Academic Science

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 5
May 2017

Video Steganography & Steganalysis – A Review

Mrs. Alaknanda S. Patil,
Electronics Engineering Department,
Sathyabama University, Chennai, TN-India.

Dr. G. Sundari
Electronics Engineering Department,
Sathyabama University, Chennai, TN-India

Abstract: *The steganography is the process to hide the secret message behind the other cover message. It carries the security and aauthenticity. The type of steganography is depends on the cover message used, if cover message used is video to hide any type of data, it is video steganography. The secret data hidden behind the video can be image, audio or text. Video steganography is more favorable because of the combination of group of images and audio. The different combination can be done to transmit the secret data as – random image frame can carry image, audio or text. As well audio of video can also embedded with audio or text, depends upon application. This paper gives the variety of algorithms to study the video steganography.*

Keywords – Steganography, Video steganography, Image Steganography, Stego-image, Least Significant Bit.

I. INTRODUCTION:

In the current digital world, the secrecy in the transmitted and received data is very important to avoid the misuse of information. There are variety of methods to transmit the secret data as watermarking, cryptography and steganography. Steganography is the safe and assured technique to embed the secret information in the carrier to maintain the confidentiality. The reason is, different methods are available to embed data in the carrier, depends upon the type of carrier. The retrieval of the secret data is difficult by steganography method. The carrier can be image, audio, text or video [1]. Steganography is a greek word, gives meaning as "covered writing" [2]. 'Secret message' means, the message to be transmitted confidentially. 'Cover message' or 'Carrier message' means, message in which the secret message is to be hidden & 'Stego message' is cover or carrier message after embedding the secret message. The secrecy can be increased by encrypting the stego message by stego-key. The better computational complexity gives the better steganography algorithm, which results in good design of steganographic algorithm. [3].

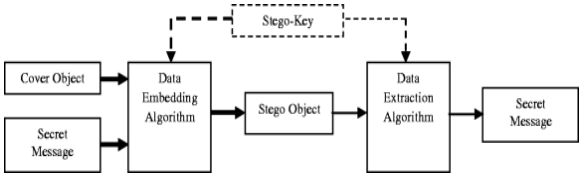

Fig.1 : Steganography block diagram[2]

II. VIDEO STEGANOGRAPHY: Tremendous work has been done in the Image Steganography with lots of challenging methods. But now a day, video transmission is more popular due to handy use of internet for different social medias [2]. Video files are the combination of lots of images and audio file. The frames of the video are selected to embed the secret data. The main advantage of video steganography is huge amount of data can be hidden in video[3]. Video steganography can be in spatial domain or frequency domain.

Different methodologies are available in video steganography with some pros & cons in every methodology[1]. For e,g. - Least Significant Method , masking and filtering [3], Spread Spectrum method[4], Steganography with Discrete Cosine Transform, bit plane complexity segmentation steganography [1].

III. STEGANALYSIS

The recovery of the secret message back is nothing but the process of Steganalysis. The detection of

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 5
May 2017

difference between the stego message and cover message is nothing but secret message. Steganalysis mainly relates with visual attacks, statistical attacks and structural attacks, depends upon the algorithm used for steganography[1]. Steganography is the process occurring at the transmitter and steganalysis is occurring at the receiver. Every better steganography algorithm must a steganalysis algorithm to defeat the system & extract the secret message[2]. The design of good steganography and steganalysis algorithm is a enending process[3].

IV. LITERATURE SURVEY

Dr. Souvik Bhattacharyya, Indradip Banerjee & Gautam Sanyal have explained Image, Text, Audio & Video steganography & steganalysis in detail. Image steganography is mainly consists of two types as – spatial domain steganography & Transform domain steganograaphy. Different methods in spatial domain steganography explained here is Data hiding by Least Significant Bit (LSB), Data hiding by Multi Bit Plane Image Steganography (MBPIS), Data hiding by Multiple Based National System (MBNS), Data hiding by Quantization Index Modulation (QIM), Data hiding by Pixel Value Differencing (PVD) & Data hiding by Grey Level Modification (GLM). Different methods in transform domain steganography elaborated here is, Discrete Cosine Transform (DCT) based Data Hiding & Discrete Wavelet Transform (DWT) based Data Hiding. Image steganalysis can be explained by targeted steganalysis, blind steganalysis & semi-blind steganalysis. Some contributed work for Video Steganography explained here are – Application of Bit Plane Complexity Segmentation (BPCS) Steganography to Wavelet Compressed Video, An Optical video Cryptosystem with Adaptive Steganography, A Secure Covert Communication Model Based on Video Steganography, etc. Some work for Video Steganalysis is also explained here as – Video Steganalysis Exploring the Temporal Coorelation between frames, Video Steganalysis Based on Asymptotic Relative Efficiency, Video Steganalysis based on Mode detection, etc.[1]

Sadek M. M., Khalifa A. S. & Mostafa, M. G. M. have given critical review of steganography, specially, video steganography. The study of different Video Steganographic techniques have been done here. E.g. a) Substitution Based Technique - It gives the better embedding capacity as redundancy of cover message is replaced by secret message. Some of substitution methods are Least Significant Bit (LSB) technique, Bit Plane Complexity Segmentation (BPCS), Tri-way Pixel Value Differencing (TPVD), etc. b) Transform Domain Techniques – it is more robust than other methods as secret message embedding takes place in frequency domain, then coefficients are represented in original form. Some examples of this methods are – Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) & Discrete Wavelet Transform (DWT). DFT are not favorably used as rounding off of errors takes place, where as DCT is more popular because of easy embedding and extraction phenomenon. c) Adaptive Techniques – also can be called as ‘Masking and Embedding’. It finds the region of interest i.e. good area to embed the secret message. D) Format Based Technique – different video formats are selected to hide the secret data, where only high frequency coefficients are changed and low frequency coefficients are preferred to keep without change. It will retain the visual quality after embedding process. d) Cover Generation Technique – integration of new object to use it as cover message. The blending of secret key & secret message will create the cover message. Use of this technique in video steganography requires lots of relevant images to create video, which results in more difficult for attacker[2].

Ronak Joshi, Pratik Jain & Lalit Gupta have studied about different types of steganography as – Text Steganography, Image Steganography, Audio Steganography & Video Steganography with steganalysis techniques. They have suggested the dual steganography concept for more stronger algorithm to hide the secret data, e.g. the combination of Steganography and Cryptography [3].

The Text, Image, Audio & Video Steganography is described in this paper along with one more method as – Network or Protocol Steganography. It gives the embedding of secret data with network protocol as TCP, IP as cover message. Some Steganography Techniques are explained here as – Spatial Domain Steganography, Spread spectrum Technique, Statistical Technique, Transform Domain Technique and Distortion Technique. Spread spectrum Technique is seems to be more strong & robust steganography technique by elaboration of Jasleen Kour, Deepankar Verma, as – the secret message is spread over a wide frequency range of cover message. Some considerable factors which affects on Steganography are mentioned here as: robustness – ensures the intactness of embedded secret data under any transformations of stego message. Imperceptibility – undetectability of changes in the stego message. Payload (secret message) capacity – maximum amount of secret message to be hidden in the cover message. Peak Signal to Noise Ratio (PSNR) – it must be high for better quality of message. Mean Square Error (MSE) – it must be smaller for better stego message & Signal to Noise Ratio (SNR)[4].

Natarajan Meghanathan & Lopamudra Nayak have analysed the Image Steganography, Audio Steganography & Video Steganography. Image steganography can be of two types, mainly as – Specific & Generic. Specific steganalysis algorithm are depend upon format of digital image (GIF, Bmp, etc.), where as Generic algorithm are not dependent but having more computational complexity[5].

R. Amirtharajan & John Bosco Balaguru Rayappan have been mentioned critical analysis of Text, Image, Audio & Video Steganography[6].

The extraction of embedded data over wide band in spectrum domain is mainly considered in this paper. The spectrum considered can be of any digital medium like audio, image or video, but results checked are of only images. Authors have claimed that 'the multicarrier spread-spectrum extraction with the help of multicarrier iterative generalized least squares algorithm' is invented first time [7].

The data is embedded in a MPEG compressed video in this paper. Motion vectors are used to encode and reconstruct the secret message. Choice of motion vector is based on macroblock prediction error. The future work suggested here is to increase the size of embedding payload by maintaining the robustness and low distortion [8].

Because of large content of redundancy, video is the better medium for steganography. Many of the image steganography algorithms can be used for the video steganography. The spread spectrum (SS) embedding method is considered in this paper for the steganalysis. The features are extracted of original video & received video, compared it, if received video found suspicious, hidden message as well as original video is detected [9].

Cover message used in this paper is color video (MPEG / AVI) and secret message considered is image (png). Hash based LSB technique is used here to hide secret data, i.e. hash function is used to select the position of insertion in LSB of cover media. The eight bits of secret message is divided into 3, 3, 2 bits and inserted into the LSB of R, G, B frames. Spatial domain analysis is given here with PSNR, MSE & Image Fidelity analysis for quality assurance of secret data recovery [10].

Calibration based approach of motion vector reversion based technique is explained in this paper, as the tendency of motion vector reversion is very sensitive. The advantages of this system are, this algorithm can work with low embedding rate as well mathematical and experimental analysis can be shown. Future works suggested are – to improve adaptability, to adapt certain feature selection / fusion technique [11].

The RGB frames of color video are used to embed the eight bit secret data, by separating it in 3, 3, 2 bits. These separated bits are embedded in LSB of video frames. Generic algorithm is used to decide the embedding of secret data. Uncompressed domain analysis is given here with improved PSNR & Image Fidelity analysis for quality assurance of secret data recovery [12].

Cover media considered is video, i.e. group of still images, any random frame of image can be selected to embed secret data. The combination of audio

steganography with phase coding algorithm and image steganography with 4LSB algorithm is proposed in this paper. Secret information of image is to be embedded in image and secret information of text is to be embedded in audio of video file. Hence stego audio – video file is to be transferred. Computer forensics technique is used for authentication. The PSNR & histogram are checked at transmitter as well as at receiver; similarity at both places gives increased data security [13].

The detection method for vector-based steganography is illustrated in this paper. LSB of motion vector is modified, SAD (sum of absolute difference) is used to figure-out the difference of actual SAD and locally optimal SAD. The corrupted videos, because of various steganography and modification methods, are use here for steganalysis. AOSO (Adding Or Subtracting One Operation) method is used for SAD because of its advantage as – it is not designed for any certain video codec, applicable to various LSB methods [14].

The carrier considered in this paper is video & secret message may be image or text. The video frame is selected randomly to encrypt the secret message with the help of secret key. The random video frame selection is with the help of feedback shift register to avoid repetition. The embedding and extraction process are taking place parallelized. This method is based on LSB method. Different advantages of this methodology are stated by author as – it takes less time to compute, improved results, high volume of data can be encoded & can be used for real time system because of parallelization [15].

Authors have considered video as the cover message and the secret message is image. The secret message is inserted in a in a mosaic frame of video by a lossless data hiding scheme with a secret key. The secret image is divided into cells and a color characteristic of each cell is transformed to the divided target blocks. It gives the improved PSNR and improved security. The steganography of video with audio is suggested future scope [16].

Only visual features of video are considered in this paper, without any change in the audio. Robust temporal registration scheme is used by utilizing visual-audio fingerprints in 2 stages – video frames are compressed by 1-D motion and exact frame to frame matching is computed with the help of sliding window based dynamic programming technique. This method can restrict the pirate video. Future scope given by author is – accuracy can be improved by using keypoint based features, the fingerprint extraction process can be parallelized to reduce computation complexity as well reduce processing time [17].

Authors told the reason of popularity of video steganography is moving sequence of images and audio files. Enhanced Hidden Markov Model (EHMM) is used to recover data with improved speed. EHMM is implemented here with some features as – different sized AVI video can be used, data hiding time is reduced by 3-50%, data retrieval rate is improved by 22-77%, minimum computational cost is 20% and security improved by 4-77%. Future scope mentioned here are – any video file can be considered instead of only AVI, invent the algorithms to embed large amount of secret data [18].

Random key function is used for encoding and decoding the secret data to improve the security. Secret data is embedded into the random R, G, B pixel values of cover video / image using encryption key. Cover video / images are pre-processed to prevent overflow – underflow. The security and PSNR is checked for strength of steganography. The same size video can embed different sized / length secret data [19].

The exhaustive review is given in this paper related to steganography concept used in Smartphones. Smartphone Object Method, Smartphone Platform Method & Smartphone Communication Method are explained in depth. The idea explained here for embedding data is – LSB alteration applied to video frames, as well embedding manipulation in tags. Future scope suggested as – 1) energy consumption in video steganography of network & security mechanism is expected to count, & 2) develop mitigation techniques for steganalysis, mainly for local channels [20].

Motion vector steganalysis gives benefit to spatial as well temporal domain. This algorithm is tested

over 5th and 7th levels of cross sections of motion vector planes for steganalysis. This system doesn't require recompression of the stego-video [21].

Video is first transformed by lazy lifting wavelet transform and then apply LSB algorithm to insert the secret message. This method gives high payload capacity and low computational complexity. It gives two layered security by image steganography and audio steganography [22].

The text can be embedded as a secret message in the video, in this paper. Video is transformed first using DCT & secret message is embedded using LSB methodology. This method gives higher security to retrieve data. The encryption and decryption of secret data is also possible with the help of images. MSE & PSNR is checked for authenticity of the steganography [23].

V. CONCLUSION

The various methods of the video steganography and steganalysis are available with variety of algorithms. Every system claims for data security, authenticity, sturdiness during travel of stego-signal with more or less complexity. The methodology implemented to hide the secret data in the carrier must be unique to carry the authenticity of transmission; otherwise data can be hacked, which will not serve the purpose of steganography.

VI. REFERENCES

[1] Dr. Souvik Bhattacharyya, Indradip Banerjee, Gautam Sanyal, "A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Journal of Global Research in Computer Science, ISSN – 2229-371X, Vol 2, No. 4, April 2011.

[2] Sadek M. M., Khalifa A. S. & Mostafa, M. G. M., 'Video Steganography: A Comprehensive review", Multimed Tools Appl (2015) 74:7063. Doi:10.1007/s11042-014-1952-z.

[3] Ronak Joshi, Pratik Jain, Lalit Gupta, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue 6, Nov-Dec.2012, pp-4634-4638, ISSN: 2249-6645.

[4] Jasleen Kour, Deepankar Verma, "Steganography Technique – A review paper", International Journal of Emerging Research in Managements & Technology, ISSN:2278-9359, Vol.3, Issue 5, May 2014.

[5] Natarajan Meghanathan, Lopamudra Nayak, "Steganalysis Algorithms for detecting the hidden information in Image, Audio and Video Cover Media", International Journal of Network Security & its Application (IJNSA), Vol.2, No.1, January 2010.

[6] R. Amirtharajan, John Bosco Balaguru Rayappan, "Steganography – Time to Time : A Review", Research Journal of Information Technology 5(2); 53-63, 2013, ISSN 1815-7432 / DOI : 10.3923/rjit.2013.53.66.

[7] Ming Li, Michel K. K., Dimitris A. Pados, Stella N. Batalama, Michael J. Medley, "Extracting Spread-Spectrum Hidden Data From Digital media", IEEE Transactions on Information Forensics And Security, Vol. 8, No. 7, July 2013.

[8] 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.

[9] Nematollah Zarmehi, Mohammad Ali Akhaee, "Digital video steganalysis toward spread spectrum data hiding", IET Image Processing 2015, ISSN 1751-9659, doi: 10.1049/iet-ipr.2014.1019.

[10] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash Based Least Significant Bit Technique For Video Steganography (HLSB)", https://www.researchgate.net/publication/268063895 , International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[11] Yun Cao, Xianfeng Zhao, and Dengguo Feng, "Video Steganalysis Exploiting Motion Vector Reversion-Based Features", IEEE SIGNAL PROCESSING LETTERS, VOL. 19, NO. 1, JANUARY 2012.

[12] Kousik Dasgupta, Jyotsna Kumar Mondal, Paramartha Dutta, "Optimized Video Steganography using Genetic Algorithm (GA)", International Conference on Computational Intelligence: Modeling, Techniques and Applications (CIMTA) 2013, Available online at www.sciencedirect.com

[13] Sunil K. Moon & Rajeshree D. Raut, "Application of data hiding in Audio – Video using anti-forensics techniques for authentication and Data Security", International Advance Computing Conference (IACC) at Gurgaon, 21 – 22 Feb. 2014, IEEE.

[14] Keren Wang, Hong Zhao, and Hongxia Wang, "Video Steganalysis Against Motion Vector-Based Steganography by Adding or Subtracting One

Motion Vector Value", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 5, MAY 2014.

[15] Sudeepa K B, Raju K, Ranjan Kumar H S & Ganesh Aithal, "A New Approach For Video Steganography Based on Randomization and Parallelization", International Conference on Information Security and Privacy (ICISP2015), 11-12 Dec 2015, Nagpur, India, Available online at www.sciencedirect.com

[16] Gija Susan Issac & Jobi Jose, "Secured Transmission Of Image/Video By Performing Reversible Color Transformation", International Conference on Emerging Trends in Engineering, Science and Technology (ICETEST- 2015), Available online at www.sciencedirect.com

[17] Dr. R. Roopalakshmi, Revanur Venkatesh & K. M. Rahul, "Robust Temporal Registration Scheme for Video Copies Using Visual-Audio Features", 3rd International Conference on Recent Trends in Computing 2015 (ICRTC-2015), Available online at www.sciencedirect.com.

[18] Mritha Ramalingam & Nor Ashidi Mat Isa, "Fast retrieval of hidden data using enhanced hidden Markov model in video steganography", Applied Soft Computing 34 (2015) 744–757, Contents lists available at ScienceDirect, j ourna l ho me page: www.elsevier.com/locate /asoc

[19] Mritha Ramalingam & Nor Ashidi Mat Isa, "A Steganography Approach over Video Images to Improve Security," Indian Journal of Science and Technology, Vol 8 (1), 79-86, January 2015.

[20] Wojciech Mazurczyk & Luca Caviglione, "Steganography in Modern Smartphones and Mitigation Technique", IEEE Communication Surveys & Tutorials, Vol. 17, No. 1, First Quarter 2015.

[21] Kasim Tasdemir, Fatih Kurugollu and Sakir Sezer, "Spatio-Temporal Rich Model-Based Video Steganalysis on Cross Sections of Motion Vector Planes", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 25, NO. 7, JULY 2016.

[22] Khushman Patel, Kul Kauwid Rora, Kamini Singh & Shekhar Varma, "Lazy Wavelet Transform Based Steganography in Video", 2013 International Conference on Communication Systems and Network Technologies, IEEE Computer Society.

[23] Poonam V. Bodhak & Baisa L. Gunjal, "Improved Protection In Video Steganography Using DCT & LSB", International Journal of Engineering and Innovative Technology (IJEIT), Vol 1, Issue 4, April 2012.