International Journal of Computer Science
Oddity...Probe...Reviste...

http://www.ijcsjournal.com Volume 1, Issue 1, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-001 PAGE NO: 001-005

A Secured Data Hiding Techniques for Motion Vectors using stenography

C.AGJELIA LYDIA [#1], *A.MANJULA* [*2]

[#1] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
agjelia@gmail.com

[*2] *PG IN COMPUTER SCIENCE AND ENGINEERING*
NPR COLLEGE OF ENGINEERING AND TECH
NATHAM DINDIGUL,INDIA
mnjlarumugma@gmail.com

Abstract— **A technique for high capacity data hiding in MPEG-2 streams is presented Data hiding techniques to reduce the signaling information resulting from an improvement of Inter-coding.. The objective is to maximize the payload while keeping robustness and simplicity by transforming the co-efficient. We propose a robust error resilient approach for MPEG video transmission over internet. In this work, we develop an error resilient video encoding approach to help error concealment at the decoder and the modification is performed via rate-distortion optimization.. We introduce a new block shuffling scheme to isolate erroneous blocks caused by packet losses. And we apply data hiding to add additional protection for motion vectors. Apart from the advantage of increase message payload, excessive bit rate and quality distortion the proposed solution overcome the packet loss and provide security to the hidden message in MPEG Video.This paper deals with data hiding in compressed video. we target the motion vectors used to encode and reconstruct both the forward predictive (P)-frame and bidirectional (B)-frames in compressed video.**

***Index Terms*— Data hiding, motion vectors, Motion Picture Expert Group (MPEG), steganography, packet loss.**

I.INTRODUCTION

Digital watermarking, or information hiding, refers to techniques for embedding additional data in host media. Most of the previous research has focused on still image watermarking. Although video watermarking has more potential for commercial applications, less research has been conducted on high capacity data hiding in video streams. Ancillary data embedded in a video stream can carry information about the content itself, low-level descriptors for

video indexing retrieval and segmentation. Other applications include annotation, subtitling, multi-lingual services, tele-text, etc. Due to the data intensive nature of video, in most applications it is required to hide data in the compressed stream. Compared with still images, video watermarking presents a much higher capacity or bandwidth. At the same time the computational complexity in video watermarking is higher due to the amount of data that need to be processed. In this paper, we focus on a blind data hiding technique tailored to MPEG-2 video streams.

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

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 1, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-001 PAGE NO: 001-005

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.

Methods such as spread spectrum are used, where the basic idea is to distribute the message over a wide range of frequencies of the host data. Transform domain is generally preferred for hiding data since, for the same robustness as for the spatial domain, the result is more pleasant to the Human Visual System (HVS). For this purpose the DFT (Discrete Fourier Transform), the DCT (Discrete Cosine Transform), and the DWT (Discrete Wavelet Transform) domains are usually employed.
Recent video data hiding techniques are focused on the characteristics generated by video compressing standards. Motion vector based schemes have been proposed for MPEG algorithms. Motion vectors are calculated by the video encoder in order to remove the temporal redundancies between frames. In these methods the original motion vector is replaced by another locally optimal motion vector to embed data. Only few data hiding algorithms considering the properties of H.264 standard [8-10] have recently appeared in the open literature. In [8] a subset of the 4×4 DCT coefficients are modified in order to achieve a robust watermarking algorithm for H.264. In [6] the blind algorithm for copyright protection is based on the intra prediction mode of the H.264 video coding standard.

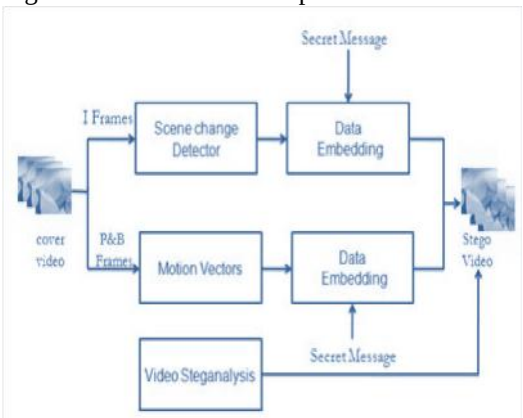
II.TYPES OF HIDING TECHNIQUES

They are different inthe following characteristics:

☐ **(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.



At the encoder, the intra-predicted (I)-frame is encoded using regular image compression techniques similar to JPEG but with different quantization table and step; hence the decoder can reconstruct it independently. The I-frame is used as a reference frame for encoding a group of forward motion compensated prediction (P)- or bi-directionally predicted (B)-frames. In the commonlyused Motion Picture Expert Group (MPEG-2) standard , the video is ordered into groups of pictures (GOPs) whose frames can be encoded in the sequence: [I,B,B,P,B,B,P,B,B].

III.EXISTING WORK

Video data hiding techniques are focused on the characteristics generated by video compressing standards. Motion vector based schemes have been proposed for MPEG algorithms . Motion vectors are calculated by the video encoder in order to remove the temporal redundancies between frames. In these methods the original motion vector is replaced by another locally optimal motion vector to embed data. Only few data hiding algorithms considering the properties of H.264 standard.

In a subset of the 4×4 DCT coefficients are modified in order to achieve a robust watermarking algorithm for H.264. In [6] the blind algorithm for copyright protection is based on the intra prediction mode of the H.264 video coding standard. The well established H.264/AVC video coding standard has various motion-compensation units in sizes of 16×16, 16×8, 8×16, 8×8, and sub8×8 . For sub8×8, there are further four sub-partitions of sub8×8, sub8×4, sub4×8, and sub4×4. In this paper we propose a new data hiding scheme, which takes

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 1, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-001 PAGE NO: 001-005

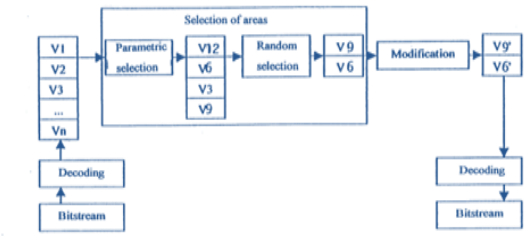
advantage of the different block sizes used by the H.264 encoder during the inter prediction, in order to hide the desirable data. The message can be extracted directly from the encoded stream without knowing the original host video. This method is best suited for content-based authentication and covert communication applications.

The 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 methods is mainly 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.

IV. WORK ON COMPRESSED MOTION VECTOR

Since a video can be viewed as sequences of still images, video watermarking is an extension of image watermarking. The applications for still image watermarking can thus be extended to video watermarking by embedding data in singleframes. In order to minimize the color distortion in the watermarked video, the Y component of the YUV color space is used for the data embedding process. Embedding the watermark into the U and the V components may result in undesirable color distortions. As enlightened we can use the similar data hiding method for video. The Y component of MPEG-2 intraframes (I frames) is used to embed the watermark signal. outlines the embedding process. In order to avoid strong reduction of the video quality, due to concatenation of MPEG-2 coding, the embedding stage is not carried out on the fully decompressed data. Only data extracted directly from the compressed stream is used. The complete data hiding process is outlined in the sequel. First, the candidate I frame for data hiding is extracted. Then the Variable Length Code (VLC) of the intracoded block is obtained. The VLC of AC components of the selected block is decoded to get the quantized values which are integer numbers. The watermark is embedded in these AC components by applying the following modulation rule:

- To embed the bit '1', the value of the selected AC component is changed to the nearest even number. To embed bit
- '0', the value of the selected AC component is changed to the nearest odd number.



Since MPEG-2 is the most popular video compression standard, several experiments have been conducted to validate the proposed approach. In these experiment the watermark is embedded in the mid-frequencies bands of compressed video sequences. The watermark remains detectable even when the video undergoes compression ratios at which the host signal is significantly degraded. Since very person has a different visual sensitivity

Published by SK Research Group of Companies (SKRGC).

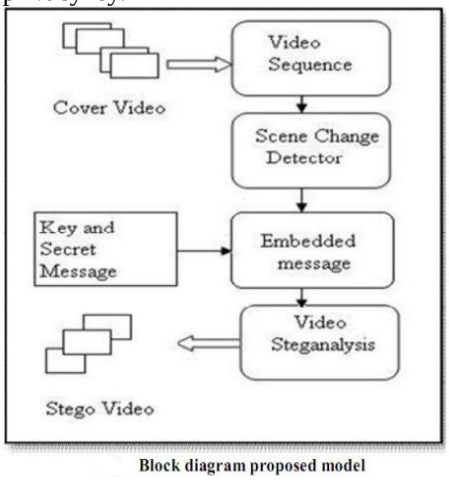
International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 1, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-001 PAGE NO: 001-005

threshold, it is hard to give theoretical limits. The performed experiments show that even the 'perfect eyes' cannot detect the watermark in a movie unless they do a frame by frame assessment using the original sequences to find the differences.

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.,

This is based on the video device processing power, the required compression ratio, and the reconstruction quality.Admin has to be choose one video file along with one key, both will be compression and createone encoding key send to the member. The Authenticated member uncompressed the video file and takes the second privacykey.



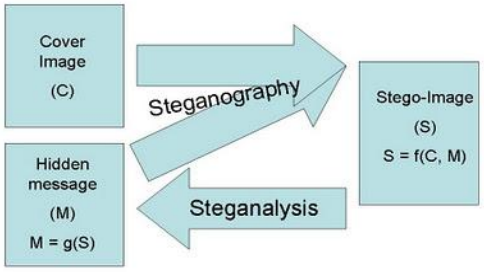
Block diagram proposed model

B. Motion Vector

In video compression, a motion vector is the key element in the motion estimation process. It is used to represent a macro block in a picture based on the position of this macro block (or a similar one) in another picture, called the reference picture. Authenticated person after taking the second privacy key he has only the authority what are the video which was sent by Admin, the member can see the video in our application, in that video it can detect the motion vector. After seeing this, the member obtain both of the key and given to the login section and send the message to the Admin.

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 being hidden within a carrier such that the changes so occurred in the carrier are not observable. The information about the user defined information, the carrier are not observable. The information about the private Key is used to encrypt the text.



Stego Magic which was used to compress the original message using stego analysis and can be decrypted to get the original text after data hiding through can be done through these stego analysis.

Here with it can detect the errors and eliminate the errors while compression can be established using this stegnographical method.

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 private key used to encrypt the text and the average time of the frame format is given. The encryption of the text is done by using the AES standard algorithm

Published by SK Research Group of Companies (SKRGC).

International Journal of Computer Science
Oddity...Probe...Reviste...
http://www.ijcsjournal.com Volume 1, Issue 1, No 1, 2013. ISSN: 2348-6600
Reference ID: IJCS-001 PAGE NO: 001-005

since the key size is larger for the AES.

E.Peak signal-to-Noise Ratio

Larger SNR and PSNR indicate a smaller difference 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.

CONCLUSION

In this paper, we propose and investigate the data hiding method using the motion vector technique for the moving objects, operating directly in compresseddomain. This offers excellent performance without error correction coding. In particular, the hiding capacity obtained under MPEG attack using our schemes can be very high without requiring complicated embedding and decoding schemes. The proposed watermark method for video is at least robust against MPEG-1/ MPEG-2 compression attacks. 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 and same criteria of MPEG file format is compared with the .avi file format is done.

REFERENCES

[1] High-Capacity Data Hiding in MPEG-2 Compressed Video *Yulin Wang and Ebroul Izquierdo*Department of Electronic EngineeringQueen Mary, University of London.

[2] Secured Data Transmission Based Video Steganography B.Suneetha1, Ch.Hima Bindu2 & S.Sarath Chandra3 International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315-4489, Vol-2, Iss-1, 2013

[3] M. Rama Koteswara Rao, Bhookya Nageswararao Naik International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com Vol. 2, Issue4, July-August 2012, pp.1577-1582

[4] International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013 3 ISSN 2250-3153

[5] Chiou-Tung Hzu; Ja-Ling Wu , "Digital watermarking for video",Digital Signal Processing Proceedings, 1997. DSP97., 1997 13th International Conference on , Volume:1997 Page(s): 217 -220 vol.1

[6] Arena, S.; Caramma, M.; Lancini, R. " Digital watermarking applied to MPEG-2 coded video sequences exploiting space and frequency masking " ,Image Processing, 2000. Proceedings. 2000 International Conference on , Volume:1 , 2000 Page(s): 438 -441 vol.1

[7] Checcacci, N.; Barni, M.; Bartolini, F.; Basagni, S. "Robust video watermarking for wireless multimedia communications",Wireless Communications and Networking Conference, 2000. WCNC. 2000 IEEE , 2000 Page(s):1530 -1535 vol.3

[8] Jun Zhang; Maitre, H.; Jiegu Li,"Embedding watermark in MPEG video sequence ", Multimedia Signal Processing, 2001 IEEE Fourth Workshop on , 2001 Page(s): 535 -540

[9] H. Nakazawa,A.Kosate,G. Morrson, and H. Tominaga, "A study on digital watermarking on MPEG2 video for copyright protection,", 1997 Symposium on Cryptography and Information Security,SCIS'97-31D,Fukuoka,1997.

[10] H.Inaba andM. Kasahara,"Note on digital watermark for video image,"1998 Symposium on Cryptography and Information Security,SCIS'98-82F ,Hamanako,1998.

[11] 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.

[12] 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