ISSN:0975-9646

A Secure Data Hiding Technique in Compressed Video Using a Secret Key

V.Manjula, J.Rajani, K.Radhika

Asst.Prof, Dept of CSE.
Institute of Aeronautical Engg
Hyderabad, India

Abstract —**This paper deals with data hiding in compressed video. Unlike data hiding in images and raw video which operates on the images themselves in the spatial or transformed domain which are vulnerable to steganalysis, we target the motion vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video. The choice of candidate subset of these motion vectors are based on their associated macro block prediction error, which is different from the approaches based on the motion vector attributes such as the magnitude and phase angle, etc.**

A greedy adaptive threshold is searched for every frame to achieve robustness while maintaining a low prediction error level. The secret message bit stream is embedded in the least significant bit of both components of the candidate motion vectors. The method is implemented and tested for hiding data in natural sequences of multiple groups of pictures and the results are evaluated. The evaluation is based on two criteria: minimum distortion to the reconstructed video and minimum overhead on the compressed video size. Based on the aforementioned criteria, the proposed method is found to perform well and is compared to a motion vector attribute-based method from the literature.

Keywords-Steganalysis, Candidate motion vectors (CMV), Huffman Coding, Quantization index modulation (QIM).

I. INTRODUCTION

Data hiding and watermarking in digital images and raw video have wide literature. This paper targets the internal dynamics of video compression, specifically the motion estimation stage. We have chosen this stage because its contents are processed internally during the video encoding decoding which makes it hard to be detected by image steganalysis methods and is lossless coded, thus it is not prone to quantization distortions. In the literature, most work applied on data hiding in motion vectors relies on changing the motion vectors based on their attributes such as their magnitude, phase angle, etc.

The data bits of the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold, and are called candidate motion vectors (CMVs). A single bit is hidden in the least significant bit of the larger component of each CMV, the data is encoded as a region where the motion estimation is only allowed to generate motion vectors in that specified region. Using the variable macro block (16 x 16, 16 x 8, 8 x 16, 8 x 8) sizes of H.264, the authors in
used every 2 bits from the message bit stream to select one of the four sizes for the motion estimation process.

We embed the data in video using the phase angle between two consecutive CMV. These CMV are selected based on the magnitude of the motion vectors as in. The message bit stream is encoded as phase angle difference in sectors between CMV. The block matching is constrained to search within the selected sector for a magnitude to be larger than the predefined threshold.

The methods in focused on finding a direct reversible way to identify the CMV at the decoder and thus relied on the attributes of the motion vectors. In this paper, we take a different approach directed towards achieving a minimum distortion to the prediction error and the data size overhead. This approach is based on the associated prediction error and we are faced by the difficulty of dealing with the nonlinear quantization process;

II. RELATED WORK

Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent un authorized copying directly. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections

An effective data-hiding scheme that embeds data in digital videos using the phase angle of the motion vector of the macro block in the inter-frame. The scheme can be applied to either compressed or uncompressed videos. Furthermore, the embedded data can be extracted directly without using the original video sequences.

The embedding is designed to achieve efficient trade-offs among the three conflicting goals of maximizing information-embedding rate, minimizing distortion between the host signal and composite signal, and maximizing the robustness of the embedding. We introduce new classes of embedding methods, termed quantization index modulation (QIM) and distortion-compensated QIM (DC-QIM), and develop convenient realizations in the form of what we refer to as dither modulation. Using deterministic models to evaluate digital watermarking methods, we show that QIM is provably good" against arbitrary bounded and fully-informed attacks, which arise in several copyright applications, and in particular it achieves provably better rate-distortion-robustness trade-offs than currently popular spread-spectrum and low-bit(s) modulation methods.

III. Overview Of Data Hiding Technique

The following figure shows data hiding technique in compressed video.The input video is seperated into frames.Then the frames are subjected to DCT and huffman coding to compress the frame. Using the secret key and LSB algorithm data is inserted.This generated video is stego video. The secret data can be extracted using inverse LSB and secret key.

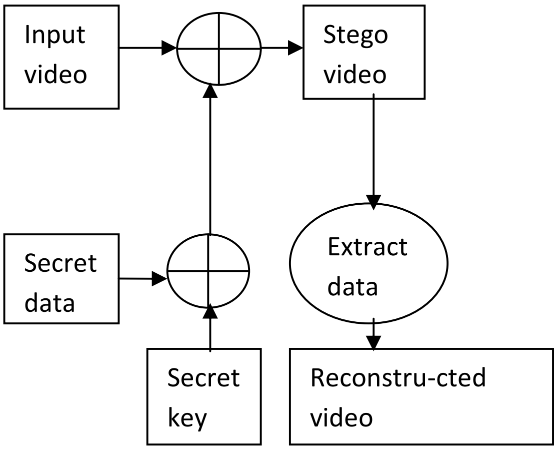

FIGURE 1.Data hiding technique

A. LSB algorithm

Embedding message is performed for two pixels *X* and *Y* of a cover image at a time and then adjusting one pixel of the (*X*, *Y*) to embed two secret bits message *s1 s2*. The embedding flowchart is shown in Fig.2 and the embedding procedure is described as following:

Step 1. If the LSB of *X* is the same as *s1*, go to step 2.Otherwise, go to step 3.

Step 2. If the value of *f (X, Y)* is the same as *s2*, do not change any pixel. Otherwise, the value of pixel *Y* is increased or decreased by 1.

Step 3. If the value of *f (X* −1, *Y) is* the same as *s2*, the value of pixel *X* is decreased by 1. Otherwise, the value of pixel *X* is increased by 1.Where the function *f*(*X*, *Y*) is defined as

$$f(X',Y') = LSB\left(\left\lfloor \frac{X'}{2} \right\rfloor + Y'\right)$$

Since this new LSB matching method just only increase or decrease 1 in two adjacent pixels, the difference of the two neighborhood pixel between cover image and stego-image is very small. Hence, it can keep high quality while hiding data.

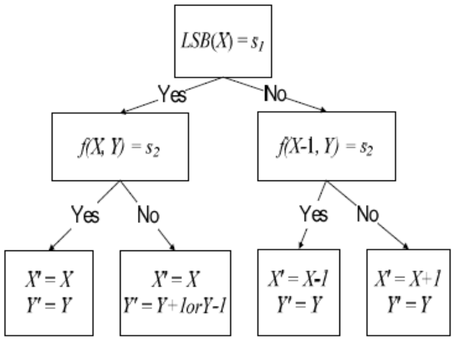

FIGURE 2: The LSB matching embedding procedure.

B. Data hiding algorithm

Input: Video

Output: Stego video

Step 1: Read the input Video

Step 2: Perform frame seperation

Step 3: Apply Integer DCT on each 8×8 block.

Step 4: Perform Zigzag Scanning on each 8×8 block.

Step 5: Apply Huffman coding to compress the frame.

Step 6: Apply secret key to hide the data.

Step 7: Apply LSB Algorithm to embed data

Step 8: Generate Stego video

C. Data Extraction algorithm

Input: Stego video

Output: Hidden data

Step 1: Read Stego video.

Step 2: Perform decoding using IDCT and Inverse Huffman coding.

Step 3: Extract hidden data using ILSB and Secret Key.

D. *Secret key generation algorithm*

Step 1: Take a key which is a prime number

```
Step2:  Generate two prime numbers p, q
        nearer to given key.
Step3:  Calculate n=p*q;
Step 4: Calculate m= (p-1)(q-1).
Step 5: Generate e
           Assume e=1; x=1;
           While (mod(m,e)==0)
           e = e+1;
Step 6: Generate d
           Take s=1+x*m;
           While (mod(s,e) ~= 0)
            x = x+1;
            s=1+x*m;
            d=s/e;
```

IV.Experimental Results

The relative performance of reconstructed frame from sample video was tested. All the frames considered are of size 256 X 256. The transforms were made on blocks of size 8 X 8, which is a typical value used in common image and video compression techniques. With such a block size, there are 64 coefficients. The number of non zero coefficients in the transform domain is varied between 1 and 64. The MSE and the PSNR of the reconstructed frame as compared to the reference frame, for varying amount of number of non zero coefficient used, is presented as follows.

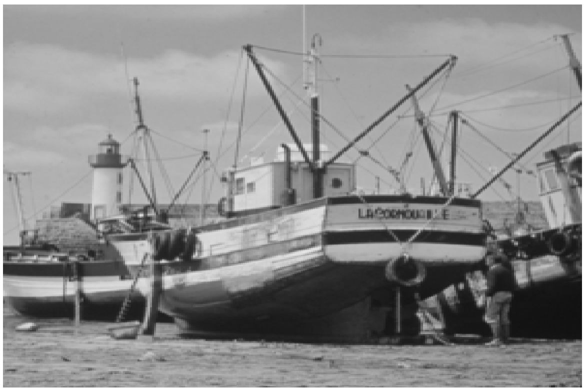

FIGURE.3 Sample Boat frame

To establish an objective criterion for digital image quality, a parameter named PSNR (Peak Signal to Noise Ratio) is defined as follows:

$$PSNR = 10\log_{10}\frac{255^2}{MSE}$$

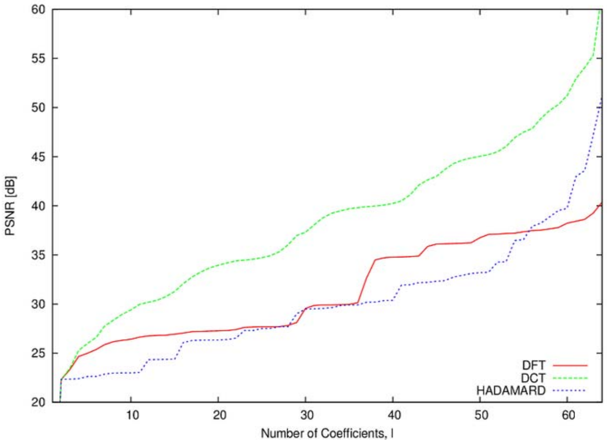

FIGURE.4 PSNR for boat frame

MSE (Mean Square Error) stands for the mean-squared difference between the cover-image and the stego-image. The mathematical definition for MSE is:

$$MSE = (\frac{1}{M \times N})\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij} - b_{ij})^2$$

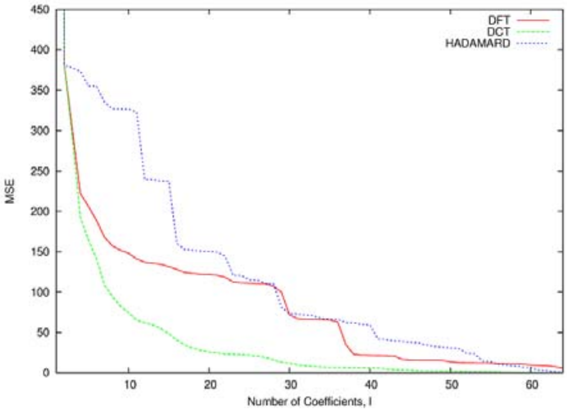

FIGURE.5 MSE for boat frame

Where a_{ij} means the pixel value at position (*i*, *j*) in the cover image and b_{ij} means the pixel value at the same position in the corresponding stego-image. The calculated PSNR usually adopts dB value for quality judgment. The larger PSNR is, the higher the image quality is (which means there is only little difference between the cover-image and the stego-image)

V.Conclusion And Future Work

A greedy search for the suitable value of the threshold to be used for choosing the macroblocks corresponding to the CMV is done such that the candidates will be identically identified by the decoder even after these macroblocks have been lossy compressed. The embedding and extraction algorithms are implemented and integrated to the MPEG-2 encoder/decoder and the results are evaluated based on two metrics: quality distortion to the reconstructed video and data size increase of the compressed video. The method is compared to another one from the literature that relies on a motion vector attribute. The proposed method is found to have lower distortion to the quality of the video and lower data size increase. Future work will be directed towards increasing the size of the embedded payload while maintaining the robustness and low distortions

References

[1] A.Z. Tirkel, R.G. Van Schyndel, C.F. Osborne, A digital watermark, Proceedings of ICIP 1994, Austin Convention Center, Austin, Texas, Vol. II, 1994, pp. 86–90.

[2] W. Bender, N. Morimoto, A. Lu, Techniques for data hiding, IBM Syst. J. 35 (3/4) (1996) 313–336.

[3] T.S. Chen, C.C. Chang, M.S. Hwang, A virtual image cryptosystem based upon vector quantization, IEEE Trans. Image Process. 7 (10) (1998) 1485–1488.

[4] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread spectrum image steganography, IEEE Trans. Image Process. 8 (8) (1999) 1075–1083.

[5] K.L. Chung, C.H. Shen, L.C. Chang, A novel SVD- and VQ-based image hiding scheme, Pattern Recognition Lett. 22 (9) (2001) 1051–1058.

[6] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 36 (25) (2000) 2069–2070.

[7] Chi-Kwong Chan, L.M. Cheng, Improved hiding data in images by optimal moderately signi7cant-bit replacement, IEE Electron. Lett. 37 (16) (2001) 1017–1018.

[8] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671–683.