Impact Factor (SJIF):4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 6, June-2017

Secrete Data Hiding In H.264/AVC Compressed Video Bitstreams For Privacy Info Protection.

Bhagyashri Baburao Raut
DEPT of Electronics and telecommuncation
ME IInd year ICOER wagholi
Pune

Prof Raskar V. B
DEPT of Electronics and telecommuncation
ME IInd year ICOER wagholi
Pune

Abstract — The project presents that encryption of compressed video bit streams and hiding privacy information to protect videos during transmission or cloud storage. Digital video sometimes needs to be stored and processed in an encrypted format to maintain security and privacy. Data hiding approach is necessary to perform in these encrypted videos for the purpose of content notation and tampering detection. In this way, data hiding in encrypted domain without decryption preserves the confidentiality of the content. In additions, it is more proficient without unscrambling taken after by information covering up and re-encryption. Here, information stowing away specifically in the encoded adaptation of H.264/AVC video stream is drawn nearer, which incorporates the accompanying three sections, i.e., H.264/AVC video encryption, information implanting, and information extraction. By examining the property of H.264/AVC codec, the code expressions of intra forecast modes, the code expressions of movement vector contrasts, and the code expressions of lingering coefficients are scrambled with stream figures. At that point, an information hider may install extra information in the encoded space by utilizing bits substitution system, without knowing the first video content. Mayhem crypto framework is utilized here to scramble/unscramble mystery content information before/after information installing/extraction. So as to adjust to various application situations, information extraction should be possible either in the scrambled space or in the unscrambled area. The venture recreated comes about demonstrates that utilized techniques gives better execution as far as calculation productivity ,high information security and video quality after decoding. The parameters, for example, Mean square blunder, PSNR, relationship are assessed to quantify its proficiency.

Keywords- Data Hiding, Encrypted Domain , H.264/AVC codeword substituting.

I. INTRODUCTION

There are various works have been focused on image only few joint data hiding and encryption approaches that focus on video have been proposed. The widespread of the internet and World Wide Web has changed the way digital data is handled. Data hiding deals with the ability of embedding data into a digital cover with a minimum amount of perceivable degradation that is the embedded data is invisible or inaudible to a human observer. Data hiding consists of two sets of data namely the cover medium and the embedding data which is called the message. The digital medium or the message can be text, audio, picture, or video depending on the size of the message of the capacity of the cover .Watermarking is known to be a very difficult task robustness distortion payload ,security, complexity are many constraints to deal with. When applied to a video stream the difficulty seems to be growing into image watermarking. Video encryption has been heavily researched in the recent years. Digital videos are the very popular because of their frequency on their internet.

There are various techniques are present for hiding private data in videos. Digital video needs to be stored in encrypted format. To protect videos during transmission or cloud storage, encryption of compressed video bit streams and hiding privacy information can be done. For the purpose of content notation and or tampering these it is necessary to perform data hiding in these encrypted video.With the rapid growth of Internet and multimedia applications in distributed environments, it becomes easier for digital data owners to transfer multimedia documents across all over the world via the Internet. Therefore, multimedia security has become one of the most aspects of communications with the continuous increase in the use of digital data transmission. In addition, some applications, such as TV broadcast video in demand and video conferencing require a special and reliable secure storage or transmission of digital images and videos which may use in many applications. H.264 is the most widely-deployed video compression system and has gained a dominance comparable only to JPEG for image compression. A secure approach to encrypt H.264, also referred to as "naive" encryption approach, is to encrypt the entire compressed H.264 bitstream with the available encrypted schemes. Secure adaptation requires a scalable bitstream and specific encryption routines that preserve the scalability in the encrypted domain.

Therefore, it becomes highly desirable to develop data hiding algorithms that work entirely on encoded bitstream in the encrypted domain However, there are some significant challenges for data hiding directly in compressed and encrypted bitstream.

1. The first challenge is to determine where and how the bitstream can be modified so that the encrypted bitstream with hidden data is still a compliant compressed bitstream.
2. The second challenge is to insure that decrypted videos containing hidden data can still appear to be of high visual fidelity.
3. The third challenge is to maintain the file size after encryption and data hiding, which requires that the impact on compression gain is minimal.
4. The fourth challenge is that the hidden data can be extracted either from the encrypted video stream or from the decrypted video stream, which is much more applicable in practical applications.

II. PROBLEM STATEMENT

Cryptography is the art of keeping information secret by transforming it into an unreadable format by using special keys, then rendering the information readable again for trusted parties by using the same or other special keys. Moreover, modern cryptography does not confine itself to only maintaining the secrecy of information but goes beyond that by ensuring the identity of communicating parties (authentication), ensuring that information has not been tampered with others (integrity), and preventing that any of the communicating parties denies having received or sent information. The main objective is to enhance compression performance and provides a provision of a network friendly video representation addressing conversational applications. H.264/AVC has achieved a significant improvements in rate distortion efficiency relative to existing standards H.264 /AVC covers all common video conferencing and high definition video storage. To address the need for flexibility and customizability, the H.264/AVC design covers a video coding layer (VCL), which is designed to efficiently represent the video content, and a network subtraction layer (NAL) which formats the VCL representation in a manner appropriate for conveyance by a variety of transport layer or storage media. Relative to prior video coding methods, as exemplified by MPEG-2 video, some highlighted features of the design that enable enhanced coding efficiency include the following enhancement of the ability to predict the values of the content of a pictures 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.

III. LITERATURE REVIEW

W. Hong, T. S. Chen, and H. Y. Wu have recommended that the greater part of the work on reversible information stowing away concentrates on the information inserting/removing on the plain spatial space [6]. The five MSBs of every

pixel of the unscrambled picture will be indistinguishable to those of the cover picture. As per the information concealing key, it is simple for the information hider to reversibly implant information in the encoded picture. Along these lines the information hider can profit by the additional space Emptied out in past stage to make information concealing procedure easy.

In the field of video, W. Puech , Z. Erkin, M. Barni, S. Rane proposed[11] SE(Selective Encryption) of H.264 video is proposed by doing recurrence area specific scrambling, DCT square rearranging and pivot. It performs SE by pseudo-haphazardly rearranging indication of DCT coefficients in Region of intrest. A plan for commutative encryption and watermarking of H.264/AVC. Here SE (specific encryption) of some MB header fields is consolidated with watermarking of greatness of DCT coefficients however they are not design consistent. SE plot in view of H.264/AVC has been introduced on CAVLC and CABAC for I and P outlines. This technique satisfies continuous requirements by keeping the same bitrate and by creating a totally agreeable piece stream [5].

Till now, couple of fruitful information concealing plans in the encoded space have been found in the open literature.[6] A watermarking plan utilizing Parlier cryptosystem is proposed in view of the security prerequisites of purchaser merchant watermarking protocols[4]. In Walsh-Hadamard change picture watermarking calculation is utilized as a part of the scrambled area utilizing Paillier cryptosystem is displayed [4]. Be that as it may, because of the imperatives of the Paillier cryptosystem, the encryption of a unique picture indicates high overhead away and calculation. Take note of that, few investigates on reversible information stowing away in scrambled pictures are discovered as of late. The encryption is performed by utilizing bit-XOR operation. In these techniques, the host picture is in an uncompressed arrange.

In [3] a vigorous watermarking calculation is proposed to install watermark into packed and scrambled JPEG2000 pictures. As advancement of the interactive media and Internet innovation, more data including pictures, sound and other sight and sound, are being transmitted over the Internet. Because of some interior components of pictures, for example, vast information limit and high relationship among pixels, early encryption calculations are not appropriate for down to earth picture encryption. As of late, the picture encryption advances in view of disorder hypothesis have been created to conquer the inconveniences show in early encryption methods.

As said the previously mentioned works have been centered around picture. With the expanding requests of giving video information security and security assurance, information covering up in scrambled H.264/AVC recordings will without a doubt end up plainly well known sooner rather than later. Clearly, because of the requirement of the fundamental encryption, it is exceptionally troublesome and once in a while difficult to transplant the current information concealing calculations to the encoded space. To the best of our insight, there has been no cover the execution of information stowing away in encoded H.264/AVC video streams. Just couple of joint information covering up and encryption approaches that emphasis on video have been proposed. For instance, in [7], amid H.264/AVC pressure, the intra-forecast mode (IPM), movement vector contrast (MVD) and DCT coefficients' signs are encoded, while DCT coefficients' amplitudes are watermarked adaptively.

A consolidated plan of encryption and watermarking is exhibited [8], which can give the get to perfectly fine as the confirmation of video substance all the while. The IPMs of 4 × 4 luminance obstruct, the sign bits of surface, and the sign bits of MVDs are scrambled, while IPM is utilized for watermarking. Be that as it may, the watermarked bitstream is not completely design agreeable thus a standard decoder may crash since it can't parse a watermarked bitstream.

IV. PROPOSED SYSTEM

H.264 is an industry standard for video compression, the process of converting digital video into a format has low bitrate capacity when it is stored or transmitted. The main objective behind the H.264 development was to build up a high performance video coding standard by adopting a back to basics approach with simple and straightforward design using well known blocks. H.264/AVC based on conventional block based motion compensated video coding as same as the exiting standards, but with a numbers of new features and advantages significantly improve its rate-distortion performance and distinguish it from the exiting standards such as MPEG-2, MPEG-4 Part 2, H.263 however, at the same time, sharing common features with the exiting standards.

Special attention is given to the improvement of working with the losses during transmission over different networks or robustness to data errors. The H.264/AVC consists of two conceptual layers. The Video Coding Layer (VCL) which is efficiently represents the content of the video data, and the Network Abstraction layer (NAL) that is designed to convert the VLC representation into format suitable for specific transport layers or storage media. Some key

concepts of the NAL are NAL unites. Each NAL unit is effectively a packet that contains an integer number of bytes, including a header and payload. In H.264/AVC, each frame is divided in Macro-Blocks (MBs) of 16x16 pixels. These macro-blocks are encoded separately; the encoding method is an Entire Transform followed by quantization of the MB, a prediction between MBs in intra (I frame) or inter (P frames), and an entropy coding using either run length coding (CAVLC)[9] or arithmetic coding (CABAC), as presented in Fig. In intra frame, the current MB is predicted spatially from neighboring MBs which were previously encoded and reconstructed. In inter frame, the current MB is predicted spatially and temporally from previous frames. The purpose of the reconstruction in the encoder is to ensure that both the encoder and the decoder use identical reference frames to create the predictions

A. BLOCK DEIAGRAM OF SYSTEM

a) Video encryption and data Hiding

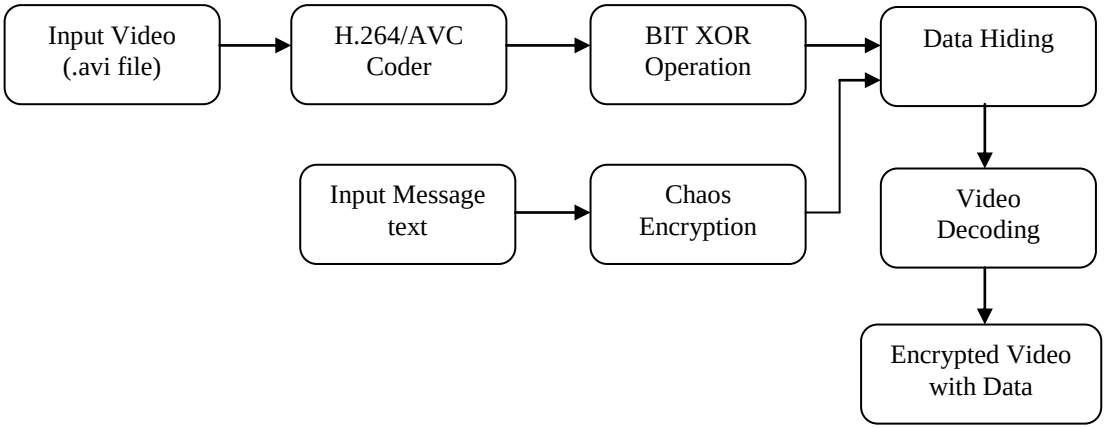

Fig 4.1 Video encryption and data Hiding

b) Data Extraction and Video Decryption.

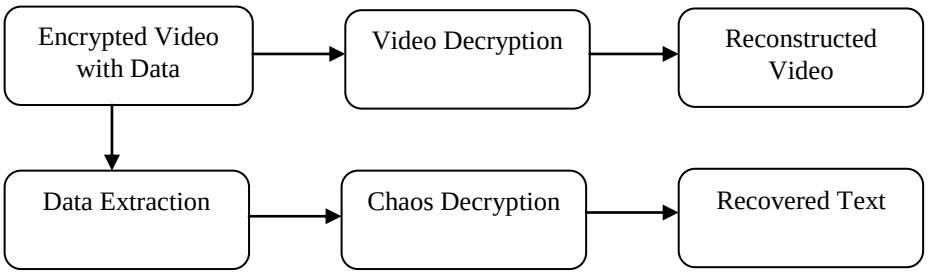

Fig 4.2 Data Extraction and Video Decryption

REFERENCES

[1] Dawen Xu, Rangding Wang, and Yun Q. Shi, *Fellow, IEEE"* Data Hiding in Encrypted H.264/AVC VideoStreams by Codeword Substitution", VOL. 9, NO. 4, APRIL 2014

[2] *Advanced Video Coding for Generic Audiovisual Services*, ITU, Geneva, Switzerland, ar. 2005.

[3].X. P. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Process. Lett.*, vol. 18, no. 4, pp. 255–258, Apr. 2011.

[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].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.

[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] 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.

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

[10] 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.

[11]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.

[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] Jiancheng Zou, Chang Zhen Xiong, Dongxu Qi, et al. *The Application of Chaotic Maps in Image Encryption*. 2005. IEEE Proceedings of on NEWCAS 2005, pp. 331-334, June. 2005