Data Embedding Scheme in Video Streamiing Encrypted Domain

Mestry Dipti
M.E. student,
Department of Electronics and Telecommunication
Alamuri Ratnamala Institute of Engineering and Technology, Asangaon.

Prof. R.D. Patane
H.O.D,
General Engineering Department,
Terna College of Engineering, Navi Mumbai

Abstract — **To maintain security and the privacy of digital video during transmission over the internet from the untrustworthy system administrators, the videos are encrypted. The encryption adds to the confidentiality and the integrity of the video. A novel method is proposed where secret data is directly embedded into the compressed and encrypted H.264/AVC bit stream. This includes three parts i.e. H.264/AVC video encryption, data embedding and data extraction. The codewords of the IPM (Intra Prediction Mode), the codewords of MVD (Motion Vector Difference) and the codewords of the residual coefficient are encrypted with stream ciphers. The data hider can then embed secret information into the encrypted video by using codeword substitution method without knowing the content of the original video. At the receiver end, the embedded data can be extracted either in encrypted or decrypted domain. We also compute PNSR, SSIM and VQM to validate the feasibility and efficiency of the proposed work.**

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

I. INTRODUCTION

With the ever increasing usage of the internet, multimedia, cloud computing has become an important technology trend. This provides large storage solution for video data but also attracts more attack and is prone to untrustworthy system administrators, H.264/AVC; a video compression format (1) is standard for high definition digital video. The capability of hiding data directly in encrypted H.264/AVC video streams , avoid leakage of video content, that helps in addressing the security and privacy concerns (2), (medical videos, surveillance videos etc,) with the ever increasing concept of cloud computing. In this paper data is hidden directly in the encrypted version of H246, video stream. This includes three stages, of H.264/AVC video encryption, data embedding and data extraction. Here by studying the properties H.264/AVC codec, the codewords of IPM's, codewords of MVD's and the codewords of residual coefficients are encrypted using a stream cipher. The encryption algorithm is then combined with Exp-Golomb entropy coding and Context adaptive variable length coding (CAVLC) (3); this helps in keeping the codeword length unchanged. Using codeword substitution method the data is hidden in the encrypted domain. This method ensures both the format compliance and strict file size preservation also the hidden data can be extracted from either the encrypted video stream or from the decrypted video stream.

II. LITERATURE SURVEY

Some successful data hiding schemes in encrypted domain have been reported in the open literature such as watermarking scheme in encrypted domain using Pallier cryptosystem (4), similarly Walsh-Hadamad transform based image watermarking algorithm using Pallier cryptosystem in encrypted domain has been reported in (5). But due to constraints of Pallier cryptosystem, the encryption of the original image results in increase amount of the storage and computation. A robust watermarking algorithm is also proposed in (6) to embed the watermark into the JPEG 2000 compressed and encrypted images. But as it can be seen the above mentioned works are focused on image and not on video.

With regards to the various methods of video encryption and data embedding, Spyridon K. Kaptos, Eleni E. Varsaki and Athanassios N. Skodras proposed a method taking advantages of various block sizes of H.264 / AVC encoder during the interprediction stage to hide the desired data. In this method the data can be reconstructed directly from encoded stream. Here, the motion estimation process aims to find out the closest macroblock of current frame. Then, each macroblock within the current frame is motion compensated i.e. its best match is subtracted from it and the residual macroblock is coded. The encoder selects the block type from the standards of H.264 such as 4x4, 4x8, 4x16, 16x4, 16x8, 16x16, and 8x8 as per the requirement data to be embedded than the coding efficiency.

A combined scheme where in encryption and water marking both provides for authentication of the video content is described in (8). The IPM's of 4x4 luminance block, the sign bits of texture, sign bits of MVD's are encrypted, while IPM is used for watermarking. However, the standard of decoder may crash as it cannot parse a not format compliant watermarked bit stream. In other methods such as (8) and (9) the encryption and watermark are embedded in the encoding process while during decoding process decrypting and watermark detection is accomplished. Here, the encryption and watermark embedding may increase the bit rate of H.264 / AVC bit stream. Hence, it was stressed to develop data hiding algorithm that can work on encoded bit stream and that too in encrypted domain. To achieve this following challenges are to be meet with: 1. Determining how the bit stream can be modified so that the encrypted domain can still be a compliant compressed bit stream with the data hidden in it. 2. The decrypted video should have high visual fidelity even with hidden data. 3. Maintaining the file size after encryption and data hiding. 4. To be able to extract the data either from the encrypted video stream or from decrypted video stream.

III. EXISTING SYSTEM

The existing system is indicated in the Fig -1 and Fig – 2.

A. Encryption in H.264 / AVC video steam

By analyzing the three sensitive codec i.e. IPM's, MVD's and residual coefficients of H.264 / AVC we encrypt the code word of IPM's, MVD's and residual coefficients. The encrypted bit stream is still H.264 /AVC compliant and can be decoded by any standard H.264 / AVC decoder. The IPM's , MVD's and residual coefficients are encrypted with the stream ciphers in compressed domains and not during encoding H.264 / AVC, selective encryption in H.264 / AVC in compressed domain has been presented on CAVLC and CABAC i.e. Context adaptive length coding and context adaptive binary arithmetic coding respectively as mentioned in (10) and (11). While performing format compliant encryption on the compressed bi stream the internal states of the encoder are to be preserved (12) otherwise the remaining data is interpreted as false and may lead to format violations.

a. Intra-Prediction Mode (IPM) Encryption – Four types of intra coding types are supported as H.264 / AVC standard, they are Intra_4x4, Intra_16x16, Intra _chroma and I_PCM (3). IPM's in the Intra_4x4 and Intra_16x16are chosen to encrypt. In Intra_16x16 four intra prediction modes (IPM's) are available. IPM for Intra_16x16 is specified in mb_type i.e. macroblock type field. The mb_type values are taken from the standard. The mb_type is encoded with the Exp-Golomb code. Care is taken to encrypt the codeword of IPM without changing its CBP. Also the encrypted codeword should have the same size as the original. Hence each Intra_16x16 block, encryption is done by performing a bitwise XOR between the last bit of the codeword and the pseudo-sequence. We can say that in the entire IPM encryption changes actual mode to other mode without harming the bit stream compliance.

b. Motion Vector Difference (MVD) Encryption – The motion vector of the H.264 / AVC are also encrypted to protect the motion information. Exp–Golomb entropy coding (13) is used for encoding of motion vector differences. Here too, the encryption process takes care that the resulting cipher text are format compliant and the length of the codeword remains unaltered.

c. Residual Data Encryption – For the security to be maintained, the residual data in both the I-frames and P-frames are encrypted. CAVLC entropy coding is used for encoding the quantized coefficients of residual block (13). As it is not possible to modify all the elements, only codewords of sign of trailing ones and levels are modified where '0' is assigned for '+' and '1' for '-'. Hence once again the encryption keeps the codeword format compliant and its length unchanged.

B. Data Embedding

Code word substitution method is used for embedding the data into the encrypted bit stream. The method satisfies the following:

1. After codeword substitution the syntax of the bit stream remains the same, so that it can be decoded by standard decoder.
2. The substituted codeword length remains same as original.

3. The visual degradation that may be caused due to data embedding should be limited to minimum.

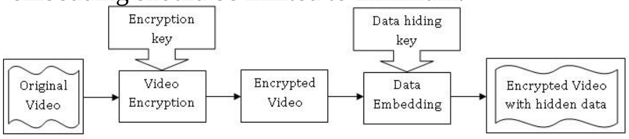

Fig – 1 Video encryption and data embedding

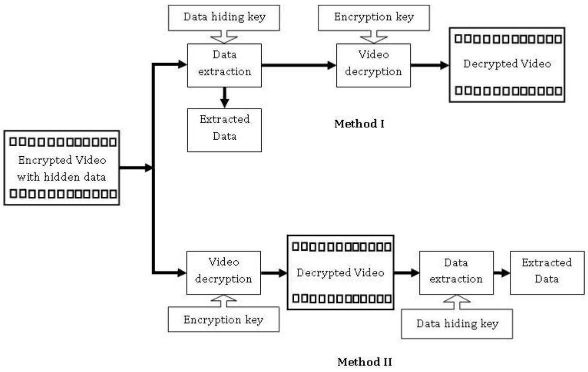

Fig – 2 Data extraction and video decryption

C. Data Extraction

The data extraction process is simple and fast. In given figure, the original video is encrypted using an encryption key. Here, the bit XOR (exclusive OR) operation is used to perform the encryption. Codeword substitution method is used for hiding the data. So, we get an encrypted video with hidden data in it. This process is accomplished at the sender's end.
Similarly, we can see in the Fig – 1 and Fig - 2 the same process is indicated from the receiver's end.

The data that is hidden can be extracted by either of the mentioned methods:
Method 1- Extracting the data in within encrypted domain - In this scheme the data hidden is extracted first and then using the key the video is decrypted. After decryption we get the original video.

Method 2 - Extracting the data in within decrypted domain – Using the key the video is decrypted first and after that the data which is hidden is extracted. After this we get original video.

IV. PROPOSED SYSTEM

In the proposed system the video will be compressed after data hiding. The compression of the data in the video can be of two types: lossy and lossless compression. We will be using arithmetic compression method for compressing the amount of data stored in the video.

A. Arithmetic Compression

Arithmetic compression is an entropy coding technique used in lossless data compression, in which frequently occurring or seen symbols are encoded with fewer bit than the less frequently occurring or seen symbols. It converts a message or a file which is composed of symbols to a floating point number greater than or equal to zero and less than one. Basically it depends on a model to characterize the symbols it will be processing for compression. The model will tell the encoder the probability of a character is in the given message; if given the accurate probability, the characters will be encoded optimally else the encoder may expand a message rather than compressing it!

As shown in the Fig – 3 arithmetic compression will be performed on the video after encryption and data hiding or embedding. Similarly at the receiving end the video will be decompressed as mentioned in method 1 or method 2. The advantage of implementing arithmetic compression is that the bandwidth of the video will decrease which will aid in easy transmission of the video.

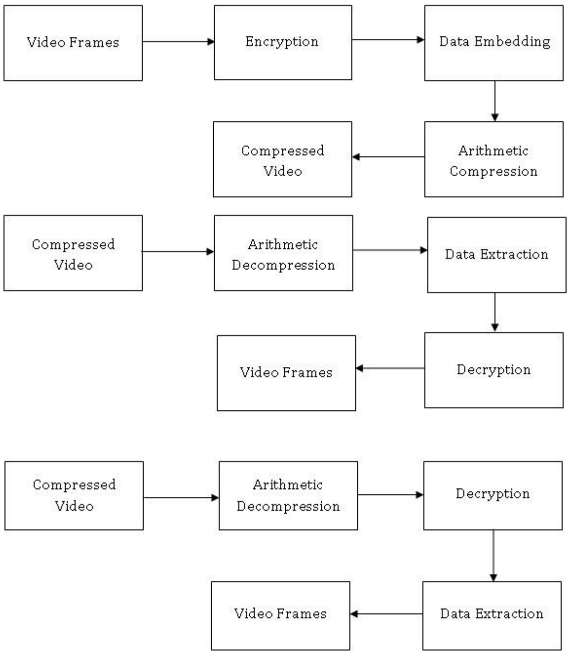

Fig – 3 Proposed method using arithmetic compression for video compression

V. CONCLUSION

The data embedding in the H.264/AVC video stream can be done in the encrypted form too, hence providing maximum benefit of the confidentiality. Even the data extraction can be done either in the encrypted or decrypted domain. Hence, the objective of hiding the data while preserving the confidentiality and file size is achieved with small degradation in the quality of the video.

ACKNOWLEDGMENT

I would like to acknowledge Prof. R.D. Patane, for guiding me throughout the project development.

REFERENCES

[1] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A. Luthra, “Overview of H.264/AVC video coding standard,” IEEE Trans. Circuits Systs. Video Technol., vol. no. 13, no.7, pp. 56-576, Jul. 2003.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras “Data Hiding in H.264 Encoded Video Sequences” in IEEE trans, 2007.

[8] 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.

[9] 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.

[10] Z. Shahid, M. Chaumont, and W. Puech, “Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 5, pp. 565–576, May 2011.

[11] M. N. Asghar and M. Ghanbari, “An efficient security system for CABAC bin-strings of H.264/SVC,” *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 3, pp. 425–437, Mar. 2013.

[12] 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.

[13] I. E. G. Richardson, *H.264 and MPEG-4 Video Compression: Video Coding for Next Generation Multimedia*. Hoboken, NJ, USA: Wiley, 2003.