IMPROVED PROTECTION IN VIDEO STEGANOGRAPHY USED COMPRESSED VIDEO BITSTREAMS

S. Suma Christal Mary M.E (Ph.D)
Lecturer Department of CSE
PSN College of Engg & Technology
Tamilnadu, India

***Abstract*----- In this paper propose a new method for the real-time hiding of information used in compressed video bitstreams. This method is based on the real-time hiding of information in audio steganography. This method of steganography is very similar to the two discussions of image steganography and video steganography. A new compressed video secure steganography(CVSS) algorithm is proposed. In this algorithm, embedding and detection operations are both executed entirely in the compressed domain, with no need for the decompression process. The new criteria employing statistical invisibility of contiguous frames is used to adjust the embedding strategy and capacity, which increases the security of proposed algorithm. Therefore, the collusion resistant properties are obtained. Video steganalysis with closed loop feedback manner is design as a checker to find out obvious bugs.**

Keywords; Video Steganography, Real-Time Steganography, Information Hiding, Compressed bit streams

I. INTRODUCTION

The Steganography is of Greek source and means "enclosed or hidden writing". Data hiding should be used concealed transmissions, closed captioning, indexing, or watermarking. It is in contrast to cryptography, where the survival of the message itself is not masked, but the content is hidden. Steganography is implemented in different fields such as military and Industrial applications. By using lossless steganography techniques messages can be sent and received securely. Traditionally, steganography was based on hiding secret information in image files .Lately, there has been growing interest in implementing steganographic techniques to video files as well as audio files. The advantage of using video files in hiding information is to be added security against hacker attacks due to the relative complexity of video compared to image files and audio files. Image-based and video-based steganography techniques are mainly classified into spatial domain and frequency domain based methods. The main aim of steganography is to hide information in the other wrap media so that other persons will not observe the existence of the information. This is a major distinction between this method and the other methods of secret exchange of information because, for example, in cryptography, the individuals perceive the information by considering the implied information but they will not be able to realize the information. However, in steganography, the existence of the information in the sources will not be noticed at all. Most steganography jobs have been carried out on images, video clips, texts, music and sounds. For video stream usually being accessible in compressed form, steganography algorithms that are not applicable in compressed bit-stream would require complete or at least partial decompression. This is an unnecessary saddle best avoided. If the requirement of strict compressed domain steganography is to be met, the steganography needs to be embedded in the compressed domain. Nowadays, there are large amount of video watermarking algorithms been proposed. Some of them are applied for compressed video. To be useful, a steganographic technique should not be easily detectable. If the existence of secret message can be detected with a probability higher than random guessing, the corresponding steganographic technique is considered to be invalid. Similar to cryptography and steganography may suffer from the attack method (steganalysis). Much of the research work in the field of steganalysis has been carried out on images. One approach is based solely on the first order statistics and is applicable only to idempotent embedding. Another major stream is based on the concept of blind steganalysis, which is formed by blind classifiers. The classifier should be trained to learn the differences between cover and stego-image features at first. In this paper, we propose a secure compressed video steganography architecture taking account of steganalysis module, operated in a closed-loop manner to enhance the anti-steganalysis capability of the stegovideo with data embedded. steganography.

This paper is organized as follows: Section 2 describes the compressed video bit streams. In Section 3, the video secure steganography detail. The Section 4 is the

performance analysis. We give the experimental results in Section 5.In Section 6, a conclusion is explained.

II. COMPRESSED VIDEO STREAMS

The framework for CVSS included four function parts, the video sequence parser, the scene change detector, the secret message embedder and the video steganalysis. Compressed video sequence supported compression through the elimination of temporal, spatial and statistical redundancies with the use of motion compensation, block quantization inside a discrete cosine transform (DCT), and Huffman run-level encoding. With this compression, the video bit-stream consists of variable length codes (VLCs). The cover video sequence *U* pass through the sequence parser module at first, that have VLD (variable length decoder), to be parsed as VLC code denotes the corresponding various segments of the video including, intra coded macro blocks, DCT coefficients and motion vectors, etc. After that, the second module, scene change detector, can divide the sequence into several slow speed and single scene video sub-sequences. In the video sequence, a shot is defined as one object is shot with the same camera in a same place. The scene is defined as several continuous shots. The pictures in one scene have the similar features. Scene change detector is to find out the scene change point among the group of pictures. In proposed framework, DCT coefficients are used in the scene change detector module for the real time requirement. Embedding operations are taken place in I frames, therefore detector searching the scene change point among I frames in the compressed format.The I frames in MPEG standard is coded in intraframe manner, we can obtain the DC picture with abstracting the DC coefficients from the DCT coefficient codes. Eq1 describes the compare method between two conjoint I frames: therefore the scene change point is found. Also the variances var(*i*) *U* of each DC picture from I frame will be calculated and provided to the embedding process module. With the third module, message embedder, secret message *M* is hidden into the compressed video sequence without bringing perceptive distortion. There have two different embedding modes, inter-frame and intra-frame. To avoid the collusions attack [19], statistical invisibility is employed to adjust the capacity of the secret message adaptively. Also the chaotic dynamic system and VLC maps embedding algorithm will be used at the same time. This module is the key part in the framework, and will be described detailedly in the next section. The last module, video steganalysis, is used as a checker for the message hiding security in the stegovideo sequence. With the principle of collusion deviation of the DC and AC coefficients between contiguous frames is statistical visible. Also the correlation between frames in one scene is used as another measurement of the data change. Using the first and higher order measurements statistics as input of the artificial intelligence classifier, the embedding of message can be detected in the stego-video sequence with a constant probability. If the stego-video cannot pass through the checker, the scale factor must be adjusted to manipulate the strength of hidden message. With these four modules, we can obtain the final stego-video *X* with anti-steganalysis capability by holding the original statistical invisibility.

III. VIDEO SECURE STEGANOGRAPHY

In the proposed algorithm, the positive even and negative odd DCT coefficients represent zero and positive odd and negative even coefficients represent one. And the value 1 should be modified into -1 or 2, and value -1 should be modified into -2 and 1.

Algorithm**:** To Compressed video secure stego-system

Input: Cover video *U,* key stream *key,* message *S*

Output: **S**tego-video *X,*adjust coefficient β .

A.Preprocess:
*Step 1***:** Encrypt message

$C \leftarrow Ekey\ (\ M\ )$;

Step 2: For each I frame *i F* calculate the pixel value variance $2\sigma\ Fi$ with the DCT DC coefficients; the accuracy of the prediction, we propose another measure to evaluate the prediction rule changes.

Step 3: **A**llot payload to each frame.

Step 4: For each *si* , arrange the message bit to available DCT AC coefficients, and estimate the change of special pixel values variance ΔDi ;

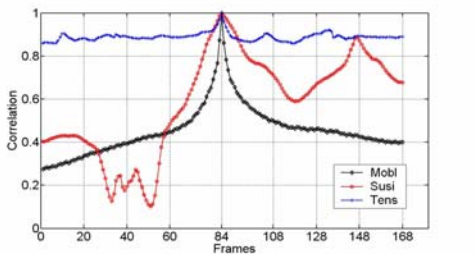
Step 5: calculate the correlation of 2
$\sigma\ Fi$ and ΔDi
if $Corr\ Fi\ Di < T$
goto step3 to adjust the coefficient β ;

B.Embedding:
Step 6: for each *i s* , manipulate the message bit embedding from the least value DCT coefficients to finish the embedding process.
Return *X* and β ;

IV. EXPERIMENTAL RESULTS

In this experiment, the sequences that are collect from the simulations consist of color compressed video sequences in the MPEG-2 format. 42 m2v format compressed video streams are obtained from the online video database on www.mpeg2.de. Fig2 shows several frames with same sequence number from the different correlation kind compressed video streams. And three different correlation types of the video streams is shown in Fig.3. Fig 4 shows the PSNR value and correlation value change magnitude of the stego-video, it means the perception quality and intra frame correlation of test video is little changed.

(Fig:1)



(Fig:2)

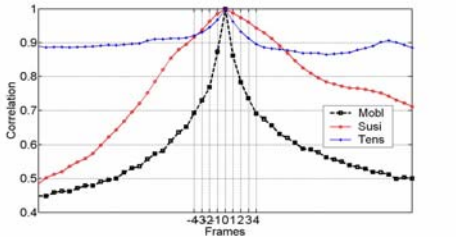
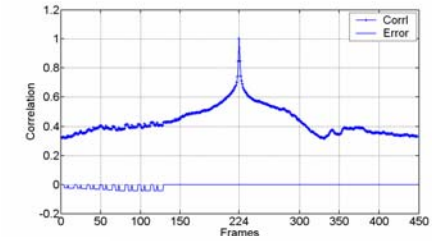
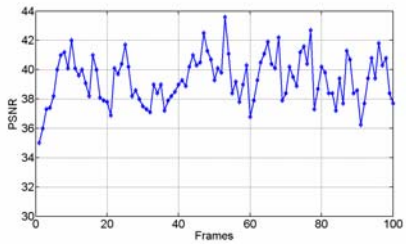


Fig.1,Fig.2 Two different correlation types of the video streams and the zoom in

(Fig:3)





(Fig:4)

Fig.3 &4 Two different PSNR and correlation change magnitude of the stego-video after message embedding

CONCLUSIONS

In this paper, a new method of real-time steganography using video bit streams was provided. The basis of this method is using the combination of video, audio, text. With this method, the data should be transferred more secured manner. In order to hide information in the output message, one can make use of other methods of image steganography, which is impartial to the provided furtively. By improving this method, we can get the video files without any noise distraction. one new secure and file-size preserving compressed domain steganography is proposed. Embedding and detection are both done entirely in the compressed domain to meet the real time requirement. Change of the spatial pixel values variance can be estimated in the compressed domain, and the embedding payload is allotted according to the variance of each cover frame. Therefore the correlation of the continuous frames is unchanged. The performance of the steganography algorithm is studied and the experimental results showed this scheme can be applied on compressed videos with no noticeable degradation in visual quality.

REFERENCES

[1] K. Su, D. Kundur, and D. Hatzinakos, "Statistical invisibility for collusion-resistant digital video watermarking," IEEE Trans. Multimedia, 2005,(7)1:43-51

[2] U. Budhia, D. Kundur, T. Zourntos. Digital Video Steganalysis Exploiting Statistical Visibility in the Temporal Domain. IEEE Trans. Information Forensics and security, 2006, (1)4:502-516.

[3] G. C. Langelaar. Watermarking Digital Image and Video Data. IEEE Signal Processing Magazine, 2000,
(17)5:20-46.

[4]Y. J. Dai, L. H. Zhang and Y. X. Yang. A New Method of MPEG Video Watermarking Technology. International Conference on Communication Technology Proceedings (ICCT), 2003.

[5] C. Lu, J. Chen and K. Fan, "Real-time Frame-Dependent Video Watermarking in VLC Domain", *Signal Processing: Image Communication 20*, 2005

[6] J. Haitsma and T. Kalker, "A Watermarking Scheme for Digital Cinema", *Proceedings of the IEEE*
International Conference on Image Processing, Vol. 2,2005, pp. 487–489.

[7] C. Busch, W. Funk and S. Wolthusen, "Digital Watermarking: From Concepts to Real-Time Video
Applications", *IEEE Computer Graphics and Applications*, January/February 2004, pp. 25-35.

[8] G. C. Langelaar and R. L. Lagendijk. Optimal Differential Energy Watermarking of DCT Encoded Images and Video.IEEE Transactions on Image Processing, 2001,10(1): 148-158.

I am working as a lecturer in PSN college of Engg. & Tech. My area of interest Network Security, Cyber Security. I am doing Ph.D degree in the area of Cyber Security