

Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images

H. B. Kekre

Sr. Professor, Computer Engg.
MPSTME,SVKM's NMIMS
Vile Parle West, Mumbai-56

Dhirendra Mishra

Assoc. Professor, Computer
Engg.
MPSTME, SVKM's NMIMS
Vile Parle West, Mumbai-56

Rhea Khanna, Sakshi

Khanna & Aadil Hussaini
B.Tech. Students
MPSTME, SVKM's NMIMS
Vile Parle West, Mumbai-56

ABSTRACT

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. This paper presents a comparison between the basic LSB technique which involves replacement of least significant bits in order to hide the colored message image behind the colored cover image, with the other technique for increased capacity of hiding information using an advanced LSB methodology wherein the bit replacement takes place in accordance to range specified for the color images. There have been many techniques for hiding messages in images in such a manner that the alterations made to the images are perpetually indiscernible. This paper proves experimentally that the technique for increased capacity of information hiding in LSB's method gives better performance in all the parameters and is a safe technique for embedding secret messages.

General Terms

Steganography, LSB Technique [12-20], Increased capacity of information hiding in LSB's method[1].

Keywords

Information Hiding, LSB, increased capacity, Steganography.

1. INTRODUCTION

Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. Colour images are used as a medium to hide images are called cover-images. Cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. In the literature, many techniques about data hiding have been proposed. One of the common techniques is based on manipulating the least significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity [11]. Information hiding techniques have been receiving much attention today. Steganography sometimes is used when encryption is not permitted. Or, more commonly, steganography is used to supplement encryption. An encrypted file may still hide information using steganography, so even if the encrypted file is deciphered, the hidden message is not seen. Hence in this paper we have explained two methods and compared it with the help of experimental results.

The new approach that is the method in which there is an increased capacity [1] of hiding shows better results than the simple LSB technique [13]. The main purpose of steganography is to hide the occurrence of communication. While most methods in use today are invisible to the observer's senses, mathematical analysis may reveal statistical discrepancies in the stego medium. These discrepancies expose the fact that hidden communication is happening. "Information Hiding using LSB(Least Significant Bit) Technique with Increased Capacity", International Journal of Cryptography and Security, Special issue on Steganography [10] discusses the technique for hiding the message image by specifying the range for pixel values and embedding the required MSB (Most Significant Bit) bits into the LSB of the cover image.

2. LSB TECHNIQUE

The Least Significant Bit embedding technique suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file. This technique can be used for hiding images in 24-bit, 8-bit or gray scale format. We emphasize strongly on image Steganography providing a strong focus on the LSB techniques in image Steganography. This paper explains the LSB embedding technique and presents the evaluation results for 2,4,6 Least significant bits [9]. Select the message image that is to be hidden behind the cover image [16-18]. Embed the required number of bits in order to hide the MSB (Most Significant Bit) of the message image behind the LSB (Least Significant Bit) of the cover image. Since the MSB contains the most important information of the image and the LSB contains the least important information of the image, replacing the LSB of the cover image with the MSB of the message image will help us to form a stego image which would contain the message [14]. This message can be retrieved only by that receiver who knows that it is a stego image sent by the sender. The main purpose of steganography is to hide the occurrence of communication. While most methods in use today are invisible to the observer's senses, mathematical analysis may reveal statistical discrepancies in the stego medium. These discrepancies expose the fact that hidden communication is happening. Current trends favour using digital image files as the cover file to hide another digital file that contains the secret message or information. LSB insertion is a common simple approach to embedding information in a image But it is vulnerable to even slight image manipulation.

Converting image from a format like GIF or BMP to JPEG and back could destroy the information hidden in LSBs [12]. One of the most common methods of implementation is Least Significant Bit Insertion, in which the least significant bit of every byte is altered to form the bit-string representing the embedded file. Altering the LSB will only cause minor changes in color, and thus is usually not noticeable to the human eye. While this technique works well for 24-bit color image files, steganography has not been as successful when using an 8-bit color image file, due to Limitations in color variations and the use of a colormap. LSB technique is an easy simple method for hiding data. But stego- images can draw suspicion or be easily detected from statistical analysis.

3. INCREASED CAPACITY OF INFORMATION HIDING USING ADVANCED LSB METHODOLOGY

The cover image used is a color image [1]. Before embedding the data we use 8 bit secret key and XOR with all the bytes of the message to be embedded. Message is recovered by XOR operation by the same key. Every pixel value in this image is analyzed and the following checking process is employed.

3.1 Steps for implementation.

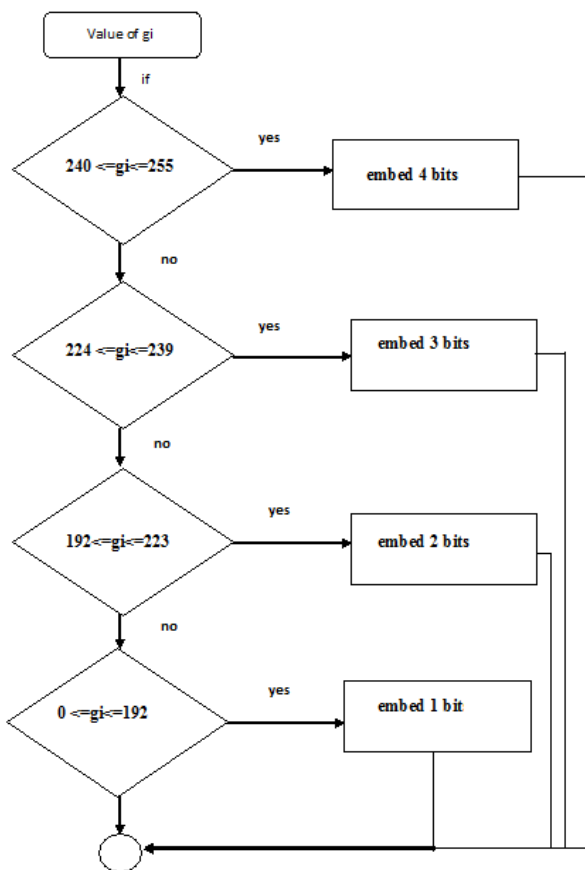


Figure 1. Flow chart for embedding bits.

The Steps to be carried out for implementation of the technique is as follow [1-5].

1. If the value of the pixel say g_i , is in the range $240 \leq g_i \leq 255$ then we embed 4 bits of secret data into the 4 LSB's of the pixel. This can be done by observing the first 4 Most Significant Bits (MSB's). If they are all 1's then the remaining 4 LSB's can be used for embedding data.
 2. If the value of g_i (First 3 MSB's are all 1's), is in the range $224 \leq g_i \leq 239$ then we embed 3 bits of secret data into the 3 LSB's of the pixel.
 3. If the value of g_i (First 2 MSB's are all 1's), is in the range $192 \leq g_i \leq 223$ then we embed 2 bits of secret data into the 2 LSB's of the pixel.
 4. And in all other cases for the values in the range $0 \leq g_i \leq 192$ we embed 1 bit of secret data in to 1 LSB of the pixel.
- Similarly, we can retrieve the secret data from the values of the stego image by again checking the first four MSB's of the pixel value and retrieve the embedded data. These steps have been carried out to get efficient results[1-3].

The flowchart depicted in Figure 1, simply illustrates the patten to be followed for embedding the required MSB (Most Significant bits) of the message image into the LSB (Least Significant bits) of the cover image.

If the value of g_i falls within a particular range as described in Figure 1, then follow the yes instruction and carry out the required mentioned operation and exit, else move on to the next condition and repeat the procedure.

4. EXPERIMENTAL RESULTS AND DISCUSSIONS

In our experiments that were carried out the results obtained were as such. Three colored cover images “man.jpg”, “woman.jpg”, “bird.jpg” each of size 300x300. Figure 2(a) represents the three cover images which will carry the message image. Figure 2(b) represents the colored message image of size 300x300 which is to be hidden behind these respective cover images. Let us understand what the difference between LSB is and MSB. LSB, the least significant bit is the lowest bit in a series of numbers in binary; the LSB is located at the far right of a string. For example, in the binary number: 10111001, the least significant bit is the far right 1. The most significant bit (MSB) is the bit in a multiple-bit binary number with the largest value. This is usually the bit farthest to the left, or the bit transmitted first in a sequence. For example, in the binary number 1000, the MSB is 1, and in the binary number 0111, the MSB is 0.

Consider Figure 3, Figure 4 and Figure 5 ,it consists of the stego images of LSB replaced from the cover image in order to embed the MSB of the message image in it [16-19]. Each of the image looks similar to the other since the number of bits replaced is minimal, however the MSE and RME values obtained for each vary drastically, this can be observed in Table 1. On the other hand the technique for Increased capacity of Information Hiding in LSB's Method [1-5] for the same cover image and message image can be seen in Figure 6. Since in this technique, if the value of the pixel say g_i , are in the range as per allotted then we embed those many number of bits of secret data into the LSB's of the pixel.

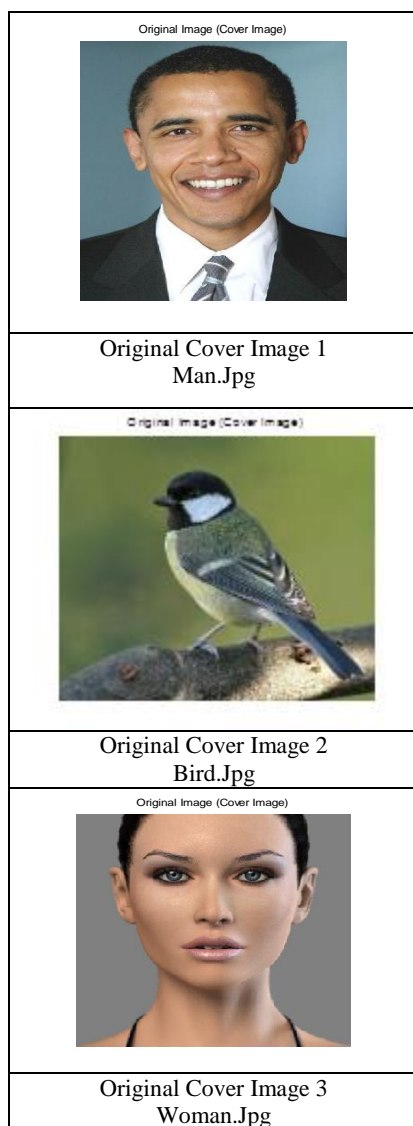


Figure 2(a). Cover Images.(300x300)

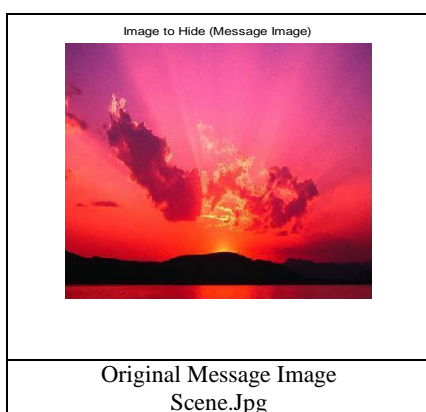






Figure 2(b). Message Image.(300x300)

So, in this case bits need not be replaced specifically. As per the range is encountered the bits of secret data are embedded unlike the usual LSB technique [17]. Its Mean squared error (MSE), Root mean squared error (RME) values are calculated for checking its efficiency in Table II [1-5]. MSE measures the average of the squares of the errors. The error is the amount by which the value implied by the estimator differs from the quantity to be estimated. The difference occurs

because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate.

Consider Figures 3, Figure 4, Figure 5.

Stego image	Stego image
	
MSE: 46.2320	MSE:10.1844
4 Bits Replaced	3 Bits Replaced
Stego image	Stego image
	
MSE:2.3690	MSE:0.8004
2 Bits Replaced	1 Bit Replaced

**Figure 3. Stego Images for basic LSB bit replacement
 Cover: Man.jpg, Message: Scene.jpg (300X300)**

We know that lower the MSE values, better is the quality of the stego image obtained Higher the value of PSNR better it is for the reconstruction of the image.

In Figure 3, the cover image used is man.jpg 300X300 in size and the message image used is scene.jpg 300X300 in size .Even though the differences between these images is not noticeable prominently ,its MSE values vary which is evident in Table I.

Similarly in Figure 4, the cover image used is woman.jpg 300X300 in size and the message image used is scene.jpg 300X300 in size .Even though the differences between these images is not noticeable prominently ,its MSE values vary which is evident in Table I.

Similar is the case for Figure 5. Wherein the cover image used is bird.jpg 300X300 in size and the message image used is scene.jpg 300X300 in size .





Stego image 	Stego image 
MSE:44.3828 4 Bits Replaced	MSE: 9.0706 3 Bits Replaced
Stego image 	Stego image 
MSE:2.0061 2 Bits Replaced	MSE: 37.1753 1 Bit Replaced

Figure 4. Stego images for basic LSB bit replacement
Cover: Woman.jpg ,Message:Scene.jpg(300X300)





Stego image 	Stego image 
MSE:0.3011 4 Bits Replaced	MSE:10.5129 3 Bits Replaced
Stego image 	Stego image 
MSE:2.5129 2 Bits Replaced	MSE:0.8691 1 Bit Replaced

Figure 5. Stego images for basic LSB bit replacement
Cover: Bird.jpg ,Message:Scene.jpg(300X300)

Even though the differences between these images are not noticeable prominently, its MSE values vary which is evident in Table I [12-15] . In this case when 4 bits are replaced it states that the 4 Most significant bit of the message image (Scene.jpg) are embedded in the 4 Least Significant bit of the respective cover images , in this manner it is difficult for an intruder to detect message hidden behind the cover image.





MSE : 0.1876

MSE:0.2028

MSE:0.4068

Figure6. Stego images for increased capacity of information hiding using advanced LSB method.

The replacement of bits such as 4,3,2,1 are smaller as compared to replacing bits like 6,7 since in the latter case the message is visible in the stego image itself. Figure 6 depicts the stego images for increased capacity of information hiding wherein the message and the cover images used are cited as above ,with their respective MSE values displayed. Consider Tables I & II ,Table I depicts the results for LSB Technique [12] by replacing 4,3,2,1 bits respectively and Table II depicts the Results for the technique for increased capacity of information hiding in LSB's method [1-5] .

It can be observed that the MSE values for stego images for the latter technique are better than the MSE values for the stego image of the former technique. Since we know that lower the MSE values, lesser is the error between the original cover image and the stego image as a result of which the message image is hidden successfully behind the cover image.

TABLE I
Results for LSB Technique by replacing 4,3,2,1 bits.

LSB	BITS	MSE	RME
A)Fig.3	4 Bits	46.2320	6.7994
	3 Bits	10.1844	3.1913
	2 Bits	2.3690	1.5392
	1 Bits	0.8004	0.8947
B)Fig.4	4 Bits	44.3828	6.6620
	3 Bits	9.0706	3.0117
	2 Bits	2.0061	1.4164
	1 Bits	0.3011	0.5487
C)Fig.5	4 Bits	37.1753	6.0972
	3 Bits	10.5129	3.2424
	2 Bits	2.5129	1.5852
	1 Bits	0.8691	0.9323

TABLE II
Results for The technique for increased capacity of information hiding in LSB's method.

Increased Capacity Technique	BITS	MSE	RME
A)Fig.3	1-4 Bits	0.1876	0.4331
B)Fig.4	1-4 Bits	0.2028	0.4503
C)Fig.5	1-4 Bits	0.4068	0.6378

TABLE III
Distinctive features of the advanced LSB methodology.

	Basic LSB	Advanced LSB
Error	High	Low
Stego Image	Poor quality	Good quality
Message retrieval	Poor	Good

5. CONCLUSION

After comparing and contrasting the Basic LSB technique with the advanced LSB methodology in Table III, we have come up with a conclusion which is as follows. As seen from TABLE I, the MSE (Mean squared error) Values for Figure 3, Figure 4, and Figure 5 are dramatically higher in comparison to the MSE values in TABLE II. The value for the basic LSB technique [15] for MSE ranges from 46.2320 to 37.1753 which illustrates that there is a high rate of mean squared error. Thus in this case the stego image and the original cover image display major differences in terms of their pixel values. On the contrary the MSE values for the advanced LSB methodology produces the required results which are within the range 0.1876 to 0.4068 and thus in this case the stego image and the original cover image do not vary drastically. This simply illustrates that the basic LSB technique [18-20] fails to match up to the level of its opponent technique in various parameters. The technique for increased capacity of information hiding in LSB's method [1] gives better performance in all the parameters i.e. MSE, RME. Thus the comparison between these two approaches simply illustrates that in order to hide the most significant bits (MSB) of the message image in the required Least significant bits (LSB) (4,3,2,1 bits) of the cover image and that the stego image be obtained efficiently i.e. it escape the human vision, and also the reconstruction of the image be done tactfully without any major flaws in the pixel values, the increased capacity of information hiding using the advanced LSB methodology [1] should be adopted in lieu of the basic LSB

technique. Since the main purpose of image hiding is to obtain a good reconstruction quality of the image i.e. retrieving the required message from the cover image for obtaining the secret information that travelled behind the cover image, the advanced LSB methodology gives better results.

Thus, in order to obtain the message image efficiently the recipient should use the advanced LSB technique described in the paper.

7. REFERENCES

- [1] Dr. H. B. Kekre, Ms. Archana A. Athawale, "Information Hiding using LSB Technique with Increased Capacity", International Journal of Cryptography and Security, Special issue on Steganography, 2008.(Accepted for publication).
- [2] H.C. Wu, N.I Wu, C.S. Tsai and M.S. Hwang, "Image Steganographic scheme based on pixel-value differencing and LSB replacement methods", VISIP(152), No. 5, October 2005
- [3] Johnson, Neil F, "Steganography", 2000.
- [4] J. Fridrich and M. Goljan, "Practical steganalysis of digital images— State of the art," in Proc. SPIE Security Watermarking Multimedia Contents, vol. 4675, E. J. Delp III and P. W. Wong, Eds., 2002, pp. 1–13.
- [5] N. Provos, "Defending Against Statistical Steganalysis", 10th USENIX Security Symposium, Washington, DC, 2001.
- [6] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," Lecture Notes in Computer Science, vol.1768, Springer-Verlag, Berlin, 2000, pp. 61–75.
- [7] W. Dixon, F. Massey: Introduction to Statistical Analysis. McGraw-Hill Book Company, Inc., New York 1957.
- [8] A. Ker, "Steganalysis of LSB Matching in Grayscale Images." IEEE Signal Processing Letters, vol. 12(6), 2005.
- [9] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen," IEEE Computer, pp. 26-34, Feb 1998.
- [10] X. Zhang and S. Wang, "Steganography using multiple-base notational system and human vision sensitivity," IEEE Signal Process. Lett., vol. 12, no. 1, pp. 67–70, Jan. 2005.
- [11] Petitcolas F, Anderson R, Kuhn M: 'Information Hiding – A Survey' Proceedings of the IEEE, Vol. 87. July 1999.
- [12] Neeta, D, "Implementation of LSB Steganography and Its Evaluation for Various Bits" Dept. of Computer. Sci.
- [13] V. Lokeswara Reddy, "Implementation of LSB Steganography and its Evaluation for Various File Formats" Department of CSE, K.S.R.M. College of Engg.,
- [14] B.Schneier, "Terrorists and Steganography", 24 Sep.01.
- [15] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001.
- [16] Niels Provos and Peter Honeyman, University of Michigan, "Hide and Seek: An Introduction to

- Steganography" Computer Society IEEE Security & Privacy.
- [17] Mamta Juneja, Parvinder S. Sandhu, and Ekta Walia "Application of LSB Based Steganographic Technique for 8-bit Color Images" World Academy of Science, Engineering and Technology 50 2009.
- [18] Eric Cole , "Hiding in Plain Sight: Steganography and the Art of Covert Communication"
- [19] Hiding data in images by simple LSB substitution, Chi-Kwong Chan*, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong.
- [20] Data Hiding in Images by Hybrid LSB Substitution Chin-Chen Chang Hsien-Wen Tseng ,Dept. of Inf. Eng. & Computer.Sci., Feng Chia Univ,Taiwan.