RESEARCH ARTICLE OPEN ACCESS

Secured Data Transmission Using Video Steganographic Scheme

B.suneetha
Sr asst.professor, DADI Institute of Engineering &Technology,anakapalli

Abstract
Steganography is the art of hiding information in ways that avert the revealing of hiding messages. Video Steganography is focused on spatial and transform domain. Spatial domain algorithm directly embedded information in the cover image with no visual changes. This kind of algorithms has the advantage in Steganography capacity, but the disadvantage is weak robustness. Transform domain algorithm is embedding the secret information in the transform space. This kind of algorithms has the advantage of good stability, but the disadvantage of small capacity. These kinds of algorithms are vulnerable to steganalysis. This paper proposes a new Compressed Video Steganographic scheme. The data is hidden in the horizontal and the vertical components of the motion vectors. The PSNR value is calculated so that the quality of the video after the data hiding is evaluated.
Index Terms—Data hiding, least significant bit(LSB), encryption, decryption, PSNR.

I. INTRODUCTION

A Steganography system, in general, is expected to meet three key requirements, namely, imperceptibility of embedding, accurate recovery of embedded information, and large payload (payload is the number of bits that get delivered to the end user at the destination) [1]. In a pure Steganography framework, the technique for embedding the message should be unidentified to anyone other than the sender and the receiver. An effective Steganography should posses the following characteristics [10-11]:

Secrecy: Extraction of hidden data from the host medium should not be possible without the knowledge of the proper secret key used in the extracting procedure.

Imperceptibility: After embedding the data in the medium, it should be imperceptible from the original medium.

High capacity: The maximum length of the hidden message that can be embedded can be as long as possible.

Resistance: The hidden data should be able to survive when the host medium has been manipulated, for example lossy compression scheme.

Accurate extraction: The extraction of the hidden data from the medium should be accurate and reliable.

This paper explains a way in which so that a video file is used as a host media to hide secret message without affecting the file structure and content of the video file. Because degradation in the quality of the cover object leads to noticeable change in the cover object which may leads to the failure of objective of Steganography.

In this paper we consider the motion estimation stage of video compression. The contents are processed during video encoding/decoding. This makes less vulnerable to video steganalysis methods and is lossless coded, thus not prone to quantization distortions. The data bits of the message are hidden in motion vectors. A single bit is hidden in the least significant bit of the each motion vector.

The rest of the paper is organized as follows: in Section II we overview the terms of video compression and decompression. The proposed method is given is explained briefly in Section III and algorithm for our proposed method is given in Section IV followed by the results and analyses in Section V. Finally, the paper is concluded in Section VI.

II. OVERVIEW

In this section, we overview lossy video compression to define our evaluation. There are three types of *pictures* (or frames) used in video compression: I-frames, P-frames, and B-frames centered mainly on amount of data compression. They are different in the following characteristics:

- **I**- (Intra-coded) frames are the least compressible but don't require other video frames to decode.
- **P**- (Predicted) frames use data from previous frames to decompress and are more compressible than I-frames.
- **B**- (Bi-predictive) frames use both previous and forward frames for data reference to get the highest amount of data compression.

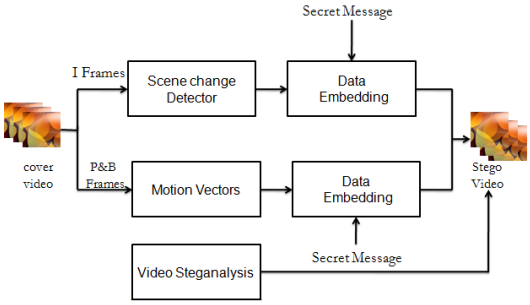

Fig.1: Block diagram of the video Steganography using I, P, B frames separately

At the encoder, the I- frame is encoded using image compression techniques. So the decoder reconstructs it. The I-frame is used as a reference frame for encoding P or B frames. In Motion Picture Expert Group (MPEG-2) standard, the video is ordered into groups of pictures (GOPs) whose frames are encoded in the sequence: [I,B,B,P,B,B,P,B,B]. The temporal redundancy between frames is exploited using block-based motion estimation which is applied on macroblocks $B_{ij}$of size $b\times b$ in P or B and searched in target frame(s). The motion field in video compression is translational with horizontal component $d^x$and vertical component d^y. It's representation in vector form is$d(x)$ for the spatial variables $X = (x, y)$in the underlying image. The search window is constrained by assigning limited n-bits for $\boldsymbol{d}$i.e., both d^x and$d^y \in [-2^{n-1}, 2^{n-1}-1]$. An exhaustive search in the window of size $b+2^n X b+ 2^n$ is done to find the optimal motion vector which satisfies the search criterion. Since $\boldsymbol{d}$ does not represent the true motion in the video, the compensated frame $\tilde{P}$ using $(x + \boldsymbol{d(x)})$ is associated with a prediction error $E(x) = (P - \tilde{P})(x)$ in order to be able to reconstruct $P=\tilde{P} + E$ with minimum distortion at the decoder in case of P frame. Similar operation is done for the B-frame but with the average of both the forward compensation from a previous reference frame and backward compensation from a next reference frame. E is of the size of an image and is thus lossy compressed using JPEG compression reducing its data size. The lossy compression quantization stage is a nonlinear process and for every motion estimation method, the pair $(\boldsymbol{d},E)$ will be different and the data size $\boldsymbol{D}$ of the compressed error $\tilde{E}$ will be different. The motion vectors $\boldsymbol{d}$ are lossless coded and thus become an attractive place to hide a message that can be extracted by a special decoder.

The decoder receives the pair $(\boldsymbol{d},\tilde{E})$, applies motion compensation to form $\tilde{P}$ or$\tilde{B}$ and decompress $\tilde{E}$to obtain a reconstructed E_r. Since E and $E_r$are different by the effect of quantization,then the decoder in unable to reconstruct P identically but it alternatively reconstructs $P_r= \tilde{P} + E_r$. The reconstruction quality is usually measured by the mean squared error $P - P_r$, represented as peak signal-to-noise ratio (PSNR) and we denote it by R.

III. PROPOSED WORK

A. Video Compression

Video compression uses modern coding techniques to reduce redundancy in video data. Video compression typically operates on square-shaped groups of neighboring pixels, often called macro blocks. These pixel groups or blocks of pixels are compared from one frame to the next and the video compression code sends only the differences within those blocks. In areas of video with more motion, the compression must encode more data to keep up with the larger number of pixels that are changing. Generally, the motion field in video compression is assumed to be translational with horizontal component and vertical component and denoted in vector form by for the spatial variables in the underlying image. Such as three steps search, etc. Administrator chooses one video file along with one key compress and send to the member. The Authenticated member decompresses the video file and takes the second privacy key.

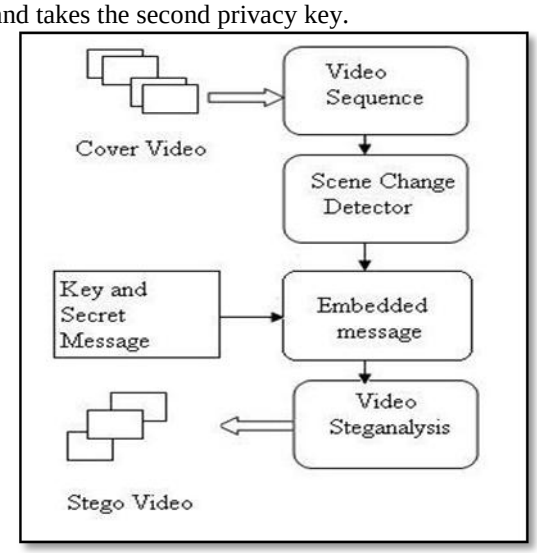

Fig.2: Block diagram proposed model

B. Motion Vector

In video compression, a motion vector is used for motion estimation process. It is used to represent a macro block in a picture. Authenticated person after taking the second privacy key, can see the video in our application, in that video it can detect the motion vector. After seeing this, the member uses the key to see the message sent to the administrator.

C. Encryption

Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Original message is hidden

within a carrier such that the changes occurred in the carrier are not observable. The information about the private key is used to encrypt the text.

D. Extraction of original data

Decryption is the process of converting encrypted data back into its original form, so it can be understood. When the user inputs the correct key that is used at the decryption process, this will extract the original message that is encrypted and embedded.

E. Peak signal-to-Noise Ratio

Larger SNR and PSNR indicate a smallerdifference between the original (without noise) and reconstructed image. The main advantage of this measure is ease of computation but it does not reflect perceptual quality. An important property of PSNR is that a slight spatial shift of an image can cause a large numerical distortion but no visual distortion.

IV. ALGORITHM FOR PROPOSED MODEL

Algorithm for Encoding

Step 1: Input cover video file or stream.
Step 2: Read required information of the cover video.
Step 3: Break the video into frames.
Step 4: Compress the frame where the data is to be inserted using any compression technique, DCT was used in this paper.
Step 5: The data was hide using LSB algorithm.

Algorithm for Decoding

Step 1: Input stego video file or stream.
Step 2: Read required information from the stego video.
Step 3: Break the video into frames.
Step 4:Using the motion vector, the frame where the data is hide is chosen.
Step 5:The data is extracted from the LSBs of the identified frame.

V. EXPERIMENTAL RESULTS

Any Steganography technique is characterizedmainly by two attributes, imperceptibility andcapacity. Imperceptibility means the embeddeddata must be imperceptible to the observer(perceptual invisibility) and computer analysis (statistical invisibility). The performance of the proposed technique is evaluated using five different video streams (bulb.avi, pearson.avi, plot.avi, sample.avi and sinewave.avi)and one secret data.The perceptual imperceptibility of the embedded data is indicated by comparing the original image or video to its stego counterpart so that their visual differences, if any, can be determined.

Video name	Resolution (W*H)	Frame/Sec.	No. of Frames	size
Bulb	**232 X 232**	**15**	**80**	**740KB**
Person	**356 X 244**	**15**	**50**	**199KB**
Plot	**560 X 420**	**15**	**40**	**26.9MB**
Sample	**611 X 352**	**12**	**60**	**555KB**
Sine wave	**436 X 344**	**10**	**101**	**460KB**

Table 1: Cover video file information

Video Name	PSNR (dB)	MSE	Payload (Bytes)	ΔD (Bytes)	ΔR /Frame (dB)
Bulb	**38.71**	**9.51**	**4439**	**42014**	**0.483**
Person	**37.14**	**12.55**	**2545**	**23267**	**0.742**
Plot	**34.07**	**25.44**	**3032**	**27302**	**0.851**
Sample	**38.52**	**9.13**	**3054**	**30874**	**0.642**
Sine wave	**33.87**	**26.94**	**2286**	**22726**	**0.335**

Table 2: Obtained results information

Additionally, as an objective measure, the Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) between the stego frame and its corresponding cover frame are studied. The quantities are given as below.

$$\mathrm{MSE} = \frac{1}{H \times W} \sum_{i=0}^{h} (\mathrm{P(i,j)} - \mathrm{S(i,j)}) \quad (1)$$

Where, MSE is Mean Square error, H and W are height width and P (i,j) represents original frame and S(i,j) represents corresponding stego frame.

$$\mathrm{PSNR} = 10 \log \frac{L^2}{\mathrm{MSE}} \quad (2)$$

where, PSNR is peak signal to noise ratio, L istakenas 255.The cover file video details are given in Table 1 and results are tabulated in Table 2.

VI. CONCLUSION

In this paper, we propose and investigate the data hiding method using the motion vector techniquefor the moving objects, operating directly incompressed domain. This algorithm provides high capacityand imperceptible stego-image for humanvision of the hidden secret information. By embedding the data in the moving objects the quality of the video is increased. In this paper, the compressed video is used for the data transmission since it can hold large

volume of the data. The adaptive based compression technique is evaluated such that the data is embedding in the vertical and horizontal component pixels. The PSNR value is calculated to show that the frame is transmitted without any loss or distortion. As a result, the motion vector technique is found as the better solution since it hides the data in the moving objects rather than in the still pictures. The encryption enhances the security of the data being transmitted.

REFERENCES

[1] Hussein A. Aly, *"Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error*", Ieee Transactions On Information Forensics And Security, Vol. 6, No. 1, March 2011

[2] J. Zhang, J. Li, and L. Zhang, "*Video watermark technique in motion vector,"* in *Proc. XIV Symp. Computer Graphics and Image Processing*, Oct. 2001, pp. 179–182.

[3] C. Xu, X. Ping, and T. Zhang, "*Steganography in compressed video stream,"* in *Proc. Int. Conf. Innovative Computing, Information and Control (ICICIC'06)*, 2006, vol. II, pp. 803–806.

[4] P.Wang, Z. Zheng, and J. Ying, "*A novel videowatermark technique in motion vectors,"* in *Int. Conf. Audio, Language and Image Processing (ICALIP)*, Jul. 2008, pp. 1555–1559.

[5] S. K. Kapotas, E. E. Varsaki, and A. N. Skodras, "*Data hiding in H.264 encoded video sequences,"* in *IEEE 9th Workshop on Multimedia Signal Processing (MMSP07)*, Oct. 2007, pp. 373–376.

[6] D.-Y. Fang and L.-W. Chang, "*Data hiding for digital video with phase of motion vector*," in *Proc. Int. Symp. Circuits and Systems (ISCAS)*, 2006, pp. 1422–1425.

[7] X. He and Z. Luo, "*A novel steganographic algorithm based on the motion vector phase,"* in *Proc. Int. Conf. Comp. Sc. and Software Eng.*, 2008, pp. 822–825.

[8] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia "*Application of LSB Based Steganographic Technique for 8-bit Color Images*, World Academy of Science, Engineering and Technology 50 2009 Published

[9] Mritha Ramalingam "*Stego Machine – Video Steganography usingModified LSB Algorithm*",World Academy of Science, Engineering and Technology 74 2011 Published

[10] Saurabh SinghInvertis University Bareilly, India and Gaurav Agarwal Invertis University Bareilly, India "*Hiding image to video: A new approach of LSBreplacement*", International Journal of Engineering Science and TechnologyVol. 2(12),2010,6999-7003Published

[11] JOSEPHGILVARRY School of Computer Applications Dublin City University "*Calculationof Motion Using Motion Vectors Extracted from an MPEG Stream*" Technical report 20 September 1999 Dublin City University Published