International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 4, April 2016

Data Hiding in Encrypted H.264/AVC Video Streams by Code word Substitution

[1] Shraddha Arun Dangare [2] Meenal Ravindra Pathak [3] Sayali Narayan Mahamulkar [4] Chandrama Thorat
[1][2][3][4] Computer Department
JSPM's Rajarshi Shahu College of Engineering (RSCOE), Pune, India
[1] shraddhadangare9@gmail.com [2] meenalpathak1@gmail.com [3] sailee.m43@gmail.com
[4] chandrama1684@gmail.com

***Abstract*: As we know, in the field of Computer Science, Cloud computing is a very important as well as rapidly developing technology trend. To maintain security and privacy in the encryption domain the digital videos need to be stored and processed. To avoid content notation and interfering detection, it is compulsory to perform data hiding in these encrypted videos. Thus the confidentiality of the content/text is preserved using Data Hiding in encrypted domain without decryption. It is more efficient to perform it without decryption which is followed by data hiding and re-encryption. Here, a scheme of data hiding in an encrypted version of H.264/AVC video stream is proposed, which includes important 3 parts, viz., data embedding and abstraction and H.264/AVC video encryption. With the help of the property of H.264/AVC codec, the encryption with stream ciphers is done using the following code words: the code words of intra prediction modes, the code words of motion vector differences, and the code words of residual coefficients. In this technique without knowing the video content a data hider can encode additional data in the encrypted domain by using code word substitution technique. There are two aspects for data extraction in which data can be extracted either in the encrypted domain or in the decrypted domain. Even after encryption and data embedding, video file size is strictly preserved. Experimental results have demonstrated the feasible as well as efficient proposed scheme.**

***Keywords*— Data hiding, encrypted domain, H.264/AVC, code word substitution.**

I. INTRODUCTION

The project is data hiding in Encrypted H.264/AVC Video Streams by Code word Substitution. This project is to provide safe way for transferring sensitive information through video. It is basely designed for digital video and data hiding. The system is divided into three parts respectively:- H.264/AVC video encryption, Data Embedding, Data Extraction. H.264/AVC is recent video coding standard of the Video Coding Experts Group and the ISO Moving Picture Experts Group. The main goals of the H.264/AVC standardization efforts have been enhanced compression performance and provision of a network friendly video representation for applications. H.264/AVC has achieved a significant improvement in rate-distortion efficiency relative to existing standards. Data Embedding should be embed the additional content that is data in a encrypted video by using code word substitution technique without knowing the contents of the video. Data extraction takes place in two parts respectively. Data extraction takes place by extracting the contents which are embedded in the encrypted video. Video decryption should take place after the data extraction by using encryption key.

II. RELATED WORK

W. Hong, T. S. Chen, and H. Y. Wu have proposed that most of the work on reversible data hiding focuses on the data embedding/extracting on the plain spatial domain. The five MSBs of each pixel of the decrypted image will be identical to those of the cover image. According to the data-hiding key, it is easy for the data hider to reversibly embed data in the encrypted image. Thus the data hider can benefit from the extra space Emptied out in previous stage to make data hiding process effortless.

In the field of video, W. Puech , Z. Erkin, M. Barni, S. Rane proposed SE of H.264 video is proposed by doing frequency domain selective scrambling, DCT block shuffling and rotation. It performs SE by pseudo-randomly inverting sign of DCT coefficients in Region of interest. A scheme for commutative encryption and
Watermarking of H.264/AVC. Here SE (selective encryption) of some MB header fields is combined with watermarking of magnitude of DCT coefficients but they are not format compliant. SE scheme based on H.264/AVC has been presented on CAVLC and CABAC for I and P frames .This method fulfills real-time constraints by keeping the same bit rate and by generating a completely compliant bit stream.

III. SYSTEM ARCHITECTURE

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.

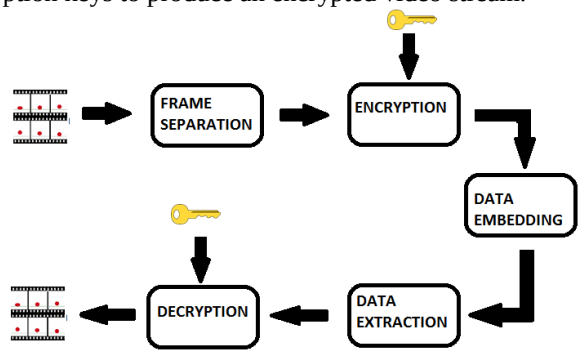

Fig. System Architecture

Then, the data-hider can embed the additional data into the encrypted video stream by using code word 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 version. Encryption and data embedding are depicted and the data extraction and video decryption done by using CAVLC algorithm & RC6 algorithm.

A. *Data Embedding:*

In the encrypted bit stream of H.264/AVC, the proposed data embedding is accomplished by substituting eligible code words. On the other hand, the code words substitution should fulfill the following three limitations. First, the bit stream 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. The code words of Levels which suffix Length is 2 or 3 would be divided into two opposite code spaces denoted as C0 and C1. The code words assigned in C0 and C1 are associated with binary hidden information “0” and “1”. Suppose the additional data that we want to embed is a binary. Third, data hiding does cause visual degradation but the impact should be kept to minimum. That is, the embedded data after video decryption has to be invisible to a human observer.

B. *Encryption of H.264/AVC Video Stream:*

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. Compared with, the proposed encryption algorithm is performed not during H.264/AVC encoding but in the H.264/AVC compressed domain. In this case, the bit stream will be modified directly. Selective encryption in the H.264/AVC compressed domain has been already presented on context-adaptive variable length coding (*CAVLC*) and context-adaptive binary arithmetic coding (*CABAC*). In this paper, we have improved and enhanced the previous proposed approach by encrypting more syntax elements. We encrypt the code words of IPMs, the code words of MVDs, and the code words of residual coefficients. The encrypted bit stream is still H.264/AVC compliant and can be decoded by any standard-compliant H.264/AVC decoder, but the encrypted video data is treated completely different compared to plaintext video data. In fact, performing the format-compliant encryption directly on the compressed bit stream is extremely complicated as the internal states of the encoder have to be preserved, otherwise the remaining data is interpreted falsely which may easily lead to format violations.

IV. CONCLUSION

The existing system just addresses the calculation of smoothness and the process of image recovery and lacks in addressing the data encryption & data embedding process. Time consumption rate is also high when compared to the recent methods developed. The block encryption methods are not robust to noise. 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. An algorithm is used to embed additional data in encrypted H.264/AVC bit stream, which consists of video encryption, data embedding and data extraction phases.

The data-hider can embed additional data into the encrypted bit stream using code word substituting, even though he does not know the original video content. Since data hiding is completed entirely in the encrypted domain, here we can preserve the confidentiality of the content completely.
Reversible data hiding in encrypted images is a new topic getting attention because of the secured environmental requirements. Data hiding in reversible manner in encrypted images is providing double security for the data such as image encryption as well as data hiding in encrypted images both are done here.

REFERENCES

[1] J. G. Jiang, Y. Liu, Z. P. Su, G. Zhang, and S. Xing, "An improved selective encryption for H.264 video based on intra prediction mode scrambling," *J. Multimedia*, vol. 5, no. 5, pp. 464–472, 2010.

[2] D. K. Zou and J. A. Bloom, "H.264 stream replacement watermarking with CABAC encoding," in *Proc. IEEE ICME*, Singapore, Jul. 2010, pp. 117–121.

[3] D. W. Xu and R. D. Wang, "Watermarking in H.264/AVC compressed domain using Exp-Golomb code words mapping," *Opt. Eng.*, vol. 50,no. 9, p. 097402, 2011.

[4] D. W. Xu, R. D. Wang, and J. C. Wang, "Prediction mode modulated data-hiding algorithm for H.264/AVC," *J. Real-Time Image Process.*,vol. 7, no. 4, pp. 205–214, 2012.

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