ISSN No. 0976-5697

Volume 6, No. 5, May - June 2015

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

An Analytical Study on Video Steganography Techniques

[1]Heena Goyal, [2]Preeti Bansal
[1]M.tech Student, [2]Assistant Professor
ECE Department
CEC, Landran, Mohali

Abstract- Steganography refers to the art and science of secret communication in which the information is concealed in such a way so that it does not drive an eavesdropper's scepticism. Steganography is defined as the process of whipping information by embedding messages within other. Video steganography is a transpire technology as a steganographic media over traditional cover medias such as audio and image. Generally videos are transmitted more frequently on internet websites such as face book, YouTube, Daily booth and various other social networking sites thus imposing a large impact on video steganography. This paper proposes an up-to-date comprehensive review on the various video steganographic techniques found in the literature in the last few years. There are various techniques available but the user often gets confuse in the choice of which technique is to opt. In this paper a detailed survey of different steganography techniques which is very helpful for video steganography researchers to obtain better results & high efficiency and security.

Index terms- Video Steganography, Data security, LSB, DWT, PSNR.

I. INTRODUCTION

Steganography refers to the art and science of writing concealed messages such that only the sender and the intended recipient is able to identify the presence of a secret message inside the cover media. The word Steganography commences from two Greek words ―Stegano means "covered or concealed" and graphy means "writing or drawing". It is the art and science to block the survival of communication. The concept of steganography is thousand years old. The Greeks and Nazis used it to conceal secret information by drawing on wax tablets, postage stamps, invisible inks such as- milk, vinegar, honey etc. Nowadays digital files are rapidly used such as text, audio, image and video files for hiding data in a carrier files. Any of the files can be used as a cover media such as Text steganography, Image steganography, Audio steganography or Video steganography.

a. Steganography Vs Cryptography- Steganography and cryptography both are different terms. Steganography is not a replacement of cryptography. Steganography is the guide of the cryptography. Cryptography refers to hide the content of a message where as steganography refers to conceals the existence of a message.

The fringe benefit of steganography over cryptography is that it does not grab attention of the users as it includes both security and encryption.

Video steganography is a highly prominent technology to hide secret information such as text, image, audio or even video itself inside the cover media (video). Video steganography is preferred because it can hide large amount of data and thus imposing high security.

The paper is organized as follows. Section II presents a model of steganography. Section III reviews a set of related work. Section IV represents the empirical evaluation of parameters. Section V concludes the paper.

II. GENERAL MODEL OF STEGANOGRAPHY

The general model of steganography consists of encoder, decoder and communication channel. The model is shown in the form of the prisoner's problem where Tom & Jerry are two friends who want to communicate in order to escape from the jail. But Alice is continuously examining them. In fig 1, there is Tom, who wishes to send a secret message to Jerry. To do so, Tom embeds a secret message into cover media and obtains a stego video. Then the stego video is sent via communication channel. It is also possible that Alice may come to know about the algorithm used by Tom & Jerry for encoding and decoding the secret message and will try to detect the secret message. But Alice has no idea about the secret key that they shared with each other. Hence, Alice can't decode the secret message.

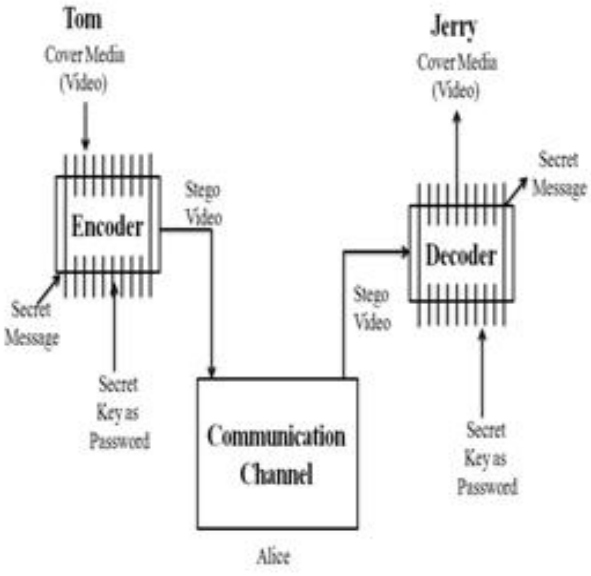

Figure.1. A general model of steganography.

III. REVIEW OF RELATED WORK

The review on some literatures is given below:

ShengDun Hu in 2007[1] proposed a novel video steganography based on non uniform rectangular partition in which an uncompressed secret video is hided inside the cover video. The advantage of this technique is that having high encoding speed of the image.

Hanafy in 2008[2] presented a steganographic model based on PWM (pixel wise manipulation) technique in which the secret data is embedded in a pseudo random fashion using a secret key. The model is evaluated between original video and steganographic video in terms of peak signal to noise ratio and mean square error.

Imran Khan, Vijay Chaudhari in 2010[3] presented a steganography algorithm based on Neural Network for still images. In this the features are extracted of cover image and embedded secret data and then input these features to neural network and obtain the output. The major advantage of neural network is that it has the capability to approximate any non linear functions.

Balaji in 2011[4] proposed a new method to secure data by creating an index and then that index was further used in a frame of the video. At the reception, only the frames which have hidden data are analyzed with so called index used during the transmissions. This technique has the advantage that it is not easily detected by any attacker and also the time utilization in this process is less.

Feng Pan in 2010[5] proposed a video steganography using motion vector and linear block codes to embed secret messages in the motion vectors of cover media during compression. The advantage of this technique is that it has very low computational complexity and highly imperceptible to human eyes.

Elahm Ghasemi et al in 2011[6] presented a steganography scheme using Integer Wavelet Transform and Genetic Algorithm. The secret data is embedded in integer wavelet transform coefficients using genetic algorithm in 8x8 blocks on the cover media. The chief advantage of using Genetic Algorithm is that it helps in reducing the error between the cover and stego images and thus increasing the embedding capacity with low distortion.

Dauti, Manjula et al in 2012[7] proposed a method to secure data using Discrete Wavelet Transform (DWT) and Hybrid Wavelet Transform (HWT) in which the secret data is compressed using HWT and then encrypted and embedded in frequency domain. The chief advantage of using this technique is that the size of hidden media can be twice or more than twice the size of cover media and moreover the Entropy and Mean Square Error (MSE) are improved as compared to previously obtained results.

Paul, Acharya et al in 2013[8] proposed a Least Significant (LSB) replacement technique using a video steganography in which the secret video is embedded in the original video by creating an index based chaotic sequence and then arranging the pixels according to the sequence. The major advantage of this technique is that there is no perceptual difference between the original video and stego video.

Kelash et al in 2013[9] proposed a steganographic algorithm based on colour histogram has the ability to hide large size of data without any error and provides a high level of authentication to guarantee integrity of video. The advantage of using this technique is that it provides a high security and resistance against attackers.

Sunil Moon et al in 2013[10] proposed a steganography technique using computer forensics to enhance data security in which they used video as cover media for hiding the secret message and computer forensics for authentication. The algorithm used is 4LSB Substitution (Least Significant Bit) to embed secret information behind selected frame of video. The advantage of this technique is that it is very difficult to find in which part of video secret data is hiding and also with 4 LSB method embedding capacity is 4 times as that to 1 LSB method.

Table1. Previous Techniques with results

Author Name	**Technique Used**	**Parameter calculated**
ShengDun Hu (2007)	Least Significant Bit	PSNR= 29.75 dB
Hanafy, Salama, Mohasseb (2008)	Pixel Wise Manipulation	PSNR= 51 dB
Imran Khan, Vijay (2010)	Neural Network	PSNR= 49.54 dB
Feng Pan (2010)	Motion vector, Linear Block Codes	PSNR= 43 dB
Balaji, Naveen (2011)	Least Significant Bit Insertion Method	Retrieval time is few seconds.
Elahm Ghasemi, Jamshid (2011)	Genetic Algorithm, Discrete Wavelet Transform	PSNR= 39.94 dB
Dauti, Manjula (2012)	Hybrid Wavelet Transform	MSE= .000027
Paul, Acharya, Yadav (2013)	Least Significant Bit	PSNR= 31dB
Kelash, El-Sayed (2013)	Histogram	PSNR= 48.91dB
Sunil K. Moon, Rajeshree (2013)	4 Least Significant Bit, Histogram	PSNR= 50dB

IV. PERFORMANCE MEASUREMENT METRICS

The PSNR and MSE are the two metrics that helps in calculating results. The PSNR and MSE values are calculated using equations below. The Peak Signal-to-Noise Ratio (PSNR) is given by:

$$\text{PSNR} = 20\ \log_{10}\left(\frac{\text{MAX}}{\sqrt{\text{MSE}}}\right) \qquad (1)$$

Where MAX= Maximum Possible Pixel Value of an image. Generally it is 255.

The mean-squared error (MSE) is given by:

$$\text{MSE} = \frac{1}{m*n}\sum_{i=0}^{m-1}\ \sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \qquad (2)$$

Where m,n- represents the size of image.

The Peak Signal-to-Noise Ratio (PSNR) is calculated to measure the quality of stego image. The PSNR is calculated in decibels (dB). Larger value of PSNR indicates better quality of an image.MSE is the difference between true value and the estimated value. PSNR and MSE are inversely proportional to each other.

V. CONCLUSION AND FUTURE WORK

In this paper, work done by various authors has been analysed on different techniques in the domain of video steganography. The algorithms are based on various formats such as Joint photographic Expert (JPEG), Bit Map format

(BMP), Graphic Interchange Format (GIF), Audio Video interleave (AVI). Video Steganography is a vital and rapidly growing research area. It is a form of security through ambiguities and puzzles. It is a kind of book on magic.

The future scope of this stance depends on the combined focus and overall development in the field of video steganography so as to gain high security and higher value of peak signal to noise ratio.

VI. REFERENCES

[1] Sheng Dun Hu, Kin Tak, U.,"A Novel Video Steganography based on Non uniform Rectangular Partition," IEEE International Conference on Computational Science and Engineering (ICCSE), pp. 57-61, August 2007.

[2] Hanafy, A. A., Salama, G. J., Mohasseb, Y. Z., "A Secure Covert Communication model based on Video Steganography," IEEE Military Communication Conference (MILCOM), pp. 1-6, Nov 2008.

DOI: 10.1109/MILCOM 2008.4753107.

[3] Imran Khan, Vijay K. Chaudhari, "Neural Network Based Steganography Algorithm for Still Images," IEEE International Conference on Emerging Trends in Robotics and Communication Technologies (ICETRACT), pp. 46-51, Dec 2010.

DOI: 10.1109/INETRACT.2010.5706192.

[4] Balaji, R., Naveen, Garewal, "Secure Data transmission using Video Steganography," IEEE International Conference on Electro/ Information Technology (EIT), pp. 1-5, May 2011. DOI: 10.1109/EIT.2011.5978601.

[5] Feng Pan, Li Xiang, Xiao Yang, "Video Steganography using Motion Vector and Linear Block Codes," IEEE International Conference on Software Engineering and Service sciences (ICSESS), pp. 592-595, July 2010.

[6] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, "A Steganographic method based on Integer Wavelet Transform and Genetic Algorithm," IEEE International Conference on Communication and Signal Processing (ICCSP), pp. 42-45, Feb 2011.

[7] Danti, A. ,Manjula, G. R., "Secured data hiding of Invariant Sized secret image based on discrete and hybrid wavelet transform," IEEE International Conference on Computational Intelligence and Computing Research(ICCIC), pp. 1-6, Dec 2012.

DOI: 10.1109/ICCIC.2012.6510181.

[8] Paul, R., Acharya, A. K., Yadav, V. K., Batham, S., "Hiding large amount of data using a new approach of Video Steganography," IEEE 4th International Conference on Information Technology (CIT), Sep 2013. DOI: 10.1049/CIT 2013.2338.

[9] Kelash, Hamdy M., Abdel Wahab, O. F., Elshakankiry, O. A, EL-Sayed, H. S., "Hiding data in Video Sequences using Steganographic Algorithms," IEEE International Conference on Convergence (ICTC), pp. 353-358, Oct 2013. DOI: 10.1109/ICTC.2013.6675372.

[10] Sunil K. Moon, Rajeshree. D. Raut, "Analysis of secured Video Steganography using Computer Forensics Technique for Enhance Data Security," IEEE International Conference on Image Information Processing (ICIIP), pp. 660-665, 2013.

[11] Bhattacharyya S., Banerjee I., Sanyal G. ,"A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier," Journal of Global Research in Computer Science (JGRCS), April 2011.

[12] Bhautmage P., Jeya Kumar, Dahatonde., "Advanced Video Steganography Algorithm", International Journal of Engineering Research and Applications (IJERA), vol. 9, no. 5, pp. 85-90, February 2013.

[13] R. Poornima, "An Overview of digital video Steganography," International Journal of Computer Science & Engineering Survey (IJCSES), vol.4, pp.80-84, February 2013.

[14] Nosrati M., Karimi R., Hariri M., "A Novel Steganographical Approach to Text Message Hiding in RGB Carrier Image", International Journal of Basic and Applied Scientific Research (IJBACR), March 2011.

[15] Liu B., Liu F. and Wang, "Inter-Frame Correlation Based Compressed Video Steganalysis", IEEE Conference Publications on Image and Signal Processing (CPISP), vol. 3, pp. 42-46, May 2008.

[16] Ansari N., Zhicheng Ni, Yun-Qing Shi, "Reversible data hiding", Circuits and Systems for Video Technology, IEEE International Transactions on image processing (ITIP), vol. 16, no. 3, pp. 354-362, March 2006.