IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A NOVEL APPROACH FOR SECRET DATA TRANSFER USING LSB BASED STEGANOGRAPHY WITH WATERMARKING

Parul Baweja [*], Kumar Saurabh

[*] ECE Deptt.,OITM Hissar, India

ABSTRACT

In any communication, security is the most important issue in today's world. Lots of data security and data hiding algorithms have been developed in the last decade, which worked as motivation for our research. In simple words, Steganography can be defined as the art and science of invisible communication. In this paper we present the combination of LSB steganography and watermarking that will allow an average user to securely transfer secret messages by hiding them in a digital image file using the local characteristics within an image. Watermarking has become a popular technique for copyright enforcement and image authentication. The goal of this paper is to provide the two tier security i.e protection against detection and protection against removal. The performance of purposed method is estimated with the parameters PSNR, MSE and results show that this proposed technique is more efficient and secure

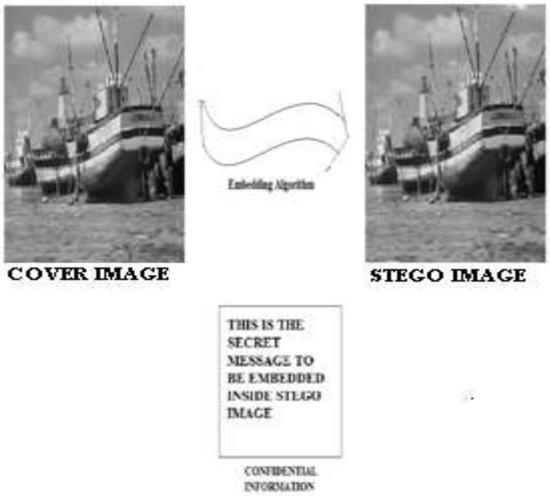
KEYWORDS: *LSB, MSE, PSNR, STEGANOGRAPHY, STEGO IMAGE, WATERMARKING*

INTRODUCTION

Steganography: is the science of hiding information. Steganography is a process that involves embedding the secret message within another digital medium such as text, image, audio orvideo[2].The following formula provides a very generic description of the pieces of the steganographic process

cover_image+confidential_information + stego_key = stego image

Figure1:



Steganography Process

In this context, the cover_image is the file in which we will hide the confidential_information, which may also be encrypted using the stego_key. The resultant file is the stego_image (which will be the same type of file as the cover_image). The cover_image (and thus, the stego_image) are typically image or audio files.

A. Stegonography Types

Image steganography can be classified into two domains: Transform Domain (Frequency Domain technique) and Image Domain (Spatial Domain technique).Transform Domain applies image transformation and manipulation of algorithm. Image Domain applies bit insertion and noise manipulation of a covered image. In spatial domain technique, the simplest approach to hiding data within an image file is called least significant bit (LSB) insertion[5]. In this method, we can take the binary representation of the hidden_data and overwrite the LSB of each byte within the cover_image. If we are using 24-bit color, the amount of change will be minimal and indiscernible to the human eye.

B. Least Significant Bit Technique

This approach is very simple. LSB steganography is one such technique in which least significant bit of the image is replaced with secret data bit. This technique is easy to implement and allow for large amounts of data to be embedded without observable changes. Image file that is used to embed secret data is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is an easier to hide information inside image [4]. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components [3]. Suppose that we have three adjacent pixels (9 bytes) with the RGB encoding [10].

10010101 00001101 11001001

10010110 00001111 11001011

10011111 00010000 11001011

When the number 360, can be which binary representation is 101101000 embedded into the least significant bits of this part of the image. If we overlay these 9 bits over the LSB of the 9 bytes above we get the following (where bits in bold have been changed)

1001010**1** 0000110**0** 1100100**1**

1001011**1** 0000111**0** 1100101**1**

1001111**0** 0001000**0** 1100101**0**

Here the number 360 was embedded into the grid, only the 5 bits needed to be changed according to the embedded secret message.On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size

C. Watermarking Model

Watermarking is a protection against removal of the secret information. Digital watermarking is a technique that is used for copyright protection and authentication for digital contents over the internet. Digital watermarking is also called data embedding. Digital watermarking is a method that inserts some information into a multimedia object to ensure a security service and generates a water-marked multimedia object, which can be an image, audio, video or text [3]. A watermarking system is divided into three steps embedding, attack and detection. In digital watermarking, embedding a host image with information which is called watermark and produce the watermarked signal. Then watermarked signal is transmitted to another person. If this person makes a changes to the watermarked signal is called an attack. There are various types of attack is possible on the watermarked signal[6]. Detection is an algorithm which accept attacked signal as input and extract the watermark signal from the attacked signal. There are many possible modifications, for example, lossy compression of the data (in which resolution is diminished), cropping an image or video or intentionally adding noise.

D. Discrete Wavelet Transform(DWT)

DWT is used for digital images. Many DWTs are available and Depending on the application appropriate one should be used. The most simplest transform is hear transform. To hide text message wavelet transform can be used. When DWT transform is applied to an image it is decomposed into 4 sub bands are:-

a) LL

b) HL

c) LH and d) HH.

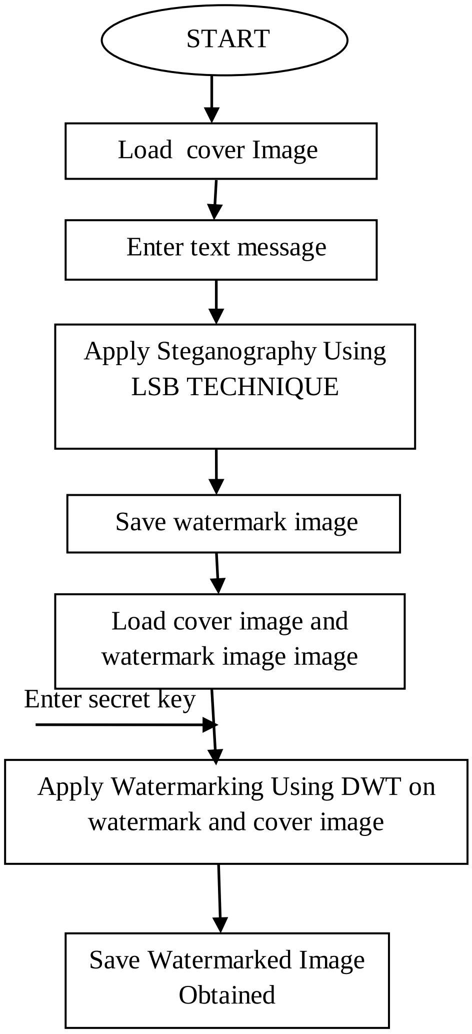
The LL part contains the most significant features. So if the information is hidden in LL part,the stego image can withstand compression or other manipulations. Sometimes distortion may be produced in the stego image and then other sub band can be used[1]

PROPOSED METHODOLOGY

The Research is divided into 5 phases to achieve our desired goal.

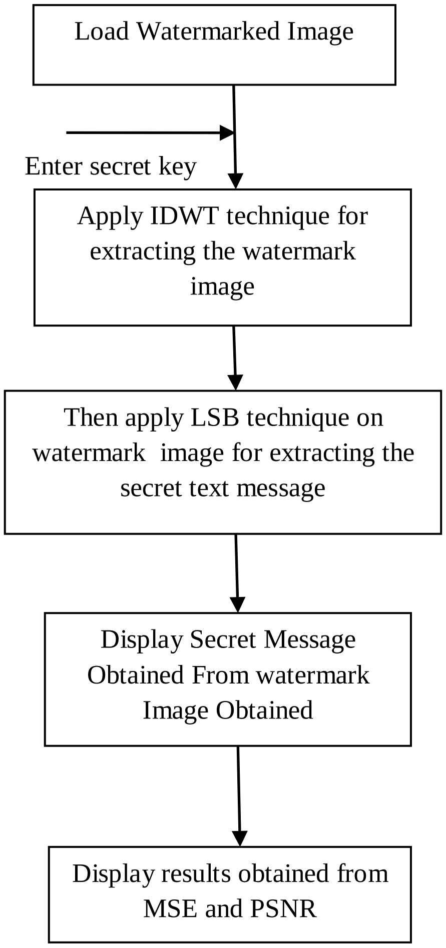
Step 1: I will develop a code for Image Steganography i.e., embedding purpose of the message for the hiding process using LSB(Least significant bit) technique

FIGURE 2


START
Load cover Image
Enter text message
Apply Steganography Using LSB TECHNIQUE
Save watermark image
Load cover image and watermark image image
Enter secret key
Apply Watermarking Using DWT on watermark and cover image
Save Watermarked Image Obtained

SENDER SIDE FLOWCHART

FIGURE 3


Load Watermarked Image
Enter secret key
Apply IDWT technique for extracting the watermark image
Then apply LSB technique on watermark image for extracting the secret text message
Display Secret Message Obtained From watermark Image Obtained
Display results obtained from MSE and PSNR

RECEIVER SIDE FLOWCHART

Step 2. After then add watermarking using DWT(discrete wavelet transform).

Step 3: After that at receiver side again I will remove watermarking using DWT and then using LSB technique find out the hidden data. Thus finally I will recover my secret message.

Step 4: I will then finally verify our result by developing code for MSE (Mean square error) and PSNR.(Peak signal- to- noise ratio)

RESULTS AND DISCUSSION

The quality of the image is measured by quality metrics; some arithmetic index is calculated to identify the reconstructed image quality. The most commonly metrics which are used for comparing the quality are ***Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).*** Between two images, PSNR block computes the peak signal-to-noise ratio, in decibels. This ratio is frequently used as a quality measurement between the cover image and watermarked image. If the Higher is PSNR, then better the quality of the watermarked image or reconstructed image [8]. The MSE represents the cumulative squared error between the cover image and the watermarked image, whereas PSNR represents a measure of the peak error [9]. The lower the value of MSE, then lower the error.

To compute the PSNR, the block first calculates the mean-squared error using the following equation:

$$\mathbf{MSE=\sum ([f\ (i, j)-F\ (i, j)]^{2}) /N^{2}.}$$

In this equation, cover image f (i, j) that contains N by N pixels and a reconstructed or watermarked F (i, j) where F is reconstructed by decoding the encoded version of f (i, j).

The root mean squared error (RMSE) is the square root of MSE. Some formulations use N rather N^2 in the denominator for MSE.

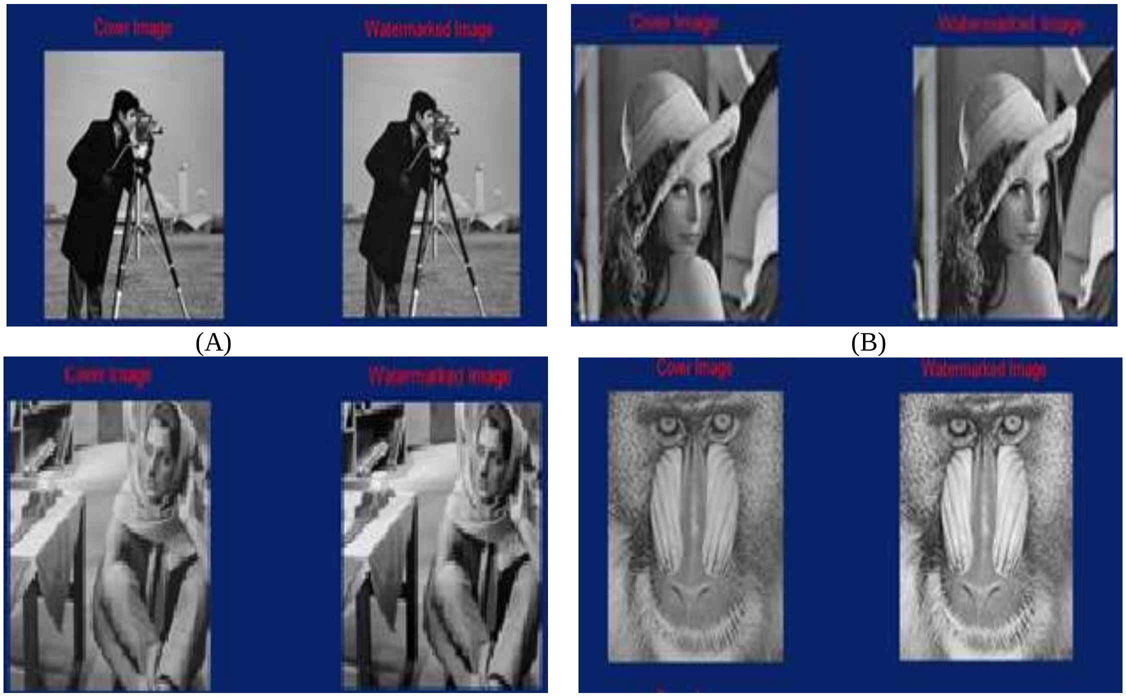
$$\mathbf{RMSE= SQRT(MSE)}$$

PSNR in decibels (dB) is computed by using

$$\mathbf{PSNR=10log_{10}(255/RMSE).}$$

In this section measure experimental results of each image quality for four images that were embedded with a image watermarks. To show the effectiveness of the proposed method we have used these four images of size 512*512.Fig4 show the cover images, watermarked images side by

Figure 4:



(A) (B)

(C) (D)

Experiment Results (Cover & Watermarked image)

Table 1. PSNR & MSE between cover and watermarked Image

Image Name	PSNR	MSE
Image(A)	56.6280	0.1413
Image(B)	54.6366	0.2236
Image(C)	54.2212	0.2460
Image(D)	54.7148	0.2196

From figure 4 and TABLE 1 we can conclude that our proposed technique assures the better quality of watermarked image. Watermarked images are more near to the cover image.

CONCLUSION

Proposed approach of steganography based on effective LSB and watermarking technique, assures that it is quite efficient and easy to embed the content of the image in itself as a watermark.This model provides protection against detection and protection against removal so as to provide high security.Experimental results show that our Technique gives better peak to signal noise ratio and less root mean square error than other techniques used so far .Finally we conclude that our Proposed approach gives higher security with good image quality. The future work is to extend proposed technique for videos and to modify given scheme to improve image quality by increasing PSNR value and lowering MSE value.

ACKNOWLEDGEMENTS

I would like to express my gratitude to my guide Mr. Kumar Saurabh for his valuable help and guidance. Finally I bow to the almighty, who gave me strength to carry out this work with sincerity and dedication.

REFERENCES

[1] Mohammad Abdullatif,Akram M. Zeki,Jalel Chebil,Teddy Surya Gunawan,"Properties of Digital Image Watermarking" 2013 IEEE 9th International Colloquium on Signal Processing and its Applications.

[2] Shilpa Guptal ,Geeta Gujral &Neha Aggarrwal Enhanced least significant algorithm algorithm for image steganography IJCEM Vol. 15,Issue 4,July 2012.

[3] P.W. Chan, M.R. Lyu, R. Chin, "Copyright Protection on the Web: A Hybrid Digital Video Watermarking Scheme," Poster Proceedings 13th International World Wide Web Conference (WWW'2004), pp. 354-355, New York, May 17- 22, 2004.

[4] Ki-Hyun Jung & Kee-Young Yoo, "Steganographic method based on interpolation and LSB substitution of digital images", Springer Science+Business, Media New York 2014.

[5] Sonia Bajaj, Manshi Shukla"Performance Evaluation of an approach for Secret data transfer using interpolation and LSB substitution with Watermarking", Sonia Bajaj et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6213-6217

[6] Pallavi Patil, D.S. Bormane DWT Based Invisible Watermarking Technique for Digital Images International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013

[7] C. Rey, J. L. Dugelay, "A survey of watermarking algorithms for image authentication", EURASIP Journal on Applied Signal Processing (JASP) 2002, pp. 613-621.

[8] A.N. Netravali and B.G. Haskell, "Digital Pictures: Representation, Compression, and Standards (2nd Ed)", Plenum Press, New York, NY (1995).

[9] M. Rabbani and P.W. Jones, "Digital Image Compression Techniques", Vol TT7, SPIE Optical Engineering Press, Bellvue, Washington (1991).

[10] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," in Proceeding of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sand to South Africa,June/July2005.3GPP RP-040461, Study Item: Evolved UTRA and UTRAN, December 2005