ISSN : 2494-9150 Vol-02, Issue 01, APR 2016.

Review on Data Hiding in Encrypted Compressed Video Streams by Codeword Substitution

[1]Snehal N. Honade, [2]Prof. Dipak B. Pawar
[1]PG Student, [2]Head of the Department E&TC, E&TC Department, BSCOER, Pune, Maharashtra, India.
[1]snehalhonade25@gmail.com, [2]dipak_harekrishna@yahoo.com

Abstract - In order to maintain security and privacy, Digital video needs to be stored and processed in an encrypted format. It becomes necessary to perform data hiding in these encrypted videos for the purpose of content notation and/or tampering detection. Thus, data hiding in encrypted domain without decryption preserves the confidentiality of the content. In this paper, data hiding technique directly in the encrypted version of H.264/AVC video stream is proposed. It includes H.264/AVC video encryption, data embedding, and data extraction. Firstly, Due to the property of H.264/AVC codec, the codewords of intraprediction modes, the codewords of motion vector differences, and the codewords of residual coefficients are encrypted with stream ciphers. Then, by using codeword substitution technique, data is embedded in the encrypted domain, without knowing the original video content. Data extraction can be done either in the encrypted domain or in the decrypted domain in order to achieve different application scenarios. Video file size is strictly preserved even after its encryption and data embedding.

Keywords — H.264/AVC, codeword substitution, encrypted domain, data hiding

I. INTRODUCTION

Cloud computing has become an important technology trend, which can provide highly efficient computation and large scale storage solution for video data. But 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 [1]. For example, Data hiding technique can be used by a cloud server to embed the additional information (e.g., video notation, or authentication data) into an encrypted version of an H.264/AVC video. With the hidden information, the server can manage the video or authenticate its integrity without knowing the original video content, and thus the security and privacy can be protected. In addition to cloud computing, this technology can be used in various important applications. For example, In order to protect the privacy of the people, medical videos or surveillance videos are encrypted; a database manager may embed the personal information into encrypted videos to provide the data management capabilities in the encrypted domain. Till now, some of the successful data hiding schemes in the encrypted domain have been reported in the open literature. A watermarking scheme in the encrypted domain using Paillier cryptosystem is presented in [2] which is based on the security requirements of buyer-seller watermarking protocols. In [3], Walsh-Hadamard transform based image watermarking algorithm in the encrypted domain is proposed using Paillier cryptosystem. However, due to the limitation of the Paillier cryptosystem, the encryption of an original image results in a high overhead in computation and storage. Several researches on reversible data hiding in encrypted images are reported in [4]–[8] recently. Bit-XOR (exclusive-OR) operation is used to perform encryption. However, in these methods, the host image remains in an uncompressed format. In [9], a robust watermarking algorithm is presented for watermark embedding into compressed and encrypted JPEG2000 images.

As said the above mentioned works have been concentrated on images. With the increasing demands of video data security and privacy protection, data hiding technique in encrypted H.264/AVC videos will surely become helpful in the near future. In [10], the intra-prediction mode (IPM), motion vector difference (MVD) and DCT coefficients sign are encrypted, and DCT coefficients amplitudes are watermarked adaptively, during H.264/AVC compression. A combined scheme of encryption and watermarking is presented in [11], which provides the access right and authentication of video content simultaneously. However, it's necessary to perform data hiding technique directly in the encrypted domain to

achieve certain requirements. This proposes an efficient method to embed secret data directly in encrypted H.264/AVC video bit stream. Firstly, by analyzing the property of H.264/AVC codec, the codewords of IPMs, the codewords of MVDs, and the codewords of residual coefficients are encrypted with a stream cipher. The encryption algorithm is combined with the Exp-Golomb entropy coding and Context-adaptive variable-length coding (CAVLC) [12], which keeps the codeword length unchanged. Then, data hiding technique is performed in encrypted domain using codeword substitution method. This technique can ensure both the format compliance and the strict file size preservation. It 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.

A. Commutative Encryption And Watermarking In Compression Of Video

The video encryption and watermarking scheme based on H.264/AVC codec, gives a solution for the commutation of encryption and watermarking. In this scheme, parameters such as IPM, MVD and residual coefficient's sign are encrypted, while the amplitude of dc or ac is watermarked adaptively. In order to minimize computational cost, the selected parameters are encrypted partially. Traditional watermark embedding scheme is modified to keep sign encryption and amplitude watermarking independent. The coefficients are selected adaptively according to macro block type to keep them robust and imperceptible.

B. Seperable Reversible Data Hiding In Image

In separable reversible data hiding, an encryption key is used in the encryption of original image and data-hiding key is used to embed data into the encrypted image. From encrypted image containing data, receiver with data-hiding key is able to extract the additional data without knowing the original image content. With the encryption key, receiver can decrypt the received data to obtain original image, but cannot extract the embedded data from image. If the receiver has both the data-hiding key and the encryption key, he can extract the embedded data and recover the original image without any error when the amount of additional data is not too large.

C. The Exp-Golomb Encryption Algorithm (EGEA)

In AVC, the IPM coefficients are encoded with Exp-Golomb codes. It is composed of R zeros, one '1' – bit and R bits of information (Y). Here, the intra-prediction mode is X=2R+Y-1, and R = [log2 (X+1)]. This process is similar to table permutation. The main difference is that the permutation operation happens only in the codeword with the same length, and the key changes with the intra/inter-prediction mode. The decryption process is symmetric to the encryption one.

D. The CAVLC Encryption Algorithm (CEA)

During CAVLC encoding, parameters such as the number of coefficients, trailing ones (coeff_token), the sign of each T1, the levels of the remaining non-zero coefficients, the total number of zeros before the last coefficient and each run of zeros are encoded. In order to keep low cost and keep the code format unchanged, only few of the parameters are encrypted. Thus, we propose to encrypt only the signs of T1 and the levels of the remaining non-zero coefficients while keep other parameters unchanged. Considered that these parameters are often of variable length, the stream cipher is more useful for length-kept encryption. So the stream cipher is used to encrypt the selected parameters. The encryption process is realized during encoding process, thus the code format keeps unchanged, which makes it practical to decode or decrypt the videos correctly.

E. Selective Encryption Algorithm For Secure Advanced Video Coding

During AVC encoding, spatial information (IPM and residual data) and motion information (MVD) are encrypted partially. Among them, IPM coefficients are encrypted based on Exp-Golomb entropy coding, the intra-macro blocks, DCs are encrypted based on context adaptive variable length coding (CAVLC) , and the inter-macro blocks MVDs are sign-encrypted with a stream cipher followed with variable length coding. This encryption scheme is secure in perception, keeps format compliance, and achieves high time efficiency though reducing the encrypted data volumes.

F. Enhanced Selective Encryption

It operates in compressed domain based on context adaptive binary arithmetic coding.

Merits: Suitable for streaming over heterogeneous network because of number change in bit rates.

Demerits: Performed on the entropy coding stage of H.264/AVC using AES encryption algorithm in CEB mode. Hence it does not affect the bitstream and H.264/AVC bit stream compliance.

G. Codeword substitution Method

The previous method performs encryption and data embedding almost simultaneously during H.264/AVC compression phase and not on compressed domain. Hence the compression and decompression cycle is the time consuming and it affects real time implementation.

Merits: Data hiding performed entirely in the encrypted domain preserves confidentiality of the content during cloud storage. The technique operates directly on the compressed bit stream. The scheme can ensure both the format compliance and strict file size preservation. In order to adapt to various application scenario, data extraction is possible either from encrypted domain or from decrypted domain.

II. PROPOSED SCHEME

In this section, a new technique of data hiding in the encrypted version of H.264/AVC videos is presented; it 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. It produces an encrypted

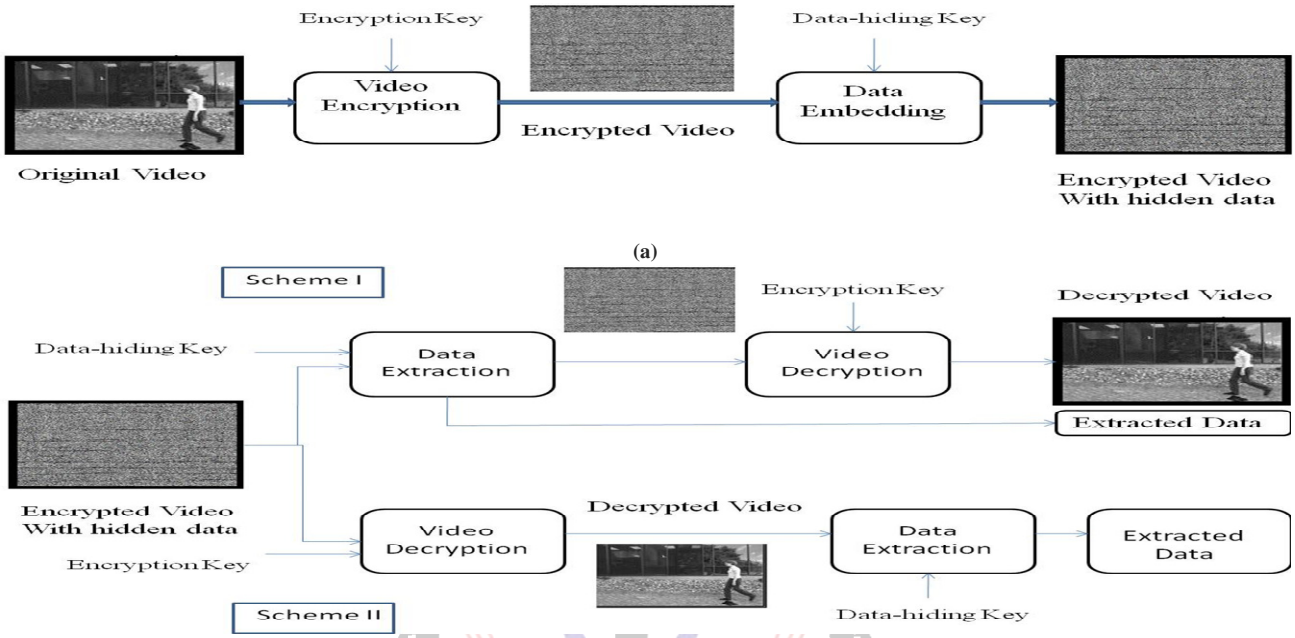

Fig. 1. Diagram of proposed scheme.

video stream and then, the data-hider (e.g., a cloud server) can embed the additional data into the encrypted video stream by using codeword substitution technique, without knowledge of original video content. At the receiver end, the hidden data extraction can be done either in encrypted or in decrypted domain. The diagram of proposed framework is as shown in Fig. 1, in which part (a) shows encryption and data embedding, and part (b) shows data extraction and video decryption. Chaos encryption algorithm can be used for encryption of additional data into the original video content.

A. Encryption of H.264/AVC Video Stream

Video encryption often requires the scheme to be time efficient to meet the requirement of real time applications and format compliance. It is not desirable to encrypt the whole compressed video bitstream like what the traditional ciphers do because of format compliance and computational cost. Alternatively, only a fraction of video data is encrypted to increase the efficiency and to achieve security. The key issue is then how to select the sensitive data for encryption. According to the analysis given in [13], it is reasonable to encrypt both spatial information (IPM and residual data) and motion information (MVD) during H.264/AVC encoding. In this paper, an H.264/AVC video encryption technique with improved performance is proposed which includes security, efficiency, and format compliance.

Due to the property of H.264/AVC codec, three sensitive parts are IPMs, MVDs, and residual coefficients are encrypted with stream ciphers for the encryption of original video content. Compared with [13], the proposed encryption algorithm is performed in the H.264/AVC compressed domain and not during H.264/AVC encoding. Here, the bitstream will be modified directly.

B. Data Embedding

In the encrypted bitstream of H.264/AVC, the proposed data embedding is done by codeword substitution technique. Eligible codewords of Levels are substituted for data embedding. Since the sign of Levels are encrypted, it is desired that data hiding should not affect the sign of Levels.

Besides, the codewords substitution should satisfy the following three limitations, Firstly, the bitstream after codeword substitution should remain syntax compliance so that it can be decoded by standard decoder. Secondly, to keep the bit-rate unchanged, size of the substituted codeword should be same as that of the original codeword. Third, impact of visual degradation caused by data hiding should be kept to minimum. That means, the embedded data after video decryption has to be invisible to a human observer. Hence value of Level related to the substituted codeword should keep close to the value of Level corresponding to the original codeword.

C. Data Extraction

In this scheme, the hidden data can be extracted either in encrypted or decrypted domain, as shown in Fig. 1(b).

1) Scheme I: Encrypted Domain Extraction. For privacy purpose, a database manager (e.g., cloud server) may only get access to the data hiding key and have to manipulate data in encrypted domain. Data extraction in encrypted domain guarantees the feasibility of proposed scheme in this case. In encrypted domain, as shown in Fig. 1(b), encrypted video with hidden data is directly sent to the data extraction module, and the extraction process is done further.

2)Scheme II: Decrypted Domain Extraction. In some case, user wants to decrypt the video first and then 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 in it. The received video can be decrypted using the encryption key, that means, the decrypted video still includes the hidden data, which can be used to trace the source of the data. Data extraction in decrypted domain is suitable for such case. As shown in Fig. 1(b), the received encrypted video with hidden data is first pass through the decryption module and then data extraction is done.

III. CONCLUSION

In this paper, different encryption algorithms and data hiding techniques are discussed. Now a day, Data hiding in encrypted domain has started to draw attention because of the privacy-protecting requirements from cloud data management. In codeword substitution based hiding, an algorithm is used to embed additional data in encrypted H.264/AVC video bit stream, which consists of video encryption, data embedding and data extraction stages. The proposed technique can preserve the bit-rate exactly even after encryption and data embedding, and is simple to implement as it is directly performed in the compressed and encrypted domain, i.e. there is no need of decrypting or partial decompression of the video stream thus making it ideal for real-time video applications. The data hider can embed additional data into the encrypted bit stream using codeword substitution, even though he does not know the original video content. Since data hiding is performed entirely in the encrypted domain, thus preserve the confidentiality of the content . With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides different practical applications.

ACKNOWLEDGMENT

It is my pleasure to get this opportunity to thank my respected Guide Prof. D. B. Pawar who imparted valuable basic knowledge of Electronics specifically related to Signal Processing. We are grateful to Elec. & Telcomm. Dept. of Bhivrabai Sawant College Of Engineering & Research, Pune for providing us infrastructure facilities and moral support.

REFERENCES

[1] 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.

[2] 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.

[3] 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.1 -15.

[4] 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.

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

[6] 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.

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

[8] 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.

[9] A.V.Subramanyam, S.Emmanuel, and M.S.Kankanhalli, "Robust watermarking of compressed and encrypted JPEG2000

images, "IEEE Trans. Multimedia, vol.14, no.3, pp.703-716, Jun.2012.

[10] 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.

[11] S.W.Park and S.U.Shin, "Combined scheme of encryption and watermarking in H.264/scalable video coding (SVC), "New Directions Intell. Interact. Multimedia, Vol.142, no.1, pp.351-361, 2008.

[12] 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.

[13] 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.

[14] 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.

