IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.6, Issue.10, Oct. 2018 E-ISSN: 2347-2693

A SECURE VIDEO STEGANOGRAPHY TECHNIQUE BASED ON MOTION DETECTION

Karamjit Kaur[1*] , Vijay Laxmi[2]

[1,2]University College of Computer Application Guru Kashi University, Talwandi Sabo, Punjab, India

[*]*Corresponding Author: karmnsidhu@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 20/Oct/2018, Published: 31/Oct/2018

***Abstract*—** Steganography is a sort of cryptography in which the mystery message is covered up in an advanced picture. While cryptography is engrossed with the security of the substance of a message or data, Steganography focuses on hiding the specific presence of such messages from recognition. In the proposed system, maximum motion and high intensity between every consecutive frame is evaluated. The frame must be found in which maximum motion and intensity is there and this frame is marked as the target frame. This technique provides a large amount of security to the stego video as it is very difficult for the attacker to guess or find the target frame in which secret message is hidden. The proposed system hides the image in video frames that is indistinguishable. Video is collection of frames that contains multiple redundancies which 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 to safe information from unauthorized person. In the proposed work, Least Significant Bit (LSB) along with motion estimation is used to hide the message into a video in such way that does not raise suspicion. The proposed system generates the better results in terms of PSNR, MSE as compared to existing system.

***Keywords*—** Video Stegnography, Data hiding, Securing Data, LSB Technique, Maximum motion stegnography technique.

I. 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 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 unauthorized person can't access the confidential information. The solution for security related issues lies in security techniques that are Cryptography and Steganography.

Cryptography is a technique in which message is encoded in some secret form so that one can't read original information that is sent from one location to another. In cryptography, the encrypted message is directly shown to unauthorized person but he can't convert it into readable form.

Steganography is combination of two Greek words "steganos" which means to cover, conceal or protect and "graphein" means to write [4]. Steganography is technique to conceal the information in some other host object. It has been used since ancient time by the people. In ancient time, secret information is hidden in the back of wax, scalp of the slaves, in rabbits etc [5].

Both Steganography and Cryptography techniques are used to keep the information secret from unauthorized person, but they different in way to represent the secret data. In cryptography the person who wants to hack information can sense that there is secret code carries through the internet .On the other hand, in steganography hacker does not even scene there is secret message hidden in the carrier object that is transferred from one location to another. In steganography only the sender and intended recipients knows about the message that is hidden in an innocent cover file in such a way nobody can imagine that there is secret information inside the cover file.

Another technique that is based on both steganography and cryptography is Watermarking. Watermarking is the process of protecting the copyright of original data by identifying the unauthorized person [13].It provides more security to transfer confidential information through internet.

A. Types of Video Steganography

Steganography can be classified into different categories, which are mentioned as:-

1) 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.

2) Audio Steganography

In Audio steganography model the secret message is embedded in audio waves. Audio steganography methods can embed messages in WAV, and even MP3 sound file. In audio steganography, the secret message is embedded in the form of noise of high frequency that carries along with audio signals. Audio signals used as covert medium for communication as they are unpredictable in nature.

3) Image Steganography

It includes image files as hosts for steganography messages takes advantage of the limited capabilities of the human visual system. Image Steganography comprises list of techniques both in spatial domain and temporal domain which embed secret message under the pixel of image. All spatial domain technique directly changes the bits of image pixels and hides secret information and temporal domain techniques transform the pixel into frequency domain o hide data.

B. Video Steganography System

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 steganography 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 and stego key that creates a stego model.

1) Characteristics of Video Steganography

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

- **Secrecy:** Video steganography technique must be secure enough such that unauthorized person cannot extract hidden information from the video.
- ***Undetectable*:** The viewer cannot even sense the presence of secret message. There is no such algorithm exists that identify whether a video contains a hidden message or not.
- ***Capacity*:** The maximum amount of the hidden message that can be embedded in a video.
- ***Accuracy*:** The extraction of the hidden data from the medium should be accurate and reliable.

II. RELATED WORK

Ramadhan J. Mstafa et al. (2017) proposed a robust and secure video steganography based on motion based method in 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 proposed algorithm. The PSNR value of proposed algorithm is 49.01 dB and Hiding Ratio (HR) is 3.40% [16].

Vanket P. Patil et al. (2017) represents Most Significant Bit technique to enhance PSNR, payload capacity and security of image .In MSB, the most significant bits of original image are used to hide information. The secret message is embedded into 5th and 6th bit of cover image. The encoding algorithm calculates difference between 5th and 6th bit and compare it to secret data bit. If difference is not equal to data bit it transverse 5th bit to make them equal. Data bits of original image remain same in encoding and decoding process. The comparison is done with existing techniques to enhance the PSNR value which provide better payload capacity than existing LSB based techniques. In this paper the PSNR value for color image is 52.68 and payload capacity is 786432 bits of transmitting [23].

Ramadhan J. Mstafa et al. (2017) provide a review on various video steganography techniques. In this paper, video steganography techniques are classified into raw domain and compressed domain. In compressed domain, a video is divided into different frame that are I-frame, P-frame and B-frame. Different prediction techniques are used for motion estimation. In raw domain each video is first transform into frame as still images and then each frame is used to hide secret message. Video steganography techniques in raw domain are further classified into spatial domain and transform domain. In spatial domain LSB, ROI and BPCS techniques are used. In transform domain, DCT, DWT and

DFT techniques are discussed. A complete analysis based upon embedding capacity, video quality and robustness of all existing techniques is also represented in this paper [15].
Achmad Solichin et al. (2016) represent Least Significant Frame method in which a frame is used to embed secret data based on optical flow. In this method, movement of the object is calculated with the help of optical flow which measure between bits or pixel. The Horn-Schuunk method obtains the value of optical flow which find component horizontally or vertically. When there is significant movement in the video, the pixel value changes that is more difficult to detect that there is secret data included. It provides more protection and security to embedded message than existing techniques. More improvement is needed in future to improve the robustness of stego video [2].

Kasra Rezagholipour et al. (2016) proposed a video steganography algorithm based on motion vector of moving object which calculate motion vector of moving object. In proposed algorithm, mean shift method of motion detection is used which perform both background and foreground detection of objects. A video is decomposed into number of frames and object tracking is done in each frame by converting it into binary image. Mean shift algorithm consider adjacent frames and perform background subtraction to search matching area and also noise elimination is done to provide more accurate results. To check association of object between adjacent frames threshold value is checked against the matching criteria and if object is not matched with current frames then its ID must erased. Capacity of hidden information and video quality also improved in proposed method [6].

Amritpal Singh et al. (2015) provide an improved LSB based image steganography technique for RGB images to improve the image quality. In this paper bit plane slicing scheme is used to convert he image into red green and blue plane. This technique does not affect visual quality of an image and introduce minimum noise in stego image. In this paper human visual system is defined according to perception of human eye to different colors and required light energy for each red, green and blue pixels. In this paper the wavelength of different colors according to human eye is also represented .To embed the 8 bit message with the original image, 2 bits of red plane, 2bits of green and 4 bits of blue plane is used. The value of PSNR obtained in proposed technique is 47.5897 and MSE is 0.1654 [1].

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 cover video. In spatial domain Random LSB substitution method is used in which secret data is randomly distributed into red, green and blue channels. In transform domain, Haar Wavelet transforms technique is used to encode data which divide 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 remaining three bands. The decoding process applies inverse integer wavelet technique (IIWT) which provides more security. In this paper, the algorithm is implementing using AVI video file with PSNR, MSE and BER as performance parameters. The data is embedded in frequency domain and hiding capacity can be improved in future using Region of Interest (ROI) [7].

III. METHODOLOGY

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

LSB CODING: - Least significant bit (LSB) coding is the simplest way to embed information in a digital video file. LSB coding allows for a large amount of data to be encoded. [16]

Standard LSB ALGORITHM:
It performs bit level manipulation to encode the message. The following steps are:
a. Receives the video file in the form of bytes and converted in to bit pattern.
b. Each bit of video is converted into bit pattern.
c. Replaces the LSB bit from video with LSB bit from image.

Fibonacci Technique: Apart from the LSB method the Fibonacci method provide a kind of encryption. Fibonacci numbers are defined by the linear recurrence relation
$Fn = Fn-1 + Fn-2$, $n \in N$, $n > 1$, with $F0 = 0$, $F1 = 1$
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 video frame. We have calculated the motion between consecutive frame 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 motion between different frames by dividing each frame into number of sub block of pixel. The matching is done with the help of reference frame and current frame. The motion estimation include following steps:
Step1: Each frame is divided into sub blocks based upon the values entered by the user in term of Block size [height width] and Overlap [r c] parameters.

Step 2: Calculate the motion vector of consecutive frames which return Maximum displacement [r c] parameter.
Step 3: Search a new block location by predicted a motion of reference frame and current frame.

A. Video Embedding Phase

The embedding process starts by select the video in which we want to embed the secret message .Video that we are select to embed secret data is known as cover video or cover object which carries secret message from sender to receiver. After this, we select the secret image which is an image that covered into a video. After embedding, the video is reshaped with secret image .The video that obtain secret message is called stego video. The stego video is saved on disk.

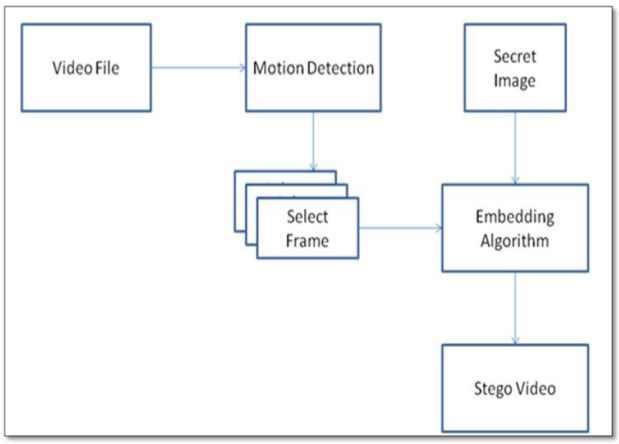

Figure1. Block Diagram of Embedding Phase

B. Data Extraction Phase

Data extraction is practice of retrieve the secret message from the stego videos. This process is achieved by converting the distorted videos into frames. This process is achieved by converting the distorted videos into frames. At the receiver side, the stego video will be selected.

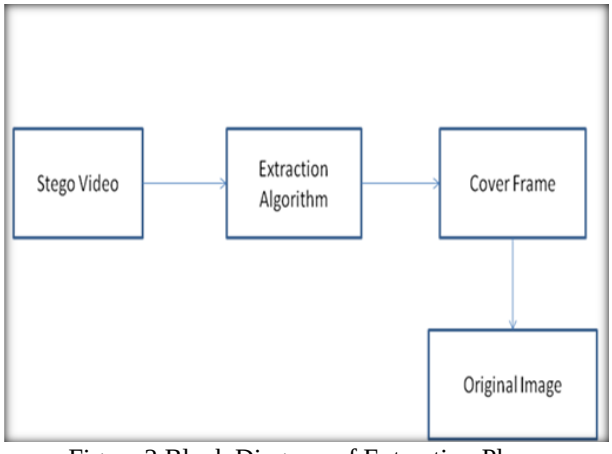

Figure 2 Block Diagram of Extraction Phase

IV. Results and Discussion

The proposed system hides the image in video frames. Video is collection of frames that contains multiple redundancies which 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 to safe information from unauthorized person.

1)*Evaluation Parameter:* Steganography techniques allow concealing the secret information inside the cover video data, thus the quality of the cover data will be changed. In order to evaluate whether the distortion level is acceptable or not, different Parameters has been used:

a) ***Mean Square Error (MSE)***: MSE measures the average of the squares of the errors. The average squared difference between an original image and resultant (stego) image is called Mean Squared Error.

b) ***Peak Signal to Noise Ratio (PSNR)*** is a common used to calculate the difference between the carrier and stego data. The *PSNR* is the ratio between the maximum possible power of a signal and the power of corrupting noise. PSNR is usually expressed in terms of the logarithmic decibel scale.

The result of proposed technology based upon the PSNR and MSE is compared with Achmad [2] that use different frames based upon the optical flow method and movement of the object is calculated with the help of optical flow which measure movement between bits or pixel. To test the proposed system with existing system, standard videos like rhinos, traffic and ball having different resolution are used as input. The algorithm that is proposed provides better performance in terms of PSNR and MSE as compared in existing system [2]

Table1 Comparison of proposed system with the existing on the basis of the PSNR

Cover video	PSNR in Existing technique	PSNR in Proposed technique	Improvement (%)
Video2	64.1656	71.3561	7.1905
Rhinos	62.3298	70.6999	8.3701
TrafficVideo	62.5482	70.4967	7.9485
Shuttle	65.1506	72.2969	7.1463
Ball	62.2357	69.6534	7.4177

The above table represents the comparison of the existing and proposed system on the basis of PSNR parameter. It is shown that the PSNR of the proposed system gives better results than that of the existing system on the same type of the data given.

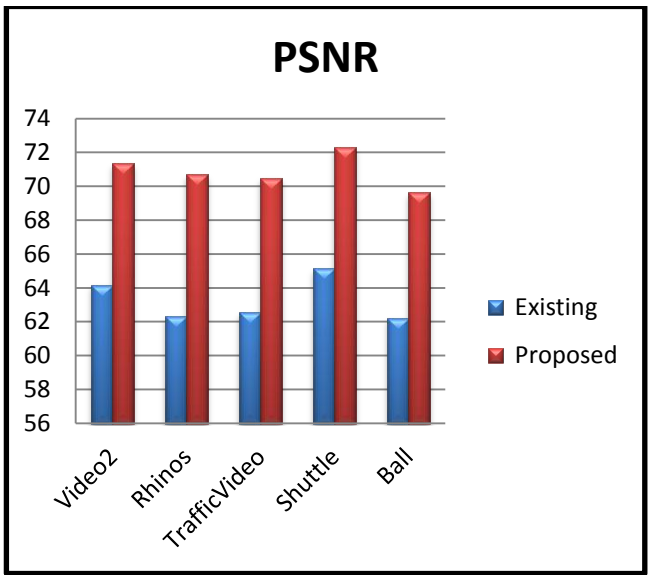

Figure3. Comparison of Proposed system and existing on the basis of PSNR.

Table 2 Comparison of proposed system with the existing on the basis of the MSE

Cover video	MSE in Existing technique	MSE Proposed technique	Improvement (%)
Video2	0.0057	0.0048	0.0009
Rhinos	0.006	0.005	0.001
TrafficVideo	0.0068	0.0057	0.0011
Shuttle	0.0046	0.0038	0.0008
Ball	0.006	0.005	0.001

The table represents the comparison of the existing and proposed system on the basis of MSE parameter. It is shown that the MSE of the proposed system is less than that of the existing system on the same type of the data given.

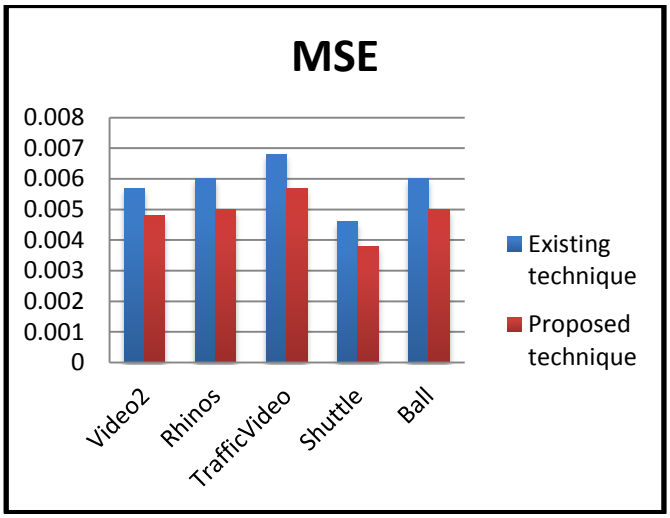

Figure 4.Comparison of existing and proposed system on the basis of MSE.

V. CONCLUSION AND FUTURE SCOPE

A. CONCLUSION

In the proposed work, Least Significant Bit (LSB) is used to hide the image message into a video. In Proposed algorithm from the input video a frame with maximum motion detection and high intensity of pixel is extracted. To calculate the highest value of pixels this is treated as the target frame for hiding message. In this target frame image will hide using Least Significant approach. The resultant video becomes the stego video. Reverse process is performed on the stego 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 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 the better results in terms of PSNR and MSE than that of existing system. Least significant bit technique is user friendly and one can embed more information but secret information can be detected if anyone knows about presence of message.

B. FUTURE SCOPE

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

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] Hitendra Donga, Kishor Atkotiya, "STEGO: A Tool for Implementing Text-Audio-Video Steganography", International Journal of Computer Sciences and Engineering, Vol.5, Issue.8, pp.159-162, 2017.

[6] Kasra Rezagholipour, Mohammad Eshghi, "Video Steganography Algorithm based on motion vector of moving object", IEEE Eighth International Conference on Information and Knowledge Technology (IKT), Hamedan, Iran 2016.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] Mukesh Dalal, Mamta Juneja, "H.264/AVC Video Steganography Techniques: An Overview", International Journal of Computer Sciences and Engineering, Vol.6, Issue.5, pp.297-303, 2018.

[13] 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.

[14] 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

[15] 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.

[16] 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).

[17] 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).

[18] 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).

[19] R. Shanthakumari and Dr.S. Malliga, " Video Steganography Using LSB Matching Revisited Algorithm", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. IV(Nov – Dec. 2014), PP 01-06.

[20] 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

[21] 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.

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

[23] 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.

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

