Analysis of Random Bit Image Steganography Techniques

Dipesh Agrawal
IT Department
NRI IST, Bhopal

Samidha Diwedi Sharma , Ph.D
Professor & Head IT Department,
NRI IST, Bhopal

ABSTRACT
Steganography is an art of hiding information in some media. This paper describes various image Steganography techniques, based on spatial domain and by considering pixel values in binary format. Spatial domain is based on physical location of pixels in an image. Generally 8 bit gray level or color images can be used as a cover to hide data. Again binary representations of these pixels are considered to hide secret information. Random bits from these bytes are used to replace the bits of secret. In this paper, many steganography techniques can be used like Least Significant Bit (LSB), layout management schemes, replacing only 1's or only zero's from lower nibble from the byte are considered for hiding secret message in an image. Along with these techniques, some more methods are proposed. By considering many parameters of an image are considered like physical location of pixels, intensity value of pixel, etc.

General Terms
Steganography, LSB, Raster Scan, Random scan, Layout Management

Keywords
LSB Steganography, intensity value of a pixel, physical location of a pixel.

1. INTRODUCTION
There are many mechanisms through which a secret data can be secured while transmitting it from source to destination through a connected media or disconnected media.

Three basic techniques are used for securing information –

Cryptography, Steganography and Watermarking
Cryptography secures the data by scrambling it using available techniques and algorithms. In this original data gets changed while at source and it is again converted into its original format at destination. Steganography is a technique of hiding secret information in any of media like – image, text, audio and video. Message to be hidden is concealed in another file called cover media. Combination of secret message and cover file is called as – stego. Which is sent over the network from source to destination [1].

Digital Watermarking describes methods and technologies that hide information, for example a number or text, in digital media, such as images, video or audio. The embedding takes place by manipulating the content of the digital data, which means the information is not embedded in the frame around the data. The hiding process has to be such that the modifications of the media are imperceptible. For images this means that the modifications of the pixel values have to be invisible.

In steganography. data can be hidden in pixels of an image.

A pixel has some integer value, based on the intensity of color that is displayed by a pixel. This integer value can be converted into binary format, i.e. in the form of bytes of 1's and 0's. individual bits from these bytes can be used to hide secret information. These bits can be selected randomly from a byte and replaced with a secret data. Pixels in which data is to be hidden are also selected randomly, from an image.

Thus, pixels used for data hiding can be selected using various algorithms and techniques, described in this paper are – Layout management schemes [2]. Also, bits from each selected pixel can chosen randomly using some algorithms, like LSB. This paper proposes new methods for selection of pixels from an image, randomly for hiding secret data. Also some techniques are proposed to select bits randomly from the bytes which represent pixels of an image

2. RELATED WORK

There are many techniques existed for random bit steganography in spatial domain. Like – Least Bit Significant Bit (LSB), Replacing only 1's or 0's, Layout Management Techniques etc. We will see each technique in detail.

2.1 Least Significant Bit (LSB)

This is a simplest and oldest technique used for steganography. Secret information is hidden into least significant bits of a byte, which represents an intensity value of a pixel [3]. We can use only LSB or last two, three or four LSBs, according to amount of data to be hidden and according to the importance of the secret data and also depending on the type of cover image and frequency of the pixels used in an image. So best LSB steganography algorithm can be designed by considering above parameters of a cover image and secret information to be hidden.

2.2 Layout Management Schemes
Another approach can be, to consider layout of pixels from an image in various ways, and according to the logical sequence of pixels, data can be hidden in the LSBs, up to four positions at max [2].

Pixels can be considered in any sequence like, starting from centre position and coming outside in a rectangular way. Similarly, starting from outer pixel, going towards the centre in a rectangular way. This approach is shown in figure given below.

Another approach is, consider pixels in snake movement, diagonal movement, starting from top left or top right

or bottom left or bottom right.

Like this, there are so many ways through which we can select pixels according to their physical location and making a logical connection between them, to hide secret information, in a random bit fashion.

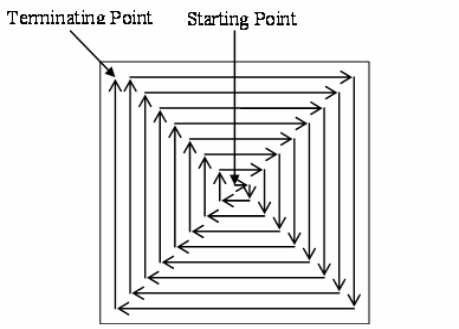

Fig. 1: Logical sequence of pixels from centre to outer side

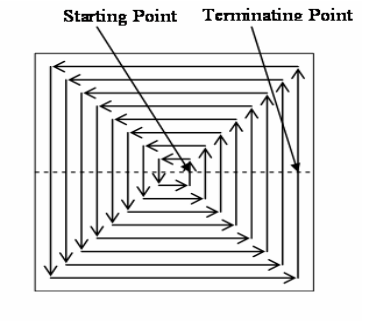

Fig. 2: Logical sequence of pixels towards centre from outer side

2.3 Replacing only 1's or 0's from a Byte

In this technique, only 1's or 0's from a byte are considered

and they are replaced by bits of a secret data. Either only 1's can be used or only 0's can be used from a cover image, to replace bits of secret information to be hidden. This can be a dynamic way to hide secret information in a cover image [4].

3. PROPOSED WORK

In our work, we proposed following methods of hiding data based on random bits of random pixel positions of an image.

3.1 Replacing Intermediate Bit

Using this technique, any bit or any intermediate bit from a given byte (of a pixel value) can be replaced by the bit of a data to be hidden. For ex. Original data is –

Table 1. Cover data

10101110	00011101	11001101	11110001
01010100	11101111	10110001	10101000

LSB to MSB position. Observe table below.

Table 2. Cover data + Secret data = STEGO

101<u>1</u>1110	**0001111<u>1</u>**	**11<u>0</u>01101**	**1110<u>0</u>001**
5th Bit	2nd Bit	6th Bit	4th Bit
01011100	**11101111**	**10100001**	**10101010**
4th Bit	3rd Bit	5th Bit	2nd Bit

Underlined bits shows the bits of secret message are replaced with the bits of original data at that position

3.2 Raster Scan Principle

This method is similar to Raster Scan principle of displaying an image on CRT display. In this, pixels from alternate horizontal lines are used for replacing the secret information. A simple LSB scheme can be used for pixels of first horizontal line. Then second line is skipped. Again third line is used to hide secret information and so on. We can also use 2:1 interlacing, 4:1 interlacing and so on.

Consider original data –

Table 3. Cover data

10101110	00011101	11001101	11110001
11100010	01011011	00111001	11000111
10101010	11100010	00101010	01011100
00000000	00011100	11000010	11111110

Message to hide is -
11001101

Message will be hidden using following technique.

Table 4. Stego data after Raster Scanning

1010111<u>1</u>	**0001110<u>1</u>**	**1100110<u>0</u>**	**1111000<u>0</u>**
11100010	01011011	00111001	11000111
1010101<u>1</u>	**1110001<u>1</u>**	**0010101<u>0</u>**	**0101110<u>1</u>**
00000000	00011100	11000010	11111110

In above table, individual bits of secret message are replaced with bits of original pixels. Pixels are selected according to the raster scan method.

3.3 Random Scan Principle

This method is similar to Random Scan principle of displaying an image on CRT display. In this, the sequence, in which pixels are drawn, they are used to hide secret information. Again any simple data hiding algorithm

like LSB, can be used to hide secret information. By this method, data can be hidden in random pixels in an image

Message to hide is – 11001101

Bits are replaced according to any random sequence from

Table 5. Cover data

10101110	00011101	11001101	11110001
11100010	01011011	00111001	11000111
10101010	11100010	00101010	01011100
00000000	00011100	11000010	11111110

Message to hide is - 11001101

Message will be hidden using following technique.

Table 6. Stego data after Random scan

10101111	00011101	**11001101**	**11110000**
11100010	**01011010**	00111001	11000111
10101011	11100011	**00101011**	01011101
00000000	**00011100**	11000010	**11111111**

In this table, individual bits of secret message are replaced with individual bits of original pixels. Where pixels are selected randomly.

3.4 Color Based Data Hiding

In this scheme one fixed color is used to hide secret data. Intensity values of this fixed color are converted into binary format and the secret information is hidden in this binary data. For ex. consider a gray scale 8 bit image, having intensity values ranging from 0 to 255.
Suppose we have fixed a colour, whose intensity value is 155. Binary value of this is - 10011011.
We will find total number of pixels from an image, having the same intensity value.
Suppose there are 50 pixels found. Then we can hide secret information i n these 5 0 pixels, using any data hiding technique like – LSB etc.
We can extend this technique by taking more than one fixed colour of pixels, from an image.

3.5 Shape Based Data Hiding

in this scheme, any shape can be taken to hide the data in an image. For ex. consider a triangular shape. As shown in figure below.

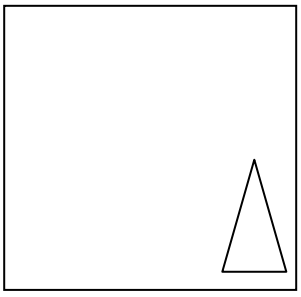

Fig. 3: Shape Based Data Hiding

According to figure, secret information can be hidden only in the pixels which are available in triangular shape, instead of hiding secret information in whole image. We can use any shape having any dimensions.
We can extend this technique, by using any shape of any dimension at any place in an image.

4. ANALYSIS WORK

Above proposed methods can be analyzed using some analysis techniques. Which are normally used for analysis of noise present in an original image. By hiding secret information in an image, image gets disturbed at certain level. This amount of disturbances in original image can be calculated by some techniques like - Signal to Noise Ratio (SNR), Peak Signal to Noise Ratio (PSNR), Structured Similarity Index Measure (SSIM), Mean Squared Error (MSE), and Average Absolute Difference (ADD) and so on [5].

4.1 Signal to Noise Ratio

Signal-to-noise ratio is also called as SNR or S/N, is defined as the ratio of signal power to the noise power corrupting the signal. The Signal to Noise Ratio (SNR) is the defining factor when it comes to quality of measurement
A high SNR guarantees clear acquisitions with low distortions and artifacts caused by noise. The better your SNR, the better the signal stands out, the better the quality of your signals, and the better you ability to get the results you desire. SNR measurement is commonly used in the field of science and engineering fields. A ratio higher than 1:1 indicates more signal than noise. While SNR is commonly quoted for electrical signals, it can be applied to any form of signal.

4.2 Peak Signal to Noise Ratio

Is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation.
Because many signals have a very wide **dynamic range**, (ratio between the largest and smallest possible values of a changeable quantity) the **PSNR** is usually expressed in terms of the logarithmic decibel scale.
Using the same set of tests images, different image enhancement algorithms can be compared systematically to identify whether a particular algorithm produces better results. The metric under investigation is the **PSNR**.

Fig. 4: Cover Image

Results obtained using a cover image of 786 bytes (Fig. 2) and a hidden message of 30 bytes (TXT file).

Table 7. Analysis of image steganography tools using different techniques

Tools	SNR	PSNR	AAD	MSE
Original Image	0,0	0,0	0,0	0,000
1Bit/Pixel	6,7	2,0	5,3	0,020
2 Bits/Pixel	3,2	9,9	6,1	0,043
3 Bits/Pixel	1,0	3,1	9,1	0,137
4 Bits/Pixel	0.5,0	1,0	10,1	0,527
Only 1's (Avg.)	1,0	3,0	5,1	0,130
Only 0's (Avg.)	1,0	3,0	5,1	0,130
Layout Mgmt	6,7	3,0	5,2	0,040
Shape Based	10,8	4,1	5,2	0,010
Color Based	10,8	10,1	9,1	0,025

Table above shows analysis of disturbances occurred in an image, due to hiding the text data into an image. There are various tools used for steganography and various analysis are used ratios are used for observing the variations occurred in an image due to hiding a textual data.

5. CONCLUSIONS

We have discussed in this paper about various techniques based on random bit image steganography. We proposed some new methods of hiding a secret data into an image. Also we analyzed these steganography methods with the help of various analysis tools, described in a paper. From this analysis we found that, the noise occurred in a cover image due to hidden data is depends on so many parameters like – amount of data to hide, size of cover image, frequency of pixels available in an image of a particular color, physical location of pixels and so on. To find the best steganography technique for our application will require these considerations and results observed.

6. REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods". *In Signal Processing 90*, (2010) 727–752.

[2] R.Amirtharajan, R. Akila, P.Deepikachowdavarapu. "A Comparative Analysis of Image Steganography". In *International Journal of Computer Applications, (0975 8887) Volume 2 – No.3,* May 2010.

[3] Sanjiv Manchanda, Mayank Dave and S. B. Singh, "Customized and Secure Image Steganography Through Random Numbers Logic". *In Signal Processing: An International Journal, Volume 1: Issue (1).*

[4] Mohammad Tanyir, Parvez and Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable Bits Image Steganography", 2008 IEEE Asia-Pacific Services Computing Conference.

[5] Rengarajan Amirtharjan, Jiaohua Qin and John Bosco Balaguru Rayappan "Random Image Steganography and Steganalysis: Present Status and Future Directions". *Information Technology Journal* 11(5), pp. 566-576, 2012