International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 12 | Dec 2018 www.irjet.net p-ISSN: 2395-0072

Data Hiding in Video Stream by Efficient Data Embedding

MS. Rupali Wankhade[1], Dr.G.R.Bamnote[2], Ms. S.W. Ahmad[3]

[1]ME FT Final Year, Computer Science & Engineering, P.R.M.I.T&R,Badnera
[2]Head & Professor, Dept.Computer Science & Engg, PRMIT&R, Badnera, Amravati
[3]Astt. Professor, Dept.Computer Sci. & Engg, PRMIT&R, Badnera

---

ABSTRACT - *Nowadays the need for security is becoming more important due to increased security requirements, data security is mostly provided with data hiding. It is an encrypted domain without decryption preserves the confidentiality of the content. In addition, it is more efficient without decryption followed by data hiding and re-encryption. In the novel scheme of data hiding directly in the encrypted version of H.264/AVC video stream, divided into three parts, which is H.264/AVC video encryption, data embedding, and data extraction with the help of data hiding code word technique. The cloud server can manage the video or verify its integrity without knowing the original contents, and thus to provide security and protection. A user can hide a data and may embed additional data in the encrypted domain by using substitution technique named code word. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. Furthermore, video file size is strictly preserved even after encryption and data embedding.*

KEYWORDS: *Data Hiding in Encrypted, codeword Substituting, H.264/AVC Video Streams.*

I. INTRODUCTION

It's known to all that cloud computing has become a crucial technology, which can provide highly efficient computation and large-scale storage solution for video bits/bytes. Given that cloud services may attract more attacks and are vulnerable to unreliable system administrators, it is desired that the video content is invoked in encrypted form. The capability of performing data hiding directly in encrypted H.264/AVC video streams would hide of video content, which provides high security and privacy with cloud computing. For example, a cloud server can add the additional information (e.g., video notation, or authentication data) into an encrypted version of an H.264/AVC video by using data hiding technique. With the secure information, the server can handle the video or verify its integrity without knowing the original content, and thus the security and privacy can be protected. In advance feature to cloud computing, this technology can also be connected to other 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. Obviously, due to the constraint of the underlying encryption, it is very difficult and sometimes impossible to convert the existing data hiding algorithms to the encrypted domain. The proposed scheme can achieve good performance in the three different ways.

- The data hiding is performed directly in encrypted H.264/AVC video bit-stream.
- This scheme can ensure both the format compliance and the strict file size preservation.
- This scheme can be applied to two different applications by retrieving the hidden data it can either encrypted video stream or may be the decrypted video stream.

2. LITERATURE SURVERY

There are number of methods used for data encryption and data hiding/embedding. Different research work can perform by many institude. To gives detail review on various methods of video encryption and data embedding. The related works in reversible data hiding techniques are as follows:

In J.Tian [1] introduced a difference expansion technique. The data embedding was discovers by exploring the redundancy in the image. This technique was best in all the technique of literature survey because the holding capacity of secret data and the visual quality of embedded images.

W.Kuo et al. [2] proposes an adaptive reversible data hiding method. A new scheme based on histogram and slope method enhancing the data hiding capacity and also the efficiency increases and maintains the high quality of image.

K.Ming et al. [3] propose the method which has the combination of data hiding, half-toning and vector quantization technique. The embedding of gray scale image in other image was done. This scheme work as follows: a) Image compression from gray scale to half tone using half-toning process. b) Computation of

difference between original image and the image on which we perform operations. c) Then VQ compression compress the difference obtains in above and embed it with secret data. Jose et al. [4] proposed the method in which a reversibly data hiding in encrypted gray scale image was done in separable manner. Encryption of the image was done by content owner use encryption key by permuting the pixels. Data hiding was done by using data hiding key using histogram modification method. M.Naor et al. [5] introduced the visual cryptography. The proposed scheme can the combination of reversible data hiding and colour visual cryptography.

S.Malik and et al. [6] has proposed another different approach for visual cryptography which has three steps: 1.Sieving 2.Division 3.Shuffling to generate random shares. The advantage was minimum computation requirement to generate the binary secret image without loss of quality of image.

K.Kang et al. [7] introduces a new method which produces the colorful meaningful shares based on pixel synchronization and halftoning of error diffusion. W.Qiao et al. [8] proposed a novel method of visual cryptography based on halftone for visual cryptography. There are three main steps involved and they are as follows: first chromatic image was dissolved into three monochromatic images having tone cyan, magenta and yellow. Secondly transformation of these three images into binary image was done using halftone technique. Next to that to get sharing images the traditional binary sharing scheme was used.

Y.Chen et al. [9] has proposed another different approach for visual cryptography was authentication mechanism. In following two procedures:

a) Encryption procedure

b) Decryption procedure

3. PROPOSED SYSTEM

A 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

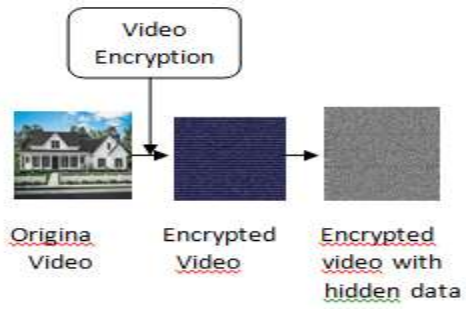

fig a: Encryption and Data embedding

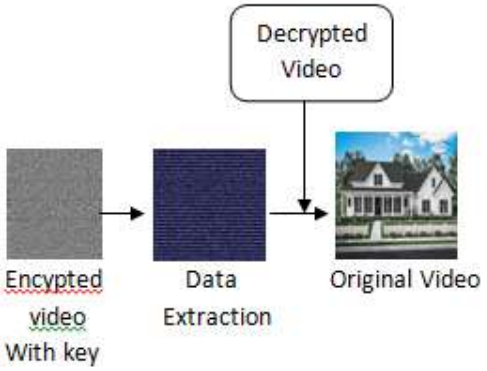

Fig b: Data Extraction And Video Decryption

video stream and 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, 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. In the 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 was not desirable to encrypt the whole compressed video bit stream like what the traditional ciphers to do because of format compliance and computational cost. Alternatively, only a fraction of video data is encrypted to increase the efficiency and to gain security. The key issue was how to select the sensitive data for encryption. According to [13], it was reasonable to encrypt both spatial information (IPM and residual data) and motion information (MVD) during H.264/AVC encoding. H.264/AVC video encryption technique 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 bitstreamis modified directly. B. Data Embedding in the encrypted bitstream of H.264/AVC, the proposed data embedding was done by codeword substitution technique. Eligible codewords of Levels are substituted for data embedding. Since the sign of Levels was encrypted, it was desired that data hiding should not affect the sign of Levels.

B. Besides, the codewords substitution should satisfy the following three limitations, Firstly, the bit stream 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 same as that of the original codeword. Third, impact of visual degradation caused by data hiding should be kept to minimum. Then embedded data after video decryption has to be invisible to a human observer. The 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, a database manager (e.g., cloud server) only get access to the data hiding key and to manipulate data in encrypted domain. Data extraction in encrypted domain has guarantees the feasibility of proposed scheme. 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. Sometime 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.

4. CONCLUSION

The recent technology in Data hiding is hiding data in encrypted video it has started to pay an attention to the storage and privacy requirements from cloud server. An algorithm is used to embed additional information in encrypted H.264/AVC bit stream presented, which have the video encryption, data embedding and data extraction stages. The bit-rate is preserved by an algorithm exactly even after encryption and data embedding, also simple to implement as it is directly performed in the compressed and encrypted domain, that is it does not require decrypting or partial decompression of the video stream thus making it ideal for real-time video applications. Additional data is been added by the data hider into the encrypted bit stream using codeword substituting, even though the original information content are not known. Besides the data hiding process is completed entirely in the encrypted domain, it can preserve the confidentiality of the content completely. With an encrypted video containing hidden data, data extraction can be carried out either in encrypted or decrypted domain, which provides different practical applications. The encryption and data embedding scheme can proposed preserve file-size. Then there are so many applications by data hiding in encrypted domain such as Content authentication , Copyright Protection, Broadcast monitoring, Finger printing, Metadata binding, Covey communication.

5. REFERENCES

[1] Jun Tian, "Reversible Data Embedding Using a difference Expansion", IEEE Transaction , Vol.13, No. 8, Aug 2003

[2] Wen Chung Kuo, Po Yu Lai, LihChyauWuu, "Adaptive Reversible Data Hiding Based on Histogram", 10th International Conference on Intelligent Systems Design and Application, l' IEEE 2010 (2002) The IEEE website.[Online]. Available: http://www.ieee.org/

[3] Kuo-Ming Hung, Wen-Kai Su, Ting-Wen Chen, Li-Ming Chen, "Reversible Data Hiding Base on VQ and Halftoning Technique", International Conference on Microelectronics, Communication and Renewable Energy (ICMiCR-2013).

[4] Jose, R.; Abraham, G, "A separable reversible data hiding in encrypted im age with improved performance", Emerging Research Areas and 2013 International Conference on Microelectronics, Communications and Renewable Energy(AICERA/ICMiCR), 2013 Annual International Conference l'IEEE 2013.

[5]MoniNaor, Adi Shamir," Visual Cryptography", in Proc. EUROCRYPT'94, Berlin, Germany, 1995, vol. 950, pp. 1-12,Springer-Verlag, LNCS

[6] Siddharth Malik, Anjali Sardana, Jaya, "A Keyless Approach to Image Encryption", 2012 international conference on Communication systems and Network Technologies l'2012 IEEE

[7] InKoo Kang, Gonzalo R. Arce , Heung-Kyu Lee, " Color Extended visual cryptography using error diffusion", ICASSP 2009 l' IEEE 2009

[8] Wei Qiao, HongdongHuaqing Liang, "A kind of Visual Cryptography Scheme For color Images based on halftone technique", International Conference on Measuring Technology and Mechatronics automation l' 2009 IEEE

[9] Yi-Hui Chen, Ci-Wei lan and Chiao Chih Huang, " A verifiable Visual Cryptography Scheme", Fifth International Conference and Evolutionary Computing l' IEEE 2011