RESEARCH ARTICLE OPEN ACCESS

Hash Based Least Significant Bit Technique For Video Steganography

Prof. Dr. P. R. Deshmukh , Bhagyashri Rahangdale

ABSTRACT
The Hash Based Least Significant Bit Technique For Video Steganography deals with hiding secret message or information within a video.Steganography is nothing but the covered writing it includes process that conceals information within other data and also conceals the fact that a secret message is being sent.Steganography is the art of secret communication or the science of invisible communication. In this paper a Hash based least significant bit technique for video steganography has been proposed whose main goal is to embed a secret information in a particular video file and then extract it using a stego key or password. In this Least Significant Bit insertion method is used for steganography so as to embed data in cover video with change in the lower bit.This LSB insertion is not visible.Data hidding is the process of embedding information in a video without changing its perceptual quality. The proposed method involve with two terms that are Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE) .This two terms measured between the original video files and steganographic video files from all video frames where a distortion is measured using PSNR. A hash function is used to select the particular position for insertion of bits of secret message in LSB bits.

KEYWORDS - Cover Video,Hash Function,LSB Insertion,Secret Message,Stego Video,Video Steganography.

I. INTRODUCTION

Now days as Internet and other digital media are getting very popular,so there is requirement to transmit a data more securely. Steganography is a kind of art and science of hidding a secret message inside the other digital files as here a video file in such a way that no one else apart from intended recipient can realize presence of data within the video[1].The video steganography uses a particular portion of container file such as Video files to embed the secret message.The steganography is term that derived from greek word: "Steganos" means "covered" and "graphia" means "writing".Steganography involves hiding information so it appears like that no information is hidden.So if any person view that video in which data is hidden but they have no idea that any hidden information is within the video hence information will not be decoded by hacker.Steganography is the process of invisible communication and it provide security by obscuring data.The steganography technique will hide presence of data even from receiver but receiver can decode data as they know the stego key.A video file can hide large quantity of information as it carry large number of frame and its storage capacity is also more.So video steganography will have biggest application in information hidding[9].Steganographic storage capacity (the amount of information that can be embedded) is always an important factor when developing a steganographic algorithm.Video files are significantly larger than audio and image files, so as it allow to hide more information. The video steganography composed of two main phases in which first phase is to embed secret message in the video files and second phase is the extraction of secret message from video files.

A video will be formed by playing fourteen images per second and when thirty images per second are played then it becomes a good quality video.In this video steganography a video frame will be divided into number of frame and in this frame secret data will be embedded[11]. Video cover file for hiding the secret data is famous as it can hide a large amount of secret message hiding data into video file is the added security against the attack of the third party or unintended receiver due the complexity of the structure of video file as compared to image file and audio file.Hash Based Least significant bit video steganography technique is a simple approach to hide data in video cover file.First of all video is converted into frames and then the least significant bit of some of the bytes inside an image is changed to a bit of each of the Red, Green and Blue color components used.Hash Based least significant bit video steganography technique is inspired from the simple LSB video steganography technique.This technique was proposed due to the simplicity of the LSB insertion.

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 LSB of RGB pixel.Bits are distributed in 3,3,2 order.So there is random distribution of the bits into those pixels takes place.After hiding information in multiple frames of a video file,these frames are combined together to make a stego video and this video now can be used as a normal streaming video[3].On the receiver side the authorized receiver has to perform the reverse process to decode the hidden message or data.Stego video will be broken into frames and then using the password data is retrived from various frames.In this paper hash based least significant bit technique for video steganography is going to be developed in MATLAB.

II. LITERATURE REVIEW

There are various kinds of steganographic methods have been proposed.Video file for hiding the secret data is most useful as it can hide a large amount of secret data. The basic requirement of hiding a data in cover file and the relation of steganography with cryptography is discussed[1].The steganography is art of hiding data within the video file or image file.An Efficient Method for Steganography in Videos in which Secret Message is first encrypted by using cryptography algorithm.Steganography is an effective means of protecting the confidentiality of the data.By hiding the data from unwanted or unauthorized viewing[2]. The technique of data hiding [3] for high resolution video is proposed.It provide proper protection on data during transmission.It results in high data carrying capacities.The stego machine [4] to develop a steganographic application to hide data containing text in a computer video file and to retrieve the hidden information is designed.This is 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..High Capacity and Security Steganography [5] using Discrete wavelet transform algorithm is proposed.The capacity of the proposed algorithm is increased as the only approximation band of payload is considered.The payload wavelet coefficients are encrypted and fused with wavelet coefficients of cover image to generate stego coefficients based on the embedding strength parameters alpha and beta.

The data hiding method using the motion vector technique for the moving objects is introduced[8,9].In this compressed video is used for the data transmission since it can hold large volume of the data.The motion vector technique is found as the better solution since it hides the data in the moving objects.It provide efficient method for hiding the data from hackers and sent to the destination in a safe manner.The most secure and robust algorithm[10] of an effective hash-based algorithm that uses a pure hash technique for coding and decoding the information in a colour image. It provide an approach is worked on perfect hash function. There is system for data hiding uses AES for encryption for generating secret hash function or key[11]. A secured Hash based LSB technique [12] in which an efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through Hash LSB method.

III. SYSTEM ARCHITECTURE

1. BLOCK DIAGRAM

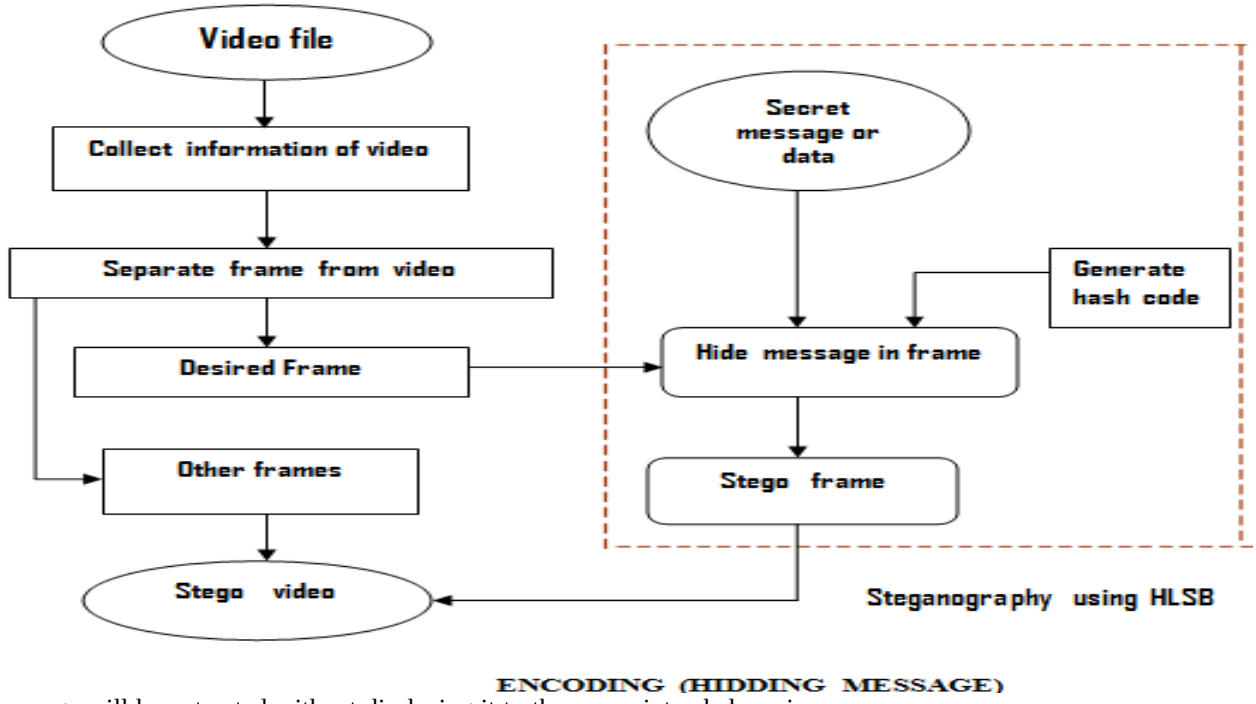
The Hash Based Least Significant Bit For Video Steganography Technique has been proposed in which it perform encoding and decoding for hidding message and extracting message respectively[4].First of all message file will be embedded within the cover file by using the steganographic tool as here use of MATLAB software.This steganographic file is again applied to steganographic tool to extract embedded data.A cover video consists of collection of frames and the secret data is embedded in these frames as payload.Data hiding in video by encoding and retrieving data by decoding is explained below.

1.1 ENCODING PROCESS

For Encoding first a video file is selected then information about the cover video will be collected.This frames of video are separated from each other then in this frame a secret message is hidded using hash based least significant bit technique. As hash code is generated then it help to embed data within the frame.Then it will find 4 LSB position in the pixel in which the secret message will be embedded. Stego frame combine with other frames and then stego video is formed.This stego video will be transmitted to the intended receiver.This encoding process which is used to hide data will be given in fig 1.

1.2 DECODING PROCESS

For decoding a stego video is taken and to extract the secret data or information from video all information about video is collected. This stego video frame will be applied to the desteganography tool to decode data.From this frame hidden information is taken out. The password will be used to decode the data as it is known to intended receiver.Here password also known as stego key. The decoding process will be given in fig 2. In this way secret



message will be extracted without disclosing it to the unintended receiver.

Fig 1.Block Diagram Of Encoding Process

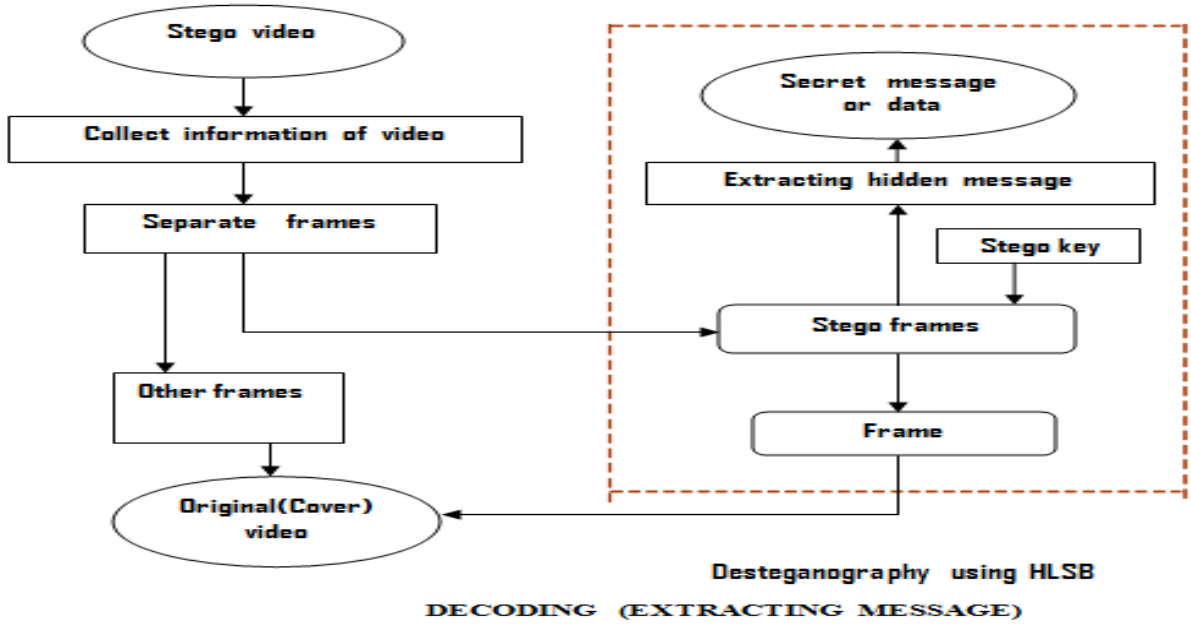


Fig 2. Block Diagram Of Decoding Process

2.ALGORITHM

2.1 HASH FUNCTION

Hash based least significant bit technique which produces hash function.This hash function deals with the LSB bit position within the pixel and

the position of each hidden image pixel and also with the number of bits of LSB[12].Hash value takes a variable size of input and returns a fixed size of digital string as output.Hash function also used for detecting duplicated record in large files.

Hash function generally given by

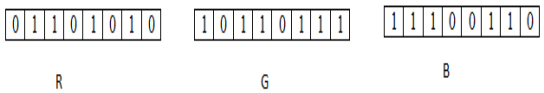
$$x = y \% z \qquad (1)$$

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.

2.2 LSB INSERTION

The least significant bit insertion method is simplest approach to hiding data 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 swaps them with a sequence of bits present in the secret data or message. 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 and hide them in LSB positions of RGB pixels of carrier frame the distribution of bits is of order 3,3,2 respectively and distributed in such a way that first 3 bits of the 8 bits secret message are inserted into R pixel and other 3 bits of secret message into G pixels and remaining 2 bits are inserted into B pixel. This bits are inserted into LSB position on basis of the returned value using hash function.As human eye has chromatic influence of the blue colour is more than the red and green colour hence this order of distribution takes place. In the LSB insertion technique, one can take the binary representation of the hidden data and overwrite the LSB of each byte in the cover file.The amount of change occurred in cover file will be minimal and not noticable to the human eye.

In following example there are 3 RGB pixels in which secret data embedded.



Let a Secret message is 200 .

Binary representation of secret message is (11001000).

Distributed in order (3,3,2) as shown in fig 3,Using the hash function.

Return values :- x=1,2,3 for(R),
x=4,1,2 for(G),
x=3,4 for (B).

where x is LSB bit position per pixel.

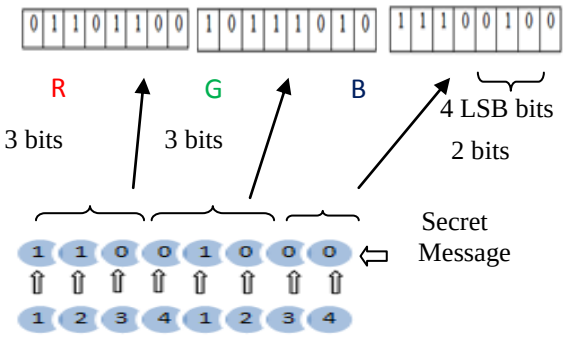


Fig 3.Distribution Of Secret Message bits

Mathematically,

The perceptual quality of video studied by using following parameter

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

H × W represents the Height and Width .

The distortion is measured using peak signal to noise ratio.

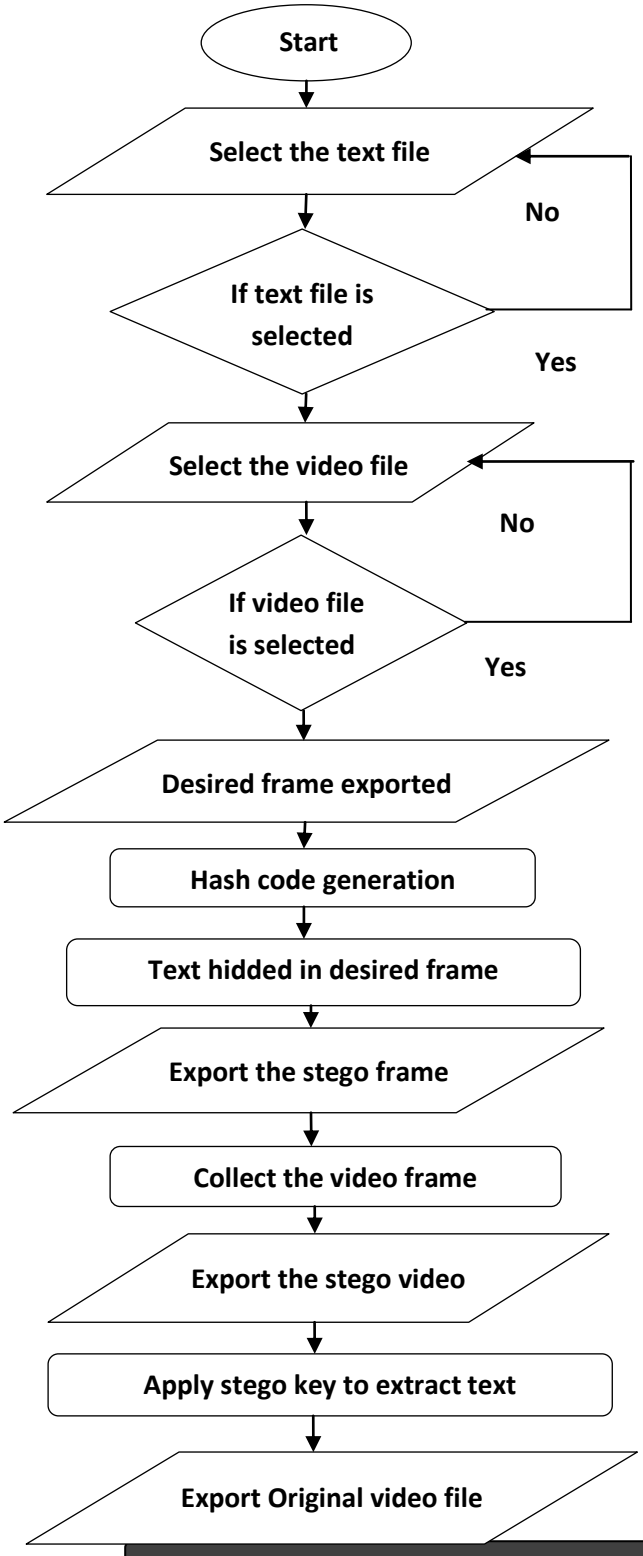
$$PSNR = 10 \log_{10} \left[\frac{L^2}{MSE} \right] \qquad (3)$$

Here MSE is mean square error,PSNR is Peak Signal to Noise Ratio and P(i,j) and S(i,j) are pixel in original frame and stego frame respectively and L is peak signal level.

3. FLOWCHART

The flowchart of the Hash based least significant bit technique for Video Steganography is presented in Fig 4. In this method first the text file is selected that is required to hide.As the text file is selected then it goes to next stage.The next stage is to select video file in which secret message has to get hide.After this number of frames will be counted and it will export the desired frame from video in which secret message get embedded.Then hash code will be generated and the text will be

embedded within the desired frame using hash code and this stego frame will be then exported and at last all steganographic frame and other frames of this all video frame are collected together.Finally this steganographic video is exported.Stego key applied to extract secret text from stego video and original video will be exported.



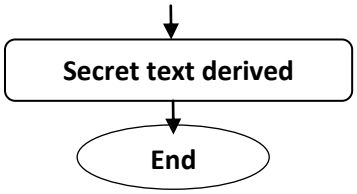


Fig 4. Flowchart of hash based least significant bit technique for video steganography

4.APPLICATION

There are various application of hash based least significant bit technique for video steganography which are as follows

- Military and Industrial application:-In Military there is requirement to hide secret message from unintended receiver like terrorist so that message will be hidded in the video file.Similar way businessman can use this technique to hide a data from business rivels.
- Protection against data alteration:-As the observer have no idea that a particular message is hidden in a video file so there will be no chances to alter the data.
- Intelligence services:- In the Intelligence services video steganography will be most useful.
- Confidential communication and secret data storing:- This hash based least significant bit technique for video steganography help in confidential communication.The secrecy of the embedded data is very important in this area.Steganography provides large capability to hide the existence of confidential data.First select a video file according to the size of the embedding data.Then,embed the confidential data by using an embedding program.When extracting, use an extracting program to recover the embedded data by using stego key.

IV. CONCLUSION

Data hiding in a video is performed using Hash based least significant bit technique for video steganography.This technique will successfully hide an text file in video by using Hash based LSB insertion technique during encoding process and some stego key or password will be used for decoding of secret message.In this way this technique for video steganography transmit the secret data or information through video transmission.The Encoding and Decoding program in matlab software hide data and retrieve the same data successfully. So it help to hide data securely

by embedding it in a video file and without disclosing to the unintended receiver.

This project uses text file to hide in video file as an secret message using LSB insertion and hash function,but in future image file can also be hidded in the video file. The proposed technique will be applied to the AVI file.The other format of video files which are other than avi format can also be used with some modification.

REFERENCE

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

[2] Gil-Choel Park,,A Study on Steganography and Steganalysis, *Journal of Security Engineering, Vol. 3, No. 4*,pp 35, November 2006.

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

[5] H.S. Majunatha Reddy and K.B. Raja,High capacity and security steganography using discrete wavelet transform, *International Journal of Computer Science and Security, 3(6),* pp. 462-472, June, 2011.

[6] ShengDun Hu, KinTak U,A Novel Video Steganography Based On Non-Uniform Rectangular Partition, *IEEE International Conference On Computational Science And Engineering CSE*,pp 57, 2011.

[7] Ankit Chaudhary, J. Vasavada, J.L. Raheja, Sandeep Kumar, Manmohan Sharma, A Hash Based Approach For Secure Keyless Steganography In Lossless Rgb Images, *The 22nd International Conference On Computer Graphics And Vision*,pp 80-83, October 01, 2012.

[8] 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 .

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

[10] 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).

[11] 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 .

[12] 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 Software Engineering, Volume 3, Issue 7*, July 2013.