the decrypted video stream.

IV. CONCLUSION

Information hiding in encrypted media is a new topic of privacy-preserving requirements of cloud data management. The encrypted H.264/AVC bit stream, which consists of encryption of videos, data embedding and data extraction phases. In the information hiding it follows the without decrypting the data, the data hiding and re-encryption takes place. The bit stream preserves exactly after encryption and data embedding. For the data embedding we use the code word substitution technique, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain and the data extraction part is either in encrypted or decrypted domain, here we can preserve the confidentiality of the hidden data content completely.

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]. T. Stutz and A. Uhl, "A survey of H.264 AVC/SVC encryption," IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 3, pp. 325–339, Mar. 2012.

[3] T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," IEEE Trans. Inform. Forensics Security, vol. 7, no. 2, pp. 455–464, Apr. 2012.

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

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

BIOGRAPHY

Gayatri Mungse, Yogesh Patil, Mayuri Rathod, Ajit Naikude, perceiving bachelor of engineering degree in I.T department of DYPIET,pimpri-18, pune, Maharashtra. They have made a survey on secure data hiding in compressed video and are working on project of same topic.