International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Analysis of Random Steganography Techniques Using Random Pixels

Dipesh Agrawal[1]
[1]*Department of Computer Engineering, SNJB's KBJ College of Engineering, agrawal.dipesh@gmail.com*

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 colour 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, based on selection of random pixels from an image and again secret data is hidden in random bits of these randomly selected pixels. For this purpose, many parameters of an image are considered like physical location of pixels, intensity value of pixel, etc.
Keywords- Shape based data hiding, color based data hiding

I. INTRODUCTION

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". This stego is transmitted over a network to specified destination. 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 [1]. 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.

II. RELATED WORK

Steganography is one more information security tool like Cryptography and Watermarking. Cryptography There are so many image steganography techniques based on spatial domain. Spatial domain means actual physical location of a pixel in an image. While hiding data in a pixel, the physical location of a pixel is considered and then the binary format of that pixel value is used to hide the data.

2.1. Least Significant Bit

One of the simplest and very popular technique of steganography is Least Significant Bit (LSB). In this technique, least significant bit or bits of a pixel are replaced by the bits of data to be hidden [1]. LSB can be extended up to 4 least significant positions from a byte, i.e. we can replace four bits of hidden data with the original value of a pixel, whose binary value is of 8 bits. So, out of 8 bits, at

max 4 bits can be used to hide data. We can replace last two bits also. Replacing four bits, may cause distortion in an image due to noticeable change in colour and intensity of an image.

2.2 Replacing only 1's and Zero's

Another technique is to consider binary values of a pixel and replace all 1's only from last 4 LSBs with the bits of data to be hidden. Same way we can do for zero's only. This will dynamically hide number of bits or bytes, in the cover medium. Detection of hidden data will be very difficult for any intruder.

2.3 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. Hence we can use any arrangement of pixels and can make logical sequence of these pixels to hide secret data.

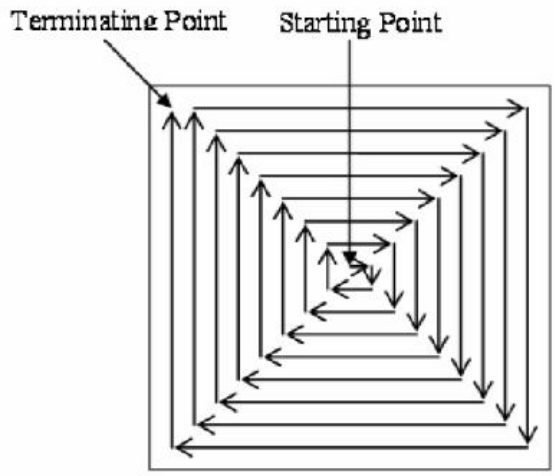

Fig. 1 Logical Sequence of pixels from center to outside

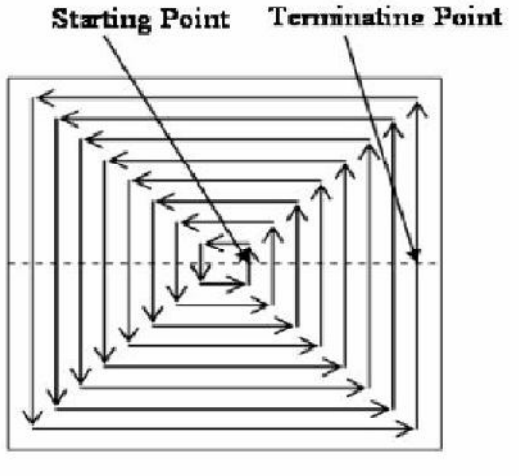

Fig. 2 Logical Sequence of pixels from outside towards center

III. PROPOSED WORK

Following methods are proposed for - hiding data based on random bits of random pixel positions of an image.

3.1 Replacing Intermediate Bits

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 No. 1. Cover Data

10101110	00011101	11001101	11110001
01010100	11101111	10110001	10101010

Message to hide is – 11001101 Bits are replaced according to any random sequence from LSB to MSB position.
In following table underlined bits shows the bits of secret message are replaced with the bits of original data at that position.

Table No. 2. Cover Data + Secret Data = Stego

10101110	00011101	11001101	11110001
5th Bit	2nd Bit	6th Bit	4th Bit
01010100	11101111	10110001	10101010
4th Bit	3rd Bit	5th Bit	2nd Bit

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 No. 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 No. 4. Cover Data + Secret Data = Stego

10101111	**00011101**	**11001100**	**11110000**
11100010	01011011	00111001	11000111
10101011	**11100011**	**00101010**	**01011101**
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.

Table No. 5. Cover Data

10101111	**00011101**	**11001100**	**11110000**
11100010	01011011	00111001	11000111
10101011	**11100011**	**00101010**	**01011101**
00000000	00011100	11000010	11111110

Message to hide is – 11001101
Message will be hidden using following technique

Table No. 6. Cover Data + Secret Data = Stego

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 in these 50 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.

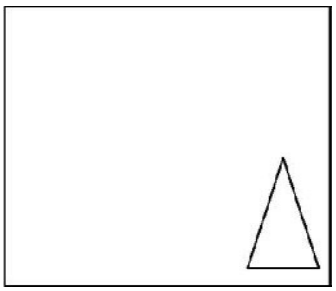

Fig. 3 Shape Based Data Hiding

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.

IV. EVALUATION AND BENCHMARKING

Besides designing digital steganography methods, an important issue addresses proper evaluation and benchmarking. This not only requires evaluation of the robustness, but also includes subjective or quantitative evaluation of the distortion introduced through the steganography process. Hence, for fair benchmarking and performance evaluation one has to ensure that the methods under investigation are tested under comparable conditions.

4.1 Performance Evaluation and Representation

Performance of image steganogrpahy depends on amount of embedded information, size and nature of embedded information, embedding strength of an image, nature and type of secret key and other many more parameters. These parameters are described in following points.

Amount of embedded information - The more information one wants to embed, the lower the steganography robustness.

Embedding strength – data is embedded such that an original image is not disturbed to human visual system. i.e. data embedding doesn't affect the clarity of original image to get the perceptibility. **Size and**

Nature of secret data - The size of the data has usually a direct impact on the original image. For example, in image steganography, very small text file is embedded to avoid the disturbances in clarity. In addition to the size of the data, the nature of the data also has an important impact on the steganography.

Secret information (e.g., key) - Although the amount of secret information has no direct impact on the perceptibility of the steganography, it plays an important role in the security of the system. The key space, that is, the range of all possible values of the secret information, must be large enough to make exhaustive search attacks impossible. Many security systems fail to resist very simple attacks because the system designers did not obey basic cryptographic principles in the design. Taking these parameters into account, it is realized that for fair benchmarking and performance evaluation, steganography methods need to be tested on different data sets. Furthermore, in order to compute statistically valid results the methods have to be evaluated using many different keys and varying images (covers). The amount of embedded information is usually fixed and depends on the application. However, if steganography methods are to be compared, it has to be assured that the amount of embedded information is the same for all methods under inspection.

4.2 Different Distortion Metrics

Distortion in images causes due to embedding of secret data into an image. Here original pixels of an image are replaced by bits and bytes of secret data, by keeping the size of image same, but other characteristics of an image may get disturbed. This distortion occurred in an image due to hiding secret data, can be measured by some standard formulas or methods. These are –

1. Average Absolute Difference,
2. Mean Squared Error,
3. LP Norm, and
4. Signal to Noise Ratio and so on. These methods are described in detail in following points [1].

V. ANALYSIS

In this section, we are doing actual analysis of steganography techniques using an image and a message to hide. Following are the details for analysis – **Image Properties –** Size in Pixels – 500 * 167 (Pixels) Size in Bytes - 250,544 Bytes 24 Bit Color Image.

5.1 Comparison and Result Observation

Table No.7 shows the results obtained after applying the parameters Average Absolute Difference, Correlation Quantity, LP Norm, Mean Squared Error; on an image in which two text messages are hidden (one is of 2KB and another is of 4KB). Values in bold indicates the amount of distortion introduced in a cover image after hiding the secret text message.

1. Average Absolute Difference – is lowest for LFSR algorithm.
2. Correlation Quantity – is lowest for shape based data hiding algorithm.
3. LP Norm – is lowest for LFSR algorithm.
4. Means Squared Error – is lowest for LFSR algorithm.

From above observations, we can conclude that, if a text message is hidden using LFSR technique, in an image, lowest amount of distortion will occur in an image

Table No. 7 Results obtained using a cover image of 2.44MB and a hidden message of 2KB and 4KB.

	Results			
	AAD	CQ	LP Norm	MSE
Color Based – Message 1	0.132	254.999	0.143	0.286
Color Based – Message 2	0.263	254.999	0.287	0.574
Shape Based – Message 1	0.148	**254.949**	0.397	0.795
Shape Based – Message 2	0.293	**254.900**	0.778	1.557
Random scan – Message 1	**0.096**	254.967	**0.095**	**0.191**
Random scan – Message 2	**0.192**	254.935	**0.190**	**0.381**
Raster scan – Message 1	0.097	254.966	0.101	0.203
Raster Scan – Message 2	0.193	254.933	0.202	0.404

In Table No. 8 given below, the fields in bold indicates the best performance of that steganography technique for the related performance analysis parameter. LFSR is best steganography technique for AAD, LP Norm and MSE. CQ is best for Shape based image steganography algorithm

Table No. 8. Performance Analysis for different algorithms by applying different distortion metrics

	Performance Metrics			
	AAD	CQ	LP Norm	MSE
Steganography Techniques	**Random Scan**	**Shape Based**	**Random Scan**	**Random Scan**
	Hide and Seek	Hide and Seek	Hide and Seek	Hide and Seek
	Color Based	**Random Scan**	Color Based	Color Based
	Shape Based	Color Based	Shape Based	Shape Based
Best Technique – **Random scan**		Average Technique – **Shape Based**		

CONCLUSION

In this paper, along with existing techniques of image steganography, some new methods for hiding data in images are discussed. Data can be hidden in pixels according to their physical locations. These physical locations can be determined using different techniques like – Layout Management Schemes, Color Based and Shape based data hiding and Random scan techniques. The secret data can be hidden in bits of random pixels from an image. While selecting these pixels, many parameters from an image are considered for ex. Color of pixels, physical location of pixels etc. performance of these techniques is analyzed using different parameters like – Correlation Quality, Mean Squared

Error, Average Absolute Difference and LP Norm. By applying these above mentioned parameters on the proposed image steganography techniques and already available techniques of steganography, it is concluded that – the proposed image steganography techniques in this thesis are better in performance and accuracy than available existing image steganography techniques.

REFERENCES

[1] Ding, W. and Marchionini, G. 1997 A Study on Video Browsing Strategies. Technical Report. University of Maryland at College Park.
[2] Fröhlich, B. and Plate, J. 2000. The cubic mouse: a new device for three-dimensional input. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems
[3] Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.
[4] Sannella, M. J. 1994 Constraint Satisfaction and Debugging for Interactive User Interfaces. Doctoral

