An Improved LSB based Image Steganography Technique for RGB Images

Amritpal Singh
Dept. of Computer Science and Engineering
Guru Kashi University
Talwandi Sabo, India
amritranu12@gmail.com

Harpal Singh
University College of Computer Applications
Guru Kashi University
Talwandi Sabo, India
harpalghuman11@gmail.com

***Abstract*—Steganography is the art and science of invisible communication by hiding secret information into other sources of information like text, video, audio, image etc. In image steganography the digital image is used as cover image in which we hide data and the message implanted image is called stego-image. There are number of steganography techniques proposed to hide data like LSB, DCT, pixel-value differencing, DFT etc. into images with precision level. But these techniques suffering from some problems like less hiding capacity, degrade the quality of image and security of hidden data after hiding more data into it. To overcome these problems this paper proposed an improved LSB technique for color images by embedding the information into three planes of RGB image in a way that enhances the quality of image and achieves high embedding capacity. The PSNR value of the proposed technique is better than previous steganography methods.**

Keywords*— Steganography; least significant bit; RGB; image quality; PSNR; data hiding.

I. INTRODUCTION

Steganography is the art and science of hiding the one information into other sources of information like text, video, audio, image etc. so that it is not visible to unintended users. It is the art of concealing a message in a cover without leaving a remarkable track on the original message. It is derived from Greek words Steganos (covered or secret) and Graphie (writing) literally means “covered writing”. Its ancient origins can be traced back to 440 BC. The main goal of steganography is to hide sensitive information inside other seemingly harmless carrier in such a way that no one apart from the authorized user can even detect that there is a secret message inside it [1]. Steganography and cryptography are similar in the way that they both are used for protecting the sensitive information from unintended users [2]. Cryptography scrambles the messages so that it becomes difficult to understand. At the same time encrypted data package is itself evidence of the existence of valuable information. Steganography goes a step further and makes the cipher text invisible to unauthorized users. Two other technologies that are closely related to steganography are watermarking and fingerprinting [3]. These technologies are mainly concerned with the protection of intellectual property. But steganography hides the information as well as keep the existence of the message secret whereas other techniques only hides the information, so individual can notice that some information is hidden.

Many steganographic methods have been proposed in the recent years [4] [5] [6]. The most common of these is replacing Least Significant Bit (LSB) of the pixels with the message bits [7]. A good steganography technique aims at three aspects: capacity (maximum information that can be hidden inside the cover image), visual quality of stego-image must remain unchanged (imperceptibility) and robustness [8]. In proposed technique Least Significant Bit(LSB) technique is selected because it is simple and easy way of hiding information, easily understand by users and the data is hidden by replacing the least significant bit of each pixel. But when we hide more data into an image by using LSB, it induces more noise hence image resolution (Quality of image) changed at the pixels where the data is hidden and the security of information is less as someone can detect the message by recovering the least significant bit of the pixels from the image. So, the need of removal of noise is very important to provide the better security and quality of the image after hiding the more data into it.

In this paper an improved Least Significant Bit steganography method for RGB images is presented which provides better image quality after hiding the information inside it. It hides the message bits into the three planes of the color image after bit plane slicing [9] in such a way that induces minimum noise in stego-image with the negligible change in the visible quality of the image which cannot be detected by naked eyes. The proposed selective approach results in better image quality, secure and reliable.

II. PROPOSED TECHNIQUE

A. *Introduction to Technique*

Inserting a message image into another carrier image, one needs two files. First one is the color image like scenery or the image of any object also known as cover image. The second file carries the message itself to be hidden.

In the first step, the cover image in which the message is to be hidden and the multiple message images containing the message are selected. The images can be in BITMAP or

978-1-4799-6085-9/15/$31.00 ©2015 IEEE

JPEG format, but more preferable is BITMAP as it is the lossless format available.

Further, the cover image is sliced into three planes namely Red, Green and Blue using bit plane slicing and the histogram is plotted for the original cover image.

In the Encoding phase, the cover image is interleaved for the adjustment of the message images with a Least Significant Bit replacement in the order of 2-2-4 in Red, Green and Blue planes respectively. That is, 2 message bits in Red plane, 2 in Green Plane and 4 in Red Plane.

The insertion technique used is LSB (Least Significant Bit). LSB insertion is a common, simple approach for embedding information in an cover (image) file [10]. The least significant bits of the cover image pixels are changed as required to insert the data to be hidden.

For example, the image of data uses LSB to hide first eight bytes of three pixels.

Pixels:

(00100111	10101011	111000001)
(11101001	00011001	001110100)
(00101010	11111110	111000111)

Data: 10101010

Result Pixels:

(00100111	10101010	111000001)
(11101000	00011001	001110100)
(00101011	11111110	111000111)

In proposed technique, message image decomposed into bits and these bits are replaced in the cover image. Selective bit insertion in 3 planes helps to reduce noise signals generated by the use of other methods like Bit Sequence Generator etc. and also enhance security from attacks.

The proposed method uses multiple processes like edge tapering to smoothen the image at the end of encoding to reduce the effect of LSB based pixel insertion. Another techniques used are uniform interleaving of the text images, bit slicing, encoding, decoding, de-interleaving, etc. for the successful running of the algorithm .

III. Theory of Color

According to the experts from "Theory of color" [11], there are four types of light receptors in human eye: the rods which are sensitive only to white, black and shades of grey, and the three types of cones which are sensitive to different colors.

The remaining receptors are called cones [11]. Cones cease to function at low light levels. Cones respond to different wavelengths of light, as follows: 'red', 'green', and 'blue-violet'.

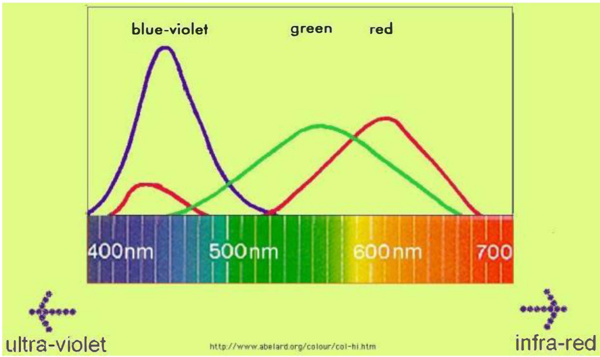


Fig. 1. Wavelength of the colors

The Fig.1, shows that there is a degree of overlap between the responses of the types of cones.

As per the Fig.1, the blue-violet cones are less sensitive to light as compared to red and green cones. Approximately twice as much light is required to obtain a perceived light level from the blue-violet cones that is similar to that obtained from the red and green cones. In other words, full response of the blue-violet cones requires more light energy than for the red or green cones. As stated in [12], blue-violet cones are less sensitive to light thereby making very difficult for human eyes to observe minor changes in the color intensity. On the other hand, the range 390 nm $\leq \lambda \leq$ 720 nm, where λ is considered the visible wavelength range . In this range, red and green are equivalently sensitive to human eye and are more sensitive as compared to blue.

In order to get maximum efficiency of the algorithm, our proposed technique uses 2-2-4 LSB Insertion. The proposed technique hides data 2-bits in 2 least significant bits of red component (Most significant Byte), 2-bits in 2 least significant bits of green component and 4-bits in 4 least significant bits of blue component (Least significant Byte) of each selected pixel. The ratio 2:2:4 is selected depending on the relative contribution of each component and on the basis of context in [12] [13], which denotes the sensitivity of red and green components of the light to be similar and are more sensitive as compared to the blue component. Thereby increasing the security and lowering the rate of distortion in the cover image after the hiding of the secret message image.

IV. Algorithm

A. Algorithm used to insert data image into the cover image:

Step 1: Read the cover image.

Step 2: Bit slice cover image to Red, Green and Blue Planes and show Image histogram.

Step 3: Read 6 text images to be hidden.

Step 4: Select images one by one to be hidden in Red, Green and Blue planes and arrange text images in interleaved manner.

Step 5: Replace bits of Cover image in order of 2:2:4 of the LSB in three planes (i.e. Red, Green and Blue planes) with the bits of message image.

Step 6: Display the reconstructed image after encoding process.

Step 7: Determine PSNR of the cover image

B. Algorithm used to retain data image from the cover image:

Step 1: Load the reconstructed image from stored location.

Step 2: Separate bits of message image in order of 2:2:4 of the LSB in three planes (i.e. Red, Green and Blue planes) from the image with hidden message.

Step 3: De-interleave and arrange the bits to reconstruct the message images.

Step 4: Display the reconstructed message images after Edge Tapering process and store the final output image.

V. RESULTS

A. Peak Signal to Noise Ratio (PSNR)

Generally, the image steganography system must embed the content of a hidden message in the image such that the visual quality of the image is not perceptibly changed. The larger the PSNR value decreases the possibility of visual attacks by human eye [14]. Higher PSNR value indicates better quality of image i.e. lower distortion. Thus to study the embedding perceptual effect, we have used the peak signal to noise ratio which is defined as:

$$\mathrm{PSNR} = 10\log_{10}\frac{(L-1)^2}{\mathrm{RMS}} \qquad (1)$$

Where

$$\mathrm{RMS} = \frac{1}{m \cdot n}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(x_{i,j} - x'_{i,j}\right)^2 \qquad (2)$$

B. Mean Square Error (MSE)

In a sense, any measure of the center of a distribution should be associated with some measure of error. If we say that the number *t* is a good measure of center, then most probably we are saying that *t* represents the entire distribution better, in some way, than other numbers.

In this context, suppose that we measure the quality of *t*, as a measure of the center of the distribution, in terms of the mean square error defined as:

$$MSE(t) = \frac{1}{n}\sum_{i=1}^{k} f_i (x_i - t)^2 = \sum_{i=1}^{k} p_i (x_i - t)^2 \qquad (3)$$

Here MSE (*t*) is a weighted average of the squares of the distances between *t* and the class marks with the relative frequencies as the weight factors. Thus, the best measure of the center, relative to this measure of error, is the value of *t* that minimizes MSE.

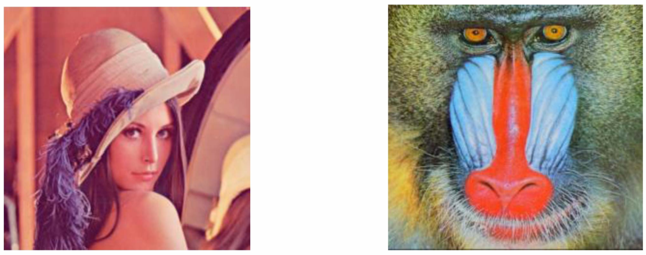
In statistics, the mean square error (MSE) is one way to evaluate the difference between an estimator and the true value of the quantity being estimated. MSE measures the average of the square of the "error" with the error being the amount by which the estimator differs from the quantity to be estimated.

TABLE I. PEAK SIGNAL TO NOISE RATIO (PSNR) OBTAINED

Image Name	Proposed Technique	LSB Technique	1-3-4 LSB Technique
Lena.jpg	55.9461	41.0053	47.5897
Baboon.jpg	55.9238	33.9879	36.3637

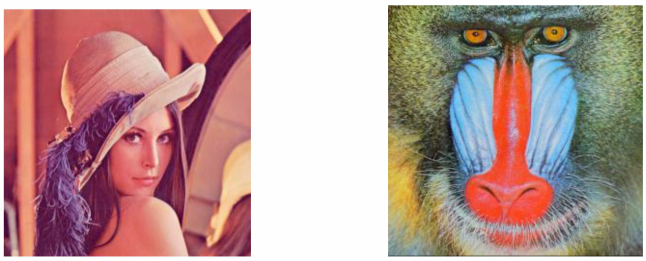
TABLE II. MEAN SQUARE ERROR (MSE) OBTAINED

Image Name	Proposed Technique
Lena.jpg	0.1654
Baboon.jpg	0.1662



(a) Lena (b) Baboon

Fig. 2. Original cover image



(a) Lena (b) Baboon

Fig. 3. Resulted Stego-image

We used standard RGB (true color) images, named Lena and Baboon as cover images in our proposed method. These are shown in Fig. 2. Hidden information is inserted into each plane of cover image after bit plane slicing on the basis of color sensitivity and stego-image is obtained. The stego-images are shown in Fig. 3. After embedding the secret message using our proposed method results in less distortion in the stego-image which cannot be detected by human eye.

The cover image and stego-image are look alike; hence it also reduces the suspicion that there is some hidden message inside the image.

CONCLUSION

The proposed method of Least Significant bit (LSB) for secret message insertion is made on the basis of sensitivity of human eyes to various color wavelengths. This selective approach induces lower noise and high security for transferring images.

The LSB approach replaces the least significant Bit of the pixel in the cover image. The earlier approaches used to hide the secret message for colored images leads to high noise in the stego-image due to this the secret information is susceptible to be detected. But our proposed method results in better image quality, secure and reliable as we have sliced the image into three planes i.e. Red, green and blue and then insert the message in each plane on the basis of color sensitivity.

There is a very bright future scope of this technique as it can be implemented in governmental, secrecy departments, military, banking sector and even in daily life. New strategies for the implementation of hiding the secret message are always in demand.

In future, random plane selection can be utilized for replacing bits with Least significant Bit (LSB), which in turn provide very high security of the embedded message. Even discrete cosine transform (DCT) can be implemented to further compress the hidden message before insertion.

REFERENCES

[1] Shashikala Channalli, Ajay Jadhav , "Steganography An Art of Hiding Data", International Journal of Computer Science and Engineering Vol.1(3), pp.137-141, 2009.

[2] Shahzad Alam, S.M. Zakariya, M.Q. Rafiq, "Analysis of Modified LSB Approaches of Hiding Information in Digital Images", IEEE 5th International Conference on Computational Intelligence and Communication Networks (CICN), pp. 280-285, 2013.

[3] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, "Steganography Using Least Signicant Bit Algorithm", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 3, pp. 338-341, 2012.

[4] Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence, Vol. 2, Issue 2, pp. 1-40, 2005.

[5] K.B. Raja, C.R. Chowdary, Venugopal K R, L.M. Patnaik, "A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images", IEEE International Conference on Intelligent Sensing and Information Processing (ICISP), pp. 170-176, December 2005.

[6] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology (IJAST), Vol.54, pp. 113-123, May 2013.

[7] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp. 749-755, Feburary 2014.

[8] Nadeem Akhtar, Pragati Johri, Shahbaaz Khan, "Enhancing the Security and Quality of LSB based Image Steganography", IEEE 5th International Conference on Computational Intelligence and Computer Networks, pp. 385-390, September 2013.

[9] H. Faheem Ahmed, U. Rizwan, " Embedding Multiple Images in an Image Using Bit Plane Slicing", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), Vol. 3, Issue 1, pp. 327-335, January 2013.

[10] Manu Devi, Nidhi Sharma, "Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images", In: Proc. IEEE RAECS UIET Panjab University Chandigarh, March 2014.

[11] http://www.abelard.org/colour/col-hi.htm

[12] E. Fred Schubert, Light Emitting Diodes, 2nd ed., Cambridge University Press, United Kingdom, pp. 276-291, June 2006.

[13] Mamta Juneja, Dr. Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", 2nd International Conference on Latest Computational Technologies (ICLCT), London (UK), June 2013.

[14] S.M Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography Using Secret Key", In: proc. IEEE 14th International Conference on Computer and Information Technology (ICCIT), pp. 286-291, December 2011.