

Comparative Study on different Video Hiding Techniques

P.Saravanan^{1*}, K. K. Thyagarajan²

¹Dept. of Computer Science and Engineering, Manonmaniam Sundaranar University, Tirunelveli, India

²Dept. of Computer Science and Engineering, RMD Engineering College, Chennai, India

*Corresponding Author: saravananphdmailam@gmail.com

Available online at: www.ijcseonline.org

Accepted: 26/Nov/2018, Published: 30/Nov/2018

Abstract— In general, the data or information hiding mechanism with different perspective is a recent trend in the video data hiding and protection on-going research issues. For the most part of the video data hiding focuses on video content in different phases with modern cryptographic algorithms in order to secure from unauthorized access over the communication channel or network. In our previous research work contemplate its focuses on the data or textual content hiding mechanism over the content sharing among different clients through networks. The objective of the previous research is achieved with the help of data compression mechanism and hiding aspect in new direction regarding to protect the multimedia data content. This research paper describes the progress in the field of video steganography and intends to give the comparison between its different uses and techniques.

Keywords— Multimedia, Data, Content, Hiding and Compression

I. INTRODUCTION

Video steganography is a combination of sound and image techniques. The video files with different formats usually have separate inner files for picture and sound. Steganographic techniques can be applied to video and sound. The mere size of any video file indicates the scope for hiding large amounts of secret information and yet goes undetected. Video Steganography is a technique to hide any type of files into a carrying Video files. The use of the video based Steganography can be more suitable than other video files, because of its size and memory necessities. The Least Significant Bit (LSB) insertion is a main approach for embedding the information in a carrier file. The Least significant bit (LSB) insertion technique operates on LSB bit of the medium file to hide the information bit.

A. Techniques of Video Steganography

There are various techniques of video steganography available in the IT field. The best technique is to hide the secret data without reducing the quality of the cover video, so that it cannot be detected by naked eyes. The embedded video is known as the “stego” video which is sent to the receiver side by the sender[1]. The variety of video steganography techniques are used now a days, to secure important information. Some much known techniques are explained briefly in the following:

a. LSB (Least Significant Bit) method

LSB is said to be the best method for data protection, because of its simplicity and commonly used approach. It is

the most easiest and effective ways of embedding data. In LSB, the cover video’s pixel values are extracted which are in bytes, then its LSB are substituted by the bits of the secret message that it is embedding. Now since here change only the LSB bits of the host video, it doesn’t gets distorted and almost looks alike as the original video[2].

b. Non-uniform rectangular partition

This method is for only uncompressed videos. In non-uniform rectangular partition, data hiding is done by hiding an uncompressed secret video file in the host video stream. But it have to make sure that both the secret as well as the cover file should be of almost the same size. Each of the frames of both the secret as well as cover videos is applied with image or text steganography with some technique. The secret video file will be hidden in the leftmost four least significant bits of the frames of the host video[3].

c. Compressed Video Steganography

This method is done entirely on the compressed domain. Data can be embedded in the block of I frame with maximum scene change and in P and B block with maximum magnitude of motion vectors. The AVC encoding technique yields the maximum compressing efficiency[4].

d. Anti-forensics technique

Anti-forensic techniques are actions taken to destroy, hide and/or manipulate the data to attack the computer forensics. Anti-forensic provides security by preventing unauthorized access, but can also be used for criminal use also.

Steganography is a kind of anti-forensic where we try to hide data under some host file. Steganography along with anti-forensics makes the systems more secure[5].

Masking and filtering Masking and filtering are used on 24 bits/pixel images and are applicable for both colored and gray scale images. It is like watermarking over an image and doesn't affect the quality of that image. Unlike other steganography techniques, in data masking the secret message is so processed such that it appears similar to a multimedia file. Data masking cannot easily be detected by traditional steganalysis[5].

B. Background Theory

For any successful video steganography system following measures should be considered:

a. Imperceptibility

Imperceptibility or undetectability refers to the visibility of modification inside the cover media. High Imperceptibility means increasing the invisibility of slight modifications in cover object. Modern day steganalysis approaches are highly intelligent to detect slight modifications. High Imperceptibility has motivated researches to design steganalysis resistant video steganography methods[6][7].

b. Payload

Payload or capacity refers to the amount of secret message that can be concealed inside cover media[8]. Video are gaining popularity as highly used cover media object due to their high embedding capacity and embedding efficiency.

c. Robustness

The attacks or methods applied on stego object to extract hidden or secret information are known as statistical attack[9]. Steganography algorithm must be robust against statistical attacks. It describes robustness feature.

d. Security

The most important feature of any steganographic algorithm is security. The embedding process should have high security with minimum vulnerability to attacks. Several approaches have been proposed to secure message in steganography[10].

f. Perceptual Quality

Increment in embedding capacity may also lead to degradation of video quality or degradation of original contents of video. Video steganography approach must handle control degradation of video quality. Generally the video steganography technique classified based on compressed domain (compressed, uncompressed video), Embedding domain (spatial domain, transform domain), classification based method(format based, video codec based).The message embedding process based on two techniques , (i)spatial domain based and (ii)transform domain based.

II. LITERATURE REVIEW

Jenifer et al. [7] proposed LSB approach for video steganography to Embed secret images. This method improves the visual quality(high values of PSNR) of secret images.This new video steganography method has many advantages and disadvantages such as user friendliness and simple method of processing images. Security is also increased.

Suryawanshi and Belsare[12] developed a hardware approach to provide secure data transmission using LSB substitution and Lifting DWT. First of all, cover video is decomposed into frames then LSB substitution is done to embed the secret image. Thus increases payload capacity. For compression, Lifting DWT is used to increase security. Finally, the whole process is implemented on FPGA hence reduces computational time.

Kousik Dasgupta et.al[8] proposed hash based LSB technique for video steganography. The Proposed Method is analyzed in term of both Peak Signal to Noise Ratio (PSNR) compared to the original cover video as well as the Mean Square Error (MSE) measured between the original and steganographic files averaged over all video frames.

Nitin Jain et al., [9] shown steganography process with edges of images can be used to hiding text message. This work is done with help of edge detection filters. By using the edge detection approach along with least significant bit(LSB) method leads to high security even with a little object as an image, the embedded image is just like the original one.

A. Swathi et al., [10] describes a data hiding scheme was be developed to hide the information in specific frames of the video and in specific location of the frame by LSB substitution using polynomial equation. In this information was embedded based on the stego key.

Shamim Ahmed Laskar et al. [11] proposed a framework for hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access.

Ashish T. Bhole et al. [12] describes steganography over Video File using Random Byte Hiding and LSB(least significant bit) Technique. Authors have given comparative analysis of video steganography techniques, encryption and decryption time and hiding data ratio (per frame) in tabular form.

Embedding the secret data in the video files is known as video steganography. It is the most advanced form of steganography which makes it very difficult to break for the attacker to retrieve and detect the confidential data as it is a collection of the images and audio. Video steganography is a combination of the audio and images steganography. It contains large amounts of data and moving streams of images and sound which makes it easier to hide the data inside the videos[15].

A data hiding technique in videos was proposed by Li et al., [16][4] which is based on video sequences. An embed point, where the secret data is to be embedded is selected using an adaptive embedding algorithm. 4x4 DCT residual blocks are adopted and a predefined threshold is determined. The blocks are traversed in an inverse zigzag manner to search for the first non-zero coefficient. The predefined threshold is compared to the value of this coefficient determined and if it is lesser than the value of the coefficient, then data is embedded at that pixel.

J. J. Chae et al., [16] proposed another technique of data hiding in video. In this method, there are two main categories. The first one involves an uncompressed raw video stream and secret data is embedded in that.

Giuseppe Cacao et al., [11] proposed the second category which embedded the secret data directly into a compressed video stream. An algorithm for video compression was proposed by Sherly A P et al. [13] known as tri-way pixel-value differencing with pseudo random dithering (TPVDD). This algorithm is used for embedding secret data. It increases the capacity of the hidden secret information and provides enhanced security.

III. PERFORMANCE PARAMETERS

A. Visual Quality

1) Mean Square Error (MSE)

MSE measures the average of the squares of the 'Error'. It is the average squared difference between a cover and stego video frame.

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [I(i,j) - I'(i,j)]^2}{M \times N} \quad \text{-----(1)}$$

In this formula,

I= Original host Frame

I'= Stego Frame

M= Number of rows in original frame.

N= Number of Column in Original frame.

2) Peak Signal to Noise Ratio (PSNR)

PSNR ratio is used to find out the visual quality of the proposed video steganography method. PSNR is an objective quality measurement used to calculate the difference between the original and the stego video frames. PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR is most easily defined through the Mean Squared Error (MSE). It is expressed by,

$$PSNR = 10 \log_{10} \frac{P \times P}{MSE} \quad \text{-----(2)}$$

Where, MAX0 is maximum intensity of image. Typical value for the PSNR is 30 to 50 dB, where higher value of PSNR is always better.

B. Embedding Payload

Embedding payload is the maximum amount of data can be embedded into the cover file without losing the quality of the original file. Embedding payload of any video steganography technique is decided by Hiding Ratio (HR)

. Hiding Ratio (HR) is expressed by,
Size of Embedded Message

$$HR = \frac{\text{Size of Embedded Message}}{\text{Video Size}} \times 100\% \quad \text{-----(3)}$$

C. Robustness

To evaluate the performance of video steganographic algorithm for correctly retrieving the secret message, two objective metrics have been used: 1) the Similarity Function (SF) and 2) the Bit Error Rate (BER). Both parameters are used to test whether the extracted secret message has been corrupted during the communication. To achieve the robustness of the algorithm, the higher SF and the lower BER must be obtained. [9]

In order to verify the efficiency and capacity of our proposed and compare with other existing video steganography algorithms. A program is designed as per the algorithm described in the previous paper. MATLAB tool is used as a programming environment. Since the steganography algorithm is meant for video sequence or frames. Therefore as many as three different video has been taken. Frames dimension in all the video is 256x256 number of frames in all the videos are different. In the first phase of testing, a text data of 1Kb size is taken and hidden by applying to our proposed algorithm.

In order to check the effect of the data hiding in the quality of the stego frames performance measure like PSNR(Peak Signal to Noise Ratio) and MSE(Mean Squared Error) are computed. For Mean Squared Error computation, following formula is used-

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [I(i,j) - I'(i,j)]^2}{M \times N}$$

In this formula,

I= Original host Frame

I'= Stego Frame

M= Number of rows in original frame.

N= Number of Column in Original frame.

From the above MSE formula it is clear that the value of this measure must be as less as possible. 0 value of MSE represent zero distortion in the stego frames in the video as compared to the original frame. A good steganography technique must be able to produce less distortion in the stego video. For computing the Peak Signal to Noise Ratio measure, following formula is used

$$PSNR = 10 \log_{10} \frac{P \times P}{MSE}$$

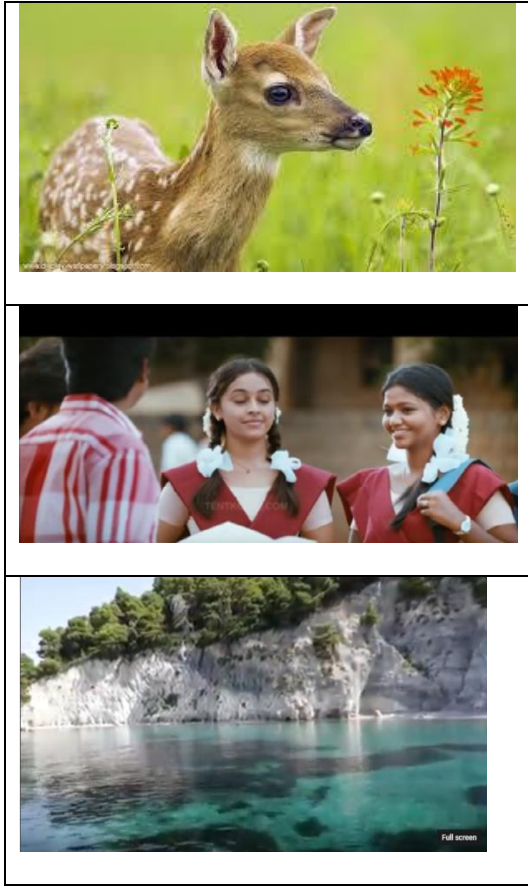


Figure 4: Video taken for testing the steganography algorithm, animal.avi(Upper), tamilmovie.avi (Middle) and river.avi(Lower)

Here

P = Maximum pixel value in the frame.

The value of MSE for zero distortion stego frames or video is zero and hence the PSNR is infinite for the zero distortion frames or video.

Table 1 PSNR and MSE Comparison(text size=1kb)

Video	PSNR between Original and Stego Video	MSE between Original and Stego Video
animal.avi	77.2568	0.6258
tamilmovie.avi	76.2556	0.7588
river.avi	76.9458	0.6554

In order to test how the quality of the stego video is affected with different capacity of payload i.e. text data or image data. Similar test is performed by taking different capacity of pay load. Computed PSNR and MSE is tabulated in table 2, table 3 and table 4 for different videos.

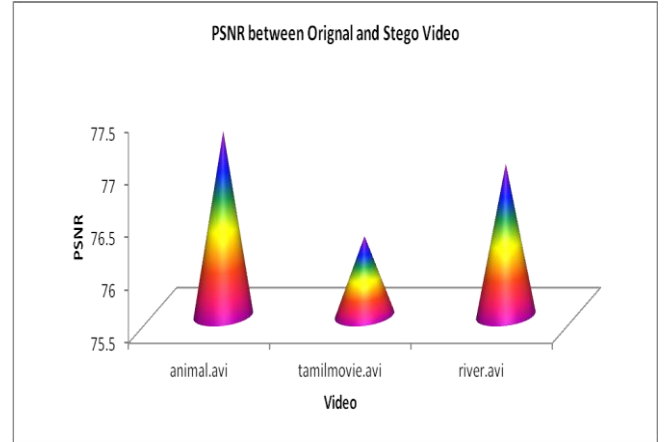


Figure 5: PSNR Comparison Graph Between Original and Stego Video

practically there are always some distortion in the stego frames as compared to the original frames and hence the value of PSNR must be as high as possible. Computed PSNR and MSE values for all the three different videos for the text size of 1 Kb is tabulated in the table 1. Higher values of PSNR and Lower values of MSE clearly shows that the proposed algorithm is very good at producing least distortion.

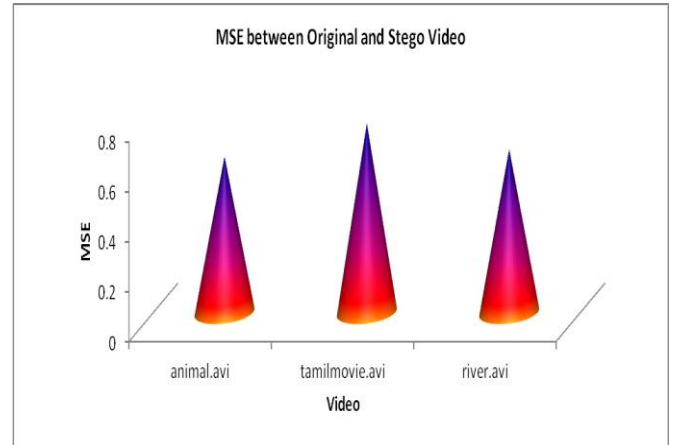


Figure 6: MSE between Original and Stego Video

Table 2: PSNR , MSE and Payload between Original and Stego Video for animal.avi


Video	PSNR between Original and Stego Video	MSE between Original and Stego Video	Payload
 animal.avi	77.2565	0.6587	1kb
	77.9845	0.6658	2kb
	74.2525	0.6758	3kb
	72.2548	0.6987	4kb

Table 3: PSNR , MSE and Payload between Original and Stego Video for tamilmovie.avi



Video	PSNR between Original and Stego Video	MSE between Original and Stego Video	Payload
	77.2562	0.7452	1kb
	77.6589	0.7584	2kb
	75.2525	0.7789	3kb
	75.8545	0.8145	4kb

Table 4: PSNR , MSE and Payload between Original and Stego Video for river.avi

Video	PSNR between Original and Stego Video	MSE between Original and Stego Video	Payload
	74.2365	0.7548	1kb
	74.9895	0.7685	2kb
	74.2325	0.7725	3kb
	73.5621	0.7456	4kb

IV.RESULT ANALYSIS

For implementation of proposed video steganography system has been experimented through Matrix Laboratory (MATLAB) software which is running on laptop with a 2 GHz Core2duo with 4GB RAM and windows10 operating system. For experiment three different video sequences i.e. river, tamilmovie and animal is taken. The PSNR of existing video steganography system for same three video sequences is 35.58.68 dB and the PSNR of proposed video steganography system for same three video sequences is ranged between 35.58.68 dB.

Table :5 HR Comparison of Proposed and Existing System.

System	Hidden Ratio (HR)
Existing System	29.45%
Proposed System	34.85%

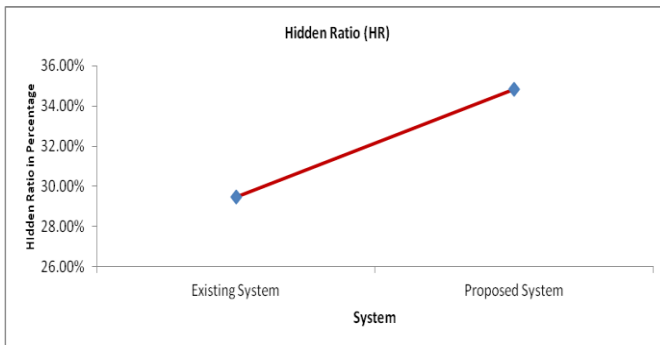


Figure 7: Comparison of HR

Even Hidden Ratio(HR) of existing system in 29.45% which is improved in proposed system. The HR of proposed system is 33% .The result of those sequences in terms of HR and PSNR is given above.

IV.CONCLUSION

There are several of issues related to video steganography i.e. robustness, security, hiding capacity, compression and decompression etc. In the proposed method here it is used advance LSB approach for embedding process i.e. improved performance of steganography system in terms of visual quality, hiding capacity, compression and robustness. Because advance LSB works on 4 bit LSB which is improved hidden capacity in terms of HR as well as SVD is used which is improved visual quality of stego video in terms of PSNR is used which is improved robustness against various attacks. So it is provided high robustness and high visual quality and high hidden capacity.

REFERENCE

- [1] Ramandeep Kaur, Pooja, “XOR Encryption Based Video Steganography”, International Journal of Science and Research (IJSR), Vol.4, Issue 11, November 2015.
- [2] Pooja Jain and Navdeep Kanwal, “Image Steganography in RGB Color Components using Improved LSB Technique Image Pattern Compression using Weighted Principal Components Algorithm”, Indian Journal of Science and Technology, 9(45), 2016.
- [3] J. Jeswani and D. T. Sarode, “A New DCT based Color Video Watermarking using Luminance Component,” IOSR Journal of Computer Engineering (IOSR-JCE), vol.16, no.2, pp. 83–90, 2014.
- [4] S.R.Hallur, S. Kuri, G. S. Sudi, and D. G.H.Kulkarni, “A Robust Digital Watermarking For Gray Scale Image,” International Journal For Technological Research In Engineering, vol.2, no. 10, pp. 2440–2443,2015.
- [5] O. S. Faragallah, “Efficient video watermarking based on singular value decomposition in the discrete wavelet transform domain,” AEU - International Journal of Electronics and Communications, vol.67, no.3, pp.189–196,2013.
- [6]. R. J. Mstafa and K. M. Elleithy, “ A highly secure video stegnography using Hamming code (7, 4)” in Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island, 2014, pp.1-6
- [7]. Ms. Pooja Vilas Shinde and Dr. Tasneem Bano Rehman, “A Survey: Video Stegnography techniques” in International Journal of Engineering Research and General Science Volume 3, Issue 3, May-June, 2015 ISSN 2091-2730.
- [8]. Syeda Musfia Nasreen,et al.,“A Study on Video Stegnography Techniques” in International Journal of Computational Engineering Research (IJCER), Vol 05, Issue 10, October–2015, ISSN (e): 2250–3005.

- [9] H. Almarabeh "Steganography Techniques - Data Security Using Audio and Video" International Journal of Advanced Research in Computer Science and Software Engineering Volume 6, Issue 2, pp.45-50, February 2016.
- [10] S. Kamesh, K. Durga Devi, S. N. V. P. Raviteja, "DWT based data hiding using video steganography", International journal of engineering sciences & research technology, pp.361-367, 2017.
- [11] Disha and K.Saini. "A review on video steganography techniques in spatial domain" IEEE Conference on Recent Developments in Control, Automation & Power Engineering, Noida, India, 2017.
- [12] D. B. Suryawanshi and S. S. Belsare "An Efficient Implementation of Video Steganography on FPGA using DWT and LSB Algorithm", International Journal of Scientific & Engineering Research, Vol.7, Issue.5, pp.450-453, 2016.
- [13] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta, "Hash based Least Significant Bit Technique", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012
- [14] A. Swathi, Dr. S.A.K. Jilani., "Video Steganography by LSB Substitution Using Different Polynomial national Journal Of Computational Engineering Research (ijceronline.com) Vol. 2 Issue. 5
- [15] Mriitha Ramalingam: Stego Machine – Video Steganography using Modified LSB Algorithm World Academy of Science, Engineering and Technology Vol:50 2011-02-26
- [16] Ashawq T. Hashim*, Dr.Yossra H. Ali** & Susan S. Ghazoul*" Developed Method of Information Hiding in Video AVI File Based on Hybrid Encryption and Steganography" Engg.and tech journal, vol 29,No.2,2011.

Technology, India in 1988. He also possesses a Post Graduate Diploma in Computer Applications from Bharathiar University, India. He obtained his Ph.D. degree in Information and Communication Engineering from College of Engineering Guindy, Anna University, India in 2007. He is in teaching profession for around three decades and served at various levels including Principal, Dean and Professor at various Engineering Colleges in Tamil Nadu-INDIA. During his tenure as a Principal and Dean he was a member of Governing Council of RMK Group of Institutions. He has written 5 books in Computing including "Flash MX 2004" published by McGraw Hill (India), which has served recommended as text and reference book by universities. He is a grant recipient of Tamil Nadu State Council for Science and Technology. He has been invited as chairperson and delivered special lectures in many National and International conferences and workshops. He is reviewer and editorial board member for many International Journals and Conferences. He is a recognized supervisor for Ph.D candidates and Master students at Anna University. He has published more than 90 papers in National & International Journals and Conferences. Three candidates have completed PhD and eleven more are doing PhD under his supervision. His research interests include Computer Vision, Semantic Web, Image & Video Processing, Multimedia Streaming, Video Coding, Content-based Information Retrieval and e-learning. He is a life member of ISTE, CSI INDIA and also senior member and invited member in many professional associations. He has been recognized by Marquis Who's Who in the World for his contribution to the technical society and his biography has been published in its 25th Anniversary Edition (2008). He has been recognized as a Teacher Par Excellence twice by the management of SSN institutions. He received Distinguished Faculty (Multimedia and Image Processing) Award in the Contemporary Academic Meet VICAM 2016 organized by Venus International Foundation.

Author Biography

Mr.P.Saravanan obtained his M.C.A., degree from Mailam Engineering College (Anna University) and received his M.E., degree in computer Science from Mailam Engineering College (Anna University).He has served at Mailam Engineering College. Since August 2008, he is the Asso.Prof of Mailam Engineering College. He has published 4 National Conference Papers, two International Conference and two International Journal.



K.K. Thyagarajan received his B.Eng. degree in Electrical and Electronics Engineering from PSG College of Technology, Madras University, India and received his M.Eng. degree in Applied Electronics from Coimbatore Institute of

