Data Hiding using Video Steganography

Prof. Dr. P. R. Deshmukh
Amravati

Bhagyashri Rahangdale
ME Scholar,
Sipna COET,
Amravati,INDIA

***Abstract*— Video Steganography is to hide the existence of the message from unauthorized party using Video as cover file and hiding data in video. Steganography means covered writing it includes process of concealing information within other file and also conceals the fact that a secret message is being sent.In this paper a technique proposed is Hash based least significant bit technique for video steganography.Least Significant Bit insertion method embed data in the lower bits of RGB pixel of video and this changes will be minimal.Data hiding is the process of embedding information in a video without changing its perceptual quality and also keep away from knowledge of existence of message. A hash function is used to select the position of insertion in LSB bits.This technique deals with two terms that are Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE).Its objective is to reduce MSE and increase PSNR.**

Keywords— ***Cover Video, Hash function,LSB,PSNR,Secret message,Video Steganography.***

I. INTRODUCTION

Steganography is the term which is obtained from greek word: "Steganos" means "covered" and "graphia" means "writing" respectively. Today Internet and digital media are very popular, so to prevent secret information from unwanted people,there is requirement to transmit a data more securely. The goal of steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second secret message present. Steganography is a kind of art and science of hiding a secret message inside the other digital files as here we are using video file which are in avi format.The video steganography uses a some frames of Video files to embed the secret message. This steganography hides information in such a way that it appears like that no information is hidden.Whenever any person view that video in which data is hidden but they have no idea that any information will not be decoded by unwanted person.Steganography provide security by obscurity.Video Steganography technique will not only hide data but also hide the presence of data.The data is hidden even from receiver but receiver can decode data as they know the password that is used to embed data. The video file can hide large quantity of information because it carry large number of frames and its storage capacity is also more. Video files are larger than audio and image files, and hide more information. The video steganography involve two steps.The first step deals with embedding secret message in the video files. The second step is the extraction of secret message from video files.This video steganography have more hiding capacity (the amount of information that can be embedded) which is always an important factor when developing a steganographic algorithm.

The second main advantage of hiding data into video file is the added security against the attack of the third party or unintended receiver due to relative complexity of the structure of video as compared to image and audio.In video steganography technique least significant bit is easy method to hide data in video cover file.In this technique from video particular frames selected in which text will embedded or hidded in that frames by using bit of each of the Red, Green and Blue colour components can be used.This technique was to the brings simplicity in LSB insertion technique and also reduces the attacks from third party.The hash based LSB technique is different from LSB technique on basis of hash function as it takes eight bits of secret data at a time and hide them in least significant bit of RGB pixel.The chromatic influence of the blue color is more to the human eye than the red and green color hence 3,3,2 order of distribution takes place.So random distribution of the bits takes place over there.After hiding information in multiple frames of a video file,these frames are combined together to make a stego video and this video look like a normal video. Authorized receiver perform the reverse process to decode the hidden message or data.Stego video will be broken into frames and then using the same password can be applied to retrieve the data. In this paper video steganography using hash based LSB insertion technique is developed in MATLAB.

II. LITERATURE REVIEW

There are various steganographic methods have been proposed in literature.Video file hides a large amount of secret data hence it is more useful. A secured Hash based LSB technique for image steganography has been implemented[1].The basic requirement of hiding a data in cover file will be explained [2].The steganography is art of hiding data within the video file or image file.Steganography is an effective means of protecting the confidentiality of the data.The technique [3] of data hiding for high resolution video is proposed.It provide proper protection on data during transmission.Hiding data using the motion vector technique for the moving objects is introduced in [4]. In this compressed video is used for the data transmission since it can hold large volume of the data.The stego machine to develop a steganographic application to hide data containing text in a computer video file and to retrieve the hidden information is designed[5].This can be designed by embedding message file in a video file in such away that the

video does not loose its functionality using Least Significant Bit modification method.The Steganography is used or secure communication.High Capacity and Security is obtained using Steganography algorithm.

A robust method of imperceptible audio, video, text and image hiding is proposed[6].The motion vector technique is found as the better solution since it hides the data in the moving objects.The most secure and robust algorithm is introduced[7]. Here a more secure and effective hash-based algorithm that uses a pure hash technique for coding and decoding the information in a colour image.An improved LSB(least Significant bit) based Steganography technique for images imparting better information security.It presents an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images[8].

A New Compressed Video Steganographic scheme in which the data is hidden in the horizontal and the vertical components of the motion vectors is proposed[9]. There is system for data hiding uses AES for encryption for generating secret hash function or key[10]. A hash based least significant bit (LSB) technique[11] has been proposed. In which a spatial domain technique where the secret information is embedded in the LSB of the cover frames.

III. PROPOSED TECHNIQUE

Earlier various kinds of steganography techniques are introduced for the video.Here we proposed the Hash Based Least Significant Bit Technique for Video Steganography which perform insertion of bits of text file in video in the least significant bit position of RGB pixel as per hash function.In this way it includes Encoding and Decoding process for hiding message and extracting message respectively.In this technique steganographic tool is developed in MATLAB software which perform Encoding and Decoding.First of all text will be embedded within the video by using the steganographic tool.This stego video file is again applied to steganographic tool to decode embedded data.There is use of following algorithm for data hiding.

A. Hash Function:-Hash function deals with the LSB bit position within the pixel and also with the number of bits of LSB.Hash value takes a variable size of input and returns a fixed size of digital string as output.Here hash function used to find position of insertion of bits in LSB.Hash function given by

$$x = y \% z \quad (1)$$

where, x is LSB bit position within the pixel,y represents the position of each hidden image pixel and z is number of bits of LSB.

B. LSB Insertion:-The least significant bit insertion method is simplest approach for hiding text within an video file.This LSB insertion is a steganographic algorithm that finds the least significant bit in some bytes of the cover file and replace them with a sequence of bits present in the secret data.The hash based LSB technique is different from LSB technique on basis of hash function as the hash function hide eight bits of secret data on a time in a frame.It hides them in LSB positions of RGB pixels of carrier frame.The distribution of bits is taken in order 3,3,2 because the chromatic influence of blue to the human eye is more that red and green pixel respectively ,so the bits are distributed as first 3 bits of the 8 bits secret message into R(red) pixel and other 3 bits of secret message into G (green) pixels and remaining 2 bits are inserted into B (blue) pixel. In the LSB insertion technique,one can take the binary representation of the hidden data and overwrite the LSB of each byte in the video file.

IV. ALGORITHM OF PROPOSED MODEL

The steps of encoding and decoding are explained below.

A. Encoding Process For Hiding Secret Information:-
Input :-Video File,Secret Text
Output:- Stego Video

Steps of encoding process:-

[1] During encoding first text file is selected .
[2] Then video file is selected in which text is to hide .
[3] Frames are separated from video and displayed on cover file.
[4] Split the secret text to insert in video and then it get hidded using least significant bit insertion technique.
[5] Hash code is used to find position for LSB insertion and also embed data within the frame. It has some password to hide data .
[6] Afterwards places splited secret text characters 3 bit in red pixel,3 bit in green pixel,2 bit in blue pixel and stego frame will be formed.
[7] Stego frame combine with other frames and stego video is formed.

B. Decoding Process For Extracting Secret Information:-
Input :- Stego Video
Output :- Secret Text

Steps of decoding process :-

[1] During decoding or extracting the data from stego video first video file selected.
[2] These stego video will be applied to extract hidden data from frame.
[3] Here the same password is used to decode the data as it is known to intended receiver.
[4] In this way secret message will be displayed on text bit and it is extracted easily.

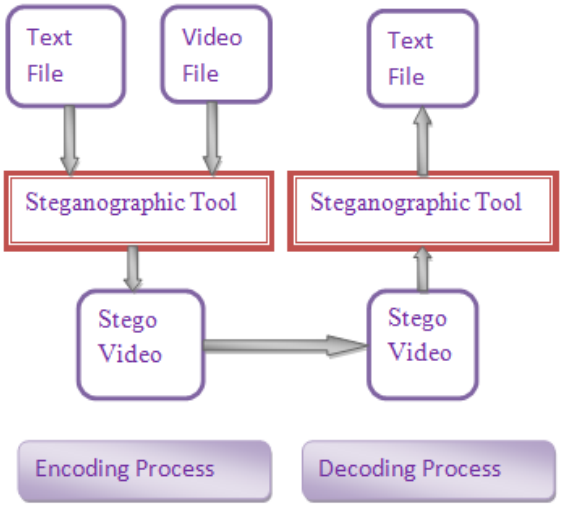

Fig.1.Block Diagram For Encoding And Decoding Process in Video Steganography

V. APPLICATION

There are various application of video steganography which are as follows

- Military application:-In Military there is requirement to hide secret message from unintended receiver like terrorist .
- Industrial application:- Businessman can use this technique to hide a data from business rivels.
- It provide Protection of sensitive data and can be used in Intelligence services.
- Confidential communication and secret data storing:-Steganography provides large capability to hide the existence of confidential data.
- Scientist can use this technique to hide secret formula.Medical records and banking data can be stored using video steganography.
- Protection against data alteration:-As the observer have no idea that a secret data is hidden in a video.so there will be no chances to alter the data.

VI. EXPERIMENTAL RESULTS

Steganography technique is characterized mainly by imperceptibility and capacity.Imperceptibility means the embedded data must be perceptually invisible to the observer. The performance of the proposed technique is evaluated using four different video streams (Road.avi,India.avi, Birds.avi,Paint.avi)and one secret text(msg.txt).The perceptual imperceptibility of the embedded data is indicated by comparing the original video with its stego video.When we hide secret text in video there will be no loss in quality of video and even noone can guess the presence of data within a video.

TABLE I.COVER VIDEO INFORMATION

Video file	Resolution WxH	No. of frames	Size
Road.avi	360x240	337	83.4 MB
India.avi	640x360	126	83.1MB
Birds.avi	540x360	248	138MB
Paint.avi	520x293	169	73.7MB

TABLE II.OBTAINED RESULT INFORMATION

Video files	No.of character in text file	Hiding capacity	PSNR	MSE
Road.avi	623	259200	55.1217	0.1999
India.avi	623	691200	58.7526	0.0866
Birds.avi	623	583200	60.3847	0.0594
Paint.avi	623	457080	57.4613	0.1166

From above table we observed that by using hash based least significant bit technique for video steganography using MATLAB software as steganographic tool we get more PSNR and as video has large hiding capacity so more hiding capacity gives more PSNR and small MSE.

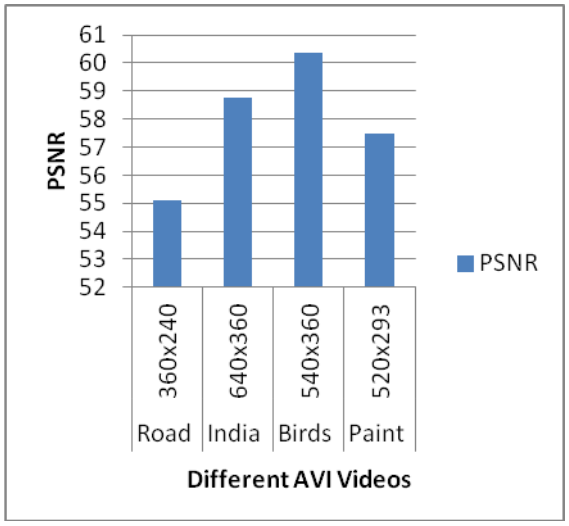

Fig. 2. PSNR VS Resolution Of Video

This graph shows variation in PSNR according to capacity of video.It gives different values of PSNR which deals with quality of video. For different resolution this quantity shows variation.

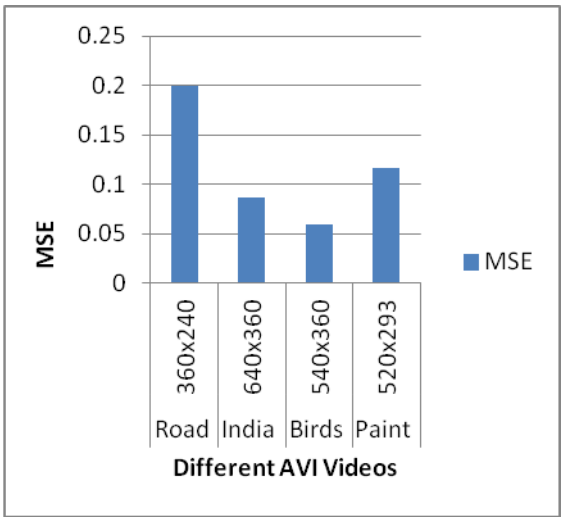

Fig. 3. MSE VS Resolution Of Video

The above graph shows variation in MSE according to resolution of video. The above two graphs in Fig 2 & Fig 3 shows the variation in PSNR and MSE for different video depending on their Resolution respectively.

The Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) between the stego frame and its corresponding cover frame are studied and calculated using equation (2)&(3).

The perceptual quality of video studied by using following parameter[12].

$$MSE = \frac{1}{H * W} \sum_{i=1}^{H} (P(i, j) - S(i, j))^2 \quad (2)$$

$$PSNR = 10 \log_{10} \frac{L^2}{MSE} \quad (3)$$

Here MSE is mean square error,PSNR is Peak Signal to Noise Ratio and H &W are the height and width ,P(i,j) and S(i,j) are original frame and stego frame respectively and L is taken as 255.

Following table will give comparison of PSNR and MSE of proposed method with other techniques.

TABLE III .OBTAINED RESULT INFORMATION

VIDEO NAME	PSNR (spatial domain method)	MSE (spatial domain method)	PSNR (Proposed method)	MSE (Proposed method)
Drop.avi	44.34	0.34	54.39	0.236
Flame.avi	42.66	0.34	60.21	0.061

The Mean squared Error (MSE), Peak Signal to Noise Ratio (PSNR) between the stego frame and its corresponding cover frame are studied.Peak signal-to-noise ratio, often abbreviated PSNR,It is the measure of quality of the frame by comparing the cover frame with the stego frame.Mean Square Error is used to measure the distortion between cover frame and stego frame.This two terms deals with variation in video frame due to encoding.Our proposed method gives very small MSE and large PSNR which is our objective,that indicate that distortion after encoding secret text in video is minimal.

The Table below shows variation in PSNR and MSE for hiding different bytes of secret messge in common video.

TABLE IV. OBTAINED RESULT INFORMATION

AVI Video	Secret Text Document	PSNR	MSE
Road (640x360) 337 Frames	File 1 (98 char)	62.0039	0.04099
	File 2 (623 char)	55.1217	0.1999
	File 3 (1224 char)	52.426	0.37194

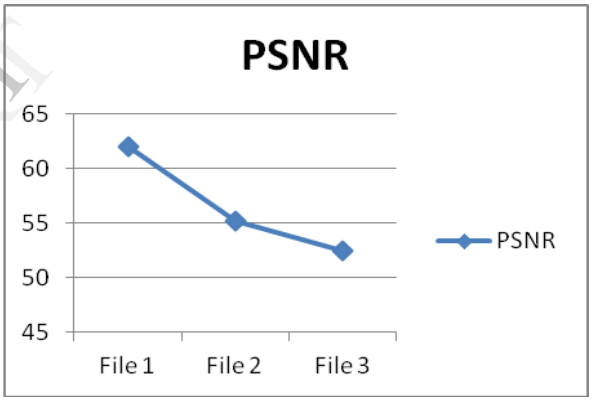

Fig. 4.Variation in PSNR

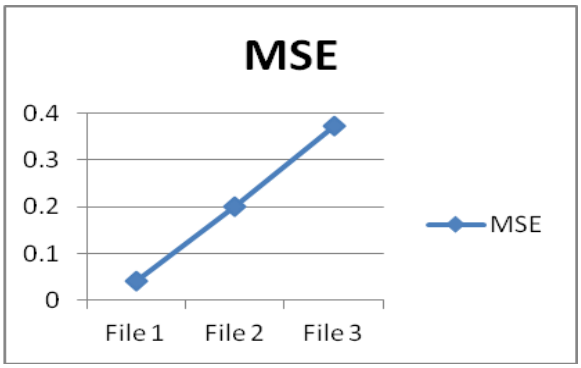

Fig. 5.Variation in MSE

The given graph from Fig 4 & Fig 5 shows variation in PSNR and MSE when secret messages having different characters encoded in same video.

VII. CONCLUSION

This technique of hiding a particular text file in the video hide it securely with minimum mean square error and hence gives maximum PSNR i.e peak signal to noise ratio.So it help to transmit data securely by embedding it in a video file and without disclosing to the unintended receiver and without any alternation in secret message .The proposed technique will be applied to the AVI file.In this way matlab software used to embed data in video file then extract it. In Future video format other than avi format can also be used with some modification and also can insert image file as here we are inserting only text file as secret message.

REFERENCE

[1] Anil Kumar, Rohini Sharma,"A Secure Image Steganography Based On RSA Algorithm And Hash LSB Technique", International Journal Of Advanced Research In Computer Science And July 2013.

[2] Kefa Rabah,"Steganography The Art Of Hiding",Information Technology Journal: 3(3),245-269,2004.

[3] A.K. Bhaumik, M. Choi, R.J. Robles and M.O. Balitanas,"Data Hiding in Video",in International Journal of Database Theory and Application ,Vol. 2, No. 2, pp. 9-16, June 2009.

[4] P.Paulpandi1, Dr.T.Meyyappan, "Hiding Messages Using Motion Vector Technique In Video Steganography", International Journal of Engineering Trends and Technology,Volume3,Issue3,pg 361-365,2012.

[5] Mritha Ramalingam, "Stego Machine Video Steganography using Modified LSB Algorithm", in World Academy of Science, Engineering and Technology, 50, pp. 497-500, 2011.

[6] Pritish Bhautmage, Prof. Amutha Jeyakumar, Ashish Dahatonde, "Advanced Video Steganography Algorithm", International Journal Of Engineering Research And Applications (IJERA) , Pp.1641-1644 1641 Vol. 3, Issue 1, January -February 2013.

[7] Satya Kumari, K.John Singh, "A Robust And Secure Steganograph Approach Using Hash Algorithm", International Journal Of Latest Research In Science And Technology, Volume 2,Issue 1 :Page No.573-576 , January-February (2013).

[8] Vipula Madhukar Wajgade, Dr. Suresh Kumar, "Enhancing Data Security Using Video Steganography",International Journal of Emerging Technology and Advanced Engineering ,ISSN 2250-2459 ISO 9001:2008 Certified Journal, Volume 3, Issue 4, pp 549, April 2013 .

[9] Mamta Juneja, and Dr. Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", 2nd International Conference on Latest Computational Technologies (ICLCT'2013,) June 17-18, 2013 .

[10] B.Suneetha,Ch.Hima Bindu & S.Sarath Chandra, "Secured Data Transmission Based Video Steganography", International Journal of Mechanical and Production Engineering (IJMPE), ISSN No.: 2315-4489, Vol-2, Iss-1, 2013.

[11] 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.