International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 571 - 574

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

Juhi Rohara, V.B. Gaikwad, Terna Engineering College, Navi Mumbai
juhirohara26@gmail.com, vb_2k@rediffmail.com

Abstract – The paper proposes data hiding with codeword substitution in encrypted H.264/AVC video streams. Here video is encrypted and data is hided in the video to maintain the security and privacy. In this way data hiding in encrypted domain without decryption preserves confidentiality of the content. By analyzing the property of H.264/AVC codec, the codeword of the intra-prediction modes, the code words of motion vector differences and code words of residual coefficients are encrypted with the stream ciphers. The data hider may embed additional data in the encrypted domain by using code word substitution technique, without knowing original content. Data extraction can be done in encrypted domain or in the decrypted domain.

Index Terms *- Data hiding, encrypted domain, H.264/AVC, codeword substituting.*

*****

I. INTRODUCTION

H .264/AVC [1] video coding standard has been developed and standardized collaboratively by both the ITUT VCEG and ISO/IEC MPEG organization. H.264/AVC is a video compression format [2] i.e. standard for high definition digital video. H.264/AVC video streams generally avoids leakage of video content which can help to address the security and privacy concerns with cloud computing. Similarly when medical videos or surveillance videos are encrypted for protecting the privacy of the people, a database manager can embed the personal information into the corresponding encrypted videos to provide the data management capabilities in the encrypted domain. With the increasing demands of providing video data security and privacy protection data hiding in encrypted H.264/AVC videos are becoming popular.

A. Motivation

The H.264 video coding standard has been created and institutionalized cooperatively by both the ITU-T VCEG and ISO/IEC MPEG associations. H.264/AVC speaks to various advances in standard video coding innovation, as far as both coding proficiency improvement and adaptability for powerful use over a wide assortment of system sorts and application spaces H.264/AVC is a video pressure design i.e. standard for high definition (HD) advanced video.

B. Objective

The fundamental target is to upgrade pressure execution and gives a procurement of a system well-disposed video representation tending to conversational applications. H.264/AVC has accomplished a critical upgrades in rate mutilation productivity with respect to existing gauges H.264/AVC covers all basic video conferencing and high definition (HD) video stockpiling. To address the requirement for adaptability and adaptability, the H.264/AVC outline covers a video coding layer (VCL), which is intended to productively speak to the video content, and a network subtraction layer (NAL) which designs the VCL representation in a way suitable for movement by an assortment of transport layer or capacity media. With respect to earlier video coding strategies, as exemplified by MPEG-2 video, some highlighted elements of the configuration that empower improved coding productivity incorporate the accompanying upgrade of the capacity to foresee the estimations of the substance of a photos to be encoded.

1. Variable block size motion compensation with small block sizes.
2. Quarter sample accurate motion compensation.
3. Motion vectors over picture boundaries.
4. Multiple reference picture motion compensation.
5. Decoupling of reference order from display order.
6. Decoupling of picture representation methods from picture referencing capability.
7. Weighted prediction
8. Improved skipped and direct motion inference.
9. Directional spatial prediction for intra coding.
10. In the loop de-blocking filtering.

II. LITERATURE SURVEY

There are several methods and devices used to data encryption and data embedding in video stream. Several research works are being performed by many institutions throughout the world to offer the best scheme in terms of cost effectiveness. This section gives a brief review on various methods of video encryption and embedding.

A. Encryption & Modified Watermarking Scheme

In the year 2007, the creators S. G. Lian, Z. X. Liu, and Z. Ren [3] proposed the commutative encryption watermarking plans for video streams pressure. The paper proposed the consolidate methodology of encryption and watermarking to give classification and proprietorship. Proposed Encryption Scheme performs the encryption of both movement and surface data, by considering MVD encryption (Motion Vector bearing) and IPM encryption (Intra Prediction mode). Amid H.264/AVC pressure the intra-expectation mode, movement vector distinction and discrete cosine change coefficients are encoded. After encryption watermarking happens on DCT coefficients. As the customary watermarking operation influences the unscrambling operation, implies the watermark can't be separated without decoding of the substance. Consequently paper proposed adjusted watermarking calculation which makes the change of conventional watermarking calculation. The watermark can be removed from the scrambled area; in

this manner it saves the secrecy of the substance. The disadvantage of this paper is that the first substance is initially watermarked and then watermarked substance is scrambled. It implies watermark can't be implanted on encoded content. The other downside is the methodologies don't work on the packed piece stream.

B. Encryption & Reversible Watermarking Scheme

To beat the disadvantage of past plan said in last passage the creators S. W. Park and S. U. Shin [4] in the year 2008 proposed reversible watermarking plan and encryption plan which was utilized to give the entrance right and the verification of the video content at the same time. The plan proposes the plans to perform the encryption of unique substance and afterward perform reversible watermarking at the same time amid pressure process. This plan likewise proposed the proficient specific encryption plan which encodes the IPM of 4x4 hinders, the sign bits of composition and the sign bits of movement vector contrast values. The Reversible watermarking plan installs the watermark into the scrambled space. The downside of this plan is, the proposed watermarking plan has tad bit overhead. The watermarked bit stream is not completely design consistent subsequently a standard decoder may crash since it can't parse watermarked stream.

C. Selective Encryption Algorithm

The creators S. G. Lian, Z. X. Liu, Z. Ren, and H. L. Wang proposed particular encryption plan [5]. Video encryption frequently requires that the plan be time effective to meet the necessity of constant and organization consistence. It is not down to earth to scramble the entire compacted video bit stream, on account of the accompanying two reasons, i.e., design consistence and computational expense. Thus, just a small amount of video information is scrambled to enhance the proficiency while as yet accomplishing sufficient security. The key issue is, the manner by which to choose the delicate information to scramble. Till now, different encryption calculations have been proposed and broadly utilized, for example, DES, RSA, IDEA or AES, the vast majority of which are utilized for content or parallel information. These calculations are hard to utilize straightforwardly for video encryption. In this manner the Selective encryption plan takes a shot at fractional encryption calculation. Amid AVC encoding touchy information as intra-forecast mode, leftover information and movement vector distinction are in part scrambled. It gives way to deal with selecting touchy information to scramble to make it time productive, secure and organize consistence. The disadvantage of this paper is that the specific encryption is performed amid H.264/AVC encoding and not on packed space.

D. Enhanced Selective Encryption Scheme

The creator Z. Shahid, M. Chaumont, and W. Puech [6] in the year 2011 proposed Selective Encryption plan which works in compacted area in light of connection versatile variable length coding and setting versatile parallel number-crunching coding. It conquers the downside of past plan. The particular encryption is performed on the entropy coding phase of H.264/AVC utilizing AES encryption calculation as a part of CFB mode, Hence it doesn't influence the bit rates and H.264/AVC bit stream consistence. The proposed strategy has the benefit of being reasonable for spilling over heterogeneous system as a result of no adjustment in bit rates.

E. Encryption scheme and Codeword Substitution Technique

The past techniques perform encryption and information implanting all the while amid H.264/AVC pressure handle and not on compacted space, hence the pressure and decompression cycle is tedious and hampers ongoing usage. Other than this, the encryption and watermark inserting would prompt increment in the bit-rate of H.264/AVC bit stream. Be that as it may, to meet the application prerequisites, it's important to perform information covering up specifically on packed piece stream in the scrambled space. To defeat the disadvantages of past plan, The creator D. Xu, R. Wang,& Yun Q Shi [7] in the year 2014 proposed Codeword substitution procedure, an information concealing calculation that work altogether in the encoded area, and along these lines jelly classification of the substance. The proposed philosophy for video encryption is to utilize standard stream figure (RC4) with encryption keys. What's more, after video encryption, code word substitution procedure produces pseudo-arbitrary arrangement as information concealing key and implant the information into the scrambled video stream without knowing the first substance. By making the comparative analysis with the previous papers, this paper [7] achieved a better performance in following aspect:

1. Data hiding performed entirely in the encrypted domain
2. Preserves confidentiality of the content.
3. The schemes operate directly on the compressed bit stream.
4. The schemes can ensure both the format compliance & strict file size preservation.
5. In order to adapt to different application scenario, data extraction is possible either from encrypted domain or from decrypted domain.

Here information covering up is in the scrambled rendition of H.264/AVC recordings, which incorporates three sections i.e. H.264/AVC video encryption, information implanting and information extraction. The substance proprietor scrambles the first H.264/AVC video stream utilizing standard stream figures and encryption keys to deliver an encoded video stream. At that point, the information hider can insert extra information into scrambled video stream by utilizing the code word substitution technique, without knowing unique video content. At the beneficiary end, the concealed information extraction can be refined either in encoded or in decoded variant.

 ISSN: 2321-8169
571 - 574

III. EXISTING SYSTEM

A. *Encryption of H.264/AVC video stream:*

Video streams should be done in such a way that it should be time efficient and format compliance. It is not practical to encrypt the whole compressed video bit-stream like what the traditional ciphers do because of following two constraints i.e. format compliance and computational cost. Hence, only a fraction of video is encrypted to improve the efficiency of while achieving the adequate security. The key issue is then how to select the sensitive data to encrypt. Here we encode the both spatial information and motion information during the H.264/AVC encoding.

1) Intra-prediction mode (IPM) encryption
2) Motion vector difference (MVD) encryption
3) Residual data encryption

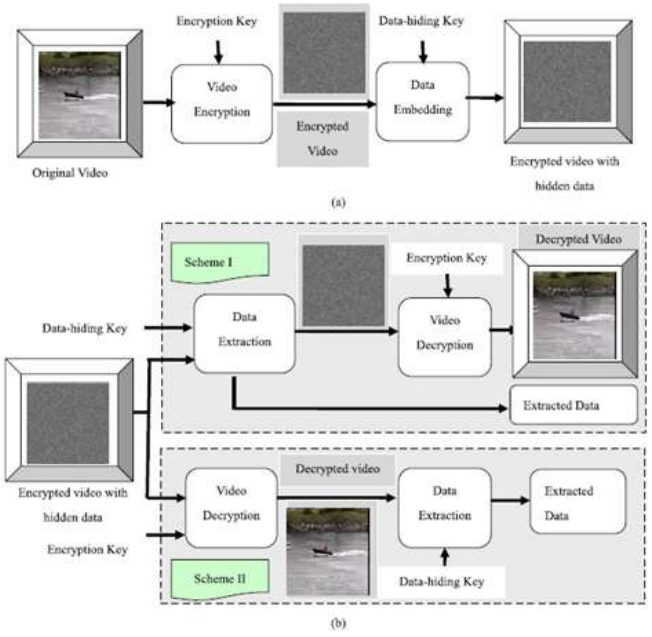

Fig - 1 a) Encryption and data embedding b) Data extraction and video decryption [7]

B. *Data Embedding:*

In the encrypted bit stream of H.264/AVC, the data embedding is accomplished by the substituting code words.

C. *Data Extraction:*

In this scheme, the hidden data can be extracted either in encrypted or decrypted domain. Data extraction process is fast and simple.

Fig1 (a) and 1(b) represents the existing method. In fig1 (a), the sender is having original video, which user encrypts with the encryption key. The encryption is performed by using bit- XOR (exclusive-OR) operation. After that data is hidden by using codeword substitution technique. Result of which is encrypted video with hidden data. All these process is done at the sender end.

In fig-1(b), process at receiver end is shown, which shows two schemes.

In fig-1(b) Scheme-1, hidden data is extracted first and by using key video is decrypted and result of which is the original video.
In fig-1(b) Scheme-2, video is decrypted first using key and after that hidden data is extracted and after that receiver will get the original video.

IV. PROPOSED SYSTEM

The proposed system will compress video after data hiding. Compression is the amount of data being stored. This can be done one of two ways, lossy compression and lossless compression. Proposed method will use the arithmetic coding. In arithmetic coding it encodes all data of data as a single fraction on interval (0,1).

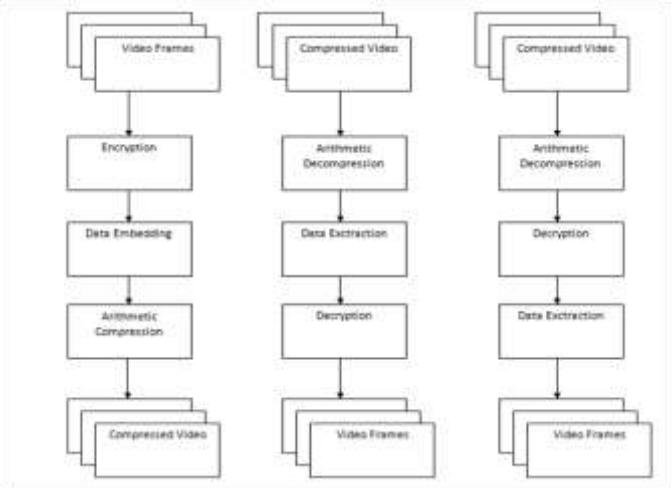

Fig - 2 proposed method with video compression

A. *Arithmetic Compression :*

Arithmetic compression is a form of entropy coding used in lossless data compression. Entropy coding is a type of lossless coding to compress digital data by representing frequently occurring patterns with a few bits and rarely occurring patterns with many bits. Normally, in arithmetic compression a string of characters such as words "hello there" is represented using a fixed numbers of bits per character as in the ASCII code. It is different from the Huffmann coding that rather than separating the input into the component symbols and replacing each with a code arithmetic coding encodes the entire message into a single number, a fraction n where $(0 \leq n \leq 1)$.

Fig-2 shows the proposed method; here sender will compress the video after performing video encryption and data hiding. At the receiver end, receiver will decompress the video first after that scheme-1 or scheme-2 which is illustrated in fig-1 can be performed. The main advantage of proposed method is that it will decrease the bandwidth so that it will be easy to transfer the video.

V. CONCLUSION

The principal goal of designing any encryption algorithm is to hide the original message and send the non-readable text message to the receiver so that secret message communication can take place. The strength of an

encryption algorithm depends on the difficulty of cracking the original message. In this paper, data is hidden by using code word substitution. The data hiding is completed by preserving confidentiality of the content and also preserves the file size.

ACKNOWLEDGMENT

I would like to acknowledge Prof. V.B. Gaikwad, for guiding me throughout the project development

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] D. Xu, R. Wang,& Yun Q Shi," Data hiding in encrypted H.264/AVC video streams by codeword substitution", IEEE Trans. Inf. Forensics Security,vol.9,No.4, pp.596-606,Apr.2014.