IJESRT: 9(9), September, 2020 ISSN: 2277-9655

International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

Chief Editor
Dr. J.B. Helonde

Executive Editor
Mr. Somil Mayur Shah

Website: www.ijesrt.com Mail: editor@ijesrt.com

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

HIDING DATA IN VIDEO FILES USING DISCRETE WAVELENGTH TRANSFORM AND FIBONACCI SERIES ALGORITHM

Lakhwinder Kaur[*1] **& Sarbjeet Kaur**[2]
[*1]Master of Technology, Adesh Institute of Engineering and Technology
[2]Assistant Professor, Adesh Institute of Engineering and Technology

DOI: https://doi.org/10.29121/ijesrt.v9.i9.2020.2

ABSTRACT

Stegnography is a process to hide the secret message which we want to hide from the outside world in an another media file while the cryptography is another security process in which a data form is changed to another so that it can not be accessed directly. In the proposed system, maximum motion and high intensity between every consecutive frames is evaluated. The proposed system also uses Fibonacci series to evaluate the next pixel in which data is to be hidden. Data is hidden using DWT algorithm. The proposed system is tested on various inputs and results evaluated are compared with the existing system.

KEYWORDS: Video Stegnography, DWT, Data Security, Data Transfer.

1. INTRODUCTION

Digital steganography is the art and science of hiding communications; a steganographic system thus embeds secret data in public cover media so as not to arouse an eavesdropper's suspicion. A steganographic system has two main aspects: steganographic capacity and imperceptibility. However, these two characteristics are at odds with each other. Furthermore, it is quite difficult to increase the steganographic capacity and simultaneously maintain the imperceptibility of a steganographic system. Additionally, there are still very limited methods of steganography to be used with communication protocols, which represent unconventional but promising steganography mediums. Digital image steganography, as a method of secret communication, aims to convey a large amount of secret data, relatively to the size of cover image, between communicating parties. Additionally, it aims to avoid the suspicion of non-communicating parties to this kind of communication. Thus, this research addresses and proposes some methods to improve these fundamental aspects of digital image steganography. Hence, some characteristics and properties of digital images have been employed to increase the steganographic capacity and enhance the stego image quality (imperceptibility). This chapter provides a general introduction to the research by first explaining the research background. Then, the main motivations of this study and the research problem are defined and discussed. Next, the research aim is identified based on the established definition of the research problem and motivations.

With the advancement of technology, the way of communication between people all over the world changed rapidly. Now people can exchange information over the internet in form of media files that contains text, audio and video. To transfer these media file online, there is need to design some secure application such that unauthorised person can't access the confidential information. The solution for security related issues lies in security techniques that are Cryptography and Steganography.

Types of steganography:

- Text Steganography
- Image steganography
- Audio steganography
- Video Steganography
- Network Steganography

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

Video Steganography

In video steganography, video is used to embed information and act as cover medium. The different frames of video are used to hide data as video is collection of image in the form of frames. Videos that can carry secret message are any types of format such as AVI, Mp4, MPEG and H.264. All image and audio steganography techniques can be implemented on videos. Video steganography also comprise of spatial domain and transform domain techniques.

Different types of steganography techniques are Linguistic, Image, Audio, Video and Network Steganography commonly used. Among these video steganography is more reliable as video is collection of pictures and audio signals. A video file contains large number of redundant bits and message can be easily embedded in repeating portion of video.

Video Steganography is a method to hide different types of files into a video file. It is difficult to detect the secret file by Human Visual System (HVS), as frames are display on screen at very fast rate. Different existing technique of image and audio steganography are also applied on video Steganography. The steganogaphy model consists of carrier video or cover object which is the carrier for secret message; secret image is secret file that is embedded and stego key for encoding and decoding. It can be described as collection of Cover object, hidden data, stego key that creates a stego model.

Characteristics of Video Steganography

The characteristics that must be followed by effective steganography techniqueare:

[1] ***Secrecy:*** An unauthorized person cannot extract hidden information from the video.
[2] ***Undetectable*:** Theviewer cannot even sense the presence of secret message. No algorithm exist that identify whether a video contains a hidden message
[3] ***Capacity:*** It can be defined by the total amount of the data that can be hidden in the image file.
[4] **Accuracy:** It is defined as the, the system is said to be accurate if the data retracted is accurate and reliable.

2. LITERATURE SURVEY

Afsha Shaukat, Steganography has always been competent in the field of data hiding by ensuring its remarkable behavior of preserving the secrecy of data. In order to maintain the secrecy of private data, the host data is being exploited to hide the information in such a way that it is unrecognizable to the human visual system thereby meeting the goals of steganography which are high embedding capacity, imperceptibility and robustness. Various amounts of work have been done in this field by a number of researchers. In this paper we have used a new image steganography technique using Fast Fourier Transform on the cover image Then the secret image is embedded into the two components of the cover image formed after applying the FFT on the cover image using the Least Significant Bit substitution method. The results obtained prove that this method is efficient and highly imperceptible to the human eye. The embedding capacity and the PSNR values clearly show the uniqueness of our proposed method.

Shivani Gupta, Several developments in the transfer of data through the internet make it easier to transfer the data faster and accurately to the destination. But in this, anyone can misuse and modify the critical information through hacking. Video steganography is a technique which is used to hide the message and to transfer the message inside a video. Video is an application of many frames of audio, text, and images. The segmentation is known as the advanced technology that provides rich information of an image. The purpose of this paper is to propose a new technique to hide the data using video steganography with the help of artificial intelligence and DWT. This paper focuses on analyzing the various video steganography techniques which were proposed for securing the data transmission. In this paper, artificial intelligence is applied in order to improve the integrity and security of data transfer. The performance of the proposed method is evaluated on the basis of Bit error, mean square error, and PSNR metrics.

Arshiya Sajid Ansari, Steganography is the technique for exchanging concealed secret information in a way to avoid suspicion. The aim of Steganography is to transfer secrete message to another party by hiding the data in a cover object, so that the imposter who monitors the traffic should not distinguish between genuine secret message

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

and the cover object. This paper presents the comparative study and performance analysis of different image Steganography methods using various types of cover media ((like BMP/JPEG/PNG etc.) with the discussion of their file formats. We also discuss the embedding domains along with a discussion on salient technical properties, applications, limitations, and Steganalysis.

3. PROPOSED METHODOLOGY

The proposed system algorithm is as below

Algorithm to embed the image message into video

Step 1: Select the video file and extract the frames from video
Step 2: Select the image which is to be hidden.
Step 3: Encrypt the selected image.
Step 4: Convert the video frame into equivalent image.
Step 5: Convert the input image to be hidden into its equivalent binary form.
Step 6: Cover Adjustment Before the embedding process takes place it is necessary to apply a pre-processing step

On the cover image. This is a very important step to preserve the overall invert ability of the transform. That is, the embedding process may modify a coefficient that corresponds to a saturated pixel color component in such a way that makes it exceed its maximum value. In this case higher values will be clipped and the embedded message bits would then be lost. Hence, the original cover pixels components (H (i, j, k)) are adjusted according to the formula shown below. It contains the number of bits to be embedded in each coefficient. This adjustment guarantees that the reconstructed pixels from the embedded coefficients would not exceed the maximum value and hence the message will be recovered correctly. Set probability for each region. Probability is like a threshold values. The probability Ps the region contains exactly S pixels. Ps changes from time to time as follows: The values of emigration and immigration rates are given $\lambda = I\ (1\text{-}K/n)$ $\mu=E/n$ Where I is the maximum possible immigration rate; E is the maximum possible emigration rate; k is the number of species of the k-th individual; n is the maximum number of species.

Step 7 : After the pixel and region placement, DWT transform are take place. The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. This transform decomposes the signal into mutually orthogonal set of wavelets. In this transform two scaling are defined - smoothing and non-smoothing one are constructed from the wavelet coefficients and those filters are recurrently used to obtain data for all the scales. If the total number of data D=2^N is used and signal length is L, first D/2 data at scale L/2^(N-1) are computed, than (D/2)/2 data at scale L/2^(N-2), ... etc up to finally obtaining 2 data at scale L/2. The result of this algorithm is an array of the same length as the input one, where the data are usually sorted from the largest scales to the smallest ones.

Step 8: The Embedding Process: Next, step is the embedding process of the proposed algorithm. Of course, it will convert the secret message into a 1D bit stream. The details of this step will depend on the particular message type. The next step that follows the cover adjustment is concerned with applying biogeography Based optimization (BBO) on the cover image. The embedding process stores (N) message bits in the least significant bits (LSB) of the cover image. After the embedding process ends the watermarked image is produced by applying the optimization technique.

Step 9: The Extraction Module The extraction process reverses the embedding operation starting from applying the BBO and dwt on each color plane of the watermarked image, then selecting the embedded coefficients, until extracting the embedded message bits from the N LSB's of the integer coefficients. Furthermore, the extracted bits are converted into its original digital form.

Step 10: End.
To extract the message from the embedded video reverse operation is to be performed.

4. RESULTS AND DISCUSSION

The proposed system is evaluated on various input data and performance of the proposed system is compared with that of existing systems. The proposed system is evaluated on the filllowing parameters:

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

- ***Mean Square Error (MSE)***: It is the calculation of averages of squares of errors. It is mainly a difference between the proposed and existing values of the images on the basis of average squared error. Formula to calculate MSE can be described as below:

$$\text{MSE}=\frac{\sum_{i=1}^{m}+\sum_{j=1}^{n}+\sum_{k=1}^{h}[C(i,j,k)-S(i,j,k)]^{\wedge}2}{m*n*h}$$

Here $C(i,j,k)$ represent original file and $S(i,j,k)$ represent stego file

- ***Peak Signal to Noise Ratio (PSNR)*** is used to calculate the similarity between the actual image values and the values changed after embedding the data into that image. It is the inversely proportional to the MSE. It can be calculated as follow:

$$\text{PSNR}=10*log10\frac{Max^{\wedge}2}{MSE}*\text{db}$$

Table : Statistics of the proposed system

Cover video	**Input image**	**PSNR**	**MSE**	**Original video size**	**Compressed video**	**RLE Compression**
Video1	Input 1	68.0175	0.0103	41472000	26956800	19139328
Video2	Input 2	63.3969	0.0297	13432320	8731008	6199016
Video3	Input 3	62.7810	0.0109	87091200	56609280	40192588
Video4	Input 4	67.7435	0.0335	69350400	45077760	32005209

Table 5.2 Comparison of proposed system with the existing on the basis of the PSNR

Cover video	**PSNR in Existing technique**	**PSNR in Proposed technique**	**Improvement**
Video1	64.6984	69.1267	4.63
Video2	62.8136	67.2269	4.41
Video3	61.81	72.7110	10.90
Video4	65.18712	71.4371	6.25

The table given above shows the PSNR comparison of the proposed method with that of previous work and it is shown the Parameter values for the PSNR shown better for the proposed system on the same type of data given.

Table 5.3 Comparison of proposed system with the existing on the basis of the MSE

Cover video	**MSE in Existing technique**	**MSE in Proposed technique**	**Improvement**
Video1	0.0109	0.0101	0.0008
Video2	0.0342	0.0125	0.0217
Video3	0.0169	0.0081	0.0088
Video4	0.0431	0.0164	0.0267

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

After embedding the message stego video is compressed and the size of file before compression and after compression is compared below:-

Table 5.4 Comparison of size of file on the basis of compression

Cover Video	Size of video before compression	Size of video after compression	Compression using Huffman
Video1	41472000	26956800	18123328
Video2	13432320	8731008	4851427
Video3	87091200	56609280	40172259
Video4	69350400	45077760	221044128

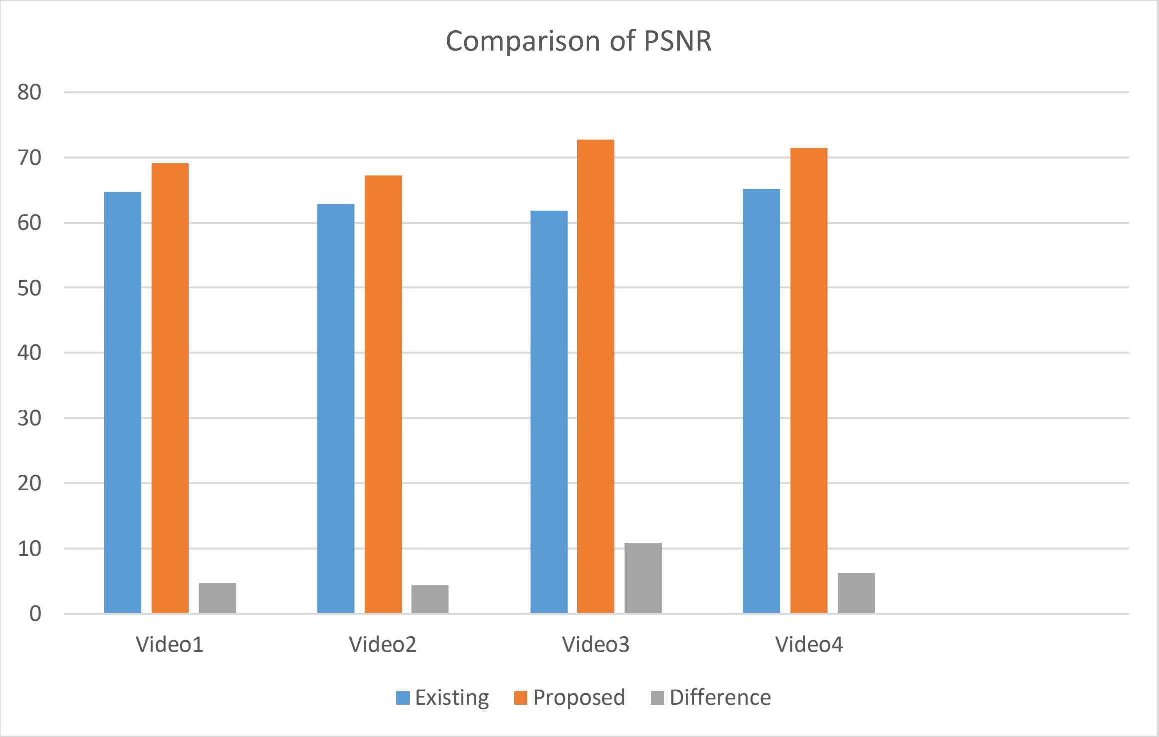

Figure 5.1 Comparison of PSNR

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

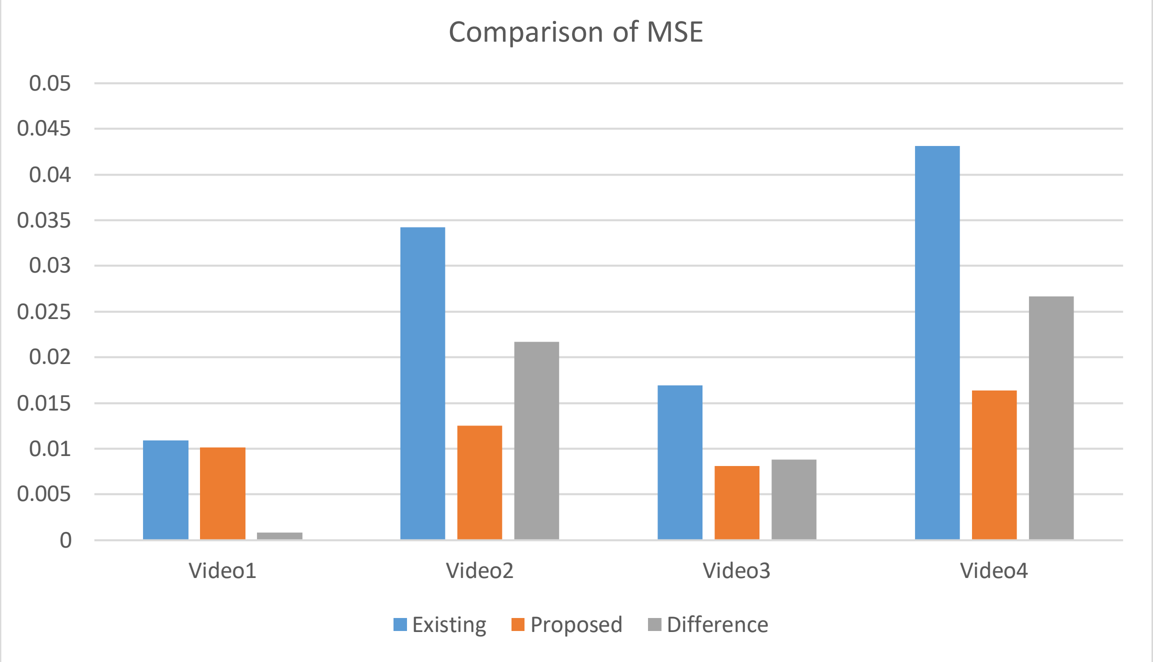

Figure 5.2 Comparison of MSE

5. CONCLUSION AND FUTURE SCOPE

Conclusion

Proposed system use LSB technique for hiding the image into video file in that frame which has highest motion. DWT technique is used to hide the data into image file in which maximum motion is detected. Huffman coding is also used to compress the image file to a great extent. Experimental results shows that the proposed system gives better results as compared to the existing system.

Future Scope

In future, more robust algorithm can be used to hide the image into video frames using multiple number generated series. Multiple compression techniques can also be used to compress the data to be hidden in the video file.

REFERENCES

[1] Amritpal Singh, Harpal Singh "An Improved LSB based Image Steganography Technique for RGB Images", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT),March 2015.

[2] Achmad Solichin and Painem "Motion-based Less Significant Frame for Improving LSB-based Video Stegnography",International Seminar on Application for Technology of Information and Communication(ISemantic), Semarang, 2016, pp. 179-183.

[3] Anush Kolakalur, Ioannis Kagalidis, and Branislav Vuksanovic"Wavelet Based Color Video Steganography", International Journal of Engineering and Technology(IACSIT), Vol. 8, No. 3, March 2016.

[4] Dipak A. Mashe "Data hiding in motion vectorss of compressed video"International Advanced Research Journal in Science, Engineering and Technology Vol. 3, Issue 4, April 2016.

[5] K.Rosemary Euphrasi, M. Mary Shanthi Rani, "A Comparative Study On Video Steganography in Spatial and IWT Domain", IEEE International Conference on Advances in Computer Applications (ICACA),Oct2016.

[6] K. Steffy Jenifer , G. Yogaraj , K. Rajalakshmi "LSB Approach for Video Steganography to Embed Images", International Journal of Computer Science and Information Technologies, (IJCSIT), Vol. 5 (1) , 2014, 319-32.

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.

[7] Kousik Dasgupta, J.K. Mandal and Paramartha Dutta,"HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY(HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.

[8] K.Vidyavathi, Dr.R.S.Sabeenian, " Estimation and Compensation of Video Motion - A Review" Journal of Convergence Information Technology (JCIT),Volume 9, Number 6, November 2014.

[9] Ms.Pooja Vilas Shinde,Dr.Tasneem Bano Rehman, "A Survey: Video Steganography techniques"International Journal of Engineering Research and General Science ,Volume 3, Issue 3, May-June, 2015
ISSN 2091-2730.

[10] Paramjit kaur,Vijay laxmi, "An Upgraded approach for robust Video Watermarking Technique Using Stephens Algorithm",International Journal of Computer Science and Mobile Computing" Vol.3,Issue.11,Nov 2014,pg. 612-622.

[11] Paramjit kaur,Vijay laxmi, "Review on different video watermarking techniques",International Journal of Computer Science and Mobile Computing" Vol.3,Issue. 9,Sept. 2014,pg. 190-195

[12] Ramadhan J. Mstafa,Khaled M.Elleithey and Eman Abdelfattah "Video Steganography Techniques: Taxonomy, Challenges, and future directions",IEEE Long Island Systems, Applications and Technology Conference (LISAT), May 2017.

[13] Ramadhan J. Mstafa, Khaled M. Elleithy,Eman Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC", IEEE(2017).

[14] Ramadhan J. Mstafa, Khaled M. Elleithy,Eman Abdelfattah, "A New Video Steganography Algorithm Based on Multiple Object Tracking and Hamming Code", 14th International Conference on Machine Learning and Applications,IEEE(2015).

[15] Ramandeep Kaur,Pooja,Varsha, "A Hybrid Approach for Video Steganography using Edge Detection and Identical Match Techniques" IEEE International Conference on Wireless Communications Signal Processing and Networking (WISPNET-2016).

[16] Saravanan Chandran, Koushik Bhattacharyya, "Performance Analysis of LSB, DCT, and DWT forDigital Watermarking Application using Steganography",International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO) - 2015

[17] Sheng Dun Hu, KinTak U, "A Novel Video Steganography based on Non-uniform Rectangular Partition" 14thIEEE International Conference on Computational Science and Engineering CSE/I-SPAN,2011.

[18] Swetha V,Prajith V,Kshema V , "Data Hiding Using Video Steganography- A Survey" IJCSET, June 2015 Vol 5, Issue 6,206-213.

[19] Venkat P. Patil, Umakant Bhaskar Gohatre, R.B. Sonawane,"An Enhancing PSNR, Payload Capacity and Security of Image using Bits Difference Base on Most Significant Bit Techniques", International Journal of Advanced Electronics & Communication Systems,21 March, 2017.

[20] Xijian Ping, Changyong Xu, Tao Zhang , "Steganography in Compressed Video Stream**",**International Conference on Innovative Computing, Information and Control (ICICIC'06) ,IEEE 2006.

[21] Afsha Shaukat,Mahesh Chaurasia,Prof. Goutam Sanyal,"A Novel Image Steganographic Technique using Fast Fourier Transform",2016 Fifth International Conference On Recent Trends In Information Technology

[22] Shivani Gupta, Gargi Kalia, Preeti Sondhi,"Video Steganography Using Discrete Wavelet Transform and Artificial Intelligence", International Journal of Trend in Scientific Research and Development (IJTSRD) Volume: 3 | Issue: 4 | May-Jun 2019

[23] Arshiya Sajid Ansari,Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez,"A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", I. J. Computer Network and Information Security, 2019, 1, 11-25.

[24] Pooja Dixit, Munesh Chandra Trivedi, Avdhesh Kumar Gupta, Virendra Kumar Yadav, Vineet Kumar Singh,"Video Steganography using Concept of DNA Sequence and Index Compression Technique", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958, Volume-8 Issue-5, June 2019

[25] Bharti Chandel, Dr.Shaily Jain,"Video Steganography: A Survey",IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 11-17

[26] Angitha John, Anjana Baby,"A Survey on Video Steganography",International Journal of Science and Research (IJSR) ISSN: 2319-7064 ResearchGate Impact Factor (2018).

IJESRT is licensed under a Creative Commons Attribution 4.0 International License.