Survey on Video Steganography Algorithms

Iti Naidu, Deepak Xaxa

Abstract: Internet is becoming more and more risky for handling the data against the intruders. Internet carry the text/audio/video/image data in digital form which can be easily tempered or stolen in the internet due to open access to the internet. Therefore it is essential to transfer the data in the internet secretly. Steganogrphy is one of the such tool which can be used for this vary purpose and can be used to exchange and share the secret data. Such secret data may be in the form of text , audio, video or even an image. Using steganography we can hide the secret information in the image , audio file or even in the video file. Hiding the secret data in a video file is known as the video steganography. This paper present a verty useful and extensive servey of video steganography their advantages/ disadvantages.

Keywords: Steganography, Cryptography, payload, Cover image, Spatial domain, frequency domain.

I. INTRODUCTION

The introduction of the internet and its popularity in the 90’s made the great change in the life style of the people in tremendous way. The emergence of internet has brought the revolution in day to day services used by the people. Internet has made it possible to avail the various services at home by using internet. Online railway reservation, online money transfer, online payment and online shopping are some of the example of the services which made the life of the people very comfortable. Along with this, internet has also become the main source of interchanging the information. This has made the postal service’s almost obsolete for the common people. On one hand the use of internet has shrunk the distance between the people for communicating with each other but at the same it also poses the problem of the secrecy of the information. Since the internet is open network and any body can access it, therefore there are chances that some of the confidential information may get stolen by some intruders who are working hard to get such kind of confidential information. Therefore it is essential to have some kind of method in the internet which can save or secure the confidential information from the hand of such malicious person.

Cryptography, steganography and the watermarking are some of the solution of this problem. In cryptography, confidential information is encrypted and then transmitted. Since the information is encrypted therefore it is not possible for any body to see the information. Only person who knows the pin or password can only be read the information, no one else. Watermarking is basically used for authentication purpose. Steganography is another efficient way to battle the problem of information secrecy. In the steganography,

Secret or confidential information is hidden inside the file called cover file. The cover file may be text, audio/image /video[1].

In steganography, confidential information is inserted in a cover file in such a way that no nobody is able to detect the hidden information inside the cover file. This is in contrast with the cryptography where the existence of the confidential information is revealed by looking some haphazard character while in steganography , no information can be obtained about the confidential information by looking in to the cover file. Two very essential parameters of the steganography are payload and embedding efficiency[4].

Embedding payload refers to the amount of data that can be hidden secretly in the cover file. Embedding efficiency refers to the ability of the steganography system to hide as much data as possible with least distortion in the cover file[2]. One of the major requirements of any steganography method is high embedding efficiency. High embedding efficiency enable the least distortion in the cover file and hence makes it difficult for anybody to detect the existence of the secret information. Therefore it will be difficult to apply any stego analysis tool to extract out the secret information from the cover file[3]. There are inverse relationship between embedding efficiency and embedding pay load. Increasing the embedding payload decreases the embedding efficiency and vice-versa [2].

II. STEGANOGRAPHY SYSTEM

The art of hiding the secret information or secret message in some other host object is called the steganography. Since ancient time, it has been used for sending the secret information.

During the ancient time, back of the wax, scalp of the slaves, rabbits etc were used for sending the secret information.

The application of the steganography has become widespread with the passage of time and with the introduction of the digital era, digital steganography has found vital role in the field of secret communication. Steganography has become vital tool to send the information secretly.

Revised Manuscript Received on 30 May 2017.
***** Correspondence Author

Iti Naidu*, M.Tech, Scholar, Department of Computer Science & Engineering, Mats University, Raipur (Chhattisgarh), India, E-mail: naidu.iti275@gmail.com

Prof. Deepak Xaxa, Professor, Department of Computer Science & Engineering, Mats University, Raipur (Chhattisgarh), India, E-mail: ziakhan5570@yahoo.com.com

Text in the digital form, video/audio digital file has now become the host file for hiding the information instead of wax or scalp of man. Some of the common term which are necessary for understanding the steganography system are given below

Cover Media- It is basically the medium in which the confidential information is hidden. Secret information is hidden in such a way that nobody can detect the existence of the information inside the cover media. Cover media can be digital text or digital audio/video and even the digital image.

Stego- Media- when the secret information is hidden inside the cover media then it is called stego media.

Secret data- Confidential information or secret message which are required to be sent is called tyhe secret data.

Steganalysis-It is the process which is used to detect the presence of secret data by applying some statistical algorithm.

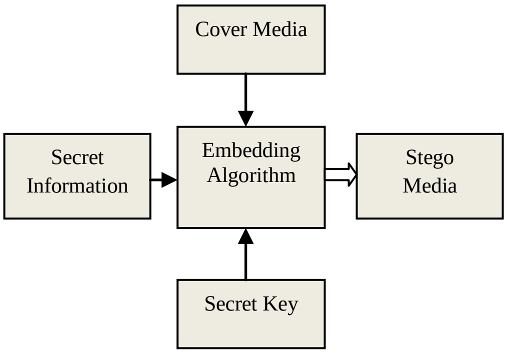

Figure 1 Steganography System

III. RELATED WORK

Video is basically consisting of still image taken in different time and when these images are run in continuous manner we see the motion picture. These still images are called “frames”. So video stegnography can be considered as the extension of the image steganography and hence most of research work in the field of the video steganography is basically the extension of the image steganography.

Least significant bit (LSB) method of steganography is considered as one of the most widely used form of the steganography. In Least significant bit method, list significant bit of the pixel of the image is used for inserting the message bit. Since video basically consist of frames or still images and images consist of tiny pixel therefore LSB method can also be applied to the video for hiding the secret data[5],[6],[7]. This is very simple method does not require much computational power but this method may lose the data if the image undergoes some kind of transformation operation.

Apart from this disadvantage it has one more disadvantage that in term of security, this method is very poor and the secret information can be easily detectable.

Another well known algorithm which are being used and explored for better performance is spread spectrum technique[7][8]. This method is much more robust than the LSB based method apart from this it is geometric transformation proof to some extent. Loss of data is very less in this method after applying the geometric transformation. This method is very good in providing the security and it is very difficult to extract the information from this method[8].

Some more noteworthy contribution in data hiding has introduced in the past which were based upon the multidimensional lattice structure. The advantage of this method is that it is able to hide large amount of data by changing the quantization level[9].

In 2002, wang in his paper[10], presented a steganographic method which can hide large amount of data. He apply Discrete cosine transform in his method. The primary goal of this technique is to increase the payload capacity of the steganography method without affecting robustness and the simplicity. I frames of the video is used to embed the secret information in this method. In his method he first computed the DCT coefficient of the I-frames and then he performed the modulation between DCT coefficients and the secret data.

In 2004, Hideki Noda et al. In his paper[11] put forward another method of steganography for compressed video. They presented a steganography method for lossy compressed video. This method proved to be very simple yet powerful for sending the large amount of data. In this method , first of all the whole video data is compressed by wavelet and then steganography method is applied in the compressed domain. Bit plane complexity segmentation method of steganogarphy is used for embedding the secret information. In this method , DWT transformed video is first quantized to get the bit plane structure followed by the application of BPSC algorithm in the wavelet domain.

For this method test is carried on the 3-D SPIHT-BPSC steganography and JPEG 2000-BPSC. First method is the combination of the BPSC and the SPIHT coding method of steganography. On the other hand second method as the name suggest is the combination of the BPSC algorithm and the JPEG 2000 standard. Experimental results on both algorithms are carried out and it was found that 3-D SPIHT-BPSC method is better in performance as compared to the counterpart JPEG 2000-BPSC method.

In the year 2007, Lane proposed another method of data hiding which is known as the vector embedding method[12].This method is used for the video standard of format MPEG-I and MPEG-II. This method, embed the audio information in the pixel of host frames.

In the year 2007,R. Kavitha, A. Murugan [13] put forward a stegnagraphy technique which was designed for the AVI video standard. In this method swapping is used. This paper also presented a comparative analysis of steganography method for JPEG image and steganography method for AVI file format. The comparison is carried out in term of quality of the host image and size of the payload. In this paper, author concluded that UTF-32 encoding in swapping algorithm will enhance the security of the key and hence enhance the security of the steganography method. Only drawback of this ytstsem is its low payload capacity.

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.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

In 2007, Yueyun Shang et al[14] put forward a data hiding algorithm for compressed video which is invertible. This method is applicable for MPEG(Motion picture expert group) standard. This method is capable of extracting the hidden data without requiring the original copy of the MPEG video. This algorithm work in frequency domain. Low payload capacity of this method is one of the drawback of this method but lower computational complexity and least visual distortion are advantages of this method.

In 2008, Amr A. Hanafy et.al.[15] proposed a steganography system which can efficiently hide the presence of secret data in the video of any format.

In this algorithm colour video pixel is used to hide the secret message. In this method, first of all the secret message is segmented in to small size block before embedding in the cover video. In the next step, these segmented blocks are then embedded in random location of the cover video. Embedding location is found out by the re-ordering of secret key which is shared by both the the transmitter and receiver.

Re-ordering operation of the secret key is dynamic in nature and change with frame of the video. This operation enhances the security of the algorithm by nullifying the chances of getting the order key with the help of statistical attack. This operation makes it very difficult for the interceptor to find out the actual location of the message block even if cover video is available to him/her. Quantitative evaluation of this method has also been carried out in this paper for 4 different types of secret messages. Peak signal to noise ratio (PSNR) and Mean square error (MSE) are the two parameters which are computed between original and stego video for performance comparison.

Testing results are very encouraging as it reveals least distortion in the stego video for different size of pay load. In this paper, authors also estimated the capacity of video file of different types.

In 2009[16], Cheng-Hung Chuang et.al. proposed a optical video crypto system. This method uses adaptive steganography for video file encryption and decryption. Double random phase encoding algorithm is used in this method for encrypting and decrypting the video file. This method, first of all covert the video file in to RGB frames i.e. red, green and blue channel. Each channel is then encrypted by using the two random phase mask. In order to generate these phase mask, two sessions key are used in this model. Asymmetric key is used in order to enhance the security even further. These key are encrypted and then embedded in the encrypted version of the video file. Content dependent data hiding algorithm is used for this purpose which produce low distortion in the cover video. Zero-LSB sorting algorithm is used for hiding the encrypted key in the video stream. Experimenatl results of this paper shows that performance wise this method outperforms the traditional steganography method.

In 2009, Eltahir[17] put forward another method of steganography which was based on the least significant bit (LSB). Main goal of this work is to increase the payload capacity of the algorithm. In this algorithm, first of all the cover video is converted in to a video frames or still images. These images or frames are then used for hiding the secret information. For embedding operation this method uses the 3-3-2 approach.3-3-2 approach means 3-LSB of Red channel, 3-|LSB of green channel and 2-LSB of the blue channel is used for embedding the secret information. Blue channel is more sensitive to the human eye as compared to the red and green channel therefore only 2 LSB of the blue cannel is used for embedding the secret information in the blue channel. This approach produces least distortion in the video frames. This method is capable of carrying the secret information which is one third of the size of video file.

IN 2009,Jafar Mansouri, published a paper titled “An adaptive scheme for compressed video steganography”[18]. Since I-frames in the video carry larger spatial variation, therefore in this method, this frames is considered for embedding the secret information. P-frames and B-frames, on the other hand carry higher temporal variation is also selected for embedding the secret data. Testing results of this method ensure its high quality and high embedding capacity.

In 2010, Feng et.al.[19] put forward a novel video steganography scheme . In this method motion vector of the video stream is used for carrying the secret data.H.264 video compression standard is used. Modification rate of the motion vector is one of the problems in motion vector based embedding method. This drawback is compensated in this method by using the linear block code as it reduces the modification rate of the motion vector. Testing simulation result confirms the good quality of the recovered data. This is possible because of using linear block code. PSNR (Peak signal to noise ratio) of 37 dB is achieved for the video in this paper which is remarkable.

In 2010,Sherly A P et.al. published a paper titled “Compressed video steganography using TPVD” [20]. This method hides the secret information in the compressed domain. In the previous method, data or message was hidden in the micro block of I-frames. these frames are very sensitive to the scene change and hence showed some poor performance. In this method, instead of I-frames, block of P-frames and B-frames are used for embedding the secret information. Both P and B frames carry maximum motion vector magnitude and hence considered as the suitable for data hiding. This method modified the previous method by adopting the tri-way- pixel value differencing method. Main advantage of this system is that it offers good payload capacity without affecting the quality of the video.

In 2011, Hao et.al.[21] proposed an steganography method which also uses the motion vector for embedding the secret data. In this method, motion vector is estimated using the matrix encoding. This method hides the secret information on the motion vector which has high vertical and horizontal component. Human visual system is capable of detecting the change in the slow moving object or slow moving frames as compared to the fast moving object or fast moving frames. High value of the motion vector represents the fast moving object in the frames and hence selected for information hiding. PSNR values obtained in this paper for the vstego video are computed to be 36dB which shows the good quality of the stego video.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

In 2011 ShengDun Hu et.al. suggested a model of steganography which was based on the non-uniform rectangular partition[22]. This method is suitable for uncompressed video. This method hide the video file in to another video file. In order to hide the video in to another video, frames of both the video are selected and the proper method is applied for embedding.

If the host video stream is represented by F and secret video stream is represented by H then the necessary condition for hiding the secret video in to the host video stream is that the frame length of the host video H must be greater than or equal to the secret video. Each frame of the secret video is segmented in to a non uniform rectangular part which is then encoded.

These encodes information then hidden in the LSB 4-bits of the host video frames. In 2012, Rongyue in his paper [23] proposed BCH coding based steganography system. In this method, secret information is embedded inside the cover object block wise by carrying out some modification. Less computational complexity and low computational time are some of the advantage of this system.

In 2012 Swathi, S. et. al. suggested a very efficient novel method in the paper[24] “ Video steganography by LSB substitution using different polynomial equations”.

It is well known fact that LSB insertion method is one of the most widely used oldest method for data hiding. In LSB method, least significant bit of the host video or image is used for embedding the secret information bit. Approach present in this method, embeds the information bit in specific location of specific frames by LSB method. Polynomial equation here work as a key for this stego system. This method makes the less secure LSB method to a powerful method of hiding data. Payload capacity can also be enhanced using this method.

Polynomial equation of different equation is used here to get the location and frames information where the secret information is to be inserted and hence the coefficients of the polynomial equation work as a key in this algorithm.

In 2012, Lakshmi narayanan et.al. suggested a steganography model which was based on the integer wavelet transform(IWT). The title of the paper was “*A high capacity video steganography based on integer wavelet transform*”[25]. In this approach they used integer wavelet transform to acquire the stego image. Approximation band of the secret image is used for embedding purpose. This improves the payload capacity of the stego algorithm. Algorithm steps for extraction is just opposite to the embedding algorithm. Experimental result of this paper shows robustness of this method along with enhanced security and larger payload capacity. one of the advantage of the integer wavelet transform is that it is able to exploit the spatial and temporal correlation within the frames and among the frames as well. Another advantage of using the integer wavelet transform is that it produce least distortion while embedding operation. These advantages of the IWT compel the researcher to use this method for stego operation.

In the year 2013 Liu et.al. in his paper put forward another algorithm for steganography which was for H.264 compressed video. This method proved to be good for preventing inter-frame distortion. For making the method more robust, information or message is first encoded using BCH code followed by the embedding operation. DCT coefficients of luminance I-frame is used for embedding the information bit. Experimental results shows that the method is able to achieve good quality along-with the robustness.

In 2013 Prajna Vasudev et.al. presented a novel “Video steganography using 32 x 32 vector quantization of DCT”[27]. This method, first convert the video into a frames. 32x32 vector quantization of DCT is extracted from each frame. Then LSB quantization algorithm is applied which provides some vacant space in the frames. This vacant space is then used for filling the information bit.

IV. CONCLUSION

In the present scenario of fast information sharing by using internet and world wide web, information security is of prime concern. Steganograpjhy has become one of the important tool for providing the information security. This paper is an attempt to present a review work accomplished in steganography. Advantage/disadvantage, application, pros/cons of each and every method of steganography have also been discussed in this paper as well.

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. 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.
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.