International Journal of Computer Networks and Communications Security

VOL. 3, NO. 9, SEPTEMBER 2015, 363–366
Available online at: www.ijcncs.org
E-ISSN 2308-9830 (Online) / ISSN 2410-0595 (Print)

A Various Issues in Image Steganography that Using LSB Technique

Mohammed Salem Atoum[1] and Mohammed M. Abu Shquier[2]

Faculty of Science, [1]Information Technology, [2]Faculty of Information Technology, [1]Irbid National University, [2]Jerash University

E-mail: [1]moh_atoom1979@yahoo.com, [2]Shquier@gmail.com

ABSTRACT

This paper presents the issues and challenges faced for image steganographic techniques. Many LSB method techniques were developed in recent year using direct or un-direct position to embed secret message into cover. Some techniques for embedding information in Image files were reviewed, and recommendations are being proposed for the best strategy of hide information in image files and the possibility of finding other new techniques hiding information in image files.

Keywords: *LSB, Steganography, Image Steganography.*

1 INTRODUCTION

Least significant bit (LSB) technique is the first and simplest technique that was used to embed secret messages into cover file. In LSB Method the cover and secret message are converted into streams of bits and then later the secret message is embedded into the cover by replacing the LSB bit of the cover with one or more bit of the secret massage and then sent to receiver. In order for the receiver to extract secret massage the receiver accesses the sequence of sample indices used in the embedding process [1-8]. However, in following some methods using LSB technique in steganography were explained:

2 STANDARD LSB

In this method researcher embedded one bit or more from secret message in cover directly. This is way simplicity and easy to detect and extract secret message. To enhancement the security of LSB standard, some researcher using Intermediate Significant Bit and Most Significant Bit (ISB and MSBA). In [9] developed LSB method to increase security by using intermediate significant bit (ISB) to hide secret message in smooth area in image. He using 2,3,4 bit in cover to hide secret message. On other hands [10] proposed techniques to embed secret message dependent for the value of MSB if last two MSB =0,1,2,3 that's meaning embedding in first, first and second, first and second and third ,first to 4 LSB respectively .However, some researcher using mathematical model for embedding. In [11] proposed two algorithms to select embedding positions based on some mathematical function (mod 4 and mod 16) which de-ends on the data value of the digital audio stream. Data embedding is performed by mapping each two bit of the secret message in each of the seed position, based on the remainder of the intensity value when divided by 4. Extraction process starts by selecting those seed positions required during embedding. At the receiver side other different reverse operation has been carried out to get back the original information.

3 THE OPTIMAL LSB INSERTION METHOD

This insertion method improves the stego-image quality by finding an optimal pixel after performing an adjustment process. Three candidates are picked out for the pixel's value and compared to see which one has the closest value to the original pixel value with the secret data embedded in. The best candidate is then called the optimal pixel and used

to conceal the secret data [12].This however makes the hiding capacity of the carrier image very low.

4 THE PIXEL VALUE DIFFERENCING (PVD) METHOD

The pixel-value differencing (PVD) method is proposed by [13]. In this approach, the payload of each individual pixel is different, and the resultant stego-image quality is extremely fine with perfect modification and invisibility. The resultant stego-images quality that the method produces is better in terms of human visual perception. However steganalysis is easy as the hidden message is not well spread across the entire image. The given image is scanned in a zigzag manner to obtain the pixels. Blocks of two consecutive pixels are obtained. Given a sub-block Fi composed of two continuous pixels P(i,x) and P(i,y) from the cover image, obtain the difference value di, the sub-range Ri such that Ri belongs to [li,ui], the width wi = ui – li + 1, the hiding capacity ti bits, and the decimal value v of ti for each Fi. Where li is lower limit and ui is upper limit of the Range Ri. The remainder values Prem(i,x), Prem(i,y) and Frem(i) of P(i,x), P(i,y) of sub-block Fi are computed respectively by using the following equations:

$$Prem(i,x) = P(i,x) \bmod wi$$

$$Prem(i,y) = P(i,y) \bmod wi$$

$$Frem(i) = (P(i,x) + P(i,y)) \bmod wi$$

Where wi is the width of the suitable range. ti bits of secret data are embedded into sub block Fi by altering P(i,x) and P(i,y) such that Frem(i) = v.

5 DISCUSSION

The capacity, robustness and imperceptibility requirement for Steganography are the important features that characterize the strength and weaknesses of the LSB technique for achieving information hiding. We further summarize the methods that have been used image steganography in a tabular format that is self-explanatory. Table 1 below presents these methods.

6 CONCLUSION

Several techniques have been discussed in this paper for embedding data in image files by using steganography systems. We expect to be hiding information by using LSB is the best strategy to hide information in image files with the possibility of finding other ways to hide information that is mentioned earlier with the increase in research on information hiding in image files.

Table 1: Summaries LSB methods

Method	Techniques
Random LSB+RC4	The embedding process is based on pseudorandom number generator. Blum Blum Shub (BBS) generator is used in this system to generate the random sequences. According to these random sequences, encrypted messages are embedded in PNG image file. In this method, message may be embedded to 1-LSB of container image if random sequence generates "1" as PRNS. In contrast, the message can be embedded to 2-LSB of container image.
square fullyEMD	Equation for embedding is $[X_i*(S^2-1)+x_{i+1}*S^2] \bmod S^4$
LSB+Fibonacci + PRNG	Using LSB to embed secret message in image file by using two steps: firstly using Fibonacci to select position of bit secondly using PRNG to choose next bit.
EDGE LSB	Use all the edge pixels in an image. Here, we first calculate the masked image by masking the two LSB bits in the cover image. Then we identify the edge pixels by using the Canny Edge detection method. After obtaining the edge pixels we hide the data in the LSB bits of the edge pixels only and send the stego object to the receiver.
Random LSB	The standard minimal linear Congruential Generator (LCG) method is used to generate the pseudo random numbers used to match the specific bits in the cover image where the secret data bits are hiding. $X_{n+1} = ({}_aX_n + c) \bmod m$
RPrime RSA+GA+random LSB	Encrypt text message using RPrime RSA encryption algorithm. And then applying proposed LSB algorithm, embed message bits to the audio bit stream in random and higher LSB layer positions (increase the robustness) to get a collection of chromosomes. Now Genetic Algorithm operators are used to get the next generation chromosomes. Next select the best chromosome according to the best fitness value. Fitness value is a value of LSB position for which we get a chromosome with the minimum deviation comparing to the original host audio sample
Radom LSB	If the integer value of the 8-bit message block is between 0 and 85, the embedding of these 8-bits under consideration, takes place in the R plane. Similarly, values ranging between 86 and 170 are embedded in the G plane, while values between 171 and 255 are embedded in the B plane
Encryption + LSB	Generate randomization key to encrypt secret message before embedding. The size of key must be less than or equal to 16 characters long. These 16 characters can be any of the 256 characters (ASCII code 0 to 255). The relative position and the character itself is very important in our method to calculate the randomization number , the encryption number and the relative shift of characters in the starting key matrix
Inverse and shift LSB	This method is chosen due to its minimal effect on the image. LSB is used by inversing the binary values of the watermark text and shifting the watermark according to the odd or even number of pixel coordinates of image before embedding the watermark.
EMD	Equation for embedding is $[X_i*(S-1)+x_{i+1}*S] \bmod S^2$
LSB+GA	Select the bit by using GA and embedding secret message in it.

7 REFERENCES

[1] Atoum, M. S., Rababah, A. and Al-attili, A. I. (2011).New Technique for Hiding Data in Audio Files. International Journal of Computer Science and Network Security, 11(4), 173-17

[2] Atoum, M. S., Suleiman, M., Rababaa, A., Ibrahim, S., and Ahmed, A. (2011). A steganography Method Based on Hiding secretes data in MPEG / Audio Layer III. International Journal of Computer Science and Network Security, 11(5), 184-188.

[3] Atoum, M. S., Ibrahim, S., Sulong,G. and Ahmed, A. (2012). MP3 Steganography: Review. Journal of Computer Science issues, 9(6).

[4] Atoum, M. S., Ibrahim, S., Sulong, G., and Ahmed, A. (2013).New Secure Scheme in Audio Steganography (SSAS). Australian Journal of Basic and Applied Sciences, 7(6), 250–256.

[5] Atoum, M. S., Ibrahim, S., Sulong, G., Zeki, A and Abubakar, A. (2013). Exploring the Challenges of MP3 Audio Steganography. Proceding IEEE from 2nd International Conference on Advanced Computer Science Applications and Technologies (ACSAT) ,Sarawak, Malaysia.

[6] Atoum, M. S. (2015). A Comparative Study of Combination with Different LSB Techniques in MP3 Steganography. In Information Science and Applications(pp. 551-560). Springer Berlin Heidelberg.

[7] Atoum, M. S., Ibrahim, S., Sulong, G., and Zamani, M. (2013). A New Method for Audio Steganography Using Message Integrity, Journal of Convergence Information Technology,8(September), 35–44.

[8] Atoum, M. S., Alarood, Alaa. (2014). Audio Steganography. Multimedia Security. International Islamic University Malaysia. Information technology faculty

[9] Zeki, A.M. (2009), Watermarking Techniques using Intermediate Significant Bit. PhD. Thesis, Universiti Teknologi Malaysia.

[10] Devi, K. J. (2013). A Secure Image Steganography Using LSB Technique and Random Pseudo Random Encoding Technique. (Doctoral dissertation).

[11] Bhattacharyya, S. (2011). A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier. Journal of global research in computer science, 2(4)

[12] Chan, C.K. and Cheng, L.M. (2004). Hiding Data in Images by Simple LSB Substitution. Pattern Recognition, 37(3), 469–474.

[13] Wu, D. C., & Tsai, W. H. (2003). A steganographic method for images by pixel-value differencing. Pattern Recognition Letters, 24(9), 1613-1626.