INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 1)
Available online at: www.ijariit.com

Hiding secret image data into video files using 3- LSB technique

Harinderjot Singh
rubydhillon20@icloud.com
Adesh College of Engineering and Technology, Faridkot, Punjab

ABSTRACT

Steganography is a process to hide the secret message which we want to hide from the outside world in another media file while the cryptography is another security process in which a data form is changed to another so that it cannot be accessed directly. In the proposed work, 3-Least Significant Bit (3-LSB) will be used to hide the image message into a video. In the Proposed algorithm from the input video, a frame with maximum motion detection and high intensity of a pixel is extracted using threshold value .60 to calculate the highest value of pixels which is treated as the target frame for hiding message. This target frame image will hide using Least Significant approach. The resultant video becomes the stegno video. The reverse process is performed on the stegno video to extract the image file from that video file. The proposed system is tested on various input videos and various input images are used as a message to hide in these videos. Performance of the proposed system is also compared with the performance of the existing system and it is evaluated that the proposed system generates better results in terms of PSNR, MSE and Hiding Capacity than that of the existing system.

Keywords— *Video steganography, Least significant bit technique, Maximum motion detection*

1. INTRODUCTION

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 the form of media files that contains text, audio, and video. To transfer these media file online, there is a need to design some secure application such that unauthorized person can't access the confidential information. The solution for security-related issues lies in security techniques that are Cryptography and Steganography.

Steganography is a mix of 2 Greek words "steganos" that intends to hide, hide or guarantee and "graphein" signifies to compose [4]. Steganography is a system to cover the info in another host object. it's been utilized since archaic time by the final population. In archaic time, mystery information is roofed up within the back of wax, the scalp of the slaves, in hares then forth [5].

2. VIDEO STEGANOGRAPHY

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

Different types of steganography techniques are Linguistic, Image, Audio, Video and Network Steganography commonly used. Among this video, steganography is more reliable as a video is the collection of pictures and audio signals. A video file contains many redundant bits and messages can be easily embedded in repeating a portion of a 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 displayed on the screen at a very fast rate. Different existing techniques of image and audio steganography are also applied to video Steganography. The steganography model consists of carrier video or cover object which is the carrier for a secret message; a secret image is a secret file that is embedded and stego key for encoding and decoding. It can be described as a collection of Cover object, hidden data, stego key that creates a stego model.

2.1 Characteristics of Video Steganography

The characteristics that must be followed by effective steganography technique are:

(a) Secrecy: An unauthorized person cannot extract hidden information from the video.
(b) Undetectable: The viewer cannot even sense the presence of a secret message. No algorithm exist that identify whether a video contains a hidden message
(c) Capacity: It can be defined by the total amount of the data that can be hidden in the image file.
(d) Accuracy: It is defined as the system that is said to be accurate if the data retracted is accurate and reliable.

3. LITERATURE SURVEY

Ramadhan J. Mstafa et al. (2017) proposed robust and secure video steganography based on a motion-based method in the DWT-DCT domain. In this paper the steganography model has three stages, The first phase is motion-based multiple object tracking in which movement of each object is detected using Gaussian Mixture Model, second is data embedding stage in which Discrete Cosine Transformation (DCT) and Discrete

Wavelet Transformation (DWT) method is used and third is data extraction stage. Hamming code and BCH code are also used to decrypt data. The main emphasis is given to embedding efficiency, hiding capacity and robustness. Different noise is added to test the visual quality and bit error rate for the proposed algorithm. The PSNR value of the proposed algorithm is 49.01 dB and the Hiding Ratio (HR) is 3.40% [13].

Vanket P. Patil et al. (2017) represent the Most Significant Bit technique to enhance PSNR, payload capacity and security of image. In MSB, the most significant bits of the original image are used to hide information. The secret message is embedded into the 5th and 6th bit of cover image. The encoding algorithm calculates the difference between the 5th and 6th bit and compares it to the secret data bit. If the difference is not equal to data bit, it transverse the 5th bit to make them equal. Data bits of the original image remain the same in the encoding and decoding process. The comparison is done with existing techniques to enhance the PSNR value which provides better payload capacity than existing LSB based techniques. In this paper, the PSNR value for a color image is 52.68 and the payload capacity is 786432 bits of transmitting [18].

Ramadhan J. Mstafa et al. (2017) provides a review of various video steganography techniques. In this paper, video steganography techniques are classified into a raw domain and compressed domain. In a compressed domain, a video is divided into a different frame that is I-frame, P-frame, and B-frame. Different prediction techniques are used for motion estimation. In the raw domain, each video is first to transform into the frame as still images and then each frame is used to hide the secret message. Video steganography techniques in a raw domain are further classified into spatial domain and transform domain. In spatial domain LSB, ROI and BPCS techniques are used. In the transform domain, DCT, DWT and DFT techniques are discussed. A complete analysis based upon embedding capacity, video quality and robustness of all existing techniques are also represented in this paper [12].

K. Rosemary Euphrasi et al. (2016) represent the comprehensive approach based on spatial domain and IWT domain. The authors represent steganography to embed and extract secret data in the cover video. In the spatial domain, the Random LSB substitution method is used in which secret data is randomly distributed into red, green and blue channels. In the transform domain, Haar Wavelet transforms technique is used to encode data that divides the frequency domain into four sub-bands namely AC, HC, VC, and DC. The approximate value is calculated with the help of AC and detail coefficients are including the remaining three bands. The decoding process applies the inverse integer wavelet technique (IIWT) which provides more security. In this paper, the algorithm is implemented using the avi video file with PSNR, MSE, and BER as performance parameters. The data is embedded in the frequency domain and hiding capacity can be improved in the future using Region of Interest (ROI) [5].

3.1 Research Gap

Existing systems for Steganography can hide very limited data which can be termed as less than 10% as they use only some special part to replace the bits of the secret data. Existing techniques do not provide an effective mechanism to support all formats (avi, mov., mpeg, etc) as the cover file. In video data hiding techniques, various other technologies such as compression, decompression and cryptography, and random data sampling techniques

4. PROPOSED METHODOLOGY

A secure method of video steganography using LSB based on the motion detection technique is presented. Motion estimation as important which calculates the motion between adjacent frames. Each frame is essentially divided into macro-blocks and sub-blocks.
image file.

Steps for 3-LSB Algorithm:

a. Input video the file and convert it into the frames and then extract the bit patterns.
b. Convert every character of the secret message into the bit pattern.
c. Re-write the last bit of the image file with every single bit up to three bits of the input secret message.

Fibonacci Technique: Apart from the LSB method the Fibonacci method provides a kind of encryption. Fibonacci numbers are defined by the linear recurrence relation

$$F_n = F_{n-1} + F_{n-2},\ n \in \mathbb{N},\ n > 1, \text{ with } F_0 = 0,\ F_1 = 1,$$

According to the LSB scheme, one bit is embedded in each pixel color of the image. To increase the amount of data, we could embed more bits in more, higher bit planes, the Fibonacci method introduces a new encoding of the pixel value which increases the number of available bit planes.

Maximum Motion Detection: in the proposed system we use the maximum motion and high intensity of pixel to hide the image into the video frame. We have calculated the motion between the consecutive frames and find the frame have maximum motion and hide the image in that frame. To detect a motion a block matching algorithm is used which estimates the motion between different frames by dividing each frame into the number of sub-block of a pixel. The matching is done with the help of a reference frame and the current frame. The motion estimation includes the following steps:
Step1: Each frame is divided into sub-blocks based upon the values entered by the user in terms of Block size [height width] and Overlap [r c] parameters.
Step 2: Calculate the motion vector of consecutive frames that return the Maximum displacement [r c] parameter.

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 the equivalent image.
Step 5: Convert the input image to be hidden into its equivalent binary form.
Step 6: Calculate LSB of each color of each pixel of the video frame which has maximum motion in the consecutive frames and all pixel colors according to Fibonacci numbers.
Step 7: Replace LSBs of video Frames with every last bit of the message to be hidden.
Step 8: Compress the stego video using the SPIHT technique along with the RLE compression technique.
Step 9: End.

Algorithm to extract the image message from a video

Step 1: Read the stegno video frame i.e. the image in which the message is hidden.
Step 2: Calculate the LSB of the video frame based on maximum motion.
Step 3: Extract the video frame which has maximum motion in the consecutive frames and pixels numbers matching with Fibonacci numbers.

Step 4: Add the LSB of each color of each pixel of the stegno frame in the final message.

Step 5: Convert the extracted binary message into a text message.

Step 6: Display the message to the user.

Step 7: End.

5. RESULTS AND DISCUSSION

The proposed system hides the image in video frames. Video is a collection of frames that contains multiple redundancies that provide high security to transfer data from one location to another. Video steganography gives emphasis on hiding the data in such a way so that it cannot be even detected by naked eyes. The unauthorized person may conceal data that is travel from one location to another location. A secure method is needed for safe information from unauthorized persons.

Steganography techniques allow concealing the secret data into the covered video file, hence after hiding the message into the video file, the quality of the file may get changed. To check whether the output file can be used for the other system, it can be evaluated with the help of the following parameters:

- ***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 based on average squared error. Formula to calculate MSE can be described as below:

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

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 inversely proportional to the MSE. It can be calculated as follow:

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

Table 1: 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 2: Comparison of the 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	68.0175	3.3191
Video2	62.8136	63.3969	0.5833
Video3	61.81	62.7810	0.971
Video4	65.18712	67.7435	2.5563

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 3: Comparison of the 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	0.0103	0.0006
Video2	0.0342	0.0297	0.0045
Video3	0.0169	0.0109	0.006
Video4	0.0431	0.0335	0.0096

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

Table 4: Comparison of size of a file on the basis of compression

Cover Video	Size of video before compression	Size of the video after compression	Compression using RLE
Video1	41472000	26956800	19139328
Video2	13432320	8731008	6199016
Video3	87091200	56609280	40192588
Video4	69350400	45077760	32005209

6. CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In the proposed work, enhanced Least Significant Bit (LSB) will be used to hide the image message into a video. In the Proposed algorithm from the input video, a frame with maximum motion detection and high intensity of the pixel is extracted using threshold value .60 to calculate the highest value of pixels which is treated as the target frame for hiding message. In this target frame image will hide using an enhanced Least Significant approach. The resultant video becomes the stegno video. The reverse process is performed on the stegno video to extract the image file from that video file. The proposed system is tested on various input videos and various input images are used as a message to hide in these videos. Performance of the proposed system is also compared with the performance of the existing system and it is evaluated that the proposed system generates better results in terms of PSNR, MSE and Hiding Capacity than that of the existing system.

6.2 Future Scope

In the future, the system can be extended to hide the image into more than one frame by dividing the input image to hidden into various parts to provide more security.

7. 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 Steganography", 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 vectors 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.*

[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 for digital 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" 14th*IEEE 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] Xingjian Ping, Changyong Xu, Tao Zhang, "Steganography in Compressed Video Stream**",** *International Conference on Innovative Computing, Information and Control (ICICIC'06), IEEE 2006.*

