A Novel Approach for Image Steganography using LCG

Mohammed J. Bawaneh
Information Technology Department, AL-Huson University College,
Al-Balqa Applied University, Jordan

ABSTRACT

Internet is a public channel and security issues, such as modification, interception and sniffing normally exist. Steganography is a common security technique that is utilized to solve or reduce those problems. A large number of methods is used for implementing steganography; as least significant bits (LSB), discrete cosine transform (DCT), discrete Fourier transform (DFT), Spread Spectrum coding and Perceptual Masking. This paper proposes a random and sequential LSB to embed the secret message inside the color image. The linear congruent generator (LCG) is a random generator that is used with LSB to hide a stream of bits in a bitmap image (cover image) to give a new image (stego-image) comparable to the cover image. Secret key for random LSB is a combination of four parameters (Seed, Multiplier, Non-common factor, and Cycle length). The proposed method employees red, green or blue channel to hide the secret message. Selection of channel based on the modification rate for each channel. The minimum modified channel in cover image is utilized to embed the secret message. Results show that random LSB is better than Sequential LSB in term of visual effect while the worst in term of execution time. Random LSB satisfies sufficient security to secret message due to requirements for random function parameters in the extraction process.

General Terms

Security, Image steganography

Keywords

Steganography, LCG, LSB

1. INTRODUCTION

Network is a public channel that provides multi users with multi services at the same time. It allows users to delight in the serviceable and benefits of digital data through sending and receiving processes. Users transfer their private or secret data using the public network and sometimes they want to keep their copyright. Modification, interception and sniffing are common problems in network environment; different technologies have been used to deal with passing data securely. Steganography, cryptography and watermarking are some of the technologies used today to solve or prevent network problems. The main focus of this work is the steganography technology.

Steganography was derived from the Greek word steganos, meaning covered or secret, and graphy referring to writing or drawing [1]. In more accurate words, steganography is the art of hiding something in another thing, whether it consists of invisible ink on paper or copyright information on digital media[2].

There is an important terminology that should be introduced before going too deep. First, the cover-object or cover-medium is the carrier of the message. This could be an image, a video, an audio, a text, or some other digital media. Next is the embedded message or embedded data, which refer to the message to be hidden in the cover medium. The message could be a text, an image, an audio, or a stream of data. A stego-key is used to embed the message in the cover medium. A stego-object or stego-medium is created once the message is successfully hidden in the cover-medium.

Steganography is used for several purposes but the main one is to hide the existence of communication. Usually, there is a confusion between steganography and encryption, steganography and watermarking [3]. Different security technologies have the same goal, but they are different in the working process.

Several methods are used to implement steganography such as LSB, Reorder the color palettes and Color Quantization Technique, The Computational information hiding Techniques (CPT), Fridrichs Color Parity Technique and Color parity, those methods are based on substituting one or more bits from embedded message by another from cover message. This paper will present a random LSB method that bases on LCG function. Here, the cover-object, where the data hide, is always an image, the embedded data could be a text, an image or another type of files, and in other words it’s a stream of bits and the resulting image known as a stego-image.

The rest of the paper is organized as follows. Section 2 presents related work. Section 3 describes the material and methods. The experimental result is shown in Section 4. Finally, section 5 concludes this paper with directions for future work.

2. RELATED WORK

Steganography is a very old method of passing messages in secret; it goes back to the time of the ancient Greeks. The historian Herodotus wrote about how an agent wrote a message warning of an invasion on the wood part of a wax tablet. Since messages were normally inscribed in the wax and not the wood, the tablet appeared blank to a common observer [4].

Image steganography is widely known in recent years than other steganography types because of the avalanche of electronic image information available today. It involves hiding information within an image, and provides a good illustration for such techniques [5].

In Fridrichs Color Parity Technique each pixel is computed as (R+G+B) mod 2, if the result matches the embedding bit then it is embedded otherwise it takes the next [6].

Petitcolas et al noted "the greater the number of bits used to represent colors, the less obvious the changes in palette values are in the visual representation of the final image". Furthermore, loosy compression and other image transformations can easily destroy hidden messages [7].

Chun-Hsiang and others found that LSB or the final bit in a stream affects the smallest change while the first bit of the stream has the largest influence on color selection. If the LSB of every bit stream were to be allocated for a hidden message, the resulting image file would appear unaltered [8].

N. S. Raghava and others used a random generator to encrypt the secret message before hiding it inside the cover image. JPG file was tested on this system successfully [9].

Sanjeev Manchanda, proposed a system for studying cover image and secret in aim at processing them. The hidden method was selected randomly according to user inputs [10].

Mamta Juneja1 and others proposed a new approach for steganography in color image that bases on LSB substitution and adaptive LSB substitution technique. The proposed system gave better capacity than the existing techniques and better resistance to various stegaanalysis attacks [11].

Amir Farhad Nilizadeh described a novel spatial domain method for steganography in RGB images. The proposed system used the blue layer of a certain block to embed the secret message. Each block builds a matrix of pixels using the bit difference of neighborhood pixels. The block was chosen randomly in aim at increasing the security. The results show that the proposed algorithm is resistance against the frequency and spatial domain attacks [12].

Samidha, D. and others described different image steganography techniques, based on spatial domain and pixel values in binary format [13].

3. MATERIALS AND METHODS

The main objective of this work is to make a practical comparison between sequential and random LSB using LCG as mentioned early; to accomplish that several stages are performed. First of all the cover image or host image of type bitmap must be selected. User may select another type, so the system must convert the cover to bitmap. Next to selection process the embedding process is operated, two types of embedding are performed one is the sequential LSB while the other is random LSB. Hidden information must be manipulated at the receiver part using the extraction process for sequential and random LSB.

3.1 Host Image

Pixels of host image must be 24-bit color depth, in order to accomplish that the cover object must be a bitmap image or an image of extension (.bmp). An additional step for format conversion sometimes may carry out due to user mistake in selecting the cover image. The proposed system has an embedded subsystem to handle such problem. After the required format is manipulated the embedding or hiding process takes place. Stego-image is the final product of hiding process; it has the same type and format of host image.

3.2 Embedding Process

The avenue that is used to hide the data in the image is the LSB technique. Through this way one of the least significant bits from a pixel of cover image will be replaced or changed by bits from the secret message. The replaced bit in the cover image may be red, green or blue but not all of them. Every time only one bit is replaced in pixel.

The secret message must be a stream of bits or a binary data that reads in binary reader.

The colored image that is used as a cover is a 24-bit depth in each pixel, this means each color (red, green, blue) is represented by 1 byte and so each color falls in range between 0 and 255.

Order of target pixels for hiding the secret message inside the cover image and number of replaced bits inside each pixel in cover image are the two important things that must be considered in embedding data within the cover image:

The way which is used to determine the current or next pixels is very important. Pixels are chosen using sequential LSB or random LSB technique. Random LSB utilizes LCG as a random generator to generate the location of target pixel that will be used in embedding and extraction processes.

LCG as a random generator is used to generate a sequence of random numbers (n_1, n_2,…, n_k) over an interval [0, M-1] as shown in next formula. [14]

$$\mathbf{n_i = (n_{i-1}*a + b) \bmod M}$$

where $\mathbf{n_{i-1}}$ is the previous random number or seed value in initial state, **a** is constant and called multiplier, **b** is also constant and called non-common factor while **M** is the cycle length. To achieve the cycle length without any redundancy in random number or pixels; three conditions must be taken into account as follows.

1. **b** and **M** have no common factor greater than one
2. (**a**-1) is multiple of every prime number that divides **M**
3. (**a**-1) is multiple of four if **M** is multiple of four.

Random LSB has many merits Selecting the target pixels randomly will increase the security of the data since the message bits are going to be scattered or distributed all over the stego-image in a random way. It is hard to restore the secret message from stego-image, if an attacker manipulates the embedded message by going sequentially through the pixels of stego-image. Another benefit is to reduce the effect of modification in visual appearance relatively less apparent, due to replaced bits are not adjacent so if a one bit is replaced and the adjacent ones are not then the change will not appear especially if the size of secret message was small compared to the size of cover image.

Seed, constant **a**, constant **b** and cycle length of LCG represent the secret key for embedding data inside the cover image also the same key is used for extracting data from stego-image in extraction process.

3.2.1 Sequential LSB

The proposed system deals with secret message as stream of bits. In more accurate words, each byte from the message is broken up into 8 units each one of size 1 bit. Since only one bit is replaced in each pixel. So, to hide one byte of secret message in cover image the system will require for eight pixels. The algorithm of sequential LSB carries out several steps to accomplish the main task as follow:

1. Select the cover image for embedding the secret message and convert it to a compatible format if not an RGB with 24 bits image.

2. Select the secret message to be embedded inside the cover image and manipulate it as binary data.
3. Compute the modification rate for each channel (red, green and blue channel) in order to be utilized later on.
4. Select the minimum modification rate channel
5. For each bit in secret message do.
    a. Select Pixel$_i$
    b. Manipulate the bit and pixel channel using the logical operator in aim to hide bit within the selected pixel channel.
    c. Modify the index pixel value to get the next one.
6. Repeat step 5 until you get the whole bits.
7. Stego-image is virtually converted to another format.

3.2.2 Random LSB

Each byte from the secret message is manipulated as in sequential LSB into 8 units each of size 1 bit. User must insert the seed value to initiate the LCG random generator. Since the system will generate constant **a** and constant **b**. Seed, constant **a**, constant **b** and message length must be kept in aim to be used in the extraction process at receiver part. The random LSB algorithm of works as follow:

1. Select the cover image for embedding the secret message and convert it to a compatible format if not an RGB with 24 bits image.
2. Select the secret message to be embedded inside the cover image and manipulate it as binary data.
3. Compute the modification rate for each channel (red, green and blue channel) in order to be utilized later on.
4. Select the minimum modification rate channel.
5. Insert the seed value for LCG generator.
6. Generate constant **a** and constant **b** according to length of cover image and seed value.
7. For each bit in secret message do.
    a. Select random Pixel$_i$ using LCG random generator
    b. Manipulate the bit and pixel channel using the logical operator in aim to hide bit within the selected pixel channel.
    c. Modify the seed value to generate the next random number. Next seed value is updated by the current random number
8. Repeat step 7 until you get the whole bits.
9. Stego-image is virtually converted to another format.

3.3 Extraction Process

Extraction process works according to user selection for method and parameters. Secret message has two choices for embedding, one with sequential LSB while the other with random LSB. The message can be extracted from the stego-image only if users hold two important things. Firstly, you should recognize the pixels that hide secret bits. Secondly, you should recognize the used method to embed the message in stego-image. In sequential LSB, it is easy to retrieve the message if you know the staring pixel of embedding inside the stego-image, but in random LSB you should know the LCG function that was used to select the pixels. LCG function bases on user key which is a combination of several parameters as mentioned earlier. Once you have the correct information for method and parameters you can extract the message from the stego-image using the logical bitwise operators.

3.4 Stego Image

The final result of embedding process is the stego-image, the view of this image should be comparable to the original one in visual appearance, and also they should have the same format. Observer with the naked eye should not be able to distinguish between the original image and the stego-image.

After completing the embedding process, stego-image is virtually converted to another format or extension. The main goal of this conversion is to improve the trust of sending image through public network. Converting the stego-image to other format does not apply any compression or modification in order to maintain the secret message inside the stego-image. One way to do that is Jpeg compression technique. It is a common loosy compression method for images that have in mind some of image data will be lost; this manipulation is not comfortable in circumstance of using LSB to hide the data. Such problem can be solved by converting the stego-image into a jpeg but without using the jpeg compression. Applying this step will give a stego-image an extension jpeg with the size of the original image (bmp).

4. RESULT AND ANALYSIS

The proposed system for random and sequential LSB was tested using a secret message of size 25KBytes that is embedded into 300 X 300 cover image. Four issues were considered in testing the system, first the visual appearance of stego-image that results from sequential and random LSB compared to cover image, the time needed for each one, modification rate and robustness against attacking.

When using sequential LSB, the image has some modifications in upper left corner as shown in Fig[1], this distortion is not obvious in case of random LSB as in Fig[2]. By comparing the stego-image with cover image, no a visual effect between random stego-image in Fig[2] and cover image Fig[3], but this effect appear clearly in sequential stego-image. To see these modifications more clearly look at histogram of each image in the same figures. Random LSB histogram approximately has no change compared to cover image histogram.

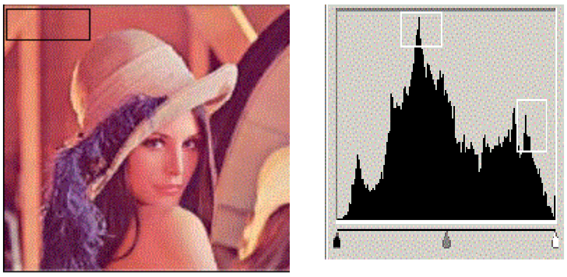

Fig 1 : Stego-Image for sequential LSB

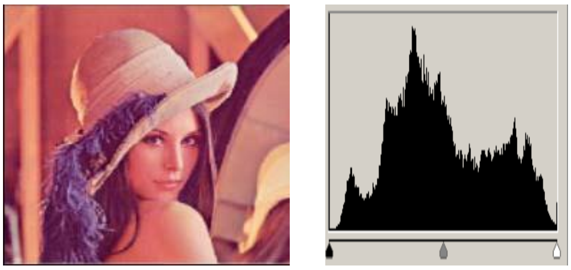

Fig 2 : Stego-Image for random LSB

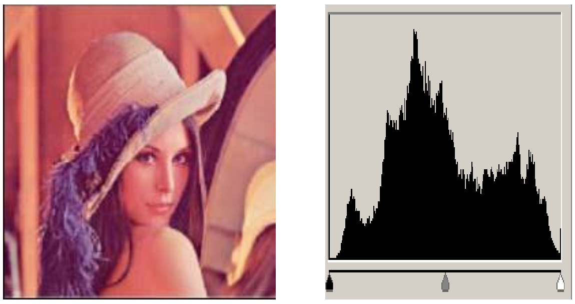

Fig 3 : Cover image

Sequential LSB takes less execution time than Random LSB as shown in table 1, so the fastest one is the sequential LSB. The time difference between them refers to discount time computation or overhead time for the next pixel selection.

Table 1: Time Results in seconds

Random LSB	Sequential LSB
0.9413	0.5107

Modification rate is computed in term of message length (MRML) and cover image length (MRCL) as follows:

MRML=Number of modified pixels/ Message length

MRCL=Number of modified pixels/ Cover image length

MRML and MRCL help in selecting the best channel for hiding the effect of visual appearance in stego-image. Table 4 shows the results of comparison between sequential and random LSB. Sequential LSB appears better than random LSB due to the selected test cover image, but some time the result may give the invers. Every time the values of MRML and MRCL are based on user selection of cover image, so neither sequential LSB nor random LSB are superior in term of MRML and MRCL.

Table4: MRML and MRCL for sequential and random LSB

	Total channels	Red channel	Green channel	Blue channel
MRML of Sequential LSB	0.8163	0.4023	0.4783	0.4958
MRML of Random LSB	0.8381	0.4303	0.4906	0.4946
MRCL of Sequential LSB	0.1871	0.0923	0.1096	0.1136
MRCL of Random LSB	0.1922	0.0986	0.1124	0.1134

In term of robustness random LSB is more robust than sequential LSB because the extraction process in random LSB requires the secret key. The key consists of several parameters, so it is very complicated for attackers to guess them.

5. CONCLUSION

Sequential LSB method is an easy way to hide some kind of data in an image, but it is not that robust to attacks. To increase the security of the hidden data the encryption and random distribution algorithms may be used. In addition, to improve performance a signature may be used to determine if stego-image is distributed or not. LSB distribution technique can be enhanced through neighborhood pixels value inside the cover image which may result in a low visual effect in the stego-image. The main goal of random function with LSB is to increase the security of steganography and avoid the overhead time of cryptography that may be used with steganography.

6. REFERNCES

[1] William .P, “Digital Image processing”, 3rd edition, 2001

[2] Stefan Katzenbeisser,Fabien A. P. Petitcolas, “Information Hiding Techniques for Steganography and Digital Watermarking”, 2000

[3] Jessica Fridrich, Miroslav Goljan, and Rui Du , ” Detecting LSB Steganography in Color and Gray-Scale Images”, State University of New York, Binghamton, 2002

[4] Sviatoslav Voloshynovskiy, Oleksiy Koval and Emre Topak, “On reversibility of random binning based data-hiding techniques”, Thierry Pun September 2006 , Proceeding of the 8th workshop on Multimedia and security MM&Sec '06, Publisher: ACM Press

[5] Jeremiah J. Harmsen , William A. Pearlman, “ Stegano-graphy and steganalysis: Capacity of steganographic channels”, August 2005 Proceedings of the 7th workshop on Multimedia and security MM&Sec '05 Publisher: ACM Press

[6] A. Francia, Tyler S. Gomez, “ Practice:Stegano- graphy obliterator: an attack on the least significant bits”, September 2006 Proceedings of the 3rd annual conference on Information security curriculum development InfoSecCD '06, Publisher: ACM Press

[7] Elke Franz, Antje Schneidewind, “Steganography II: Adaptive steganography based on dithering”, September 2004 Proceedings of the 2004 workshop on Multimedia and security MM&Sec '04 Publisher: ACM Press

[8] Chun-Hsiang Huang, Shang-Chih Chuang, Ja-Ling Wu, "Steganography and steganalysis: Digital invisible ink and its applications in steganography", September 2006 Proceeding of the 8th workshop on Multimedia and security MM&Sec '06 , Publisher: ACM Press

[9] Raghava, Ashish Kumar, Aishwarya Deep and AbhilashaChahal, "Improved LSB method for Image Steganography using H´enon Chaotic Map", OPEN JOURNAL OF INFORMATION SECURITY AND PPLICATIONS, VOLUME 1, NUMBER 1, JUNE 2014

[10] Sanjeev Manchanda,, "Pseudo random numbers Based Methods for Customized and Secure Image Steganography" , International Journal of Network Security, Vol.16, No.4, PP.366-376, July 2014 366

[11] Mamta Juneja and Parvinder Singh Sandhu, "Improved LSB based Steganography Techniques for Color Images in Spatial Domain" , Received Apr. 9, 2013; revised and accepted June 10, 2013)

[12] Amir Farhad Nilizadeh, "Steganography on RGB Images Based on a Matrix Pattern" using Random Blocks", I.J.Modern Education and Computer Science, 2013, 4, 8-18, DOI: 10.5815/ijmecs.2013.04.02

[13] Agrawal, D," Random image steganography in spatial domain", Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT), 2013 International Conference on Tiruvannamalai

[14] Morgan J.T. Byron, "Elements of Simulation", 1984, published in USA by Chapman and Hall, ISBN 0412245809