Video Steganography : A Survey

Mr. Gopal Krishn Pandey[1], Mrs. Sameena Zafar[2]

[1]*M.Tech. Scholar, E&TC Department, Patel College Of Science & Technology, Bhopal*

[2]*Assistant Professor, E&TC Department, Patel College Of Science & Technology, Bhopal*

Abstract - Now a days, it is very risky to handle the data in internet against intruders. Data is generally in the form of text, audio , video and image. Steganography is one of the best method to share the data secretly and securely. Steganography algorithm can be applied to audio, video and image file. Secret data may in the form of text, image or even in the form of video and audio. Hiding secret information in video file is known as video steganography. In this paper, a review on various video steganography techniques has been presented. Various spatial domain and transform domain techniques of video steganography have been discussed in this paper.

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

I. INTRODUCTION

Emergence of internet in 90's has changed the life style of the people drastically. On-line rail reservation, online payment, online money transfer and online shopping has made the life of the people comfortable. Apart from these, internet has now become the major source of information interchange. This is where problem started occurring in this field. Interchanging the information on line has created the threats of information to be intercepted by some unauthorised group of people otherwise known as hackers.

So there is need to develop some kind of techniques which can secure and safe the data from unauthorised person.

Steganography is one such technique which is used to counter this problem. Steganography is basically a technique to hide the secret information in cover file which may be in the form of audio, video, image or even text [1].

In steganography, secret information is hidden in such a way that nobody other than intended person knows the existence of the information within the cover file.

Cryptography is another technique which is used to secure the secret information by encrypting the information.

In this context, there is a difference between steganography and cryptography. In cryptography, encrypted data reveals some kind of secret information in the mind of hackers while in steganography, secret data is hidden in the cover file which do not create any suspicion.

Embedding payload and embedding efficiency are the two crucial parameters of any steganography system [4]. Amount of data which can be hidden in the cover file is known as the embedding payload. The capacity of steganography system to hide as much data as it can with inducing as least distortion as it can on the cover file is known as the embedding efficiency[2].

High embedding efficiency is the prime requirement of any steganography system. High embedding efficiency means least distortion in the cover file and hence it is very difficult to imagine an existence of any secret information in the cover file. This makes it difficult to apply any steg analysis tool to extract out the information from the cover file [3].

Embedding efficiency and embedding payload are generally enjoying inverse proportional relationship. Increasing the embedding efficiency will decrese the embedding payload and vice versa[2].

II. 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 are 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.

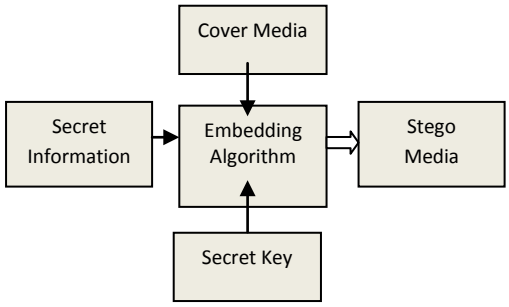

Figure 1 Steganography System

III. RELATED WORK

Most of the research work in video steganography is the extension of image steganography. One of the most common methods of image steganography is least significant bit method (LSB) which can also be applied to the video steganography. In this method least significant bit of the frames of host video is used to carry the secret information [5],[6],[7]. This method is simple and requires least computational power but in this method the secret information can be destroyed easily by some file transformation. Moreover the security of this method is very poor and can be broken easily.

Spread spectrum techniques is another well known method in video steganography which is still explored by the researcher for better performance [7][8].

The advantages of this method is, its robustness. The loss of data after applying geometric transformation is very less in this method. The security of this method is also very strong and difficult to break [8].

Some more methods of data hiding have been introduced in the past which were based on the multi-dimensional lattice structure. Data embedding rate of these method is very high and is able to embed high amount of data by changing the number of quantization level[9].

In 2002 Wang presented a steganographic algorithm for High capacity data hiding[10]. In his approach discrete Cosine transform is used. Main aim of this method is to increase the payload capacity while keeping the robustness and simplicity intact. In this method , DCT coefficients of I-frames are computed and then secret information is embedded by performing modulation between quantized DCT coefficients and secret information.

In 2004[11], Hideki Noda and his fellow researcher presented a steganography method for wavelet compressed video. In this paper an steganography method for lossy compressed video is presented. This is a easy method to send large amount of secret data. This method first compressed the video data using wavelet and then bit plane complexity segmentation steganography is used for embedding the secret data. In this method DWT transformed video is quantized to a bit plane structure and then BPSC algorithm is applied to the video in wavelet domain.

This method is tested for 3-D SPIHT-BPSC steganography and JPEG 2000-BPSC. Former method is the combination of 3-D SPIHT coding and BPSC algorithm of steganography while the latter is the combination of JPEG 2000 standard and BPSC algorithm of steganography. Experimental results reveals that 3-D SPIHT-BPSC is better performer than the JPEG2000-BPSC as far as embedding performance is concerned.

In 2007, Lane presented a vector embedding method for data hiding[12]. This method uses the MPEG-I and MPEG-II video codec standard. In this method, audio information is embedded in to the pixel of host video frames.

R. Kavitha, A. Murugan in 2007[13] proposed a steganography algorithm for AVI video file standard using swapping method. In this paper a comparative analysis of JPEG image steganography and Audio-video interleaved (AVI) steganography has been accomplished with respect to quality and size. Author suggested that by using UTF-32 encoding in the swapping algorithm will increase the strength of the key and also the security of this steganography system. The drawback of this steganography system is its low payload capacity.

In 2007, Yueyun Shang in his paper [14] presented a invertible data hiding techniques foe compressed video. This scheme is suitable for Motion Picture Expart Group (MPEG) standard. In this method , Hidden embedded data of the video can be extracted without the need of copy of original MPEG video and covert video. This scheme work only in frequency domain. Low complexity and low visual distortion is the high points of this method while low payload capacity is the disadvantage of this method.

In 2008, Amr A. Hanafy and his associates presented a steganography model[15] for hiding the presence of secret information in a cover video of any format.

In this model colored video file is pixel-wise manipulated to insert a secret data . this method first segment the secret information in to a blocks before embedding it in to the cover video. In the next level, this method embed these block in psudo random location in video file.

Loaction for embedding is derived by re ordering the secret key which is shared by both sender and receiver. Re-ordering operation is dynamic and changed with each

video frames. This increase the security of the algorithm and nullify and chance of getting the order using statistical analysis for identifying the secret message block location. Interceptor is not able to find the locations of secret message block even if cover video is available to him.

In this paper, a quantitative evaluation of this model has also been presented for four different types of secret information. Peak signal to Noise ratio(PSNR) and Mean Squared error(MSE) is computed between original cover video file and stigo video file.

Simulation result shows least degradation in stigo video file as compared to the original video file for different kind and size of secret data. The authors also estimated the capacity of video files for different video format and size.

In 2009[16], Cheng-Hung Chuang and his fellow researcher presented a optical video crypto-system with adaptive steganography for encrypting and decrypting the video sequence. A double random phase encoding algorithm is applied in this method to encrypt and decrypt the video stream. Video signal is first converted to RGB model and then all the three channel i.e Red, Green and blue channel are separated. Encryption operation is applied to each channel by two random phase mask. Session keys are used for generating these phase mask. Asymmetric method is used for cipher session key to increase the security even further. These key in ciphertext form is the embedded in the encrypted version of the video stream by adopting content dependent low data distortion embedding method. Zero-lsb sorting technique is used to hide ciphered data to encrypted video stream for key delivery. Experimental results reveals that the performance of adaptive steganography is better than the traditional styeganography.

In 2009, Eltahir presented a scheme of video steganography [17]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”[18]. 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[19] . 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” [20]. 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[21] 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 [22]. 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 [23]. 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[24] " 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"[25]. 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[26] 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"[27]. 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.

IV 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 were 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] C.S. Lu: Multimedia security: steganography and digital watermarking techniques for protection of intellectual property. Artech House, Inc (2003).

[6] J.J. Chae and B.S. Manjunath: Data hiding in Video. Proceedings of the 6th IEEE International Conference on Image Processing, Kobe, Japan (1999).

[7] Provos, N., Honeyman, P.: Hide and Seek: An Introduction to Steganography. IEEE Security & Privacy Magazine 1 (2003).

[8] I.J.Cox, J. Kilian, T. Leighton, T.Shamoon: Secure spread spectrum watermarking for multimedia. Proceedings of IEEE Image processing (1997).

[9] J.J. Chae, D. Mukherjee and B.S. Manjunath: A Robust Data Hiding Technique using Multidimensional Lattices. Proceedings of the IEEE Forum on Research and Technology Advances in Digital Libraries, Santa Barbara, USA (1998).

[10] Y. Wang, E. Izquierdo, "High-Capacity Data Hiding in MPEG-2 Compressed Video", 9th International Workshop on Systems, Signals and Image Processing, UK, 2002.

[11] Hideki Noda, Tomonori Furuta, Michiharu Niimi, Eiji Kawaguchi. Application of BPCS steganography to wavelet compressed video. In Proceedings of ICIP'2004. pp.2147-2150

[12] D.E. Lane “Video-in-Video Data Hiding”, 2007.

[13] R. Kavitha, A. Murugan, "Lossless Steganography on AVI File Using Swapping Algorithm," Computational Intelligence and Multimedia Applications, International Conference on, vol. 4, pp. 83-88, 2007

[14] Yueyun Shang, "A New Invertible Data Hiding In Compressed Videos or Images," icnc, vol. 5, pp.576-580, Third International Conference on Natural Computation (ICNC 2007), 2007

[15] Amr A. Hanafy, Gouda I. Salama and Yahya Z. Mohasseb “A Secure Covert Communication Model Based on Video Steganography,” in Military Communications Conference, 2008. MILCOM. IEEE on 16-19 Nov. 2008.

[16] Cheng-Hung Chuang and Guo-Shiang Lin, “An Optical Video Cryptosystem with Adaptive Steganography”, Proceedings of International Association for Pattern Recognition (IAPR) Conference on Machine Vision Applications (MVA’09), pp. 439-442, Keio University, Yokohama, Japan, May 20-22, 2009. (NSC97-2221-E-468-006 International Conference on Computational Intelligence and Multimedia Applications, 2007.

[17] 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.

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

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

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

[25] 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.

[26] 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.

[27] 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.