Performance Evaluation of Image and Video Steganography for optimization of PSNR

[1]Naitik P Kamdar, [2]Dolly H. Patira, [3]Dharmesh N.khandhar.

[1] (Student of Master of Engineering in Electronics & Communication, C. U. Shah College of Engineering and Technology, Surendranagar, Gujarat, India)

[2](Student of Master of Engineering in computer engineering, V.V.P.Engg college, Rajkot, Gujarat, India)

[3](Head of Department of electronics & communication c u Shah College of engineering and technology, surendranagar, Gujarat, India)

[1] naitik.kamdar1@gmail.com

[2] dollypatira2008@gmail.com

[3] khandhar_dharmesh@gmail.com

Keywords- LSB (least significant bit), Steganography, PSNR (peak signal to noise ratio),

Abstract- Computer technology has made a breakthrough in the existence of data communication. This has opened a way of implementing steganography to ensure secure data transfer. Steganography is an art of hiding the information .this paper presents .this paper presents an analysis of LSB based steganography. Combination of public key algorithm with LSB is also implementing. LSB based Steganography embed message /image in least significant bits of digital picture. Least significant bit (LSB) insertion is a simple, common approach to embedding information in a carrier/cover file.comaparative analysis is made to demonstrate the effectiveness of the proposed methods. The effectiveness of the proposed methods has been estimated by computing the PSNR (peak signal to noise ratio).the analysis shows PSNR improved in the proposed methods.

I. INTRODUCTION

An important aspect of the way of life is communication. Many devices present today have the ability to transmit various information between them using different ways of communication, like insecure public networks, different types of wireless networks and the most used: the Internet. In some cases it is needed to keep the information travelling through different kinds of channels secret. Mainly there are two ways of concealing information: cryptography and Steganography. Cryptography's main aspect is that the information is somehow distorted, scrambled by the sender using normally an encryption key also known only by the intended receiver who decrypts the message. The problem with cryptography is that a user intercepting the message, although he cannot decrypt it, he might detect that there is encrypted, secret information. On the other hand steganography is able even to hide this aspect making sure that even the fact that there is secret information, is concealed. Steganography's main aspect is at it is embedding the secret message into another message.The basic structure of Steganography is made up of three components: the "carrier", the message, and the key. Steganos means covered or secret, and graphy, means writing or drawing. So, steganography literally means covered writing. Encrypted messages are many times intercepted, but it might not be decoded. The interception of the message is also damaging because the third party would know that two parties are communicating. While Steganography attempts to hide all the evidences of the communication. If a person views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; it is not trained to look for files that have information hidden inside of them. The actual information is not maintained in its original format and thereby it is converted into an alternative equivalent multimedia file like image, video or audio which in turn is being hidden within another object. This apparent message is sent through the network to the recipient, where the actual message is separated from it. Two other technologies that are closely related to Steganography are watermarking and fingerprinting.

These technologies are mainly concerned with the protection of intellectual property, thus the algorithms have different requirements than steganography. These requirements of a good steganographic algorithm will be

discussed below. In watermarking all of the instances of an object are "marked" in the same way. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. With fingerprinting on the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. This enables the intellectual property owner to identify customers who break their licensing agreement by supplying the property to third parties. In watermarking and fingerprinting the fact that information is hidden inside the files may be public knowledge –sometimes it may even be visible while in steganography. Research in steganography has mainly been driven by a lack of strength in cryptographic systems. Many governments have created laws to either limit the strength of a cryptographic system or to prohibit it altogether, forcing people to study other methods of secure information transfer. Businesses have also started to realize the potential of steganography in communicating trade secrets or new product information. Avoiding communication through well-known channels greatly reduces the risk of information being leaked in transit. Hiding information in a photograph of the company picnic is less suspicious than communicating an encrypted file.

A. *Steganographic Techniques:*

1) *Physical steganography*

Physical Steganography has been widely used. In ancient time people wrote message on wood and then covered it with wax. Message was written on the back of postage stamps. Message was written on paper by secret inks.

2) *Digital Steganography*

Digital Steganography is the art of invisibly hiding data within data. It conceals the fact that message exists by hiding the actual message. In this, secret data can be hidden inside the image, text, sound clip which can be represented in binary.

II. METHODS OF CONCEALING DATA IN DIGITAL IMAGE

A. *Least Significant Bit (Lsb)*

LSB is the lowest bit in a series of numbers in binary. E.g. In the binary number: 10110011, the least significant bit is far right 1.

The LSB based Steganography is one of the steganographic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. E.g. 300 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS: (00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

300 :100101100

RESULT: (00100111 11101000 11001000) (00100111 11001000 11101001) (11001001 00100110 11101000)

Here number is embedded and only 5 grids are changed.

III. LITERATURE SURVEY:

Nagham Hamid, Abid yahya, R. Badlishah Ahmad and Osamah M. Al-Qershi has presented image steganography technique an overview. In this paper they have given brief description of images and some related concepts also gives an overview of steganography techniques applicable to specific image formats also describes a performance measure for the distortion caused by embedding data in an image. Various transform domain techniques and spread spectrum technique, statistical method and distortion methods, pallete methods are defined. [1].Debnath Bhattacharya, Poulami Das. Samirkumar bandyopadhyay, and Tai Hoon Kim has presented paper on text steganography, a novel approach in this paper a security model is proposed which imposes the concept of security over privacy for text messages. The model proposed combines cryptography, steganography and along with that an extra layer of security has been imposed in between them. This algorithm is supposed to be more efficient as here from the resultant image it is difficult to guess the actual data that is hidden behind it the proposed method has many applications in hiding and coding messages within standard media such as video, audio.[2].xiaolong Li,Bin yang,Daofong Cheng,and Tieyong Zeng has presented A generalization of LSB matching .recently, a significant improvement of the well-known least significant bit matching steganography has been proposed, reducing the changes to the cover image for the same amount of embedded secret data. when embedding rate is 1,this method decreases the expected number of modification per pixel(ENMPP) from 0.5 to0.375.in this paper they have proposed the so-called G-LSB-M is investigated and a construction of G-LSB-M is presented by using the sum and differences covering set of finite cyclic group[3].Nitin jain, sachin meshram and shikhar dubey has implemented a Image steganography using LSB and EDGE detection techniques in which they have determined how edges cab be used to hide text message in steganography also the simulation result using LSB embedding and canny edge detector over standard images and commute PSNR to evaluate the difference between cover and stego image in simulation result also calculated MSE between cover and stego image. A technique of information hiding using steganography particular edge detection filter has been presented using the edge detection approach along with LSB method lead to high security. [4] Shilpa gupta, geeta gujaral, neha agrawal has implemented Enhanced Least significant bit algorithm for image steganography. The rapid development of data transfer through internet has made it easier to send the data accurate and faster to destination, but in order to transfer the data securely to the destination without any modifications, there

are many approaches like steganography. This paper introduces the concept of steganography using a new algorithm "Enhanced LSB Algorithm, which has negligent distortion. Enhanced least significant bit algorithm hides information in BLUE color of the carrier image [5]. Saurabh singh and gaurav agarwal has implemented Hiding Image to Video a new approach LSB replacement. This paper represent novel approach of hiding image and video.the proposed algorithm is replaces one LSB of each pixel in video frame such that each row of pixel is hided in 1st rows of multiple frame of target. The developed system work excellently and it is very useful in sending sensitive information securely [6].

IV. MODEL

A. *Definitions.*

1) *Cover image:* It is defined as original image into which required information is embedded .it is also called carrier image.
2) Stego image: It is an unified image obtained by combination of cover and payload image.

B. *Error Analysis.*

1) PSNR

The Peak Signal to Noise Ratio (PSNR) is used to compare image compression quality. The MSE represents the cumulative squared error between the compressed and the original image, whereas PSNR represents a measure of the peak error.

To compute the PSNR, the block first calculates the mean-squared error using the following equation: In the previous equation, M and N are the number of rows and columns in the input images, respectively. Then the block computes the PSNR using the following equation:

$$PSNR = 10 \log_{10} \frac{R^2}{MSE}$$

The lower the value of MSE, the lower the error.

$$MSE = \frac{\sum_{M,N}[I_1(M.N) - I_2(M.N)]^2}{M * N}$$

In the previous equation, R is the maximum fluctuation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc.

V. ALGORITHMS OF STEGANOGRAPHY

A. *Lsb based steganography:*

1) Algorithm to embed text message

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: perform LSB operation on cover image that is Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego-image.

2) Algorithm to retrieve text message

Step 1: Read the stego-image.
Step 2: Calculate LSB of each pixels of stego-image.
Step 3: Retrieve bits and convert each 8 bit into character.
Step 4: Calculation of PSNR and MSE.

Encoding Result.

Fig (1)-Original image

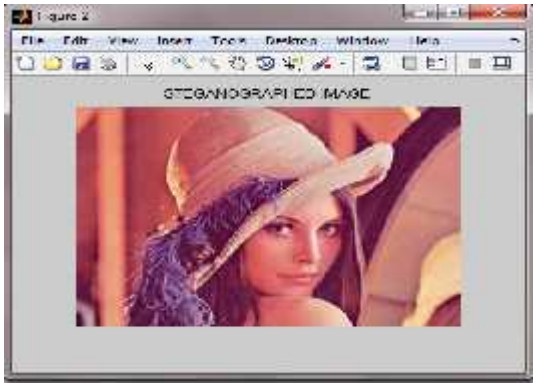


Fig (2)-Steganographic image

PSNR between Fig (1) and Fig (2) is 77.07

Decoding Result.

```
secret_msg =

My name is Naitik kamdar

PSNR_image =

   77.0710
```

3) Algorithm to hide image in image using LSB

Step 1: Read the cove image.
Step 2: Read secret image and convert it in binary.
Step 3: Calculate LSB of each pixels of cover image
Step 4: Apply LSB replacement method to replace LSB of cover image with each bit of secret image.
Step 5: Write stego image.

4) Algorithm to retrieve image

Step 1: Take stego image.
Step 2: stego color image is decomposed into three colors planes.
Step 3: Calculate LSB of each pixels of stego-image.
Step 4: Retrieve bits and convert each bit into secret message/image.
Step 5: Original hidden data.
Step 6: Compute PSNR and MSE.

Encoding Results.

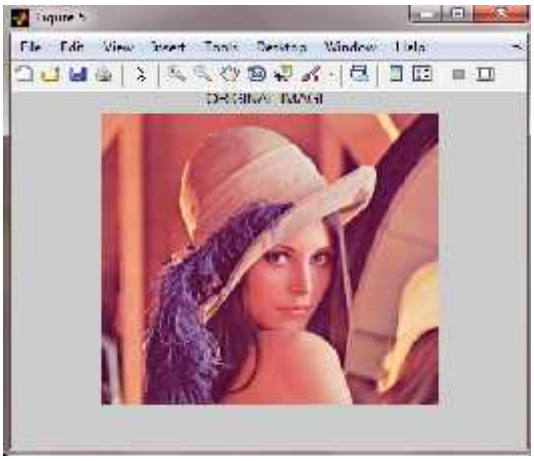


Fig (3) - Original image

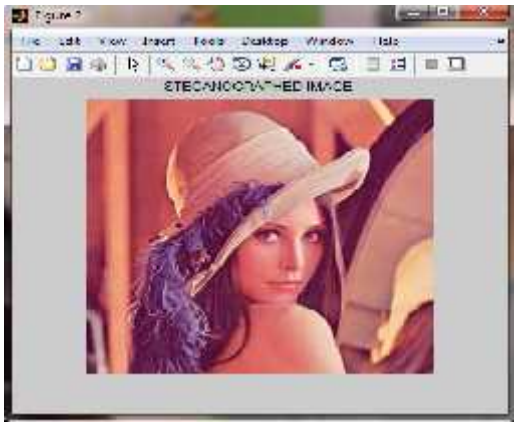


Fig (4) - steganographic image

PSNR between Fig (3) and Fig (4) is 58.50

Decoding Result.

Secret image Retrieved image

B. *Algorihms for implementing video steganography.*
Understanding

For R X C frame size, R X C=NB (Number of bit per frame) data bit will get hide.

Hiding Data

R X C=NB bits/frame

'N' number of frames required to store the whole data

1) Encoding algorithm for hiding image in video.

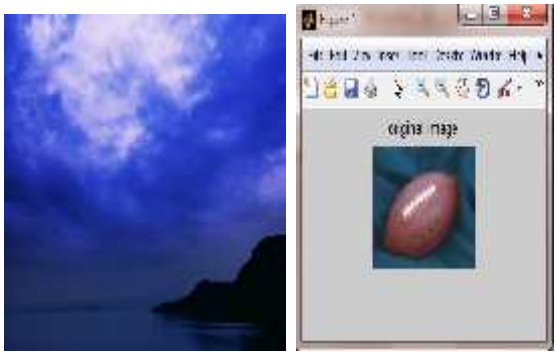
Step 1: read information to be hide
Step 2: read cover video file and converted into frames.
Step 3: rearrange information in to byte stream.
Step 4: rearrange information into bit stream.
Step 5: rearrange bit in NB*N format.
Step 6: for each frame, for each row, for each column, add +10 in values and at that location of raw put a byte to be hiding.
Step 7: Put a bit on LSB of pixel,
Step 8: N framed are generated which hides requirement data.
Step 9: Generated "non-compressed" .avi files to generate steganographic video.

2) Decoding algorithm for retrieving image.

Step 1: stego video

Step 2: extract first n frames which contain hidden information.
Step 3: for each frame for each row for each column extract LSB to generate bit stream.
Step 4: reaarange to convert to byte stream.
Step 5: rearrange to generate extracted data in predefined format.
Step 6: generated visual hidden information
Step 7: calculation of PSNR.

Simulation results of video steganography using LSB algorithm.



Cover video Secret image

Stego video Retrieved image

PSNR between cover video and stego video is 87.99

C. *Algorithm of public key encryption with LSB for hiding image in video.*

Understanding
1. R X C is frame size
Where R-Length of pixel in each raw
C-Length of pixel in each Colum
2. Hiding data
1 Bite/Raw
C Bites/frames
3. Public Key numbers in excel file

1) Encoding algorithm for hiding image in video.

Step 1: read cover video and converted into frames.
Step 2: read image /information to be hide.
Step 3: converted into bit/byte stream.
Step 4: Read the first c data byte of public key as number
Step 5: for each frame and for each row, for each column and public key in sequence put byte or bit at LSB on passion as per public key.
Step 6: N framed are generated which hides requirement data.
Step 7: Generated "non-compressed" .avi files to generate steganographic video.

2) Decoding algorithm for retrieve image from video.

Step 1: stego video.
Step 2: extract first n frames which contain hidden information.
Step 3: Read the first C data byte of public key as Number
Step 4: for each frame for each row, Extract byte or bit on LSB frame each row from column passion specified by public key.
Step 5: rearrange to generate extracted data in predefined format.
Step 6: generated visual hidden information
Step 7: calculation of PSNR.

Simulation result of video steganography for PUBLIC key encryption with LSB algorithm.

Cover video secret image

Stego video Retrieved image

PSNR between cover video and stego video is 87.9833

VI.

VII. CONCLUSION:

Steganography is the art and science of writing hidden messages in such a way that no one, apart from sender and intended receipent, suspects the existence of message, form of security. In this paper analysis of LSB and public key encryption method has been successfully implemented & results are delievered.from the result it is the clear that PSNR is high in proposed algorithms.

REFRENCES

[1] Nagham hamid,Abid yahya and R.badlishah ahmad and osamah M.Al-Qershi, image steganography technique an overview"internationaljournal of computer science and scientific(IJCSS)volume(6):issue (3);2012

[2] Debnath bhattacharya,poulami das.samir Kumar bandyopadhyay,and tai hoon Kim, "text steganography anovel approach", international journal of advanced science and technology,vol(3),feb,2009

[3] xiaolong Li,Bin yang,Daofong Cheng,and Tieyong Zeng "A generalization of LSB matching",IEEE signal processing Letters,vol.16,no.2,feb-2009

[4] Nitin jain,Sachin mesh ram and Shikhar dubey, "Image steganography using LSB and EDGE detection techniques",international journal of soft computing and engineering,ISSN: 2231-2307,vol-2,issue-3

[5] shilpa gupta ,geeta gujaral,neha agrawal has implemented Enhanced Least significant bit algorithm for image steganography.",international journal of computational engineering and management,vol5issue 4,july 2012

[6]. Saurabh singh and gaurav agarwal," Hiding Image to Video A new approach LSB replacement",international journal of engineering science and information technology,vol-2(12),2010,6999-7003

