International Journal of Electronics Communication and Computer Engineering
Volume 3, Issue 1, ISSN 2249 –071X

Least Significant Bits Based Steganography Technique

Hardik J. Patel[1] and Preeti K. Dave[2]
1 Studying in Master of Engineering in Information Technology Department of Shantilal Shah Engineering College, Bhavnagar, Gujarat, India. Phone: +919427698772, e-mail: hardikpatel.growmore@ gmail.com.
2 Assistant Professor in Electronics and Communication Department of Shantilal Shah Engineering College, Bhavnagar, Gujarat, India. e-mail: preetidave@yahoo.com.

***Abstract* — The least significant-bit (LSB) based techniques are very popular for steganography in spatial domain. The LSB technique simply replaces the LSBs in the carrier media with bits from secret information. The embedding and retrieval of secret information depends on some of the required parameters. Hence separate transmission of such parameters adds security to the technique. The experimental results are evaluated for different images.**

***Index Terms* — LSB replacement, steganalysis, information security**

I. INTRODUCTION

Steganography is a technique of information security that hides secret information within a normal carrier media, such as digital image, audio, video, etc [1]-[3]. An unauthorized attempt to detect and extract the hidden secret information from stego is known as steganalysis. If any steganalytic algorithm can detect whether given media is a carrier then the steganographic algorithm is considered to be broken [4]-[5]. The important requirement for a good steganographic algorithm is that the stego media should remain identical to the original carrier media, while keeping embedding rate as high as possible. In this paper we consider digital image as carrier and develop a steganographic algorithm in a spatial domain.

The basic LSB based technique simply replaces the LSB plane of the carrier image with the bit stream of secret information. These methods are based on assumption that LSB plane of natural images is random enough, thus are suitable for data hiding [6]. Such assumption is not always true, especially for images with more smooth regions as shown in figure 1. It is easy to identify from the image and its 8 bit planes in figure 1, that bits are following certain pattern from higher to lower bit planes for smooth region of sky, while for mountain part the details are not distinguishable with naked eyes even in higher order bit planes [7].

A gray scale image consists of 8 bit planes. Each bit plane contains different types of details which when combined together form an image. MSB of an image consists of maximum details that are visible to human eyes, while LSB possess very fine details that naked eyes cannot distinguish properly. As shown in figure 1, the details in bit plane 1and 2 are not visible to naked eyes and from bit plane 3 onwards the visibility of details is increasing. As LSBs does not add much in the details visible to human eye, they can be removed to decrease the payload.

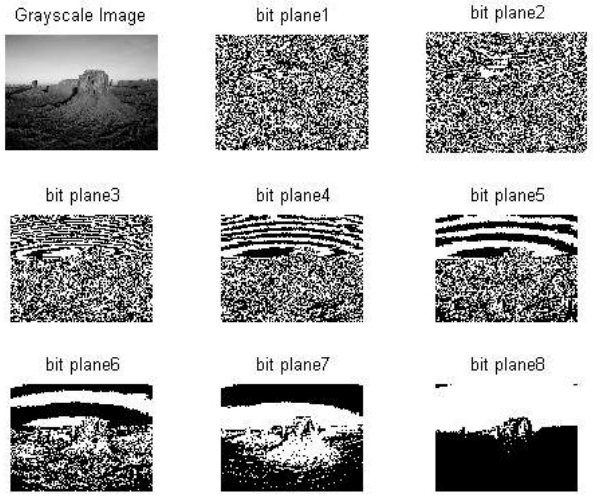


Figure 1: Different bit planes of a grayscale image

In this paper, we propose a technique based on Least Significant Bits replacement. The LSBs of carrier image are replaced by MSBs of the secret image. Number of LSBs per pixel in carrier image to be replaced can be 1, 2 or 4, based on payload available. The payload can be reduced by removing LSBs from secret image as in some case their presence or absence does not effects the visible details in given image.

Rest of the paper is arranged as follows. Section II gives details of embedding and retrieval of secret image. Section III presents experimental results and discussions. Finally, conclusion and future work are given in section IV.

II. PROPOSED METHOD

In this section, we first present a brief overview of the basic LSB based technique and then will give details for embedding and retrieval of secret image with example.

In this technique, the bits from secret image simply overwrite LSBs, i.e. maximum four least significant bits of the carrier image, while other higher order bit planes are preserved. Embedding data in higher bit planes may sometime results in visible artifacts in the stego image. It is only because of image contents and can be avoided by proper selection of carrier image.

Insertion and extraction of secret image is main part of any steganographic technique. Algorithm for embedding and retrieval of secret image along with two assumptions are given here.

A. *Assumptions*

(i) Both parties (sender & receiver) have agreed on set of carrier image to be used.

(ii) The means for exchanging required parameters is pre decided.

B. *Embedding Process*

Step 1: Select Carrier Image from the set.

Step 2: Traverse through each pixel in Carrier Image till end of Secret Image.

Step 2.1: Replace LSB(s) with bit(s) from Secret Image.

Step 3: Evaluate the Stego Image.

C. *Retrieval Process*

Step 1: Get the Stego Image.

Step 2: Traverse through each pixel in Stego Image till end.

Step 2.1: Extract LSB(s) from Stego Image.

Step 3: Get Estimate of Secret Image.

The parameters required on receiver side for retrieval of secret image from stego image are:

(i) Number of bits replaced in carrier image.

(ii) Number of bits stored for secret image data.

(iii)Size of Secret Image.

D. *Explanation with Example*

Consider the grayscale image has following pixel values and we want to insert the secret information 11001101 (one pixel data from secret image) in that carrier image.

The pixel values for carrier image along with its binary forms are shown in figure 2.

Pixel Values	
208	11010000
183	10110111
194	11000010
184	10111000
203	11001011
193	11000001
185	10111001
188	10111100

Figure 2: Part of carrier image containing 8 pixels

Replacing only 1 LSB in carrier image will give following stego image data.

i.e. Number of bits replaced in carrier image = 1

& Number of bits stored for secret image data = 8

Old Pixel Values		Secret Data	New Pixel Values	
208	11010000	1	1101000**1**	209
183	10110111	1	1011011**1**	183
194	11000010	0	1100001**0**	194
184	10111000	0	1011100**0**	184
203	11001011	1	1100101**1**	203
193	11000001	1	1100000**1**	193
185	10111001	0	1011100**0**	184
188	10111100	1	1011110**1**	189

Figure 3: Result after 1 LSB replacement

From data in figure 3, we can see that the ratio of change in bits to that remaining unchanged is small. So the variations in pixel values of given carrier image will be few and hence less detectable.

Replacing 2 LSBs in carrier image will give following stego image data.

i.e. Number of bits replaced in carrier image = 2

& Number of bits stored for secret image data = 8

Old Pixel Values		Secret Data	New Pixel Values	
208	11010000	11	1101001**11**	211
183	10110111	00	1011010**0**	180
194	11000010	11	1100001**11**	195
184	10111000	01	1011100**1**	185
203	11001011		11001011	203
193	11000001		11000001	193
185	10111001		10111001	185
188	10111100		10111101	188

Figure 4: Result after 2 LSBs replacement

Replacing 4 LSBs in carrier image will give following stego image data.

i.e. Number of bits replaced in carrier image = 4

& Number of bits stored for secret image data = 8

Old Pixel Values		Secret Data	New Pixel Values	
208	11010000	1100	1101**1100**	220
183	10110111	1101	1011**1101**	189
194	11000010		11000010	194
184	10111000		10111000	184
203	11001011		11001011	203
193	11000001		11000001	193
185	10111001		10111000	185
188	10111100		10111101	188

Figure 5: Result after 4 LSBs replacement

With above 3 different ways we can embed secret information in the given carrier image.

In the embedding techniques given above we have replaced LSBs of carrier image with bits from secret image, based on assumption that LSBs does not add much in visible data. Same is true for the secret image also and hence to reduce the payload we can remove LSBs from secret image. In case of our secret image data, we can remove the 4 LSBs (1110) at the max, and can reduce payload by 50%. The above 3 different embedding techniques will remain same with only one change in it, i.e.

Number of bits stored for secret image data = 4

The sender will send stego image and other required parameters separately through different means, mutually understood between two communicating parties well in advance. On receiver side the secret image can be extracted by giving stego image and other required parameters as input to the retrieval process.

Any attempt to extract secret data from the given stego image will have several possibilities and thus probability of guessing correct values for all the required parameters very less. So it is almost impossible to retrieve the secret image from the stego image without having access to required parameters.

III. Results And Discussion

In this section we will present some experimental results to demonstrate the effectiveness of our proposed technique. Different jpeg images of landscapes, people, plants, animals and buildings are first converted to grayscale and then used for the experiment.

E. Embedding Capacity

Embedding capacity is the property of carrier image to handle maximum possible payload still preserving its visual features.

In our proposed technique the embedding capacity is more with replacement of 4 LSBs and is reduced by 50% with 2 LSBs replacement and again reduced by 50% with only 1 LSB replacement. The table I shows the embedding capacity with different number of bits used for storing the secret data for same carrier image.

Table I: Embedding capacity for same carrier image with different number of bits being replaced

Size of Carrier Image	Number of bits to be replaced	Embedding Capacity
1024 x 1024	1	1048576 bits
1024 x 1024	2	2097152 bits
1024 x 1024	4	4194304 bits

F. Image quality

The figures 6 and 7 shows original carrier image and respective stego image along with their first LSB plane for 1 LSB replacement technique and figures 8 and 9 for 2 LSBs replacement. Here we can identify some variations in smooth region of carrier image.

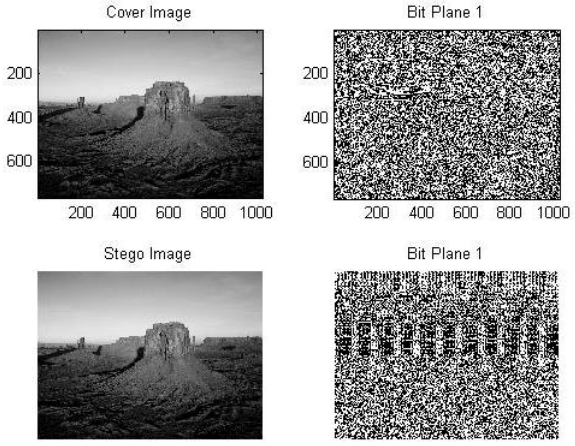


Figure 6: Image having more details before and after data embedding in LSB

The brightness of stego image is more than that of carrier image. As seen in section II replacing LSBs in the carrier image with secret data results in increase of pixel values. For grayscale image pixel value ranges from 0 to 255. The pixel value 0 denotes black color while the pixel value 255 denotes white color. Hence increase in pixel value means moving from black to white color which results in increase of brightness of stego image.

Such evaluation is possible only when we have access to original carrier image as well as the stego image.

In figure 7, carrier image contains more smooth regions then that of regions with more details. Hence it is more prone even to minor changes. The LSB plane of an image is shown before and after embedding. The variations in LSB plane are higher compared to the changes found with the previous image. The bit pattern in LSB plane is totally modified due to data embedding and hence the image can be easily identified as a carrier image even in absence of the original carrier image.

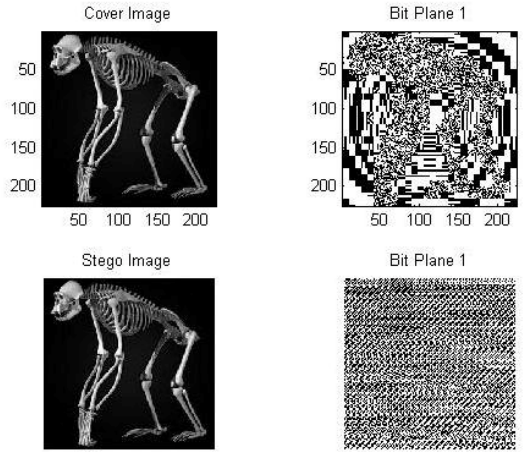


Figure 7: Image with more smooth regions before and after embedding in LSB

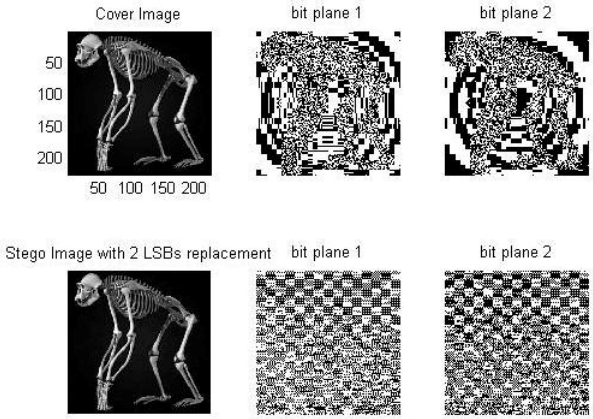


Figure 8: Carrier image before and after embedding in 2 LSBs

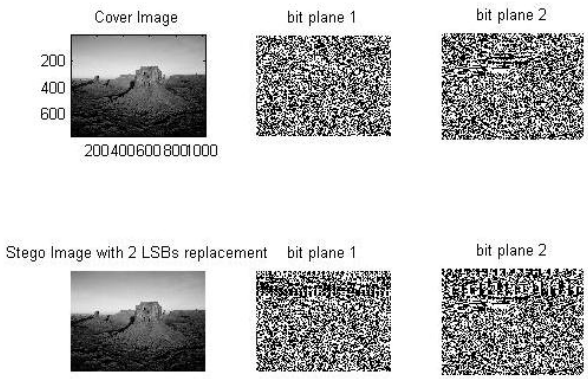


Figure 9: Carrier image before and after embedding in 2 LSBs

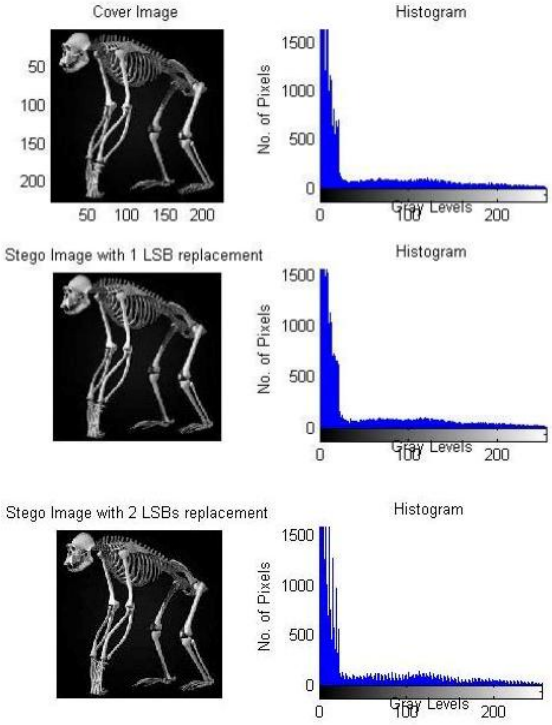
G. *Visual analysis*

Visually the stego image should be identical to the original image. Embedding data in the image may result in some visible artifacts, which is not a good sign and shows the weakness of the algorithm.

A stego image that can be identified as a carrier of some secret data only through naked eye examination is not a good result. But variations in LSBs are difficult to identify with naked eyes, as the details in lower bits planes does not add much to the visible details and hence stegos with LSB replacement can pass safely through visual analysis.

H. *Statistical analysis*

Visual features are easy to preserve but preservation of statistical features is a bit tough job and requires proper care while designing a good steganographic algorithm.



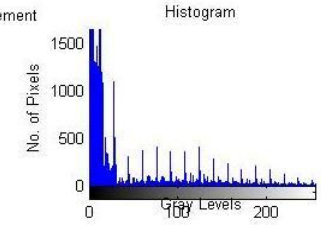


Figure 10: Image and histogram for 1, 2 and 4 LSBs replacement

One of the statistical features is the histogram of the image. The histogram is a plot of gray levels versus number of pixels in the given image. The bit replacement technique changes the pixel value directly and hence affects its histogram also.

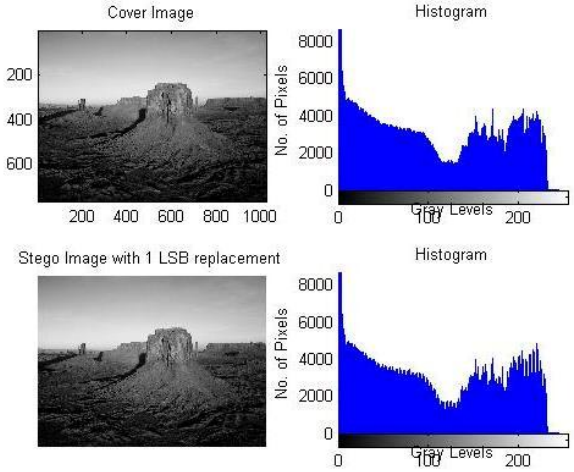
For an image most of the pixel value increases after data embedding and hence the histogram of a stego image will be more concentrated towards brighter side. If number of pixels with increasing value is equal to the number of pixels with decreasing value then the resulting histogram will be balanced.

The resultant image along with its histogram is shown here in figure 10 and 11. The analysis shows that the variation in histogram increases with increase in embedded data.

In histograms shown here, the density of pixels goes on increasing towards brighter side with increase in data bits embedded in the carrier image.

Minor variation in the histogram is not easy to identify without comparing it with original image histogram and hence the bit embedding in 1 or 2 LSBs can go undetected I absence of access to the original carrier image.

The effects on statistical features of the carrier image are based on the contents of the secret image and hence the results are shown here in figure 12, 13 and 14 for different secret image embedded in the same carrier and with 2 LSBs replacement technique.



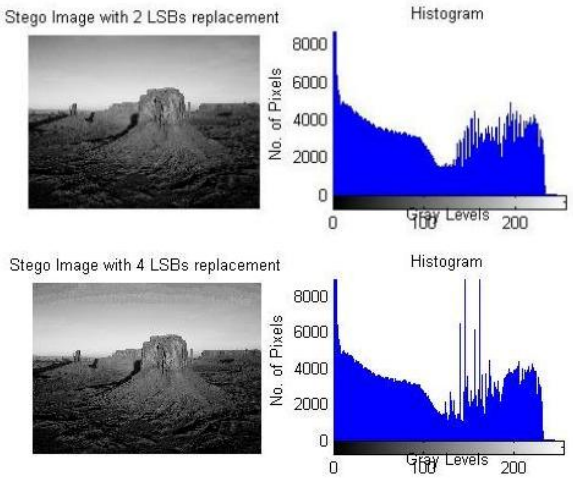


Figure 11: Image and histogram for 1, 2 and 4 LSBs replacement

IV. CONCLUSION

In this paper, LSB based steganographic technique in spatial domain is studied. The 1 LSB replacement technique is providing good results but have very less embedding capacity (Table I) and hence is not feasible every time particularly in case of high payload available. The 4 LSBs replacement technique has high embedding capacity but with complement of statistical and sometimes visible features.

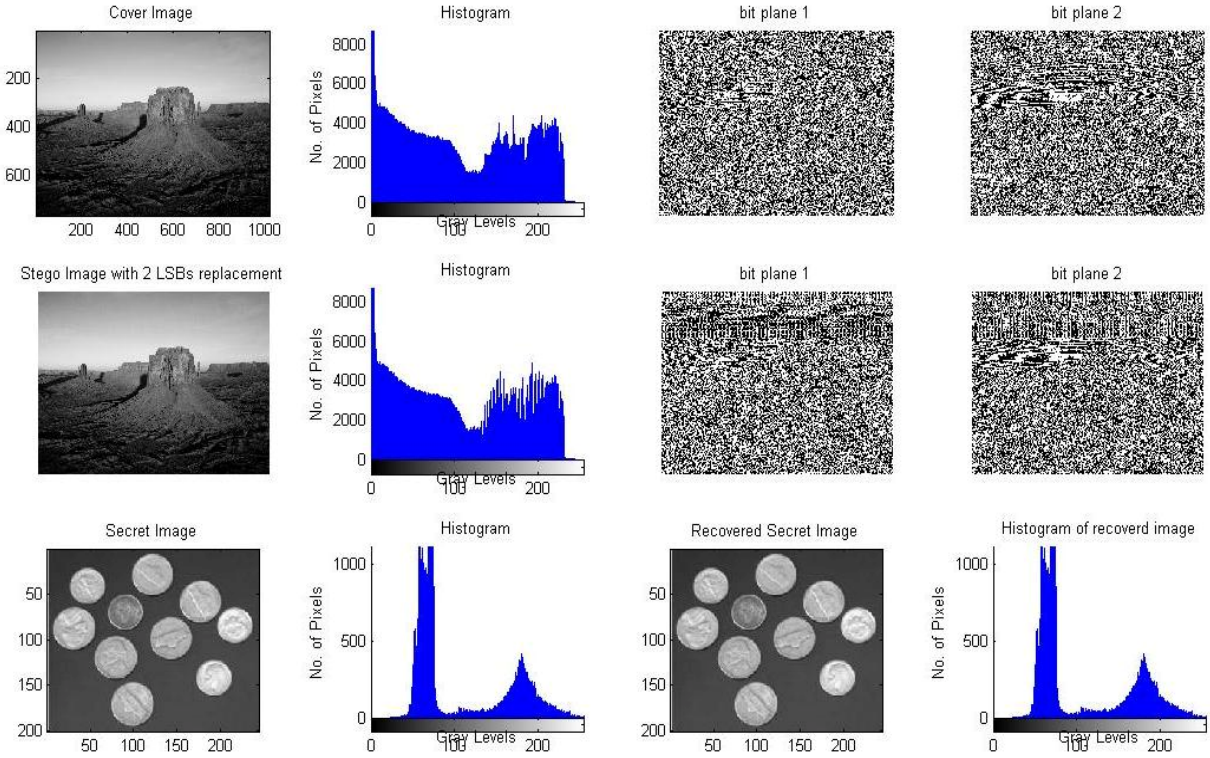


Figure 12: Effect of secret image on the carrier image

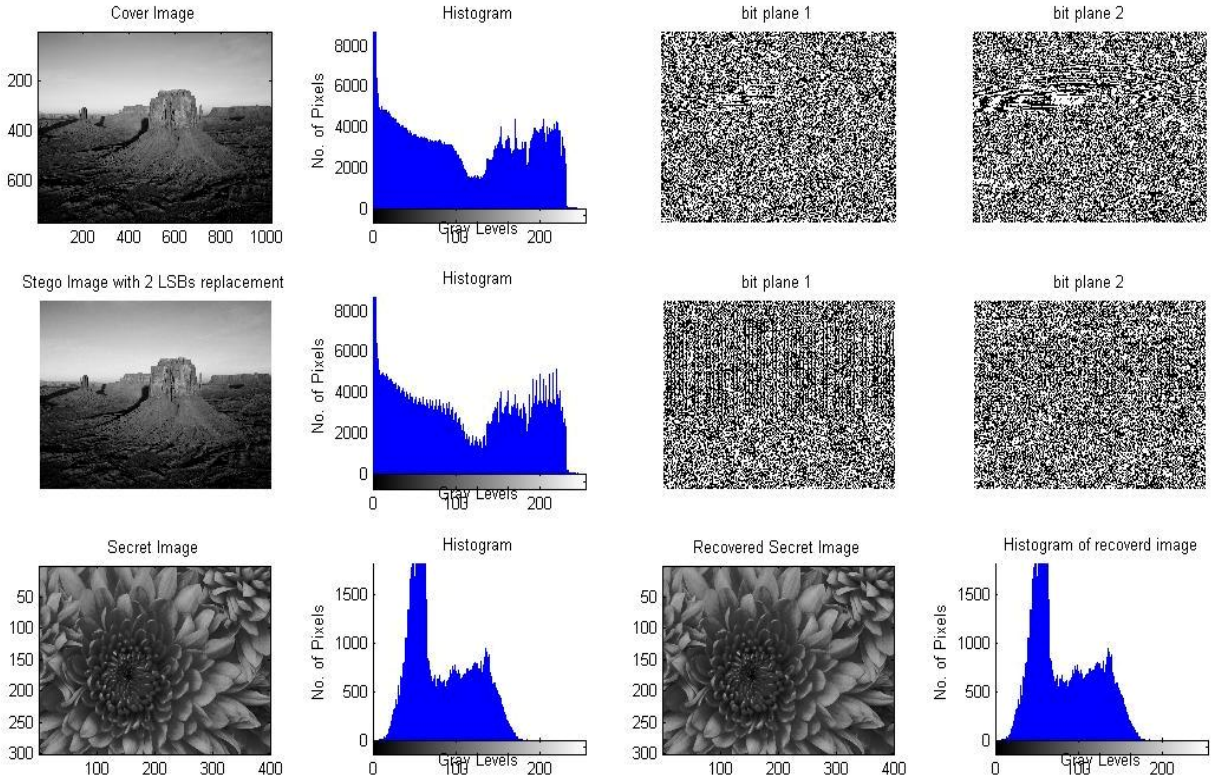


Figure 13: Effect of secret image on the carrier image

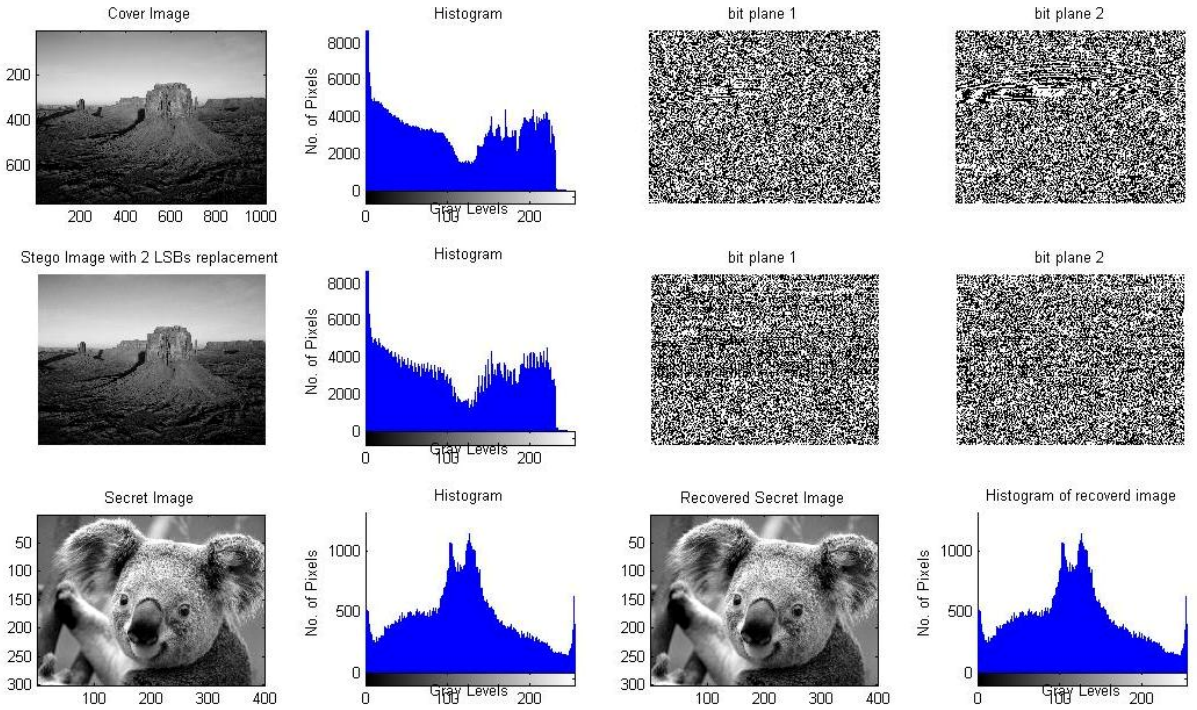


Figure 14: Effect of secret image on the carrier image

The 2 LSBs replacement technique is good enough compared to both previous techniques. It provides better payload capacity along with preservation of visual and statistical features. Hence the selection of technique can be based on the user's payload to be embedded. Appropriate technique can be used each time the data has to be transmitted secretly.

The strength of proposed technique lies in secrecy of parameters that are transmitted separately. Without knowledge of these parameters it is not possible to extract the hidden secret image from given stego image. The possibilities of probable arrangement with given stego image are high and hence probability of assuming correct values for required parameters and thus getting correct arrangement is very less. The steganalysis methods will result in random and inappropriate data which is difficult to arrange in proper and correct format.

Further the technique can be extended for different types of carrier media such as color image, audio, video etc.

REFERENCES

[1] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security and Privacy, pp 32-44, Mar 2003.
[2] Neil F. Johnson and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE computer, pp 26-34, Feb 1998.
[3] G. C. Kesseler, "Steganography: Hiding Data within Data," an edited version of this paper with the title "Hiding Data in Data," originally appeared in the April 2002 issue of Windows & .NET magazine. Sep 2001.
[4] N. F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software." In Aucsmith, pp 273-289.
[5] Gary C. Kessler, "An Overview of Steganography for the Computer Forensics Examiner," issue of Forensic Science Communications, Jul 2004.
[6] Fabien A. P. Petitcolas, Ross J. Anderson and Markus G. Kuhn, "Information Hiding-A Survey," IEEE, special issue on protection of multimedia content, pp 1062-1078, Jul 1999.
[7] Mitchell D. Swanson, Bin Zhu and Ahmed H. TewfikB, "Robust Data Hiding for Images," IEEE Digital Signal Processing Workshop, pp37-40, Sep 1996.

AUTHOR'S PROFILE

Hardik Patel
received the B.E. in Information Technology degree from Mumbai University, India in 2005.
He is currently a Master of Engineering student in Shantilal Shah Engineering College, Bhavnagar, Gujarat, India. His research interests include Digital Forensics, Cryptography, Steganography and Steganalysis.

.

Prof. Preeti Dave
received the M.E. in Microprocessor degree from M.S. University, Baroda, India.
She is working as Assistant Professor in Electronics and communication department of Shantilal Shah Engineering College, Bhavnagar, Gujarat, India. Her area of interest includes Digital Image Processing, Television Engineering and Analog Electronics.