I J C T A, 10(9), 2017, pp. 541-546 ISSN: 0974-5572
© International Science Press

Overview of Video Steganography in Compressed Domain

Mukesh Dalal* and Mamta Juneja**

ABSTRACT

The growth in communication technology and usage of internet has greatly facilitated transfer of data. However, internet is an open communication channel due to which it has greater vulnerability to be attacked by an unauthorized party. Traditionally, cryptography and encryption was used for secret communication. However, secret information is not protected once decoded because it will attract the intruders. Steganography is the art and science of secret communication that hides the existence of the secret message in communication. It can be done by utilizing any multimedia file such as image, audio, video etc. Nowadays, videos are being utilized for steganography due to its greater hiding capacity and its popularity on internet. As videos are generally stored in compressed domain so this paper provides the survey of video steganography techniques in compressed domain.

Index Terms: Compressed Domain, Cryptography, Spatial Domain, Temporal Domain, Video Steganography.

1. INTRODUCTION

Steganography is derived from two Greek words- steganos and graphia which means "covered writing"[1]. Steganography is an art and science for hiding data in a way so that no one apart from the sender and intended receiver able to see the hidden message. Steganography is the centuries old technique to hide the data and has been popular among the digital security specialists. Steganography is used for the purpose of hiding the data into similar form or other form to create the covert channel to send it over internet for the protection of the data from various snooping attacks.

Basic flowchart of steganography is shown in Fig. 1 where, the secret object/message is embedded in a cover object and transmitted over internet to the receiver, the transmitted object is called stego object. The receiver extracts the secret message from the transmitted stego object using the extraction technique.

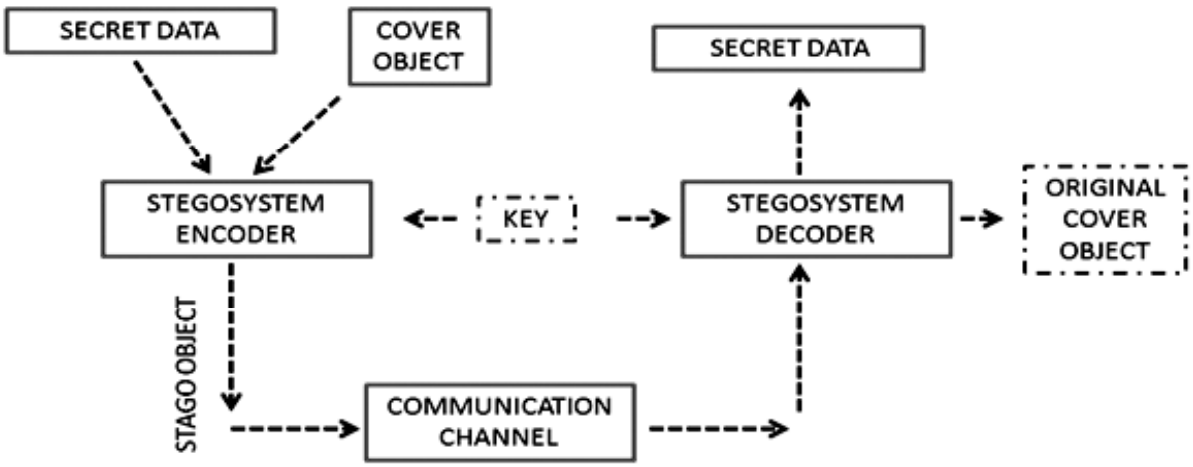

Figure 1: Basic Flow Chart for Steganography

*,** UIET, Panjab University, Chandigarh, *Emails: mukeshdalal05@gmail.com, mamtajuneja@pu.ac.in*

Video steganography is one of the leading steganography classes because of its popularity and frequent use on internet. Video steganography deals with data hiding techniques by utilizing video streams for embedding the secret data. Any multimedia file such as text, image, audio or even video data can be embedded in the videos by using the various techniques. In videos embedding can be done in compressed and uncompressed domains but nowadays compressed domains is utilized for steganography in which hiding can be done using spatial and transform domain techniques.

2. COMPRESSED DOMAIN BASED TECHNIQUES

Video steganography in compressed domain is an emerging field for secure communication. In videos hiding venues are more as compare to other multimedia types because of its complex structure and large size. Steganography in videos can be done by utilizing its motion vector components, macro-blocks, intra-prediction mode, VLC, quantized coefficients, CAVLC entropy coding etc. Researchers have utilized its complex structure very effectively for video steganography using these techniques. The literature survey in this concern is categorized in three main parts as shown in Fig. 2.

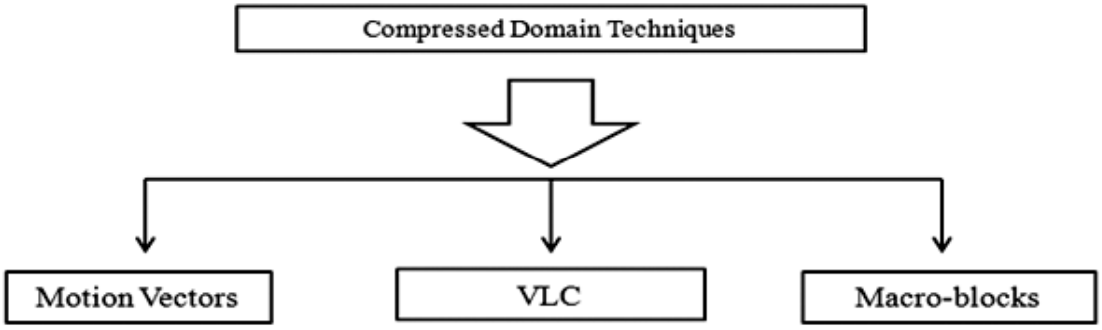

Figure 2: Compressed Domain Techniques

2.1. Motion Vector Based Techniques

Pan et al. [2] presented a steganography scheme for embedding data in a video using MVs. This scheme utilized linear block codes (6, 2) for reducing the modification rate of the MVs after embedding and embedding was done in motion vector's phase angle. A monitoring matrix of linear block codes was used as a secret key to provide additional security. The embedding capacity of the scheme was very high as this utilized 2/3 of total number of MVs with average value of PSNR 38 dB.

Cao et al. [3] used parity function for optimization of perturbation to motion estimation for an adaptive video steganography scheme. This method utilized internal dynamics of MPEG-2 standard videos with GOP sequence IBBPBBPBB, resulted in preserving the MVs statistical properties. As a result, the scheme can resists common and specific steganalysis techniques for MV steganography.

Aly et al. [4] suggested a video steganography method for hiding data using MVs based on prediction error associated with the macroblocks. They utilized horizontal and vertical MV components of P and B frames with high prediction error for data embedding. They used a prediction error threshold to help in recognition of MVs that carry's secret message bits to the decoder.

Su et al. [5] proposed a video steganography technique for hiding large amount of data in audio and video part of the compressed MPEG advanced audio coding and H.264/AVC video stream respectively. Embedding was done after examined the coding features such as quantization, intra-prediction and ME (Motion Estimation) procedures. To state the payload amount three profiles were also presented as High-profile, Medium-profile and Low-profile for embedding. Obtained results suggested that most suitable profile for embedding was Medium profile because it was able to achieve a good balance among basic requirements like payload, PSNR, bit-rate increase.

Cao et al. [6] presented a data hiding technique for better security of MV based video steganography scheme with optimized perturbations used for data hiding in the motion estimation process. These perturbations were introduced using the coding results of syndrome-trellis code (STC) which was used for minimizing the embedding impact. The proposed approach reduced the detection probability using the best steganalytic technique. Obtained results demonstrated that it outperforms the existing MV techniques with small impact on coding performance and they achieved payload 0.5 for the bit –rates 0.5 Mbit/s and 0.25 for 1 Mbit/s.

Zhang et al. [7] proposed a technique Motion Vector Modification with Preserved Local Optimality (MVMPLO) as an advancement of [5] and [6]. This was a three folded scheme: firstly a candidate motion vectors search area was designated, after that for each MV local optimality was evaluated and finally from that area one motion vector which contributed less towards degradation was selected. This approach withstands best steganalytic attacks for motion vector based steganography.

2.2. VLC

Liu et al. [8] presented a novel video steganography scheme by using variable length code (VLC) for embedding in MPEG-2 compressed videos. The embedding was done with LSB method utilizing A/S trees of VLC domain which are predefined in standard table of VLC. In VLC table A/S trees are mapped to a code tree and embedding was done automatically by generating pseudo random number sequence.

Liu et al. [9] used perturbed digital chaos instead of A/S trees[8] for the generation of pseudo random number (PRN) sequences and in [10] they utilized Variable length decoder which parsed the MVs, DCT coefficients and intra macroblocks for video steganography.

2.3. Macro-block

Yang et al. [11] proposed an algorithm to hide data in videos using 4×4 DCT coefficients. They used vector quantization for hiding 1 bit of secret data in each 4×4 DCT block and the hiding was done in the low frequency components of the subblocks. After hiding data the stego video was compressed using different quantization parameters using H.264/AVC coding standard. Experimental results showed that this technique was highly robust against compression.

Shao-dao et al. [12] proposed an approach for video steganography based on high bitrate hiding algorithm to hide video as a secret message. They embedded 1 bit of secret message in each 4x4 macroblocks of DCT using vector quantization. The utilized 8 low frequency coefficients for embedding the information and the extraction was a blind retrieval for this scheme. By analyzing the result it can be concluded that the scheme was highly robust against compression and PSNR was degraded by only 0.22dB on average and BER at receiver's end was only 0.015%. But in terms of capacity, this scheme was able to hide only 2 frames of QCIF format in 96 frames of CIF format.

Ma et al. [13] presented a technique based on intra-frame distortion drift introduced after embedding in H.264/AVC videos. In this technique the intra-frame distortion was introduced after embedding but not propagated to the neighboring blocks. They deployed the I-frame DCT quantized coefficients to hide data in the 4x4 luminance blocks and there was no intra-frame distortion drift to the covert video. They used block coefficient pairs for embedding with one used for embedding the secret data and the other one was used to fix the level of distortion. The obtained results demonstrated that the embedding capacity of the scheme was high and average PSNR was above 40 dB.

Esen et al. [14] proposed an adaptive block based techniques by utilizing forbidden zone hiding and selective embedding. The de-synchronization occurred because of adaptive block selection was handled by Repeat Accumulate (RA) codes. For embedding Y component of the frame was utilized and middle-frequency

band was chosen among DCT coefficients. There was an energy threshold used to process the block and coefficients, if the average energy was greater than the threshold value than they were processed otherwise skipped.

Shanableh et al.[15] proposed two new hiding schemes for MPEG videos where in the first scheme, quantization scale was modified to hide secret data bits in compressed MPEG videos of constant bit rate. From each macroblocks features were extracted and second order regression model was used to calculate the hidden message bits value. The decoder used this regression model for prediction of the message bits hidden which provided very high prediction accuracy but with low capacity. To overcome this limitation the second scheme used both bit rate codes constant as well as variable. This scheme used a feature of H.264/AVC videos called flexible macro-block ordering for data hiding. The results of the proposed techniques demonstrated that the average message prediction for the first scheme was 95.83% using second order regression and maximum payload was 10 Kb/s for the first proposed scheme and 30 Kb/s for the second scheme.

Lin et al.[16] presented a better error free propagation discrete cosine transformation based perturbation technique which is the advancement of Ma et al [13]. In [13], only 46% of the luma 4x4 blocks were utilized for embedding, so they utilized the remaining 54% to improve the embedding capacity. To improve the capacity the authors utilized 4 bits to embed into each luma block and as the capacity increased visual distortion occurs sometimes so to preserve the quality they used a new set of shifted 4x4 luma blocks to embed data by perturbing the quantized coefficients DCT. The results represented that the hiding capacity was improved with good visual quality calculated in terms of SSIM and the average PSNR was above 35.62 dB.

Liu et al.[17] utilized luminance coefficients of 4×4 integer DCT blocks for embedding and before embedding, the secret data and the cover video was divided into sub groups by using Shamir's (t ,n) threshold secret sharing scheme and classical algorithm was used called Lagrange Interpolation. After embedding the authors recovered the original video after extracting the secret data by using t sub-divisions of the frames. Obtained results showed that this scheme was more robust with average survival rate of 84.14%, achieved good visual quality with PSNR 36.5 dB, avert intra frame distortion drift and can also protect the cover video.

Yao et al.[18] proposed a technique concentrating on decreasing the inter-frame distortion drift caused after embedding the data. They presented a theoretical analysis for the distortion drift and based on that they were able to embed data with low inter-frame distortion in the video bit-stream. They encrypted three coding parameters viz. motion vector differences, the prediction modes and the quantized DCT coefficients. Embedding was done using histogram shifting technique in the 4x4 luminance integer DCT block coefficients of P-frame.

The comparative analysis of these techniques is done in Table 1 where the value of PSNR is the average value present in the literature.

All these techniques have some advantages and disadvantages which are listed below in Table 2.

3. CONCLUSION

In this paper various video steganography techniques in compressed domain are discussed. Researchers used videos for steganography, which are compressed in MPEG-2, MPEG-4 or H.264/AVC format, although H.265 format is also available but still not utilized for steganography. In video compressed domain, the commonly used methods for steganography are categorized according to the literature and for embedding secret data researchers utilized motion vector, macroblocks, variable length code etc. based techniques. These video steganography techniques are discussed by highlighting various quality parameters. The purpose of this paper is to explore the hiding opportunities in compressed videos for steganography.

Table 1
Comparative Analysis of Video Steganography Techniques

Authors	*Hiding Scheme*	*Quality Parameters Used*	*PSNR*
Pan et al. [2]	Phase Angle modification of Motion Vector	PSNR, Capacity	38
Cao et al. [3]	Motion Estimation	PSNR, SSIM, Encoding time, K-L Divergence	40
Aly [4]	Motion Vector and Prediction Error.	PSNR, Capacity, Increase in data size,	–
Su et al. [5]	Quantization, Intra-prediction and MVs.	PSNR, Capacity, Bitrate	35
Cao et al.[6]	Optimized perturbations to motion estimation	PSNR, Bitrate, Capacity	–
Zhang et al. [7]	Motion Vector and local optimality (MVMPLO)	PSNR, Bitrate	–
Liu et al. [8]	Variable Length Code(VLC)	PSNR, Capacity	41
Yang et al. [11]	4 × 4 DCT macroblock coefficients	PSNR, Bit Error Rate(BER)	–
Shao-dao et al. [12]	4 × 4 DCT macroblocks	PSNR, Bit Error Rate	42
Ma et al[13]	4 × 4 DCT block paired coefficients	Capacity, PSNR	40
Esen et al.[14]	Y components of middle frequency band of DCT	PSNR, Capacity	37.06
Shanableh et al. [15]	Quantized coefficients and flexible macroblocks.	Capacity, PSNR, RMSE, Distortion, Overhead	–

Table 2
Video Steganography Techniques with Pros and Cons

Authors	Pros	Cons
Pan et al. [2]	Low modification rate with high PSNR.	Only two videos were used for experiment.
Cao et al. [3]	Resist blind and specific steganalysis for MV based steganography	This method was quite complex
Aly [4]	Low distortion to the visual quality and highly robust.	Size of the video increased after embedding.
Su et al. [5]	Achieved 10% payload of video size	Visual distortion
Cao et al.[6]	High payload capacity	Visual quality affected.
Zhang et al.[7]	Resist best MV based steganalysis techniques currently present.	Complex approach and visual distortion.
Yang et al. [11]	Robust against compression useful in practical application.	Visual distortion and run-length coding is degraded.
Shao-dao et al. [12]	Robust against lossless compression.	Low hiding capacity.
Ma et al[13]	High embedding capacity and fast in computation.	Not robust against video processing operations
Esen et al.[14]	Highly robust	Visible artifacts occur.
Shanableh et al. [15]	High prediction rate at decoder side.	Increased in bit-rate overhead and low capacity.
Song et al. [16]	Low complexity and large embedding capacity	Robustness needs to be checked against attacks.
Liu et al. [17]	More Robust due to subdivision	Low Capacity
Yao et al. [18]	Lossless recovery of the cover video.	Visual quality needs to be improved.

REFERENCES

[1] "Steganography." [Online]. Available: https://en.wikipedia.org /wiki/Steganography. [Accessed: 20-Jun-2016].

[2] F. Pan, L. Xiang, X. Yang, and Y. Guo, "Video steganography using motion vector and linear block codes," Softw. Eng. …, no. 60842006, pp. 592–595, 2010.

[3] Y. Cao, X. Zhao, D. Feng, and R. Sheng, "Video steganography with perturbed motion estimation," in International Workshop on Information Hiding, pp. 193–207, 2011.

[4] H. A. Aly, "Data hiding in motion vectors of compressed video based on their associated prediction error," IEEE Trans. Inf. Forensics Secur., vol. 6, no. 1, pp. 14–18, 2011.

[5] P. C. Su, M. T. Lu, and C. Y. Wu, "A practical design of high-volume steganography in digital video files," Multimed. Tools Appl., vol. 66, no. 2, pp. 247–266, 2013.

[6] Y. Cao, H. Zhang, X. Zhao, and H. Yu, "Covert communication by compressed videos exploiting the uncertainty of motion estimation," IEEE Commun. Letter., vol. 19, no. 2, pp. 203–206, 2015.

[7] H. Zhang, Y. Cao, and X. Zhao, "Motion vector-based video steganography with preserved local optimality," Multimed. Tools Appl., no. 89, 2015.

[8] B. Liu, F. Liu, B. Lu, and X. Luo, "Real-time steganography in compressed video," in International Workshop on Multimedia Content Representation, Classification and Security, pp. 43–48, 2006.

[9] B. Liu, F. Liu, and D. Ni, "Adaptive compressed video steganography in the VLC-domain," Mob. Multimed. Networks, 2006 IET, pp. 5–8, 2006.

[10] B. Liu, F. Liu, C. Yang, and Y. Sun, "Secure steganography in compressed video bitstreams," ARES 2008 - 3rd Int. Conf. Availability, Secur. Reliab. Proc., pp. 1382–1387, 2008.

[11] M. Yang and N. Bourbakis, "A high bitrate information hiding algorithm for digital video content under H.264/AVC compression," Midwest Symp. Circuits Syst., vol. 2005, pp. 935–938, 2005.

[12] W. Shou-dao, X. Chuang-bai, and L. Yu, "A High Bitrate Information Hiding Algorithm for Video in Video," Eng. Technol., pp. 413–418, 2009.

[13] X. Ma, Z. Li, H. Tu, and B. Zhang, "A data hiding algorithm for h.264/AVC video streams without intra-frame distortion drift," IEEE Trans. Circuits Syst. Video Technol., vol. 20, no. 10, pp. 1320–1330, 2010.

[14] E. Esen and A. A. Alatan, "Robust video data hiding using forbidden zone data hiding and selective embedding," IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 8, pp. 1130–1138, 2011.

[15] T. Shanableh, "Data hiding in MPEG video files using multivariate regression and flexible macroblock ordering," IEEE Trans. Inf. Forensics Secur., vol. 7, no. 2, pp. 455–464, 2012.

[16] T. J. Lin, K. L. Chung, P. C. Chang, Y. H. Huang, H. Y. M. Liao, and C. Y. Fang, "An improved DCT-based perturbation scheme for high capacity data hiding in H.264/AVC intra frames," J. Syst. Softw., vol. 86, no. 3, pp. 604–614, 2013.

[17] Y. Liu, L. Ju, M. Hu, H. Zhao, S. Jia, and Z. Jia, "A new data hiding method for H.264 based on secret sharing," Neurocomputing, vol. 188, pp. 113–119, 2016.

[18] Y. Yao, W. Zhang, and N. Yu, "Inter-frame distortion drift analysis for reversible data hiding in encrypted H.264/AVC video bitstreams," Signal Processing, vol. 128, pp. 531–545, 2016.