IJIR

INTERNATIONAL JOURNAL OF INNOVATION RESEARCH

Available Online at http://www.journalijir.com

Vol. 4, Issue, 5, pp. 75-78, May, 2016

ISSN: 2249-1465

Research Article

DATA HIDING IN ENCRYPTED COMPRESSED VIDEO STREAMS BY CODEWORD SUBSTITUTION

Snehal N. Honade and Dipak B. Pawar

Department Of Electronics & Telecommunication TSSM's Bhivarabai Sawant College Of Engineering,Pune, India

ARTICLE INFO

Received 10th February, 2015
Received in revised form 13th March, 2016 Accepted 20th April, 2016
Published online 28th May, 2016

Keywords:

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

ABSTRACT

In order to maintain security and privacy, Digital video needs to be stored and processed in an encrypted format. Data hiding should be done 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. Size of video file is strictly preserved even after its encryption and data embedding.

INTRODUCTION

Cloud computing has become an important technology trend, which can provide highly efficient computation and storage solution for video data. But cloud services may attract more attacks and are susceptible to unreliable system administrators, thus video content should be accessed 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,

*✉ *Corresponding author:* **Snehal N. Honade**
Department Of Electronics & Telecommunication TSSM's Bhivarabai Sawant College Of Engineering,Pune, India

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.

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 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.

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

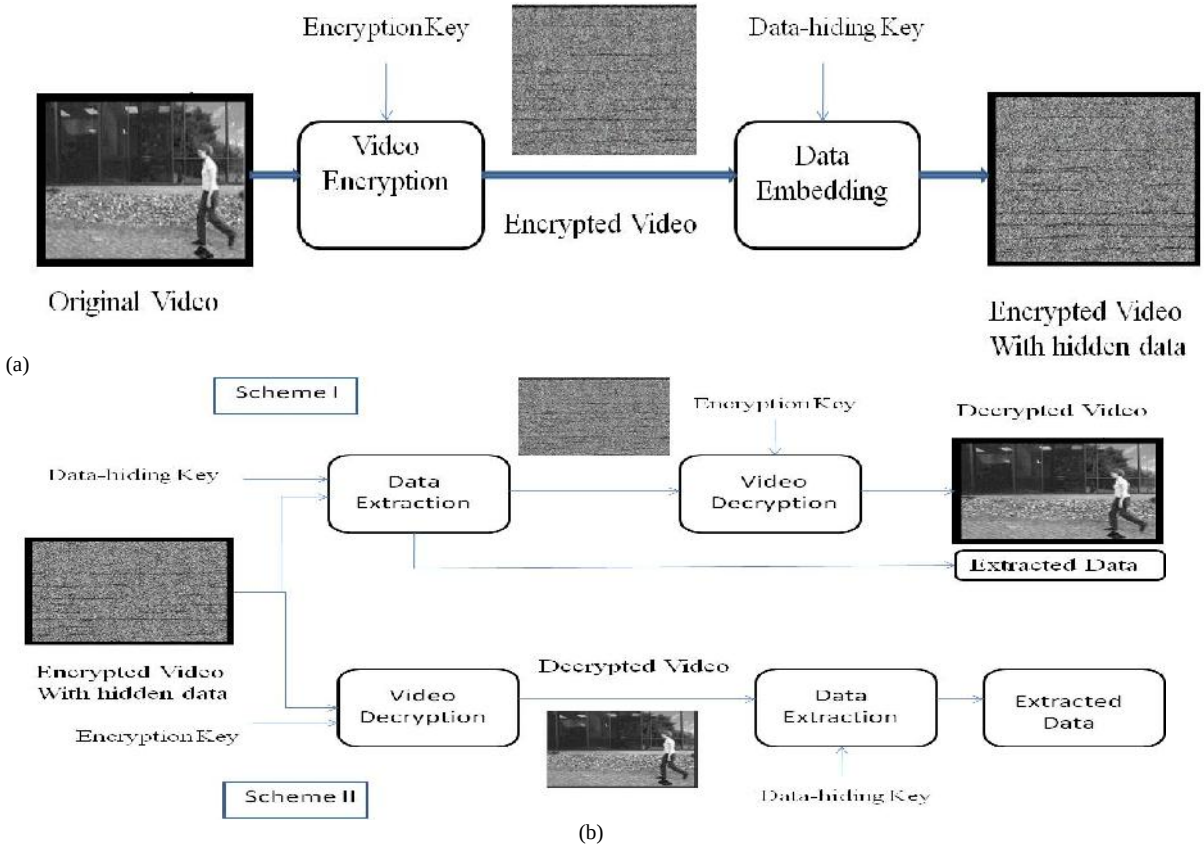

Fig. 1. Diagram of proposed scheme [14].

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 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.

Data Embedding

Steganography method which is frequently used for data hiding is the technique of LSB substitution. Every pixel of gray-level image consists of 8 bits. One pixel can hence display 256 variations. In LSB substitution technique, confidential data is embedded at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly. Data Hiding is the process of secretly embedding information inside a data source without changing its perceptual quality. Data hiding is a process to conceal secret message bits into another medium like image, audio or video files. Here, the hiding is performed under compressed bit stream of video frame. After obtaining bit streams, it is allowed to encrypt it with random binary string using bitxor operation. The text message will be encrypted before data hiding using chaos encryption technique to make second level security during transmission. Bits wrap method is used here to conceal secret text bits under encrypted compressed bit streams. It is performed using logical bitwise operations like 'bitand' and 'bitor' operations. After embedding the data, image reconstruction and data extraction will be performed to measure the system performance.

Data Extraction

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

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.

RESULTS AND DISCUSSION

The proposed data hiding scheme has been implemented and simulated on Matlab. Standard video sequences in QCIF format (176 × 144) at the frame rate 30 frames/s are used for simulation. GOP (Group of Pictures) structure is "IPPPP: one I frame followed four P frames".

The proposed video encryption scheme includes both cryptographic security and perceptual security. Cryptographic security provides the security against cryptographic attacks, which depends on the ciphers adopted by the scheme. In the proposed method, the secure stream cipher (e.g., RC4) is used to encrypt the bitstream, and chaotic pseudo-random sequence generated by logistic map is used to encrypt the additional data. They have been proved to be secure against cryptographic attacks.

Fig.2. Original Video Frames

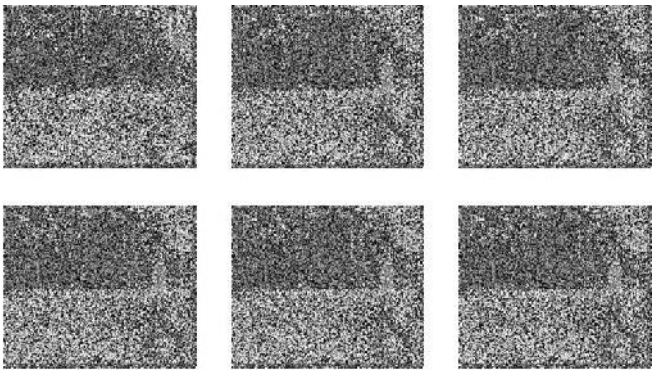

Fig.3. Encrypted Video Frames With Hidden Data

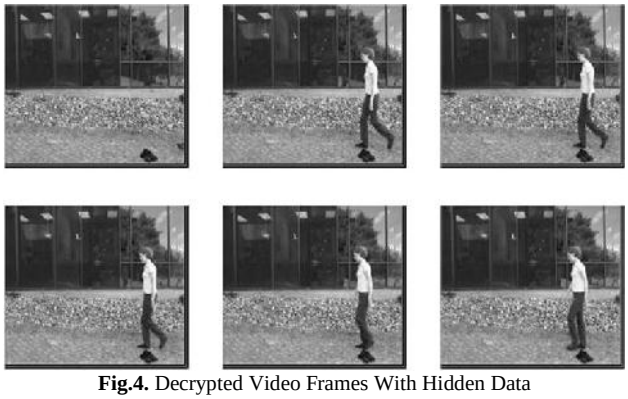

Fig.4. Decrypted Video Frames With Hidden Data

Perceptual security refers to whether the encrypted video is incomprehensible or not.Generally, it depends on the properties of encryption scheme. The proposed scheme encrypts IPM, MVD and residual coefficients, which maintains perceptual security of the encrypted video. The demonstration is shown in Figs. 2 and 3. The encrypted and decrypted video frames with hidden data are shown in Figs 2 and 3 respectively. In the experiments, no visible artifacts have been observed in all of the decrypted video frames with hidden data as shown in fig 4.

CONCLUSION

Data hiding in encrypted media is a new topic that has started to gain more attention because of the privacy-preserving requirements from cloud data management. In this paper, an algorithm to embed additional data in encrypted H.264/AVC bitstream is presented, which consists of video encryption, data embedding and data extraction phases. The algorithm is simple to implement as it is directly performed in the compressed and encrypted domain, i.e. it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications. Experimental results have shown that the proposed encryption and data embedding technique can preserve file-size, whereas the degradation in video quality caused by data hiding is quite small.

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. & Comm. 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.

****