International Journal of Advance Research in Engineering, Science & Technology(IJAREST),
ISSN(O):2393-9877, ISSN(P): 2394-2444,
Volume 2,Issue 4, April- 2015

Implementation of Image Steganography and Comparative Study of different Steganographic Techniques

Riyazahammad Nadaf[1], Reshma Nadaf[2]

[1] PG Student, M.Tech in Digital electronics, Department of E&CE, SDM College of engineering & technology, Dharwad, riyaznadaf034@gmail.com

[2]Assistant Professor, Department of E&CE, SDM College of engineering & technology, Dharwad, reshma.nadaf27@gmail.com

Abstract

With the advancement of data communication over computer network, the security of info become a major issue. A steganography is a technique of hiding multimedia info in an audio, video and image. Different technique of steganography are least significant bit (LSB) technique, discrete cosine transform (DCT), spread spectrum, discrete wavelet transform (DWT) and most efficient Hash LSB are briefly described. A comparative analysis is made to demonstrate by computing peak signal to noise ratio (PSNR) and mean square error (MSE). The stego images are tested by transmitting them and embedded data are successfully extracted by the receiver.

Keywords-*Steganography; LSB insertion; Hash LSB insertion; RGB pixel; DWT; DCT; PSNR; MSE.*

I. INTRODUCTION

The growth of internet plays an important role in information technology. The use of internet has been increasing tremendously. Providing security is also become important issue because of the use of internet. Steganography is a technique that is used to hide information in a cover so that no one can predict it. The cover can be any image, text, audio or video. Image is widely used as cover to hide info. Steganography is Greek word 'Stegnos' means secret and 'Graphy' means writing so overall meaning is secret writing. The objective of Steganography is to hide the information. Different technique of steganography are least significant bit (LSB) technique, discrete cosine transform (DCT), spread spectrum, discrete wavelet transform (DWT) and most efficient and widely used technique is Hash LSB. The block diagram of steganography is shown in fig 1.

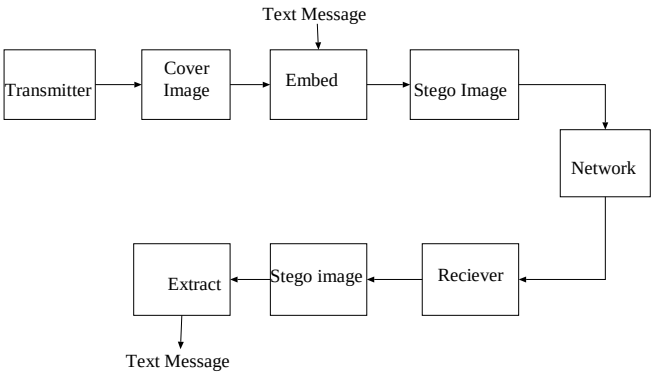

Figure 1. Block diagram of steganography

At the transmitting side Text message is to be hidden in cover image using embedding process. The image obtained after embedding text into cover image is called as stego image and then it is sent over the network to the receiver. At the receiving side by applying extracting algorithm one can extract the message hidden in the stego image. Even if third person got revealed the message, one cannot access the message as it is in the encrypted form. Without decryption key one cannot reveals the secret message.

II. TYPES OF STEGANOGRAPHY

The types of steganography are image steganography, text steganography and audio steganography are briefly described in following section

2.1 Image Steganography

Once image is taken as carrier for concealing secret info then it's known as image steganography. During this technique to cover the data one can have tendency to use component intensities.

2.2 Text steganography

By altering sure characteristic of matter component by sterilization the text info one can able to accomplish text Steganography. Text steganography isn't used typically because it has terribly touch of redundant knowledge.

2.3Audio Steganography

In audio Steganography audio is taken as carrier for concealing the secret info. It terribly vital medium and uses numerous formats like MPEG, WAVE, and AVI etc.

III. DIFFERENT TECHNIQUE OF STEGANOGRAPHY

Different technique of steganography are Least Significant Bit (LSB), hash LSB technique, Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Spread Spectrum are briefly described as follows

3.1 least significant bit (LSB) insertion technique

One of the foremost familiar technique used in steganography nowadays is called least significant bit(LSB),also called LSB (least significant bit) substitution and it is the process of alteration of the least significant bit of pixels of carrier image. It is a straightforward methodology for embedding message into the image [1]. In this approach the part of pixel info of the cover image is replaced with the message info thus it can't be detected by the human visual system. The Least Significant Bit insertion differs according to number of bits in an image. For an 8-bit image, the least significant bit i.e. the 8th bit of each pixel of the image will be changed by the 1-bit of secret message. For 24 bit image, the colors of each element like RGB

(red, green and blue) will be altered. LSB steganography contains the operation on least significant bits of cover image, audio or video. The least significant bit is the lowest bit in a sequence of binary number. In LSB substitution the least significant bits of the pixels are replaced by the bits of the secret message which gives rise to an image with a secret message embedded in it. The technique of embedding varies according to the number of bits in an image (different in 8 bit and 24 bit images).

3.2 Hash-LSB (Least Significant Bit) Process

The hash based least significant bit (H-LSB) method for steganography in which position of LSB for hiding the secret data is determined by hash function. The positions of LSB of each RGB pixel's is determined by Hash function and then text bits are embedded into these RGB pixel's independently. Then hash function returns values of hash according to the LSB present in RGB pixel values [2]. The cover image will be splits into red, green and blue i.e.RGB format [6]. Then the Hash LSB technique will uses the values specified by hash function to embed the data. In this method the secret text is converted into binary form as binary bits, each 8 bits are embedded in LSB of RGB pixel values of cover image in the order of three bits, three bits, and two bits respectively. In this technique three bits are embedded in LSB of red pixel, three bits are embedded in LSB of green pixel and two bits are embedded in LSB of blue pixel. These 8 bits are inserted in this order for the reason that the chromatic influence of blue color to the human eye is more than red and green color. So the distribution pattern elects the 2 bits to be hidden in blue pixel. Hence the quality of the image will be not sacrificed.

3.3. Discrete Cosine Transform (DCT)

DCT domain embedding techniques is the most widely used one, because of the fact that Discrete Cosine Transform based image format are widely available in public domain as well as the common output format of digital camera. JPEG image format for color components a discrete cosine transform (DCT) to transform successive 8 X 8 pixel block of the image into 64 DCT coefficients each[3]. The DCT coefficients F (u, v) of an 8 X 8 block of pixel f(x, y) are given by

$$F(u,v) = \frac{1}{4} C(u)C(v)\left[\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y) * \cos\frac{(2x+1)u\pi}{16} \cos\frac{(2y+1)v\pi}{16}\right]$$

……. (1)

Where

u= horizontal spatial frequency, v=vertical spatial frequency. C(x) =1/√2 when x=0 otherwise C (x) =1.

Embedding in DCT domain is done by replacing the DCT coefficients. For example by altering the least significant of each coefficient. The alteration of a single DCT coefficient affects all pixels of image.

3.4 Discrete Wavelet Transform (DWT)

Discrete wavelet transform (DWT) technique used to transform the image from its spatial domain into its frequency domain. This uses DWT in the process of steganography therefore one can clearly identify the high frequency and low frequency information of each image pixel [4].

A filter called the Analysis Filter pair is used to obtain the DWT of the cover image. First, the low pass filter is applied to each row of data in order to obtain the low frequency components of the row. Since the low pass filter is a half band filter, the Output data needs to be sub-sampled by two, so the output Data comprises only half the original number of samples. Then, the high pass filter (HPF) is applied for the same row of data, and likewise the high pass components are separated, and placed by the side of the low pass components. This process is done for all rows. Again filtering is done for each column of the intermediate data. The resulting 2D array of coefficients comprises 4 bands of data, each labelled as LL (Low-Low), HL (High-Low), LH (Low High) and HH (High-High). The LL band can be decomposed once again in the same way, thereby producing even more sub-bands.

3.5 Spread Spectrum

In spread spectrum methods, the message is spread over a wide frequency bandwidth than the minimum required bandwidth to send the info. This can done by modifying the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and hence hard to detect. In spread spectrum image steganography the message is embedded in noise and then combined with the cover image to produce the stego image [5]. Since the power of the embedded signal is less than the power of the cover image, the embedded image is not observable to the human eye or by computer analysis without access to the original image.

IV. RESULT

The objective of the work is implemented an image steganography technique to improve the security of the data. This paper implemented Image steganography is used to hide information in the RGB pixels value of the cover image. The performance of the this technique is evaluated and graphically represented on the basis of two measures namely Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR). Image steganography is implemented on MATLAB tool by analyzing two color images of size 256X256 as selected to hide a secret data.

The peak signal to noise ratio (PSNR) is a ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is given in following equation

$$\text{PSNR} = 10\ \text{Log}_{10}\frac{255^2}{\text{MSE}}$$

……..(2)

The mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated.

MSE is given in following equation

$$MSE = \frac{1}{A * B}\sum_{i=1}^{A}\sum_{j=1}^{B}[R(i,j) - N(i,j)]^2 \quad \text{……..(3)}$$

Where,
A is height
B is width
R (i, j) represents cover image
N (i, j) represents stego image

The cover image is shown in fig 2. Into which text message is to be hidden.

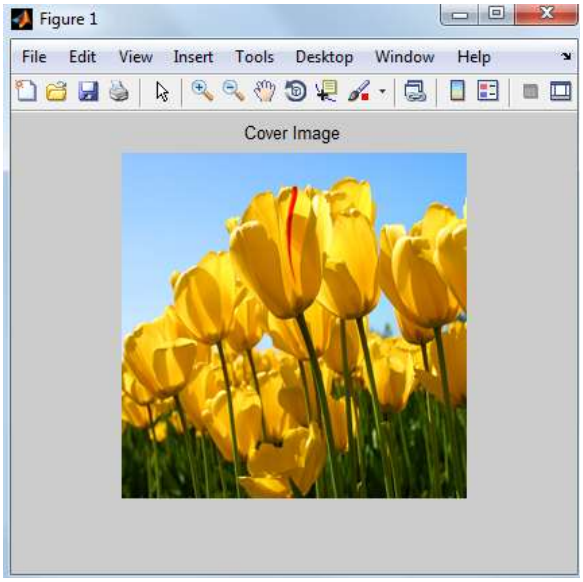

Figure 2. Cover image of Tulips

Stego image is shown in fig 3 which is produced after embedding text into cover image.

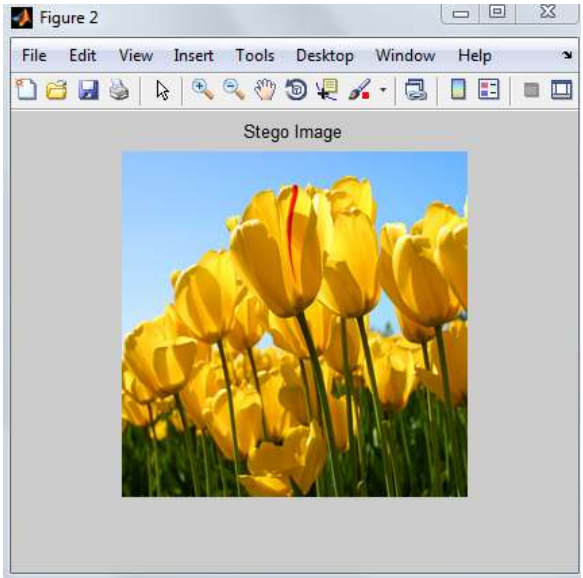

Figure 3. Stego image of Tulips

Mean square error (MSE) between cover image (fig 2) and stego image (fig 3) is 0.036011 and PSNR between them is 56.5665

The cover image is shown in fig 4. Into which text message is to be hidden.

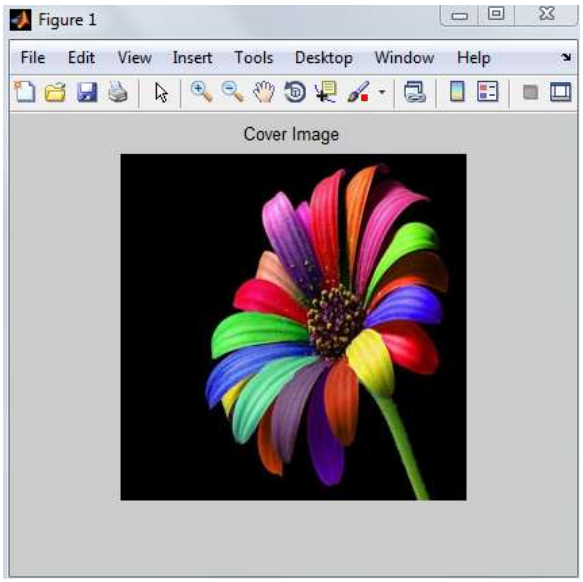

Figure 4. Cover image of Flower

Stego image is shown in fig 5 which is produced after embedding text into cover image.

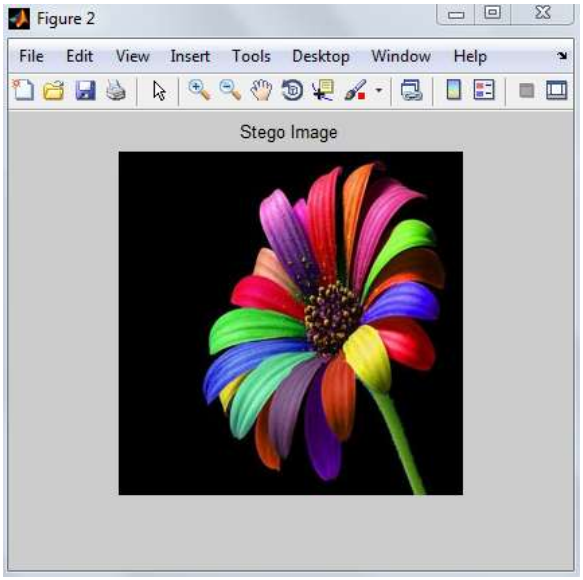

Figure 5.stego image of flower

Mean square error (MSE) between cover image (fig 4) and stego image (fig 5) is 0.036555 and peak signal to noise ratio (PSNR) between cover image (fig 4) and stego image (fig 5) is 58.5013.

The peak signal to noise ratio (PSNR) and Mean square error (MSE) of two image is summarized in table 1

Table 1. List of PSNR and MSE values of different image

Image	PSNR	MSE
Tulips	56.5665	0.036011
Flower	58.5013	0.036555

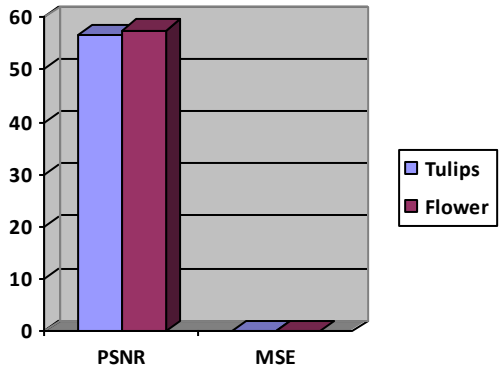

Figure 6 Chart showing PSNR and MSE value

V.COMPARISON OF DIFFERENT TECHNIQUES OF STEGANOGRAPHY

The different technique of steganography and their brief description, advantage, limitation are shown in table 2. Hash LSB technique has excellent PSNR and MSE value compared to all other techniques. The LSB technique has advantage of simple to implement and high capacity of embedding data compared to all other technique.

Table 2. Comparison of different techniques of steganography.

Method	Description	Advantage	Limitation
Least significant bit(LSB) insertion technique	Info hides in least significant bit of the pixel	High capacity , simple to implement	It has low robustness. Low security
Discrete cosine transform(DCT)	Info is embedded by changing the coefficients of transform image	Compression is used to decrease bandwidth using quantization technique. High security	Huge amount of data cannot be possible to hide. Small embedding capacity.
Discrete wavelet transform (DWT)	DWT transforms a discrete time signal(DTS) to a discrete wavelet coefficients	High capacity and high security	Large computation required and yield lowest PSNR value
Spread spectrum	In spread spectrum method, hidden data is spread all over the cover image making it harder to detect	Channel with narrowband noise increase the transmitting signal bandwidth so possibility of info received will be correct	High bit error rate(BER) and medium PSNR value
Hash LSB Technique	Hash function used to find the position of LSB's of pixel	Excellent PSNR and MSE value	Low robustness

VI.REFERENCE

[1] Juneja, Mamta, Parvinder S. Sandhu, and Ekta Walia. "Application of LSB Based Steganographic Technique for 8-bit Color Images." Evaluation 161 (2009): 15912.

[2] Kumar, Anil, and 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 3.7 (2013).

[3] Kaur, Blossom, Amandeep Kaur, and Jasdeep Singh. "Steganographic approach for hiding image in DCT domain." International Journal of Advances in Engineering & Technology 1.3 (2011): 72-78.

[4]Chen, Po-Yueh, and Hung-Ju Lin. "A DWT based approach for image steganography." International Journal of Applied Science and Engineering 4.3 (2006): 275-290.

[5]Satish, K., Jayakar, T., Tobin, C., Madhavi, K., & Murali, K. (2004). Chaos based spread spectrum image steganography. Consumer Electronics, IEEE Transactions on, 50(2), 587-590.

[6]Nadaf, Riyazahammad, and Mr BK Saptalakar. "Performance and Analysis of Face Recognition Using Skin Color Segmentation Algorithm."

BIOGRAPHY

Riyazahammad Nadaf,
Did Bachelor of engineering in Electronics and communication engineering from Tontadarya college of engineering, Gadag and currently pursuing M.Tech in Digital Electronics from sri dharmasthala manjunatheshwara college of engineering and Technology(SDMCET), Dharwad, Karnataka, India.

Reshma Nadaf,
Did M.Tech from GIT, Belgaum. Currently working as assistant professor, E&CE department in SDMCET, Dharwad, having more than 8 years of experience in teaching. Field of interest are Cryptography, VHDL and Steganography.