International Journal of Research in Advent Technology, Vol.3, No.5, May 2015
E-ISSN: 2321-9637

A Review on Video Steganography

Miss. Uma Sahu[1], Mr. Saurav Mitra[2]

[1]*M.Tech. Scholar, E&TC Department, C. V. Raman University, Bilaspur*
[2]*Asst.Professor, E&TC Department, C. V. Raman University, Bilaspur*
[1]*poojagb.2125@gmail.com*
[2]*saurabh.mit1000@gmail.com*

Abstract— Advancement in internet technology with high speed data transfer using 3G and 4G has made it possible to exchange the information with each other in the blink of eye. Exchange and sharing of information in the internet has posed the problem of information being hack by the unauthorized person or organization. Steganography is one of the solutions to this problem. Many algorithms have been proposed for image as well as for video steganography. This paper is an attempt to give a brief review work proposed in this field.

Keywords— Steganography, Discrete wavelet transform, Discrete Cosine transform, cover image.

1. INTRODUCTION

Internet has made the lives of people much easier than before. Internet can be used now to pay the bills, purchase their goods on-line, Exchange important information between people or organization which are poles apart. These information, if not protected or secured can be obtained by the hackers which they can use to full-fill their own interest.

Steganography is the technology which is developed to counter this problem. In steganography, Secret information is hidden in the cover file which may be audio file, video file, image file or even text file[1] without letting the user know the existence of any information. In this sense, steganography is different from the cryptography in the sense that in cryptography, the cover file is encrypted and person knows that some kind of information is there but person is not able to decipher it because of it being in encrypted form. On the other hand, in steganography, information is hidden in the cover file in such a way that a person is not able to even existence of some hidden information in cover file.

Embedding efficiency[4] and embedding payload are the two important factors of steganography system. The amount of data to be hidden in cover file is known as the

embedding payload. An stenography system is said to have high embedding efficiency if it is able to hide high payload in cover file while keeping the least distortion in host or cover file [2]. So a good steganography system must have a high embedding efficiency as any obvious distortion in the host or cover file may create a suspicision in person's mind and the secret information can be extracted out using some available steganalysis tool[3].

Generally the relationship between embedding payload and embedding efficiency is inversely proportional. That means if we increase the embedding payload then distortion in host file wil increase and vice-versa.

Balancing between the two factors in steganography system depends on the users and the application [2].

2. STEGANOGRAPHY SYSTEM

Steganography is the art of hiding the information in some other host object. It has been used since ancient time by the people. In ancient time, secret information is hidden in the back of wax, scalp of the slaves, in rabbits etc.

With passage of time, the application of steganography and its area has become widened. With the introduction digitization era, digital steganography has emerged as the new tool to hide the information secretly. Text, digital image, digital audio and digital video has become the host object for data hiding.

Below is some of the common term which is necessary to understand any steganography system.

Cover Media- It is the medium in which secret information is embedded in such a way that it is difficult to detect the presence of data

Stego- Media- It is medium obtained after embedding the secret information.

Secret data- The data or information to be hidden in cover media.

Steganalysis- The process of detecting, presence of secret data in cover media.

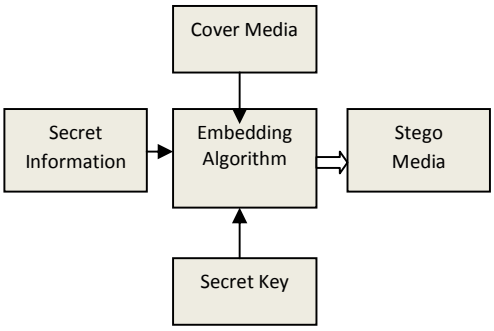

Figure 1 Steganography System

3. RELATED WORK

This section present some review work proposed for video steganography.

In 2004, Hideki Noda and his associates [5] presented a wavelet decomposition based video steganography method. Lossy compressed video is used in this method to carry the secret information through steganography. Wavelet compressed video data is used for steganography by using Bit-plane complexity video segmentation (BPCS) method of steganography. In this method, bit-plane decomposition is sued in this method to hide the secret data. Region in some of the bit plane is having noise like structure which is utilized for hiding secret data. This type of embedding does not deteriorate the quality of the host video

In this paper, the method is tested in two compressed video format i.e 3-D SPIHT nad JPEG 2000. These two compressed video is then undergoes a bit plane decomposition method for hiding the secret data and hence got the name of 3-D SPIHT-BPSC steganography method and JPEG 2000-BPSC steagnography method.

Simulation results shows that the performace of 3D SPIHT-BPSC method is better than the JPEG-2000-BPSC method in term of data embedding capacity without appreciable distortion in the host video.

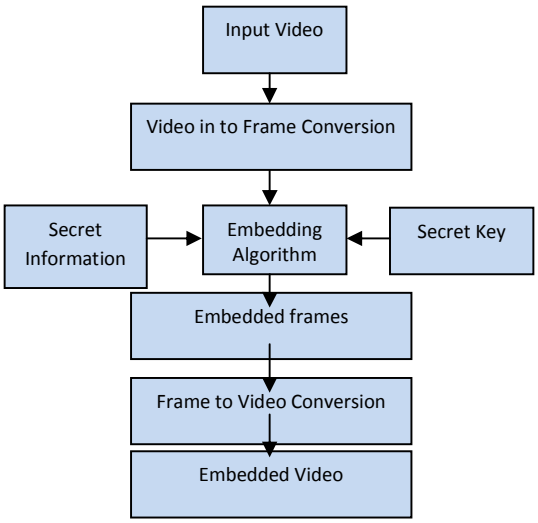

Figure 3 Basic Block diagram of Video Steganography

In 2006, Steganography method for MPEG compressed video is proposed by Chengyong Xu[6]. In this method, Control information regarding the extrcation of the secret data is embedded in I frame. Data is embedded in P and B frames. Macro block of motion vector which has a greater moving speed is used for embedding the secret data. This method is adopted to make the secret data safe in case of video processing operation. Secret data is extracted out from the compressed video without using the original video.

First of all the control information is extracted out from the I frame and then by using these control information, secret data is extracted out from P and B frames. Exparimental results reveals that this method degrades the visual quality of the host video in some extent but shows a good embedding capacity and resistivity offered against the video processing and frame adding and dropping.

In 2008 Bin Liu[7] presented a secure video steganography method in compressed video domain and named it as compressed video secure steganography(CVSS). This method perform the embedding and detecting process completely in compressed domain without going in to decompression process. In any video stream, contagious frames are statistically invisible and this property can be exploited for embedding the data and increasing the capacity of the data hiding in video stream. This is the main theme of this algorithm. This method also increases the security of the steganography application. In order to test the method, steg-analysis is also performed. Simulation results obtained clearly shows its high security property.

In 2008, Hanafy A.A. proposed video steganography method to conceal the confidential information in Host video file. In this method, colored video host file is pixel-wise manipulated for embedding the secret data. Before embedding, secret data is segmented in to blocks. Then psudo random location is computed for embedding these block in host video. A re-ordering secret key is used to derive these random location. The re-ordering of the secret is dynamic in nature and different for different video frames. This helps to block any possibility of finding the secret data statistically even if the interceptor has the access to the original video. In this paper, a quantitative evaluation of this model is also carried out by computing the average reduction in PSNR (Peak signal to noise ratio) as compared to the original video. MSE(Mean square error) is also computed for different size and types of data. Embedding capacity of the proposed method is also computed for different file format and size.

In 2009, Mozo A.J. suggested a steganography method for Flash video(.Flv extension.). Since Flash video file has small size as compared to other video file and simple structure of this make it suitable for steganography application. He experimented extensively on the structure of flash file to explore the way of hiding data in it. they made a C++ program to embed any type of data in flash

file. They also worked in extracting the hidden data from flash file. When data is hidden in flash file then its size gets increased, they also worked for compressing the flash file after hiding the data. Their experimental results were very encouraging and gives accuracy of 100% in extracting out the hidden information. The data embedding in flash files using this method doesn't affect the quality of picture and sound of the host flash file. This method explore a new way of hiding data in flash file which most commonly used in internet for video transfer.

In 2009, Eltahir[10] presented a scheme of video steganography which was based on the Least significant Bit(LSB). In this scheme, effort has been made to increase the size of secret information by hiding it into the video frames. In this scheme , video is first converted to frames then each frames were used as an image. In this method a 3-3-2 approach has been adopted to embed the secret information in to the video. 3-3-2 means 3-Least significant bit of Red, 3-LSB of Green and 2-LSB of Blue channel has been taken for data hiding. Since blue colour is more sensitive for eyes and any significant change in this colour can easily be noticed by the human eyes therefore only two bits of blue channel has been taken for data embedding. This scheme is able to have a payload size which is one third of video size.

IN 2009,Jafar Mansouri, presented a paper tiltled "An adaptive scheme for compressed video steganography"[11]. In this method I-frames having large spatial variation is selected for embedding the secret data. P and B frames with high temporal variation or with high magnitude of horizontal and vertical motion vector is also chosen for secret data hiding.
This algorithm is tested for different bit rate and the simulation results reveals its high quality and embedding capacity.

In 2010, Feng suggested a novel video steganography scheme[12] . In this scheme, motion vector is used as carriers for embedding the secret information in H.264 video compression standard. In this scheme linear block code is used for reducing the modification rate of the motion vector. Simulation results shows a good quality of stego data which proved by less modification rate of the motion vector. Simulation result for flower and foreman video shows the PSNR(Peak signal to noise ratio) to be more than 37dB.

In 2010,Sherly A P and Amritha PP presented a paper titled "Compressed video steganography using TPVD" [13]. In this method data is hidden in compressed video. In the previous method, Data is hidden in the macro block of I-frame which undergoes maximum scene change. Block of P frame and B frames are used for data hiding. P and B frame block having maximum motion vector magnitude is chosen for data hiding. This method is modify using tri-way-pixel-value differencing method. Pixel differencing is used for hiding the data. Advantage of this system is that it increase the pay load without affecting the quality of the video .

In 2011, Hao presented a video staganography method[14] which was also based on the motion vector estimation using matrix encoding. In this method, data is hidden in to a motion vector which has high both vertical and horizontal component. Human visual system can detect the change in slow moving object but not able to detect the changes in fast moving object. Motion vectors with high value indicate the fast moving object in the video and hence selected for information hiding. Results reveals that the PSNR of the stego video is more than 36 dB which confirms the good quality of the stego video.

In 2011 ShengDun Hu, KinTak U presented a steganography system based on non-uniform rectangular partition [15]. This method is used in uncompressed video. In this method video stream is hidden in to other video stream. In each frame of both video, a mechanism is applied for hiding the video stream. Suppose the host video stream is F and Information video stream is H then in order to hide the information stream in to host video, frame length of F is greater or equal to frame length of H. Each frame of information video is portioned in to non uniform rectangular part which encoded. These codes are hidden in the host video in least significant 4 bit of each frames.

In 2012, Rongyue suggested an efficient BCH coding based steganography system [16]. In this scheme, information is hidden inside a block of cover data by modifying some coefficients. Low computational time and less complexity are the advantages of this system.
In 2012 Swathi, S.A.K Jilani, proposed a novel method in his paper[17] " Video steganography by LSB substitution using different polynomial equations".
LSB insertion method is one of the oldest and easiest method of data hiding in which least significant bit of host file is used for hiding the information bit. In this method, information is embedded in specific location of specific frames by LSB substitution. Polynomial equation with different coefficients is used to get the specific frames and specific location for information embedding. Here the polynomial equation work as a stego key. This method overcomes the less secure LSB method. Pay load can also be increased by using this method.
In 2012, Lakshmi narayanan K,Prabakaran G,Bhavani R, presented an IWT based approach in their paper "A high capacity video steganography based on integer wavelet transform"[18]. In this integer wavelet transform is used in the host image to get the stego-image. Since in this algorithm only approximation band of secret image is considered therefore this method improves the capacity of the pay load. Extraction algorithm is just opposite of the embedding algorithm. Simulation result shows that this method robust secure and of greater capacity. Since integer wavelet transform perform batter in exploiting the spatial

and temporal correlation in and between the frames as well as the produce minimum embedding distortion therefore it is used in this algorithm.

In 2013, Liu in his paper[19] suggested a robust steganography scheme in H.264 compressed video. This method is able to prevent inter-frame distortion. In order to make the scheme more robust, message is encoded using BCH code and then embedding operation is performed. Coefficients of DCT of luminance I-frame component is used as host data. Simulation results show high quality and robustness.

In 2013 Prajna Vasudev, Kumar Saurabh, suggested a novel "Video steganography using 32 x 32 vector quantization of DCT"[20]. In this method, first of all the input video is converted in to a frames. From each frames 32 x 32 vector quantization of DCT is obtained followed by LSB quantization method which gives some vacant space in the frames. These vacant space are filled with the information bit

4. CONCLUSION

In the era of fast information interchange using internet and World Wide Web, Steganography has become essential tool for information security. This paper presents a review work in different steganography methods. Pros and cons of different steganography algorithm are also discussed in this paper.

REFERENCES

[1] H. Yuh-Ming and J. Pei-Wun, "Two improved data hiding schemes," in Image and Signal Processing (CISP), 2011 4th International Congress on, 2011, pp. 1784-1787.

[2] C. Chin-Chen, T. D. Kieu, and C. Yung-Chen, "A High Payload Steganographic Scheme Based on (7, 4) Hamming Code for Digital Images," in Electronic Commerce and Security, 2008 International Symposium on, 2008, pp. 16-21.

[3] L. Guangjie, L. Weiwei, D. Yuewei, and L. Shiguo, "An Adaptive Matrix Embedding for Image Steganography," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on, 2011, pp. 642-646.

[4] W. Jyun-Jie, C. Houshou, L. Chi-Yuan, and Y. Ting-Ya, "An embedding strategy for large payload using convolutional embedding codes," in ITS Telecommunications (ITST), 2012 12th International Conference on, 2012, pp. 365-369.

[5] Hideki Noda ; Tomofumi Furuta ; Michiharu Niimi and Eiji Kawaguchi "Video steganography based on bit-plane decomposition of wavelet-transformed video", Proc. SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, 345 (June 22, 2004);

[6]Changyong Xu; Xijian Ping; Tao Zhang, "Steganography in Compressed Video Stream," Innovative Computing, Information and Control, 2006. ICICIC '06. First International Conference on , vol.1, no., pp.269,272, Aug. 30 2006-Sept. 1 2006

[7] Bin Liu; Fenlin Liu; Chunfang Yang; Yifeng Sun, "Secure Steganography in Compressed Video Bitstreams," Availability, Reliability and Security, 2008. ARES 08. Third International Conference on , vol., no., pp.1382,1387, 4-7 March 2008.

[8]Hanafy, A.A.; Salama, G.I.; Mohasseb, Y.Z., "A secure covert communication model based on video steganography," Military Communications Conference, 2008. MILCOM 2008. IEEE , vol., no., pp.1,6, 16-19 Nov. 2008.

[9]Mozo, A.J.; Obien, M.E.; Rigor, C.J.; Rayel, D.F.; Chua, K.; Tangonan, G., "Video steganography using Flash Video (FLV)," Instrumentation and Measurement Technology Conference, 2009. I2MTC '09. IEEE , vol., no., pp.822,827, 5-7 May 2009.

[10] M. E. Eltahir, L. M. Kiah, and B. B. Zaidan, "High Rate Video Streaming Steganography," in Information Management and Engineering, 2009. ICIME '09. International Conference on, 2009, pp. 550-553.

[11] Jafar Mansouri, Morteza Khademi,"An Adaptive Scheme for Compressed Video Steganography Using Temporal and Spatial Features of the Video Signal", 2009 Wiley Periodicals, Inc.

[12] P. Feng, X. Li, Y. Xiao-Yuan, and G. Yao, "Video steganography using motion vector and linear block codes," in Software Engineering and Service Sciences (ICSESS), 2010 IEEE International Conference on, 2010, pp. 592-595.

[13] Sherly A P and Amritha P P, "A Compressed Video Steganography using TPVD ",International Journal of Database Management Systems (IJDMS) Vol.2, No.3, August 2010.

[14] B. Hao, L.-Y. Zhao, and W.-D. Zhong, "A novel steganography algorithm based on motion vector and matrix encoding," in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on, 2011, pp. 406-409.

[15] ShengDun Hu, KinTak U," A Novel Video Steganography based on Non-uniform Rectangular Partition ",IEEE International Conference on Computational Science and Engineering,pp 57-61,Aug.2011.

[16] Z. Rongyue, V. Sachnev, M. B. Botnan, K. Hyoung Joong, and H. Jun, "An Efficient Embedder for BCH Coding for Steganography," Information Theory, IEEE Transactions on, vol. 58, pp. 7272-7279, 2012.

[17] A. Swathi,S.A.K Jilani, " Video Steganography by LSB Substitution Using Different Polynomial Equations" , International Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5,sep 2012.

[18] Lakshmi narayanan K,Prabakaran G,Bhavani R, " A High Capacity Video Steganography Based on Integer Wavelet Transform", Journal of Computer

Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-4, February 10, 2012.

[19] Y. Liu, Z. Li, X. Ma, and J. Liu, "A Robust Data Hiding Algorithm for H. 264/AVC Video Streams," Journal of Systems and Software, 2013.

[20] Prajna Vasudev,Kumar Saurabh ," VIDEO STEGNOGRAPHY USING 32 *32 VECTOR QUANTIZATION OF DCT", International Journal of Software & Hardware Research in Engineering Vol. 1 Issue. 3,Nov.2013.