Assesment of the Image Distortion in Using Various Bit Lengths of Steganographic LSB

Yucel Inan[1],

[1]Near east University, Computer Engineering Department, Nicosia, TRNC, Mersin 10 Turkey

Abstract. Several methods developed and applied for protecting the information. One of these is the stenography. Steganographic techniques are used to transmit the information in the image to the receiver in a secure manner. There are two main principles in the steganographic process. The first one is to hide the message in the image and the second one is to reduce the distortion on the image caused by information hiding. By making changes on digital images, a lot of information can be placed in the image. Nevertheless, changes in the image should not be noticed. In this paper, the effect of using various bit length of the steganographic LSB method on the image distortion is studied. The PSNR, SNR and MSE were used to assess the distortion rates of the images. Histograms were drawn to visualize the differences between original and encoded, "stego-images".

Keywords: Cryptography, Image Steganography, LSB Method, Cover Image, Hidden Secret Image, Stego-Image PSNR, SNR, MSE, Histogram.

1 Introduction

Steganography is an important method of information hiding, it is derived from a work by Johannes Trithemus (1462-1516) entitled "Steganographia" and comes from the Greek (στεγανό-ς, γραφ-ειν) defined as "covered writing"[1]. Steganography is the art and science of communicating information by hiding it from unwanted people [2]. Information can be hidden in the desired "cover-data", which can be in the form of image, text, audio, or video. The resulting encoded data can is called "stego-object" [3-4]. Stego-object does not give a clue about the information that is hidden when compared with the cover-image [5]. The goal in steganography is to hide the existence of a message and to create a covert channel. So, steganography can be seen as part of the cryptology of storing the content of the intended message. But they both have different structures. Cryptography is the method by which the receiver can only decrypt the message

1 Corresponding author: lyinan@hotmail.com

after it has been subjected to the encryption method of the message to be transmitted. And the great advantage of steganography over cryptography is that someone who sees Information never knows whether it is a secret message within the carrier. That is, when considering today's advanced technologies, there is a possibility of broken in the encryption method, even if the password is strong enough but in steganography can not be distinguished because the existence of the secret message is unknown and therefore unnoticeable. While it saying that briefly, steganography takes its power from secrecy, cryptography does this by using encryption algorithms[6]. Steganography classified into two types, Linguistics Steganography and Technical Steganography. Figure 1 displays, four main categories of the formats technical steganography that can be used for steganography [7].

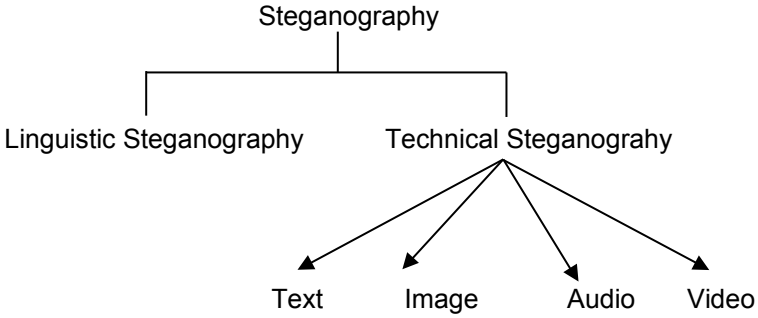


Figure 1: Categories of Technical Steganography

Linguistic steganography is uses text as the cover carrier to hide the secret message. Technique Steganography is invisible ink, hidden places, microdot and computer based, these are methods of hiding data using text, image, audio files[5]. Formally, a steganography system consists of a tripler algorithm that generates a key, encodes a message, and decodes a message.
This is shown in figure 2 below[8].

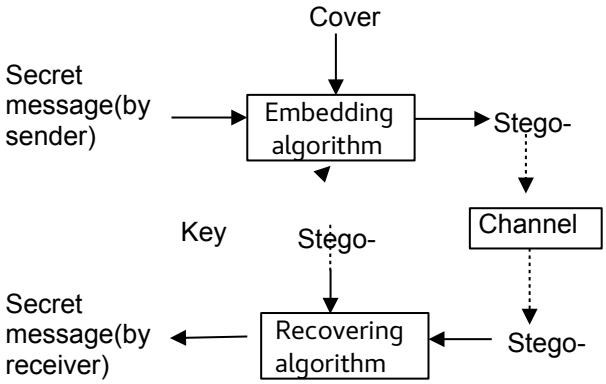


Figure 2: The Mechanism of Steganography

In this study, Cover image Kirlian Photograph[2] was used with the picture. The result is obtained by taking a contains secret message and cover image that both in the same size a 454x459 (jpg and png) in different format. Shows the LSB method experimental results of a pixel gray scale image appearing in the bit-plane in which the image is placed in five separate low order bit planes. This bit grayscale image keeps all this information inside without giving any clue about them and showing no visible decline in image quality. For this we have calculated PSNR and SNR, MSE. At the end of the calculation, PSNR produces a single value. The high value of this value means that the quality is high (the operation on the image is less effect on perceivability). The obtained PSNR, SNR and MSE values are shown in Table 2 and bit-planes image distortion of LSB images are shown in Table 1.

2 Structure of Steganography System

Image Steganography can be seen in the stages for embedding the secret message in image files, by using LSB method.

Figure 3 describes Stegangraphy of system. Firstly the cover image is converted to gray scale image. Then the cover image and the image that contains secret message are both scaled to the same dimension. After that separate LSB applications have been implemented every bit of the data to be hidden is written to the last bit of a byte of the image data. In here, The sender creates a steganogram using a concealment function. The concealment function has two parameters, the carrier channel in which the secret information is to be embedded and the secret information to be hidden. And also, a key password is present in this embedding and extract process to increase the privacy or security of the confidential information. If the recipient receives the image and he or she knows the key code to extract the confidential message, confidential information can be obtained.

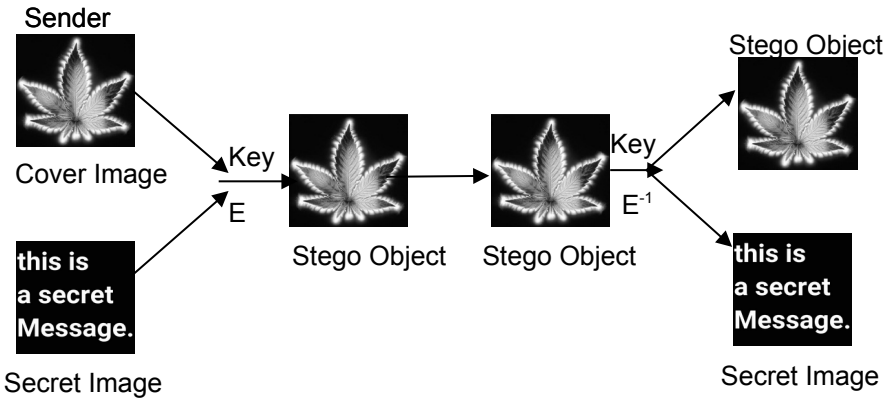


Figure 3: Block diagram of the Steganography System

2http://www.ottophoto.com/kirlian/kirlia_1/album1.html

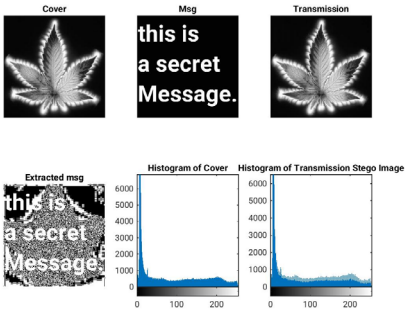
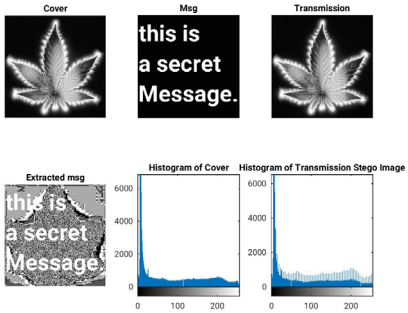
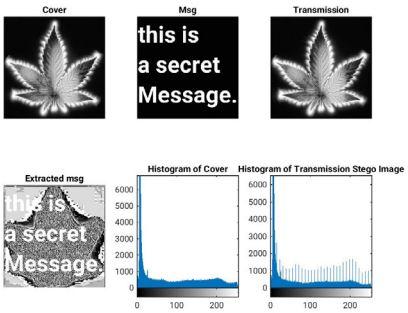
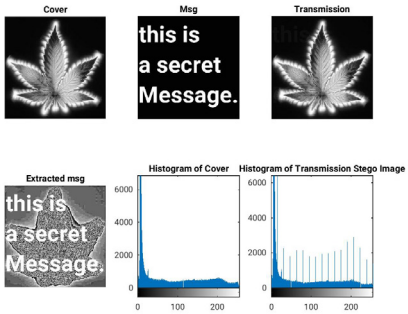
3 Bit Plane Image Distortion of LSB Method

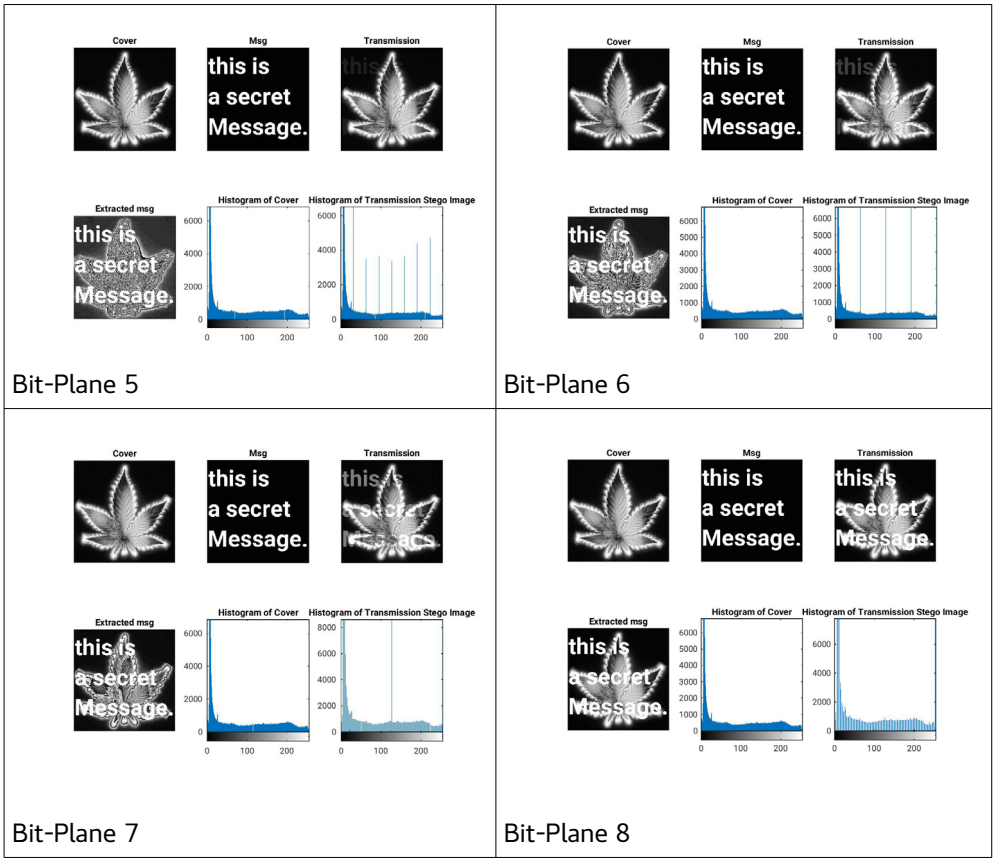
The substitution systems try to encode secret information by substituting unimportant parts of the cover by secret message bits. The receiver can discover the secret information if he/she has knowledge of the positions where secret information has been embedded. Since only minor changes have been made to the embedding process, the secret message may not be noticeable [9].

This concept is shown in Table 1, in each bit-plane is shown as a separate image to find the contribution of each bit-plane in the generation of the general view. This shows that the Bit-Plane Insert LSB method seriously reduces the cover image [10]. The effect of altering the LSBs up to the 8th bit embedding information with bit-planes for cover image shown in the next table. In Table 1 below shows a gray scale image and its bit planes from the 8th MSB bit- plane to the lowest 1.LSB bit-plane below and in lower bit-planes, the images looking like noise.

Table 1. Image distortions from 8th bit plane to the lowest 1.bit plane LSB.

LSB(Least Significant bit image distortion)Bit Plane

 Bit-Plane 1	 Bit-Plane 2
 Bit-Plane 3	 Bit-Plane 4



MSB(Most Significant bit image distortion) Bit plane

Table 2, shows the original RGB cover images and their gray scale images. In table 3 it can be resized cover image and contains secret message images both scaled to the same dimension.

Table 2. Shows the original RGB images and its gray scale images

 RGB Original Cover Image	 Gray scale image

Table 3. The cover image and the secret message images both scaled to the same dimension.

 Gray Scale Cover Image	 Gray scale Secret image

The steganography of the bit-plane image distortion of LSB method was used to embed hide in the cover image. This approach shows a grayscale image and its bit-planes from the maximum bit-plane at the top to the minimum bit-plane at the bottom. Above the first image is the gray scale original cover image and 8 images were viewed on the screen, the 1st is a 1 bit representation (Least Significant Bit) revealed 5th is 6th bit and so on. The 8th image is revealed the 8 bit (Most Significant Bit) image and the 8th image are obtained after the combination of all 8 bits. This application used for information hiding and extracting was done in the Matlab program environment. PSNR, SNR, MSE, Matlab program used image quality evaluation methods used to see distortions in images. Image quality assessment methods used to see distortions in images have been PSNR, SNR, MSE. In the data hiding applications, it is seen that the LSB method has the least degradation between the cover image and the hidden stego-image.

In the image quality evaluation methods used, the technique with the highest PSNR value is the LSB method. The error bit value with MSE is seen in the LSB method. In situations where the amount of data to be concealed should be small, it is better to choose the LSB method.

4 Image Quality Assessment Method

Evaluation of image quality is used to measure the distortion in the digital image to improve the quality of the resulting image[15]. In this analysis, we have the evaluation cover image and the confidential data to be embedded in this image. The most commonly used image quality measurements are PSNR, SNR, MSE. This study of experimental results, PSNR is used to measure the statistical quality of images containing confidential data. PSNR calculates the quality of similarity between the original image and the image containing the confidential data. image assessment methods that is:

4.1 Peak Signal Noise Ratio(PSNR)

PSNR is used to reveal the similarity between images in digital images. After the information is embedded, the distortions on the stego-object are detected by PSNR. The equation used for this calculation is given below[11]. The SNR measure is an estimate of quality of reconstructed image compared with original image. PSNR is defined as in [13].

$$PSNR = 10\log 10\left(\frac{MAX_i^2}{MSE}\right) \tag{1}$$

4.1 Mean Square Error(MSE)

It is used to compare the original image with the processed image after different types of operations have been performed on an image. The quadratic mean error estimate used to compare differences that may occur in the image. The mathematical function used to estimate the quadratic error is given below[12].

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}\left[I(x,y) - I'(x,y)\right] \tag{2}$$

In the data hiding applications, it is seen that the bit-plane Image Distortion of LSB method is the most 5th lower position degraded between the cover image and the hidden stego-object. In Table 4. The values of PSNR, SNR and MSE embed values obtained the amount of the application are shown below.

Table 4. Image degradation with different number of bits used for LSB.

Number of bits(LSB)	PSNR(db)	SNR(db)	Mse
1	58.706	51.332	0.088
2	51.170	43.796	0.497
3	44.367	36.993	2.379
4	37.357	29.983	11.951
5	30.591	23.218	56.748
6	23.956	16.582	261.535

7	17.858	10.485	1064.728
8	11.874	4.501	42233.437

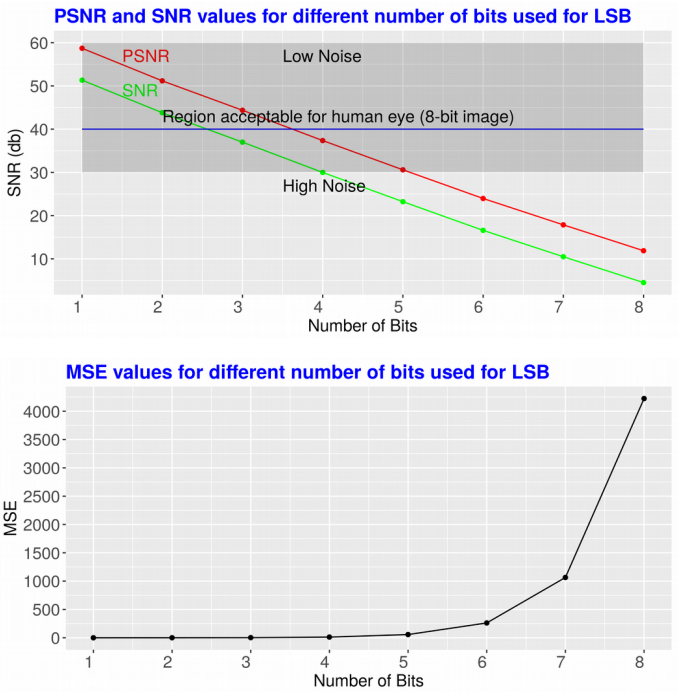


Figure 4. Shows PSNR and SNR, MSE values for different number of bits used LSB.

6 Histogram Analysis

In Steganography it is important that the embedded secret information is not understood when it gets in the hands of undesirable people. Therefore, several methods have been developed to test the robustness of the algorithms developed. The principle containing these methods is called steganaliz.. There are several methods used to detect confidential data. Histogram analysis method was tested from one of these methods. A histogram is a measure of the frequency of each element in a data sequence. It is a method that is used firmly in the field of digital image security. Table 1. Shows a cover image and historgrams of the stego-Image distortions from 8th bit-plane MSB to the lowest 1.bit-plane LSB.

6 Conclusion

In this paper we have studied bit-planes Image Distortion of LSB method for hiding information embedded in image file in gray scale image. We can slicing image into eight bit-planes to extract each bit-planes of original image. We performed the test with different value ranges and selected the opitimum range intensity level range. This range is the optimum range and causes minimal distortion on the entire image. And also MSE(Mean Square Error), SNR(Signal Noise Ratio), PSNR (Peak Signal Noise) and histogram analyszes of stego image is calculated. The histogram is visually distinguishable from the orignal cover image of the cover image and also shows that the PSNR values and the MSE values and the stego quality is a little good. Here, the factor is the distortion.

References

1. L. Y. POR, B. Delina, I*nformation Hiding: A new Approach in Text Steganography, 7th Wseas Int. Conf. (On Applied Computer & Applied Computational Science (Acacos '08), Hangzhou, China, April 6-8, 2008)*
2. Domenico Bloisi, Luca Iocchi , *Image Based Steganography and Cryptography*, Sapienza University of Rome, Italy
3. D.Seetha, Dr.P.Eswaran, *A Study on Steganography to Hide Secret Message inside an image,* International Journal of P2P Network Trends and Technology(IJPTT)-Volume3 Issue5-June (2013)
4. Nasser Hamad, *Hiding Text Information in a Digital Image Based on Entropy Function,* The International Arab Journal of Information Technology, Vol. 7,No. 2, April (2010)
5. Monika Agarwal , *Text Steganographic Approaches: A Comparison,* International Journal of Network Security & Its Application(IJNSA), Vol.5, No.1.January (2013)
6. Salony Pandey, Prof. Amit .M. Lathigara, *Hiding Text Behinde Image for Secure Communication, Salony Pandey, Prof.Amit .M. Lathigara /International Journal of Engineering Reserach and Applications(IJERA) ISSN:2248-9622 Vol.3,Issue3, May-Jun (2013), pp.1295-1297*
7. Neha Rani, Jyoti Chaudhary, *Text Steganography Techniques: A Review,* International Journal of Engineering Trends and Technology(IJETT)- Volume 4 Issue 7-july (2013)
8. L. Y. POR , B. Delina, Information Hiding: *A New Approach in Text Steganography*, 7th Wseas Int. Conf. On Applied Computer & Applied Computational Science (Acacos '08), Hangzhou, China, April 6-8, (2008)
9. Ali K.Hmood, B.B. Zaidan, A.A. Zaidan and Hamid A. Jalab, *An Overview on Hiding Information Technique in Images*, Journal of Applied Sciences,10: 2094-2100.
10. M.Naseem, Ibrahim M. Hussein, M.Kamran Khan, Aisha Ajmal, *An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding,* International Journal of Computer Applications(0975-8887) Volume 29-No.12,September (2011)

11. Khan Muhammed, Jamal Ahmad, Haleem Farman and Muhammed Zubair, *A novel Image Steganographic Approach for Hiding Text in Color Images HSI Color Model.* Middle-East Journal of Scientific Research 22(5):647-654,(2014)

12. Rengarajan Amirtharajan and John Bosco Balaguru Rayappan,*Pixel Authorized by Pixel to Trace with SFC on Image to Sabotage Data Mugger: A Comparative Study on PI Stego.* Research Journal of Information Technology, 4: 124-139,June 27,(2012)

13. Yusra A. Y.Al-Najjar, Dr.Der Chen Soong, *Comparison of Image Quality Assessment: PSNR, HVS, SSIM, UIQI*. International Journal of Scientific & Engineering Research, Volume 3, Issue 8, August-(2012) 1 ISSN 2229-5518