International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.5., 2015
(Sept.-Oct.)

RESEARCH ARTICLE

ISSN: 2321-7758

SECRET DATA HIDING IN ENCRYPTED COMPRESSED VIDEO BIT-STREAMS FOR PRIVACY INFO PROTECTION

R. RAMESH[1], U.V.RATNA KUMARI[2]

[1]PG Scholar, Department of ECE,UCEK,Kakinada,ramesh.rudra450@gmail.com

[2]Assistant Professor, Department of ECE,UCEK,Kakinada,vinayratna74@gmail.com

International Journal of Engineering Research-online (IJOER)
ISSN:2321-7758
www.ijoer.in

ABSTRACT

The project presents that encryption of compressed video bit streams and hiding privacy information to protect videos during transmission or cloud storage. For secure transmission of video it needs to be preserved and processing is done in encrypted format to maintain security and Data hiding approach is necessary to perform in these encrypted videos for the purpose of content view and tampering recognition. In this manner, hiding data in encrypted area without decryption preserves the confidentiality of the content. In addition, it is more efficient technique without decryption followed by concealment of data and re-encryption. Here, data hiding directly in the encrypted version of H.264/AVC video stream is approached, which includes the following three parts, i.e., H.264/AVC video encryption, data embedding, and data extraction. By observing the properties of H.264/AVC codec, the code words of intra prediction modes, the code words of motion vector differences, and the code words of residual coefficients are encrypted with stream ciphers. Then, a data hider may embed additional data in the encrypted domain by using bits replacement technique, without knowing the original video content. Chaos crypto system is used here to encrypt/decrypt secret text data before/after data embedding/extraction. In order to adapt to different application scenarios, data extraction can be done either in the encrypted domain or in the decrypted domain. The project simulated results shows that used methods provides better performance in terms of computation efficiency ,high data security and video quality after decryption. The parameters such as Mean square error, PSNR, correlation are evaluated to measure its efficiency.

Keywords— Encryption, decryption, chaos crypto system, H.264\AVC, bit replacement.

©KY PUBLICATIONS

I.INTRODUCTION

CLOUD computing has become a crucial technology trend, which might offer extremely economical computation and large-scale storage answer for video information. Given that cloud services might attract a lot of attacks and are vulnerable to slippery system directors, it's desired that the video content is accessible in encrypted type. The potential of playing information concealment directly in encrypted H.264/AVC video streams would avoid the discharge of video content, which can facilitate address the safety and privacy considerations with cloud computing. Digital video sometimes needs to be stored and processed in compressed format to maintain file size. For the purpose of content notation and tampering detection it is necessary to perform data hiding in compressed video.The process of data hiding would avoid the leakage of video. formation ability of performing data hiding directly in encrypted H.264/AVC video streams avoid the leakage of video data, this protects privacy and security concerns with cloud computing. a cloud server can embed the additional information into an encrypted H.264/AVC video by using data hiding technique. The third challenge is to keep up the file size when cryptography and information concealment, which needs that the impact on compression gain is negligible. The fourth challenge is that the hidden information may be extracted either from the encrypted video stream or from the decrypted video stream, which is far a lot of applicable in sensible applications.

II.LITERATURE SURVEY

Literature survey is the most significant step in software development process. Before developing the tool it is needed to find out the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers begin building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. One of reversible methods is using difference expansion to insert information. So far, several schemes related to this type. These methods usually generate some small values to represent the skin tone of the original image. Then, we can expand the generated values to embed the bits of watermark data. The watermark data is usually embedded in the LSB parts of the expanded values. Then the watermarked image is reconstructed by using the modified values Before constructing the system the above considerations are taken into account for developing the proposed system .a literature review is a body of text that aims to review the crucial points of present knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and as such, do not report any new or original experimental work. Also, a literature review can be treated as a review of an abstract accomplishment..more often associated with academic-oriented literature, such as a thesis, a literature review usually precedes a research proposal and results section. Its main goal is to establish the current study within the body of literature and to provide context for the particular reader. We introduce Tian's method to illustrate concept of this type. In Tian's method, an integer transformation is defined as

$$l = \lfloor \frac{(x+y)}{2} \rfloor,$$

where x and y are two adjacent pixels. The inverse integer transformation can be represented as

$$\begin{aligned} x' &= l + \lfloor \frac{(h+1)}{2} \rfloor, \ and \\ y' &= l - \lfloor \frac{h}{2} \rfloor, \end{aligned}$$

Where

$$h = x - y.$$

The processes of Tian's scheme are illustrates as follows.

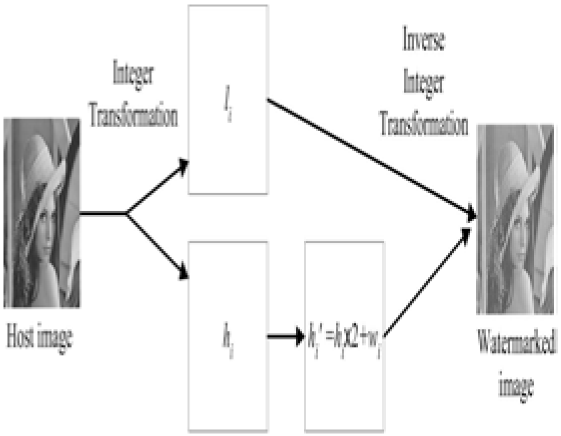

Fig1: Flowchart of the Tian's scheme

III.EXISTING SYSTEM

Several steganographic methods have been proposed in literature and most of which are performed in pixel domain. Walsh-Hadamard transform (WHT) is comparatively fast algorithm in the encrypted domain, which is especially appropriate for the applications in the encrypted domain for its transform matrix comprises only integers. Then by manipulating the relations among the adjacent transform coefficients, an WHT-based image watermarking algorithm in the encrypted domain is proposed. Due to the limitations of the encryption, extracting a watermark blindly from an encrypted image is not a easy task. Another method was reversible data hiding method for encrypted images using side match, in this original work partitions an encrypted image into blocks, and a block carries one bit by flipping three LSBs of a set of pre-defined pixels. The data retrieval and image recovery can be achieved by observing the block smoothness. Zhang's work did not fully make use of the pixels in calculating the smoothness of each block and did not consider the correlation between pixels in the border of neighboring blocks. These two issues could reduce the exactness of data extraction. This method adopts a better scheme for measuring the smoothness of blocks, and uses the side-match scheme to decrease the error rate of extracted-bits to a greater extent previous to performing experiment on the video file format and relate a variety of steganographic technique, imperative parameters, such as the numeral, size, timestamps, and location of the video tags, must be known since they are the definite data that will be changed and customized. The size of the image is LSB Coding, Spread Spectrum, Phase Coding, Echo Hiding Video files are normally consists of images and sounds, consequently nearly all of the applicable technique for hiding data into video media. Various techniques of LSB exists, where proposes the data is first encrypted using a key and then embedded in the carrier AVI video file in LSB keeping the key of encryption in a separate called key file. Steganography techniques for compressed video stream can be found in a Another video steganography scheme based on motion vectors and linear block codes has been proposed.

IV.PROPOSED METHOD

An Efficient data hiding approach on encrypted compressed video bit streams for privacy information protection based on, H.264/AVC coder and Bits replacement. The content owner encrypts the original H.264/AVC video stream using standard stream ciphers with encryption keys to produce an encrypted video stream. Then, the data-hider(e.g., a cloud server) can insert the additional data into the encrypted video stream by using bit wrapping 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. An H.264/AVC video encryption scheme with good performance including security, efficiency, and format suitability is proposed.

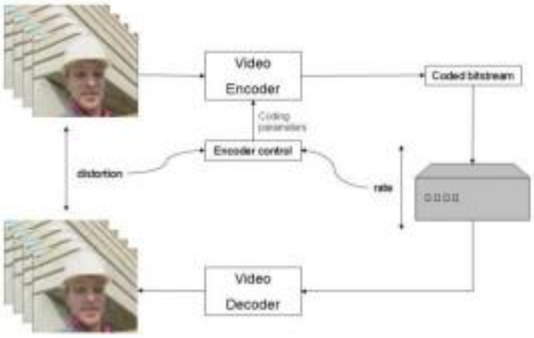

Fig2: SECRET DATA ENCRYPTION

It encrypts the original image pixel values with encryption key value generated from chaotic sequence with threshold function by bit xor operation. It is very useful to transmit the secret image through unsecure channel securely which prevents data hacking. The chaotic systems are defined on a complex or real number space called as boundary continuous space.

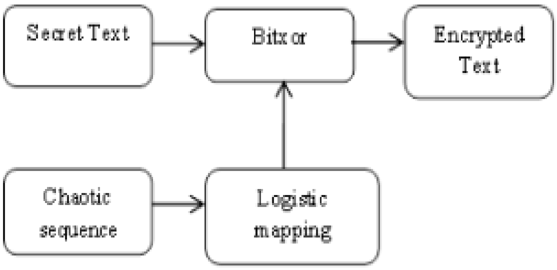

Fig.3 : Bit replacement based hiding

Encrypted Message will be hidden in I frame using bit replacement technique. It can be added data in P frames to maintain the quality of video after encryption and embedding of data.

V.VIDEO FRAMES ENCRYPTION

The process of bit wrapping method is to hide the encrypted secret data into the encrypted bit stream in the form of compression. Then the encrypted text was hidden in the encrypted compressed bit streams. This comprises embedding data, detecting, and coding techniques. The technique behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. The most frequently used steganography method is the technique of LSB substitution. In a gray-level image, every pixel consists of 8 bits. One pixel can hence display 28=256 variations.

A. Chaos Crypto system

Chaotic systems are suitable for data message encryption because they have good properties as follows: 1)chaotic motion is neither periodic nor convergent, and the domain is limited. With time passing, the points of the movement trace traverse all over domain. 2)Flexing and collapsing are carried continually through the limited domain.

B. Advantage:-

- The data hiding is performed directly in encrypted H.264/AVC video bit stream.
- This method can ensure both the format suitable and the exact file size preservation.
- It is easy to implement.
- It can preserve the bit-rate exactly after encryption and data embedding.
- It does not necessary to decrypt or partial decompression of the video stream thereby making it ideal for real-time video applications.
- Data hiding is completed entirely in the encrypted domain

VI.PERFORMANCE

To know about performance the factors PSNR, SSI, VQM plays an important role. PSNR is widely used objective video quality metric. However, it does not perfect correlate with a perceived visual quality due to nonlinear behavior of human visual system.SSI index denotes the approximate of reference image with target image.It is in the range of 0 and 1.If SSI is 1means reference image is equal to the target image. Bit rate is another parameter to know about performance,bit rate is given by

$$BITR\_VAR = \frac{BIT\_EM - BIT\_ORGI}{BIT\_ORGI} \times 100$$

Where BIT_EM is bit rate of image after encryption and embedding, BIT_ORGI is bit rate of original video. BIT_VAR denotes the variation of bit rate, if it is low then it is a better scheme. Here bit rate is unchanged because encryption and data embedding is performed directly on the codewords of reference video by using bit replacement method. So bit rate is unchanged and it is format suitable with the decoder at the decoding side. In addition the encryption process and data hiding process do not affect compression efficiency of encoders, since compression efficiency is typically defined by the bit rate.

RESULTS:

Fig4:Input Video

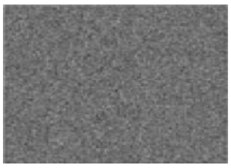

Fig5: Encrypted Video

Fig 6: Output Video

MSE		PSNR (DB)		SSI	
ORI	SGD	ORI	SGD	ORI	SGD
0.1278	0.1370	57.052	50.152	0.9946	0.9937

Table 1: PSNR, SSI, AND IN DIRECTLY DECRYPTED VIDEOS

VII.CONCLUSION AND FUTURE WORK

Efficient Data hiding in compressed video is one of the major problems in multimedia application and this topic draw attention because of the privacy-preserving requirements from cloud management. In this project H.264 codec technique is used for encoding/decoding videos. This technique ensures better quality and minimum size of video during compression and decompression. The Mean Square Error and PSNR is calculated to identify quality of images in video. From the analysis it is known that the compression of video using H.264 codec gives two times better performance than other technique. Instead of grayscale video color videos can be used for compression and next level of video coding like H.265 can be used for compression. H.265 codec provides two times higher compression rate than H.264 codec technique. This helps to reduce the file size during the transmission.

REFERENCES:

[1]. www.vcodex.com

[2]. White Papers: An overview of h.264 Advanced Video Coding.

[3]. H.264/AVC Context Adaptive Variable Length Coding.

[4]. W. J. Lu, A. Varna, and M. Wu, "Secure video processing: Problems and challenges," in Proc. IEEE Int. Conf. Accost., Speech, Signal Processing, Prague, Czech Republic, May 2011, pp. 5856–5859.

[5]. 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.

[6]. 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.

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

[8]. K. S.M. Rahman, Hossain, M.L.,"A new approach for LSB based image steganography using key"

[9]. Hema Ajetrao, Dr. P.J.Kulkarni and Navanath Gaikwad, A Novel Scheme of Data Hiding in Binary Images, in International Conference computational Intelligence and Multimedia Applications, Vol.4, pp. 70-77, Dec. 2007.

[10]. Po-Yueh Chen and Hung-Ju Lin"A DWT Basedv Approach for Image Steganography", International Journal of Applied Science and Engineering 2006. 4,v 3: 275-290