International Journal of Computer Applications (0975 - 8887)
Volume 134 - No.13, January 2016

A Review on Data Hiding Techniques in Compressed Video

R. Aparna
P G Scholar
Department of Computer Science & Engineering
College of Engineering, Perumon(CUSAT), Kerala, India

Ajish S
Assistant Professor in CSE
Department of Computer Science & Engineering
College of Engineering, Perumon(CUSAT), Kerala, India

ABSTRACT

This paper presents various Data Hiding techniques of video in compressed domain. Data is embedded into digital media for the purpose of identification, annotation, copy right and tampering detection. The identification purpose mainly falls into the area of cloud computing- making sure that the sender is the one intended; annotation refers to the property of tagging or giving captions to the video; copyright protection, which is used to prevent the recreation of the video; tampering detection is the method in which the receiver checks whether the video is tampered or disturbed during the transmission by a third party. Several factors affect the data hiding process-the quantity of data to be hidden, whether the embedding technique can handle large payloads without affecting the quality of the video, embedding in a lossy compression environment and the extent to which the data hidden is subject to modification or removal by a third party. This paper discusses the various data hiding techniques of video in the compressed environment and compares the techniques based on the quantities mentioned above. Furthermore they are analyzed in terms of their method, robustness and capacity. A comparison graph is plotted based on the efficiency analysis of the data hiding techniques and conclusions are drawn based on the analysis.

General Terms

Encryption, Data hiding

Keywords

Data hiding , Steganalysis , Video compression, Video encryption , Watermarking

1. INTRODUCTION

Data hiding is the process of embedding secret information inside a media or data source without changing its perceptual quality. Data hiding can also be said as the art and science of secretly hiding data into media or data such that only the sender and the intended receiver even has an idea or even realizes that there is a hidden message.

Data hiding techniques can be used to embed a secret message into a compressed video bit stream for copy right protection, access control, content annotation , transaction tracking, tampering detection and as such. Steganalysis, on the other hand, is the process of detecting the presence of hidden messages in multimedia and can be used for tampering of video. Steganalyis can be used in digital images and to digital video as well. Prevailing works on video-based data hiding or steganography take such current attacks into account.

Encryption is a powerful way of securing the transmission of multimedia files. Suppose the intended sender wants to add additional data along with the multimedia which is supposed to be confidential, the sender can make use of data hiding techniques. Usually data hiding finds its use in medical purposes, image/video notation, military purposes,authentication of data or tamper detection.

For example, when medical images have been encrypted for protecting the patient's confidential details, a database administrator would like to embed the personal details of the patient in the confidential video. Data hiding techniques finds an important place in authentication purposes in the context of cloud computing. Another significant yet interesting area of application is tampering detection. The data to be embedded should be a sensitive data so that the very same can be extracted from the media file and be used for comparison with the same data calculated from the media file.

The purpose of data hiding and the level of security, capacity and robustness depend upon the application and the owner of the digital media [1]. Data hiding requirements are:

(1) Impalpability: the video with the embedded data and the original video should be visually identical.

(2) Robustness: the embedded data should not be disturbed by any kind of image processing techniques.

(3) Capacity: the amount of data embedding payload should be high.

(4) Security: the data embedded should be highly secured.

Data can be embedded into a video sequence either in the compressed domain or in the non-compressed domain. Data hiding in compressed domain; which is the main concern of this paper, make use of various steps in the compression or encoding, the parameters which describe about the relationship between the frames such as motion vector difference calculation. Data hiding in non-compressed background consider the video sequence as a set of frames (image sequences). So the data hiding techniques of image will also apply for video hiding.

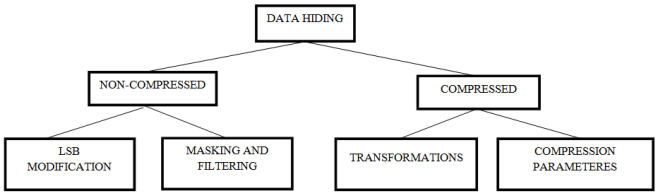

Fig. 1. Data hiding techniques

In non-compressed domain, the data hiding techniques consider video sequence as a set of images. The various techniques include the least significant bit modification, masking and filtering. In Least Significant Bit (LSB) modification, the LSB's of the pixels falling above a threshold parameter are chosen for embedding purpose. If the intended sender is looking for an easy implementation of embedding data, least significant bit modification technique is a good choice. In such a technique, each and every pixel of the image (frames of a video) is analyzed for embedding purpose because of which a lossless compression format is advised for the encoding purpose. There is a great risk that the hidden data may be lost in the transformation of a lossy compression.The major challenge faced by this technique is that the changes made by such modifications to the pixels should be too small to be recognized by the human eye. In order to overcome such challenges, the cover image is chosen with great care and preferably grayscale images are chosen as it is hard to notice the changes with the human eye.

Various technologies have been proposed for efficient data hiding in images. Reversible data hiding technique is one among them. In [2], the main aim was to embed additional data into the encrypted image. The data hider divides the image pixels into s x s blocks where the pixels for embedding are chosen based on a function. The s2 pixels are pseudo-randomly divided into 2 sets S0 and S1. The sets are chosen depending on the bit to be embedded (either 0 or 1) and the last 3 bits of the pixel value is flipped accordingly. An improvement to the above scheme was proposed in [3] where all the pixels were used in calculation of smoothness of each block and pixel correlations in the neighboring blocks were considered. Furthermore a side-match scheme was also used to reduce the error rate of extraction.A different approach was proposed in [4] were spaces for embedding of data were found out/ vacated before encryption of images. The LSBs of some pixels were embedded into the LSBs of other pixels with a traditional RDH method. The positions of the LSBs moved can be used to embed the data.In [5] a data hiding key is used to embed data into the image. The data hider may compress the LSB of the encrypted image using a data hiding key to create a sparse space to accommodate data.

Masking and filtering type of data hiding technique is done by modifying the luminance parts of an image. The changes are made such it is imperceptible to the human eye.

The remainder of the paper is organized as follows. In Section 2,data hiding techniques in compressed video which includes the sub parts, transformations and data hiding in compression parameters is described. Section 3 provides the comparison of data hiding techniques. Finally in Section 4, conclusion is drawn.

2. DATA HIDING IN COMPRESSED VIDEO

In compressed domain, the data hiding techniques make use of the compression or encoding steps[6]. The data hiding techniques can be applied to video sequences during the compression phase or after compression. Both the temporal as well as spatial models are used.[6]

2.1 Transformations

In transformations,the modifications are done to the DCT (Discrete Cosine Transform) coefficients. DCT is used by the compression algorithms to transform successive 8 x 8 pixel block of the image into 64 DCT coefficients each. After calculating the coefficients, a quantization procedure is done as a part of compression. The LSB of the quantized DCT coefficient can be used to hide information.

In reference [7], the watermark represents the frames' and macroblocks' indices which are embedded into the non-zero quantized DCT value of the blocks. The paper proposes a tampering detection technique using watermarking process. It succeeded in detecting spatial, temporal and spatio temporal tampering. [7] uses a semi-fragile watermarking protocol. Embedding process is done after the DCT and quantization phases. For embedding, some 4x4 block of each 16 x 16 macroblocks are selected for embedding. In each macroblock, the blocks that have larger LNZ (Latest Non-Zero) level position are selected that is the blocks that have the highest high frequency sample. In each selected block a single bit is embedded. To improve the security, the authentication code As is encrypted by a key called C to form the watermark signal W.

$$W = E(C, A_s) \tag{1}$$

For each selected block, the sum of the levels (S_i) within the block is computed and its LNZ level (L_i) is modified based on the sum and w_i.

$$L_i = \begin{cases} L_{i+1}, \text{if} S_i \text{is odd}, w_i \text{is zero and} L_i \neq -1 \\ L_{i-1}, \text{if} S_i \text{is odd}, w_i \text{is zero and} L_i = -1 \\ L_i, \text{if} S_i \text{is odd}, w_i \text{is one} \\ L_i, \text{if} S_i \text{ is even}, w_i \text{ is zero} \\ L_{i+1}, \text{if } S_i \text{ is even}, w_i \text{ is one and} L_i \neq -1 \\ L_{i-1}, \text{ if} S_i \text{is odd}, w_i \text{is zero and } L_i = -1 \end{cases} \tag{2}$$

To make this scheme robust against collusion attacks, the key is generated based on the macroblock features. For such a purpose, the key is generated based on the intraprediction modes in the encoder. The embedded watermark bits are extracted during the decoding process where the QDCT levels for each MB are entropy decoded. For the extraction purpose, the LNZ levels for 16 blocks of the current MB are sorted and k blocks are selected which have higher nonzero position values. In each of these selected blocks, a bit is extracted as:

$$w_i' = \begin{cases} 0, \text{if } S_i' \text{ is even} \\ 1, \text{if } S_i' \text{ is odd} \end{cases} \tag{3}$$

The key can be regenerated in the decoder as well. The main advantage of the system is its simplicity of implementation at the decoder side.

Another approach was made by Shiguo Lian et al., in [8]. Here, the intra prediction mode, motion vector difference and discrete cosine transform (DCT) coefficients' sign are encrypted while the DCT magnitudes are used for hiding data. The scheme increases the security by separating the data hiding process from the encryption, that is, the data is hid after the encryption process. Let the original coefficient be z and the watermark be w. For increased security, the watermark is encrypted with a stream cipher before the process.

The value of the coefficient is changed as
If w=1,

$$z' = \begin{cases} z, \text{if} \frac{|z|}{q}\%2 = 1 \\ \left(\lceil \frac{|z|}{q} \rceil + 1\right) q.Sign(z), \text{if} \lceil \frac{|z|}{q} \rceil \%2 = 0 \end{cases} \quad (4)$$

Otherwise,

$$z' = \begin{cases} z, \text{if} \frac{|z|}{q}\%2 = 0 \\ \left(\lceil \frac{|z|}{q} \rceil - 1\right) q.Sign(z), \text{if} \lceil \frac{|z|}{q} \rceil \%2 = 1 \text{and} z \neq -q \\ 2q.Sign(z), \text{if} z = -q \end{cases} \quad (5)$$

2.2 Compression Parameters

2.2.1 Data Hiding in Motion Vector. Hussein A. Aly, in his work [9], made use of compression parameter for data hiding, rather than focusing on raw video or images for the same. The data is embedded into the LSB of both components of motion vector. The choice of the candidate motion vector is based on the associated macroblock prediction error. The data hiding technique is evaluated based on two criteria: minimum distortion to the reconstructed video and minimum overhead on the compressed video size. If the reconstructed prediction error at the receiver side follows the condition as that in the encoder side, the decoder will identify that a data is to be extracted. The threshold for each of the frame will be different.The threshold for each frame in the GOP will be hidden in the corresponding I frame. The motion vectors representing the P-frames are used more than the motion vectors of the B-frame. Less usage of B-frames resulted in increased payload and better quality of the reconstructed video.

2.2.2 Data Hiding with Phase of Motion Vector. Ding-Yu Fang and Long-Wen Chang in [10] proposed a new method of embedding data in digital videos using the phase angle of the motion vector of the macroblock in the interframe. The candidate motion vectors are selected based on a predefined threshold T. For embedding, the phase angle of the motion vector is computed as

$$\theta = arctan \frac{MV_{iv}}{MV_{ih}} \quad (6)$$

Where MV_{iv} and MV_{ih} are the vertical and horizontal component of motion vector MV_i respectively. The rule of data embedding is as follows:

(1) If data bit is 0, they searched for MV_{2i} and MV_{2i+1} such that

$$0^0 < \theta_{2i} - \theta_{2i+1} \leq 180^0 \quad (7)$$

(2) If data bit is 1, they searched for MV_{2i} and MV_{2i+1} such that

$$180^0 < \theta_{2i} - \theta_{2i+1} \leq 360^0 \quad (8)$$

If the conditions were not met, a new pair of motion vectors was calculated such that the conditions were satisfied.

2.2.3 Data Hiding Based on Variable Block Sizes. In [11], the temporal model of H.264 encoder is used for data hiding. The variable block size used for motion compensation is used in data hiding. The H.264 standard uses 7 different block sizes (16x16, 16x8, 8x16, 8x8, 8x4, 4x8, 4x4). The basic idea of the proposed scheme [10] is to force the encoder to choose a block type not in terms of efficiency but to satisfy the data hiding requirements. The idea is to assign a binary code to each block type. For simplicity, they used only 4 block types. The data to be embedded is converted to binary codes. These binary codes are then grouped in pairs and are mapped to the macroblocks which are going to be motion compensated.

3. COMPARISON OF DATA HIDING METHODS

Fallahpour et al., in [7] used the non-zero DCT coefficients for hiding the data. The proposed method can hold more data thus increasing the data capacity. After re-encoding, the luma prediction modes may be changed which affect the synchronization in the data extraction process thus reducing robustness. A similar approach was done in [8] where the DCT coefficient are modified according to the data embedded. The payload to be applied is medium and the scheme can be said to be robust against video processing operations.Hussein A. Aly in [9] used motion vector for hiding data. Only the motion vector of P-frames are used hence resulting in decreased capacity. As the threshold for motion vector is different in different frame, the robustness is also decreased accordingly. In [10], the phase of motion vectors is used. Only the motion vectors satisfying a pre-specified condition is used for hiding data. In [11], the variable block sizes are used to hide information. It does not affect the visual quality as it is a blind scheme. The file size is increased thus reducing efficiency. Only 4 block types are used in [11] thus reducing the payload. The comparison is tabulated below. Conclusions are drawn based on the factors mentioned and a graphical analysis is presented in Figure (2).

Table 1. Comparison of Data Hiding Techniques

On The Basis Of Where Data is Hidden	Robustness	Capacity
Non-zero quantized DCT	Low	High
Amplitude of DCT is modified	Medium	Medium
LSB of both components of the motion vector	Medium	Low
Phase of candidate motion vector	Medium	Low
Data is mapped to the binary code of block size	Low	Low

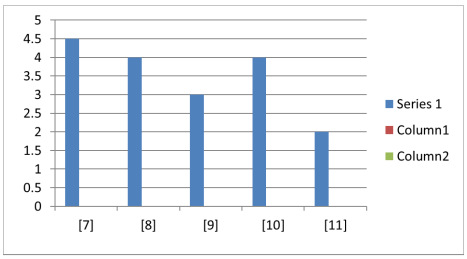

Fig. 2. Comparison Chart

4. CONCLUSION

This paper presented the various data hiding techniques in video. The paper also describes the various backgrounds in which these techniques can be used. Data hiding finds its major application in content notation and tampering detection in cloud environment, military applications and medical purposes.A brief comparison of the techniques is discussed in this paper.The future work may include data hiding using combination of compression parameters ,that is, data can be embedded in more than one compression parameter. There is a large scope to develop much more effectual data hiding techniques in video and thereby achieving more throughput.

5. REFERENCES

[1] Arup Kumar Bhaumit, Minkyu Choi, Rosslin J. Robles and MaricelO.Blitanas "Data Hiding in Video",InternationalJournel of Database Theory and Application Vol. 2,No.2, June 2009

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

[3] 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.

[4] K. D. Ma, W. M. Zhang, X. F. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," IEEE Trans. Inf. Forensics Security, vol. 8, no. 3, pp. 553-562, Mar. 2013

[5] X. P. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol. 7, no. 2, pp. 826-832, Apr. 2012.

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

[7] Mehdi Fallahpour, Shervin Shirmohammadi, Mehdi Semsarzadeh, and Jiying Zhao,"Tampering detection in compressed digital video using watermarking"IEEE Trans.Instrumentation and Measurement, vol. 63, no. 5, May 2014.

[8] Hussein A. Aly,"Data hiding in motion vectors of compressed video based on their associated prediction error",IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, March 2011.

[9] Ding-Yu Fang, Long-Wen Chang, "Data hiding for digital video with phase of motion vector", IEEE. Proc. ISCAS, 2006.

[10] Spyridon K. Kapotas, Eleni E. Varsaki and Athanassios N. Skodras, "Data hiding in H.264 encoded video sequences",IEEE Proc. MMSP 2007.

[11] 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.