



# A STEGANOGRAPHY ALGORITHM FOR HIDING IMAGE IN IMAGE BY IMPROVED LSB SUBSTITUTION BY MINIMIZE DETECTION

<sup>1</sup>VIJAY KUMAR SHARMA, <sup>2</sup>VISHAL SHRIVASTAVA

<sup>1</sup>M.Tech. scholar, Arya college of Engineering & IT, Jaipur, Rajasthan (India)

<sup>2</sup> Associate Professor Arya college of Engineering & IT, Jaipur, Rajasthan (India)

<sup>1</sup>Email: [vijaymayankmudgal2008@gmail.com](mailto:vijaymayankmudgal2008@gmail.com), <sup>2</sup> [vishal500371@yahoo.co.in](mailto:vishal500371@yahoo.co.in)

## ABSTRACT

Steganography is a branch of information hiding. It allows the people to communicate secretly. As increasingly more material becomes available electronically, the influence of steganography on our lives will continue to grow. Many confidential information were leaked to a rival firm using steganographic tools that hid the information in music and picture files. The application of steganography is an important motivation for feature selection. In recent years, many successful steganography methods have been proposed. They challenge by steganalysis. Steganalysis (type of attack on steganography Algorithm) Algorithm which detects the stego-message by the statistic analysis of pixel values[1][2], To ensure the security against the steganalysis attack, a new steganographic algorithm for 8bit(ayscale) or 24 bit (colour image) is presented in this paper, based on Logical operation. Algorithm embedded MSB of secret image in to LSB of cover image. in this n LSB of cover image, from a byte is replaced by n MSB of secret image. the image quality of the stego-image can be greatly improved with low extra computational complexity. The worst case mean-square-error between the stego-image and the cover-image is derived. Experimental results show that the stego-image is visually indistinguishable from the original cover-image when  $n \leq 4$ , because of better PSNR which is achieved by this technique.

It comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to cover up the very existence of the embedded data.

**Keywords**— *LSB Steganography, MSB, PSNR, Logic Gate.*

## 1. INTRODUCTION

Steganography is the art of passing information through original files in a manner that the existence of the message is unknown. The term steganography is arrived from Greek word means, "Covered Writing". The innocent files can be referred to as cover text, cover image, or cover audio as appropriate. After embedding the secret message it is referred to as stego-medium. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. While cryptography is about protecting the content of messages (their meaning), steganography is about hiding the message so that intermediate persons cannot see the message. Steganography refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. Images can be more than what we see

with our Human Visual System (HVS); hence, they can convey more than merely 1000 words.

## 2. LITERATURE REVIEW

### 2.1 The Scope Of Steganography

With the boost in computer power, the internet and with the development of digital signal processing (DSP), information theory and coding theory, steganography has gone "digital". In the realm of this digital world, steganography has created an atmosphere of corporate vigilance that has spawned various interesting applications, thus its continuing evolution is guaranteed. Cyber-crime is believed to benefit from this digital revolution. Hence an immediate concern is to find out best possible attacks to carry out steganalysis, and simultaneously, finding out techniques to strengthen existing steganography techniques against popular attacks like steganalysis.



**2.2 Cryptography**

Cryptography encodes information in such a way that nobody can read it, except the person who holds the key. More advanced crypto techniques ensure that the information being transmitted has not been modified in transit. There is some difference in cryptography and steganography, in cryptography the hidden message is always visible, because information is in plain text form but in steganography hidden message is invisible.

**2.3 Steganography Versus Cryptography**

The comparison and contrast between steganography and cryptography is illustrated from the following table 2.1.

S.no.	Context	Steganography	Cryptography
1	Host Files	Image, Audio, Text, etc.	Mostly Text Files
2	Hidden Files	Image, Audio, Text, etc.	Mostly Text Files
3	Result	Stego File	Cipher Text
4	Type of Attack	Steganalysis: Analysis of a file with a objective of finding whether it is stego file or not.	Cryptanalysis

Table 2.1 Comparison and contrast between steganography and cryptography

**2.4 Steganalysis**

Steganalysis is a relatively new research discipline with few articles appearing before the late-1990s. Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes" [6]. It is the art of discovering and rendering useless covert messages. The goal of steganalysis is to identify suspected information

streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information.

The challenge of steganalysis is that:

1. The suspect information stream, such as a signal or a file, may or may not have hidden data encoded into them.
2. The hidden data, if any, may have been encrypted before being inserted into the signal or file.
3. Some of the suspect signal or file may have noise or irrelevant data encoded into them (which can make analysis very time consuming).
4. Unless it is possible to fully recover, decrypt and inspect the hidden data, often one has only a suspect information stream and cannot be sure that it is being used for transporting secret information.

**2.5 Types Of Attacks**

Attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling, destroying or modifying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography-based information streams). The possible attacks on a stego media can be one of the following:

1. Steganography-only attack: Only the steganography medium is available for analysis.
2. Known-carrier attack: The carrier, that is, the original cover, and steganography media are both available for analysis.
3. Known-message attack: The hidden message is known.
4. Chosen-steganography attack: The steganography medium and tool (or algorithm) are both known.
5. Chosen-message attack: A known message and steganography tool (or algorithm) are used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms.

6. Known-steganography attack: The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

## 2.6 Least Significant Bit Substitution

In LSB steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography techniques is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bit grayscale bitmap image where each pixel is stored as a byte representing a grayscale value. Suppose the first eight pixels of the original image have the following grayscale values:

11010010

01001010

10010111

10001100

00010101

01010111

00100110

01000011

To hide the letter C whose binary value is 10000011, we would replace the LSBs of these pixels to have the following new grayscale values:

11010011

01001010

10010110

10001100

00010100

01010110

00100111

01000011.

Note that, on average, only half the LSBs need to change. The difference between the cover (i.e. original) image and the stego image will be hardly noticeable to the human eye. Figure 2.1(a), (b) that show a cover image and a stego image (with data is embedded); there is no visible difference between the two images.

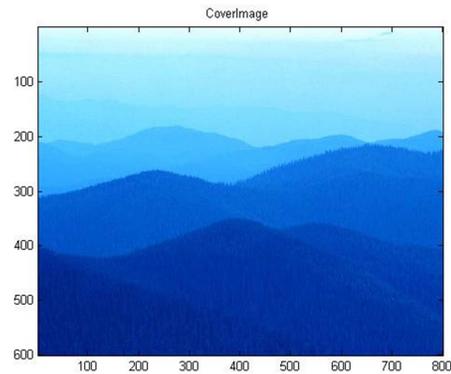


Fig: 2.1 (a) Cover Image

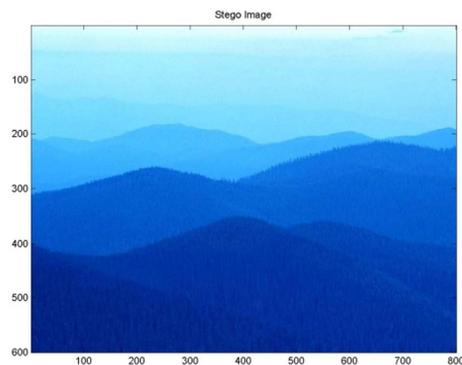


Fig: 2.1 (b) Stego Image

LSB steganography, as described above, replaces the LSBs of data values to match bits of the message. It can equally alter the data value by a small amount, ensuring the a legal range of data values is preserved. The difference being that the choice of whether to add or subtract one from the cover image pixel is random. This will have the same effect as LSB replacement in terms of not being able to perceive the existence of the hidden message. This steganographic technique is called LSB matching. Both LSB replacement and LSB matching leave the LSB unchanged if the message bit matches the LSB. When the message bit does not match the LSB, LSB replacement replaces the LSB with the message bit; LSB matching randomly increments or decrements the data value by one. LSB matching is also known as  $\pm 1$  embedding.

In the case of still grayscale images of type bitmap, every pixel is represented using 8 bits, with 11111111 (=255) representing white and 00000000 (=0) representing black. Thus, there

are 256 different grayscale shades between black and white which are used in grayscale bitmap images. In LSB steganography, the LSB's of the cover image is to be changed. As the message bit to be substituted in the LSB position of the cover image is either 0 or 1, one can state without any loss of generality that the LSB's of about 50 percent pixel changes.

There are three possibilities [3]:

1. Intensity value of any pixel remains unchanged.
2. Even value can change to next higher odd value

Odd Value change to previous lower even value

### 3 MATERIALS AND METHODS

#### 3.1 First Component Alteration Technique For Image Steganography

In the technique, a new image steganography scheme based on first component Alteration technique is introduced. In a computer, images are represented as arrays of values. These values represent the intensities of the three colors R (Red), G (Green) and B (Blue), where a value for each of three colors describes a pixel. Each pixel is combination of three components(R,G and B).

In this scheme, the bits of first component (blue component) of pixels of image have been replaced with data bits, which are applied only when valid key is used. Blue channel is selected because a research was conducted by Hecht, which reveals that the visual perception of intensely blue objects is less distinct than the perception of objects of red and green.

For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels are:

```
(00100111 11101001 11001000) (00100111
1100100011101001)
```

```
(11001000 00100111 11101001)
```

A steganographic program could hide the letter "A" which has a position 65 into ASCII character set and have a binary representation "01000001", by altering the blue channel bits of pixels.

```
(01000001 11101001 11001000) (00100111
1100100011101000)
```

```
(11001000 00100111 11101001)
```

A. Embedding phase

The embedding process is as follows.

Inputs: Image file and the text file

Output: Text embedded image

Procedure:

Step 1: Extract all the pixels in the given image and store it in the array called Pixel-array.

Step 2: Extract all the characters in the given text file and store it in the array called Character-array.

Step 3: Extract all the characters from the Stego key and store it in the array called Key- array.

Step 4: Choose first pixel and pick characters from Key- array and place it in first component of pixel. If there are more characters in Key-array, then place rest in the first

component of next pixels, otherwise follow Step (e).

Step 5: Place some terminating symbol to indicate end of the key. '0' has been used as a terminating symbol in this algorithm.

Step 6: Place characters of Character- Array in each first component (blue channel) of next pixels by replacing it.

Step 7: Repeat step 6 till all the characters has been embedded.

Step 8: Again place some terminating symbol to indicate end of data.

Step 9: Obtained image will hide all the characters that input.

B. Extraction phase

The extraction process is as follows.

Inputs: Embedded image file

Output: Secret text message

Procedure:

Step 1: Consider three arrays. Let they be Character-Array, Key-array and Pixel-array.

Step 2: Extract all the pixels in the given image and store it in the array called Pixel-array.

Step 3: Now, start scanning pixels from first pixel and extract key characters from first (blue) component of the pixels and place it in Key-array. Follow Step3 up to terminating symbol, otherwise follow step 4.

Step 4: If this extracted key matches with the key entered by the receiver, then follow Step 5, otherwise terminate the program by displaying message “Key is not matching”.

Step 5: If the key is valid, then again start scanning next pixels and extract secret message characters from first (blue) component of next pixels and place it in Character array. Follow Step 5 till up to terminating symbol, otherwise follow step 6.

Step 6: Extract secret message from Character-array.

The primary motivation of the current work is to increase PSNR.

For this purpose we employ the approach which hide secret image in to cover image with the help of logic gates

**Algorithm:**

Step1: Read the image to be embedded

Step 2: Read the image inside which message is embed

Step 3: set numSignificantBits = n ; where n= 1,2,.....8

Step 4. size1 = size(secret); and size2 = size(coverImage);

Step 5. set the "numSignificantBits"n significant bits of each byte of cover image to zero by using bit by AND operation on cover and size1 matrix

Step 6. embedd the "numSignificantBits" most significant bits of secret image to create the stego image by using  $stego = (cover \text{ zero} + secret) / 2^{8-n}$

Step 7. recover the embedded image, by using bit by shift operation

Step 8. Display Figure of cover image, Image to be hidden, stego image and recover image

Step 9. End

Note :- as the value of n will be increase the quality of stego and recover image will be degraded.

The proposed method is applicable for both 24 bit color and 8 bit gray image. So the conversion

of 24 bit color image to 8 bit grayscale image is done as follow:

**3.2 Conversion Of Color Image Into Greyscale Image**

Conversion of a color image to grayscale can be done using several approaches. Different weighting of the primary colors effectively represent the effect of obtaining black-and-white image with color images. A common strategy is to match the luminance of the grayscale image to the luminance of the color image

The proposed method is baled both 24 bit color and 8 bit gray image

To convert any color to a grayscale representation[4][5] of its luminance, first one must obtain the values of its red, green, and blue (RGB) primaries in linear intensity encoding, by gamma expansion. Then, add together 30% of the red value, 59% of the green value, and 11% of the blue value(these weights depend on the exact choice of the RGB primaries, but are typical). Regardless of the scale employed (0.0 to 1.0, 0 to 255, 0% to 100%, etc.), the resultant number is the desired linear luminance value; it typically needs to be gamma compressed to get back to a conventional grayscale representation.

To convert a gray intensity value to RGB, simply set all the three primary color components red, green and blue to the gray value, correcting to a different gamma if necessary. The method adopted in current work for experimental evaluation is to obtain the RGB values of individual pixels and to take the average to be normalized to fit in the scale 0 to 255.

The 8 bit grayscale color palette is as shown in the figure3.1 below.

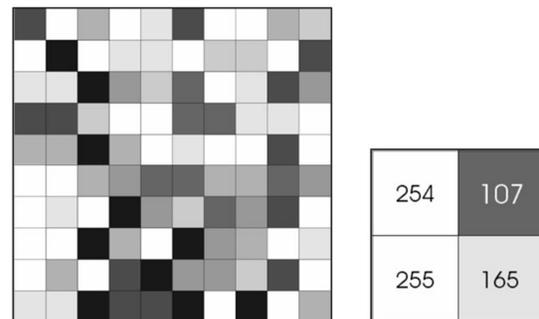


Fig. 3.1 8 Bit Greyscale Color Palette

3.3 RESULTS AND DISCUSSIONS

Table:3.1 Experimental result, change PSNR with n

n	1	2	3
PSNR	46.65	< 46.65	<< 46.65

PSNR of the obtained stego-image can be computed by

$$PSNR_{worst} = 20 \times \log_{10}(255/MSE)_{dB} \quad (3.1)$$

Table 3.1 tabulates the PSNR for some n= 1 to 3. It could be seen that the image quality of the stego-image is degraded drastically when n ≥ 3.

The results are then compared with various steganography methods as shown in the following table 3.1[2]. In current work more pixel values is change because the simple LSB replacement depends upon size of image. Comparative study of previous method and improved LSB substitution method is shown below:

Lena image	LSB3	Jae Gilyu	First component alteration technique	Improved LSB
PSNR	37.92	38.98	46.11	46.65

Table:3.2. Comparative study of various methods with proposed Technique



Fig 3.2: Lena Cover Image

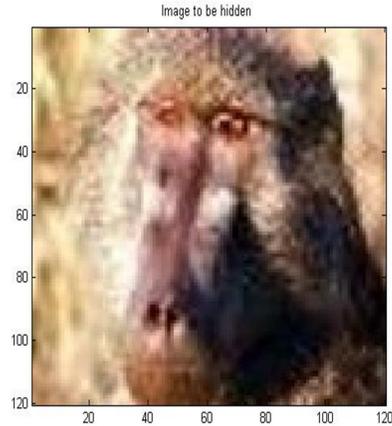


Fig 3.3: Baboon Secret image



Fig 3.4: Lena Stego image

Experimental result had shown the strength of this technique as compare to other special domain techniques[2]. For this we embedded the data in original image and get stego image. The PSNR(Peak Signal to Noise Ratio) of stego-image is calculated and compared previous work

Comparative result in table 3.2 shown that the PSNR will increase in proposed work so there is no difference in visible quality of cover (original) image and stego image. Proposed work is done with the help of MAT Lab. In previous work named as first component alteration technique, PSNR is obtained 46.11. But in proposed work the PSNR is obtained more than the previous work at the value of n=1 for small size of image. Proposed algorithm has some extra feature, which is as follow:



1. The method is applicable for both grayscale (8 bit) or color image(24 bit).
2. The same size of original image and secret image is embedded. So there is better PSNR for 100% of data embedding .

#### 4 CONCLUSION

In this a data hiding method by improved LSB substitution process is proposed. The image quality of the stego-image can be greatly improved with low extra computational complexity. Experimental result show the effectiveness of the proposed method. The results obtained also show significant improvement in PSNR than the method proposed in Ref. [2] with respect to image quality and computational efficiency.

A good balance between the security and the image quality is achieved. Our future work will focus on improving the efficiency of the proposed algorithm.

The algorithm proposed in the current work describes a method such that the stego image which is obtained thereby cannot be proved as stego image using the steganalysis approach. In the proposed algorithm, the the number of steps are very less. Thus, the computational complexity is reduced. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both grayscale and color image. Benefited from the effective optimization, a good balance between the security and the image quality is achieved. The future work will focus on improving the efficiency of the proposed algorithm.

#### REFERENCES:

- [1] J. Fridrich, Multimedia Security Technologies for Digital Rights Management. Academic Press, 2006, ch. Steganalysis, pp. 349–381. J. Fridrich, R. Du, and M. Long, “Steganalysis of LSB encoding in color images,” in Proceedings of the IEEE International Conference on Multimedia and Expo. New York, USA: IEEE Computer Society Press, 2000.
- [2] Amanpreet Kaur<sup>1</sup>, Renu Dhir<sup>2</sup>, and Geeta Sikka<sup>3</sup> .A New Image Steganography Based On First Component Alteration Technique(

- (IJCSIS) International Journal of Computer Science and Information Security, Vol. 6, No. 3, 2009)
- [3] J. Fridrich, R. Du, and L. Meng, “Steganalysis of LSB Encoding in Color Images,” Proc. IEEE Int’l Conf. Multimedia and Expo, CD-ROM, IEEE Press, Piscataway, N.J., 2000.
- [4] Finlayson, G. D., Qiu, G., Qiu, M., Contrast Maximizing and Brightness Preserving Color to Grayscale Image Conversion, 1999.
- [5] Tarun Kumar, Karun Verma, “A Theory Based on Conversion of RGB image to Gray image”, International Journal of Computer Applications Volume 7– No.2, September 2010.
- [6] Arvind Kumar, Km. Pooja, “Steganography- A Data Hiding Technique” International Journal of Computer Applications ISSN 0975 – 8887, Volume 9– No.7, November 2010.

**AUTHOR PROFILES:**



**Vijay Kumar Sharma**

received the B.E. degree in computer science & engineering from Rajasthan University, in 2005. He is a M.Tech. student of Arya college of Engineering & IT,

Affiliated by Rajasthan Technical University,INDIA. His interests are in Information system security.



**Vishal Shrivastava**

received the computer science & engineering. degree in computer science & engineering from the MPTU. He received the M.Tech. degree in computer engineering from the MPTU.

Currently, he is a Associate professor at Arya college of Engineering & IT, Affiliated by Rajasthan Technical University,INDIA. His research interests include Network security.