International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secret Data Hiding in Compressed Video Bit Streams for Privacy Information Protection

B. Vengadalakshmi[1], S. Abiramasundari[2]

[1]SASTRA University, Kumbakonam

[2]Assistant Professor, Department of Computer Science, SASTRA University, Kumbakonam

Abstract*: The project presents the 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 a compressed format to maintain security and privacy. Data hiding approach is necessary to perform in these encoded videos for the purpose of content notation and tampering detection. In this way, data hiding in encoded domain without decoding preserves the confidentiality of the content. Here, data hiding directly in the version of H.264/AVC video stream is approached, which includes the following three parts, i.e., H.264/AVC video encoding, data embedding, and data extraction. By analyzing the property 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 coded using H.264 encoding technique. Then, a data hider may embed additional data in to it 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. 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: Bits Stream, Data Hiding, Video Compression, Video Stenography.

1. Introduction

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[1].The process of performing data hiding directly in video bit stream would avoid the leakage of video content. H.264 is an industry standard for video compression, the process of converting digital video into a format that takes up less capacity when it is stored or transmitted. Video compression (or video coding) is an essential technology for applications such as digital television, DVD-Video, mobile TV, videoconferencing and internet video streaming. Standardizing video compression makes it possible for products from different manufacturers (e.g. encoders, decoders and storage media) to inter-operate. An encoder converts video into a compressed format and a decoder convert's compressed video back into an uncompressed format

2. Related Work

In[2],Several steganographic methods have been proposed in literature and most of which are performed in pixel domain. However major contribution is in the domain of Image Steganography. [3]The existing methods are mainly based on LSB where LSBs of the cover file are directly changed with message bits. In a robust image steganography technique based on LSB insertion and RSA encryption technique has been used. Maud et.al has proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information. Other Examples of LSB schemes can be found in. Whereas EzStego developed by Machado embed information into an image in the GIF format. It sorts the palette to ensure the difference between two adjacent colors is visually indistinguishable. Tseng and Pan presented a data hiding scheme in 2-color images, it embeds the information in any bit where at least one of the adjacent bits is the same as the original unchanged bit. Kawaguchi et. al. [4] proposes bit plane complexity segmentation(BPCS) method to embed information into the noisy areas of the image. These techniques are not limited to the LSB. Existing steganographic software, such as Stefano's, S-tools and Hide4PGP , are based on LSB.Video steganography of late has also gained quite Video steganography of late has also gained quite significance for researchers. 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. [5] Where as in selected LSB steganography file algorithm is proposed. Other steganography techniques in uncompressed raw video, is illustrated ,and .Steganography techniques for compressed video stream can be found in and Another video steganography scheme based on motion vectors and linear block codes has been proposed.

3. Proposed Work

An Efficient data hiding approach on encrypted compressed video bit streams for privacy information protection based on, H.264/AVC coder and Bits replacement method H.264/AVC/MPEG-4 Part 10 contains a number of new features that allow it to compress video much more efficiently than older standards and to provide more flexibility for application to a wide variety of network environments. Reduced time consumption process, It is useful to perceive video tampering Better compatible system for people privacy protection

4. Methodology Used

H.264/AVC Codec, Chaos encryption for text, Bits

Replacement based hiding

Description

H.264/AVC Codec

H.264/AVC Advanced Video Coding Standard is a video compression standard using for compressing video bit stream. H.264 Codec includes encoding/decoding (compress/decompress) technique. It perform encoding/decoding in I frame and P frame. I frame refers to intra predicted frame and P frame refers to predicted frame. Encoding performs prediction, transformation, quantization and CAVLC- Context Adaptive Variable Length Coding. Decoding performs reverse process of encoding like inverse transformation, prediction and reconstruction.

Chaos Encryption for text

The broad chaos encryption method is the simplest technique to encrypt message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security. The advantage of chaotic encryption is High level security. The encryption is achieved by iteration. Simplest. No short cuts are available. The properties of chaos are slightly producing some changes in the entire cryptography. Sensitive on initial stage and topology transitivity are the properties in it. In an initial condition, chaotic is always sensitive. Hence it will produce a slight difference in trajectory. It gives the totally different trajectory sectional value. Identical trajectory only can produce the same values.

Bit replacement based hiding

Encrypted Message will be hidden in I frame using bit replacement technique.

5. Implementation

5.1 Problem Faced

There are some problems I came across during the implementation of this technique for video with maximum size and resolution in mat lab 2010 version. Different level of frames are encoded and decoded. It took time to compress the video. This is the stage where I confirm that the encoding process has achieved the ultimate goal are not. For better performance I converted the video to grayscale video and hence it performs well.

5.2 Lesson Learnt

In this project, I learnt about the types of videos and how they are separated as frames, how to encode and decode different frames like I frame, P frames , and how to calculate mean square error of an image, PSNR of image and quality. The lessons learnt from the problem are which ultimately leads to suffice the quality factor.

5.3 Bit Stream

A byte stream is a series of bytes. Typically, each byte is from a range of 256 distinct values (octets), and so the term octet stream is sometimes used to refer to the same thing. An octet may be encoded as a sequence of 8 bits in multiple different ways (see endianness) so there is no unique and direct translation between byte streams and bit streams. In practice, bit streams are not used directly to encode byte streams; a communication channel may use a signaling method that does not directly translate to bits (for instance, by transmitting signals of multiple frequencies) and typically also encodes other information such as framing and error correction together with its data.

5.4 Steganography

Steganography **is** the art or practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Ancient Greek words staginess, meaning "covered, concealed, or protected", and graph in meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, disguised as a book on magic. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists, or some other cover text. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography which lack a shared secret are forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle.

6. Experimental Result

6.1 H.264/AVC Coder

H.264 is a standard used for video compression it converts digital video into a format that requires less capacity when it is stored or transmitted. Video compression (or video coding) is an important technology for applications such as digital television, DVD-Video, videoconferencing, mobile TV and internet video streaming. In H.264, encoder converts video into a compressed format and a decoder convert's compressed video back into an uncompressed format [13]

6.2 Chaos Cryptosystem

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. Therefore the outputs of chaotic systems are very irregular, similar to the random noise. The discrete sequences of the chaotic dynamical system are gained by the following equation.

$X_n+1 = T_n(x_k)$.

The basic Logistic-map is formulated as, $f(x)=\mu x(1-x)$
Where, x (0, 1).

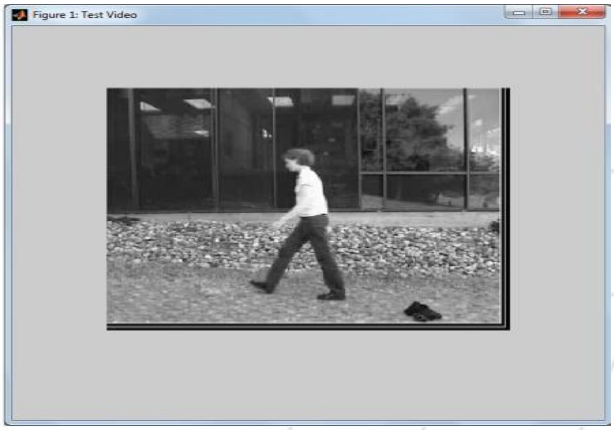
The parameter μ and the initial value x0 can be adopted as the system key (μ, x0). The research result shows that the system is in chaos on condition that

$3.569 < \mu < 4.0$. [14]

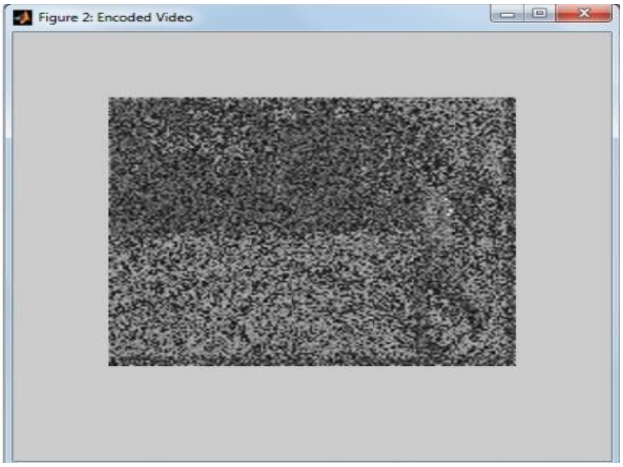
6.3 Bits Replacement Technique

The frequently used steganography method is the technique of LSB substitution. Every pixel of gray-level image consists of 8 bits. One pixel can hence display 28 =256 variations. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly.[15]

Original Video



Encoded Video



Decoded Video

Table1: Simulation Results of Images: PSNR and Compression Achieved with Intra prediction

Intra prediction Mode	*Clock, Geneva 1024x768 pixels*		*Blue hills 800 x 600 pixels*		*Lena 512 x 512 pixels*	
QP=16	PSNR (dB)	Compression Achieved	PSNR (dB)	Compression Achieved	PSNR (dB)	Compression Achieved
0	34.0	11.6	39.0	29.6	35.4	15.7
1	34.1	12.0	38.5	29.4	35.2	35.2
2	34.0	7.6	38.9	25.8	35.3	10.7
3	34.2	10.6	39.8	27.4	38.0	14.2
4	32.6	8.4	37.9	19.4	33.5	10.9
5	32.8	8.6	36.1	19.0	34.0	11.7
6	33.1	9.1	38.2	23.4	34.1	12.0
7	34.5	11.1	14.0	28.4	35.3	14.3
8	34.6	11.0	40.3	29.7	36.4	
Without Intra prediction	34.7	7.8	40.2	27.7	37.3	11.7

7. Conclusion and Future Work

Efficient Data hiding in compressed video is one of the main 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 provides 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 reversibledata 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, in Proceedings of 14th International Conference on Computer and Information Technology (ICCIT-2011), pp.-286-291, Dec. 2011.
[9] Hema Ajetrao, Dr. P.J.Kulkarni and Navanath Gaikwad, A Novel Scheme of Data Hiding in Binary Images, in International Conference onmputational Intelligence and Multimedia Applications, Vol.4, pp. 70-77, Dec. 2007.
[10] Sachdeva S. and Kumar A, Colour Image Steganography Based on Modified Quantization Table, in Proceedings of Second International Conference on Advanced Computing & Communication Technologies (ACCT-2012), pp. 309-313, 2012.
[11] R.achado,http://www.securityfocus.com/tools/586/scoreit, .EzStego., Nov. 1996. [last accessed on [16-04-2012]
[12] Y. C Tseng and H. K Pan, Data Hiding in 2-color Image in IEEE Transactions on computers, Vol. 51,
[13] Po-Yueh Chen and Hung-Ju Lin "A DWT Basedv Approach for Image Steganography", InternationalvJournal of Applied Science and Engineering 2006. 4,v 3: 275-290
[14] T. Wiegand, G. J. Sullivan, G. Bjontegaard, and A.v 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.
[15] Sangeeta Mishra Sanjeev Ghosh Payel Saha ,"Chaos Based Encryption Technique for Digital Images" Kandivali (E), Mumbai-400101.