



Daffodil
International
University

Thesis Report

Image Steganography using Least significant bit (LSB)

SUBMITTED BY

Shad Bin Akter

183-35-387

**Department of Software Engineering
Daffodil International University**

SUPERVISED BY

Mr. S A M Matiur Rahman

Associate Professor

**Department of Software Engineering
Daffodil International University**

This Report Presented in Partial Fulfilment of the Requirements for the Degree of Bachelor of Science in Software Engineering (BSc in SWE)

**Department of Software Engineering
DAFFODIL INTERNATIONAL UNIVERSITY**

Fall – 2022

APPROVAL

This Thesis titled on "Image Steganography Using Least Significant Bit", submitted by Shad Bin Akhtar (ID: 183-35-387) to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.



BOARD OF EXAMINERS

----- Chairman

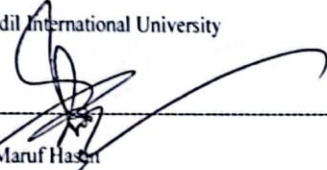
Dr. Imran Mahmud

Head and Associate Professor

Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University



----- Internal Examiner 1

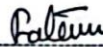
Md. Maruf Hasan

Associate Professor

Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University



----- Internal Examiner 2

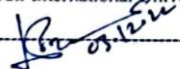
Fatama Binta Rafiq

Lecturer (Senior)

Department of Software Engineering

Faculty of Science and Information Technology

Daffodil International University



----- External Examiner

Dr. Md. Sazzadur Rahman

Associate Professor

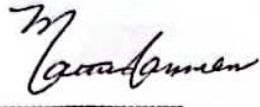
Institute of Information Technology

Jahangirnagar University

DECLARATION

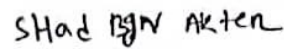
I'm Shad Bin Akter, ID: 183-35-387, a Daffodil International University student. I am announcing that I have completed my thesis under the supervision of Mr. S A M Matiur Rahmam, Department of Software Engineering. We further certify that neither this project nor any portion of this report has been submitted anywhere for the granting of any degree or certificate. This also declares that there is no plagiarism or data fabrication, and that the contents included in this study came from numerous sources and websites.

Supervised by:



Mr. S A M Matiur Rahmam
Associate Professor
Department of Software Engineering
Daffodil International University

Submitted by:



Shad Bin Akter
183-35-387
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

First and foremost, I'd want to thank Almighty Allah for his generosity in allowing me to complete my thesis report on time. I would like to offer my heartfelt appreciation to the Faculty of Science and Information Technology to maintain the thesis credit in the graduation academic program and provide me with an opportunity in the industrial work and the area of expertise.

I'd like to thank my supervisor, Mr. S A M Matiur Rahmam, Associate Professor, Department of Software Engineering. I am profoundly grateful and obliged to her for her expert, sincere, and beneficial advice, guidance and motivation to me.

I would really like to offer my heartfelt gratitude to Dr. Imran Mahmud, Professor and Head of Software Engineering Department for his relentless encouragement. I'd want to thank everyone who supported me with my thesis by making valuable suggestions. I am really glad and proud to offer my gratitude and sincere admiration to our respected faculty of the Department of Software Engineering for providing this opportunity.

I must grant with due respect the endless support and patience of my family members for finishing this thesis.

Abstract

Image steganography is the process of hiding information, which can be text, image, video or audio inside a cover image. In this paper I have proposed an approach of image steganography called the LSB (least significant bits) method. This method uses the least significant bit of image and replaces them with the bits of the information to be hidden. There is also an image quality enhancement method to enhance the image resolution if the resolution of the stego image is affected. I have compared this technique with some other methods of steganography in this paper.

Keyword: - Steganography, image steganography, LSB, encryption, decryption.

TABLE OF CONTENTS

APPROVAL	iii
DECLARATION	iv
ACKNOWLEDGEMENT	v
1 Introduction	7
2 Related works	8
3 Proposed Method.....	9
4 Discussion.....	13
5 Conclusion and Future Work.....	14
References.....	15

Image Steganography using Least significant bit (LSB)

Shad Bin Akhter

Department of Software Engineering

Daffodil international university

1. INTRODUCTION

Steganography is the practice of distorting communication by burying information among other information. Steganography involves disguising message such that potential monitors are not even aware that a message is being sent [1]. Due to its lower computational complexity, hiding images or other information in an audio file has recently caught the attention of numerous academics. Some methods use a

pseudorandom number generator to embed the information in the image's pixel coordinates, this method is independent of the secret content and image content. Confidential information the way steganography hides secret information is called concealing. Digital image with data for identification, annotation and copyright purpose. The data that is hidden will remain unaffected by changes.

Steganography originated from two Greek terms, 'stegano' that means "covered" and 'grapohos' which means "to write". The main object of steganography is to communicate secretly by preventing the viewer from seeing the genuine message.

The origin of steganography seems biological or physiological [1]. Its earliest known beginnings are from 400 BC, the Greek historian Herodotus records the story of Histaeus who employed steganography for the first time [2]. In World War 2 several steganographic methods were used. Microdots developed by the Nazis are essentially microfilm chips created at high magnification (usually over 200X). These microfilm chips are the size of periods on a standard typewriter [3]. These dots could contain pages of information, drawing, etc. the Nazis also employed invisible inks and null ciphers. One of the most noted null cipher message sent by Nazis spy follows:

Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue effects pretext for embargo on by products, ejecting suits and vegetable oils. Using the second letter from each word, the following message appears:

Pershing sails from NY June 1.

United States also used a method called Navajo "codetalkers" in World War 2. In the past few years attackers used steganography as their secret communications main method. Malicious actors used steganography to hide malicious code in twitter memes. A former GE engineer

was charged with economic espionage. The employee had encrypted files containing GE's proprietary information and hidden them in a photo of a sunset. Researchers at Guardicore Labs discovered a cryptominer that was hidden inside WAV audio files. Cybereason discovered a phishing campaign targeting US taxpayers with documents that purported to contain tax-related content, but ultimately delivered NetWire and Remcos malware – each disguised as an innocuous image file using steganographic techniques. According to a study by email security expert Proofpoint, phishing campaigns using steganography have the highest success rate of all attacks when more than one in three people targeted by them click the fraudulent email. Steganography has 4 types. Image steganography is one of the most used type of steganography. Generally steganography needs high security and capacity levels.

LSB image steganography method fulfills all the requirements of security and integrity of secret communication. LSB steganography works by replacing bits of the image 1 by 1 with the message to be hidden. The intensity of the image is only changed by 1 or 0 after hiding the information. Change in intensity is either 0 or 1 because the change at the last bit. So the pixel can slightly decrease, if so there is also an algorithm to enhance the pixel. That's why LSB is much more efficient than other methods of steganography. In medical area, it is crucial to ensure medical information security, patient information security and the growing demands for patient, client, healthcare professional and sponsor communication. Nowadays researchers using LSB technique to ensure that the information is not visible by any third party. In defense area the information is very delicate that attackers always lie up to steal those. That's why Military communication networks use sophisticated traffic security measures that go beyond just encrypting message to hide their contents.

The rest of the paper is organized as follows. The related works are presented in section 2. The proposed system is in section 3. In section 4 Discussion is presented. Lastly, the conclusion and future works are given in section 5.

2 RELATED WORKS

In recent years, steganography has become a significant topic of study with numerous used. In order to transfer the data securely and unchanged to the target LSB steganography is a trusted approach [9]. Modern image steganography is much more secure, but on a raw image the security of the method can be enhanced by combining Least significant bits (LSB), Discrete Cosine Transform (DCT) and Compression techniques [4]. Many image steganography methods were proposed. K-least significant bits are one the secure methods [5]. The security of image steganography is being enhanced day by day. The simplest method used for security purposes is LSB XOR substitution method [6]. The encoding and decoding process can be done by a random LSB insertion method [7]. The information can also be substituted with the random bit position of pixels [8]. Two hybrid image steganography algorithms that effectively combine LSB

substitution, Pixel Value Differencing (PDV) and Exploiting Modification Directions (EMD) have been developed to protect against pixel difference histogram (PDH) analysis and RS analysis [10]. The security level of the existing LSB substitution technique for RGB true color image has been enhanced using a secret key [11]. To ensure that attackers have less scope to retrieve data, a cryptographic encryption algorithm is used with the LSB approach [12]. The idea of randomly inserting and picking a pixel from a host image can be done by implementing 3D chaotic map specially 3D Chebyshev and 3D logistic maps which is called hidden map technique [13]. There is another simple but safe technique of LSB steganography to ensure the maximum possible security. Before the message is embedded on the LSB, the XOR operation is performed three times and three MSB bits are used as keys in XOR operations to simplify the encryption and decryption of message [14]. The stego key-directed adaptive least significant bit (SKA-LSB) substitution method and multi-level cryptography is a secure framework to increase payload efficiency and keep a better balance between image quality and security [15]. Stego key is encrypted using a two-level encryption algorithm (TLEA), secret data is encrypted using a multi-level encryption algorithm, and after that the encrypted data has been embedded in the host image using an adaptive LSB substitution method, depending on the secret key, red channel, MLEA and sensitive contents.

3 PROPOSED METHOD

Making a message invisible within a cover image is called image steganography. It could be anything, like: text, codes or image. In this paper the proposed method is hiding an image into another image using the LSB technique. In LSB method the bits of a cover removed by one and replace a bit of the secret message with it. So the changes in the cover image is quite invisible with normal eyes. Here is a detailed explanation of the proposed method. Figure 1 shows the flowchart of the proposed method.

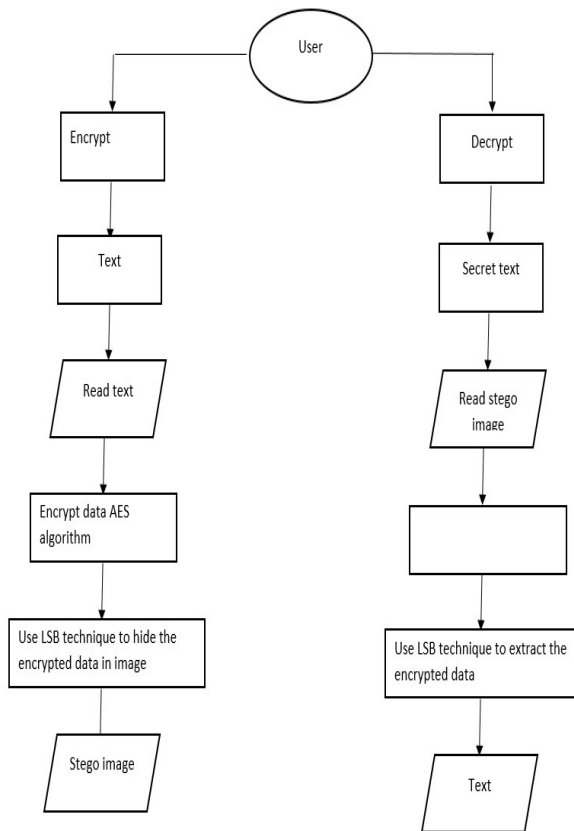


Figure 1.

In binary number, the bit furthest to the right side are called the least significant bit. Bits from right side are replacing with the bits of the hidden image which is shown in figure 2. In RGB true color image each pixel contains Red, Green and Blue. These values range from 0 – 255 (8 bit values). After converting the pixel values to binary, we go over each value individually and we sequentially replace each least significant bit with the message's bits.

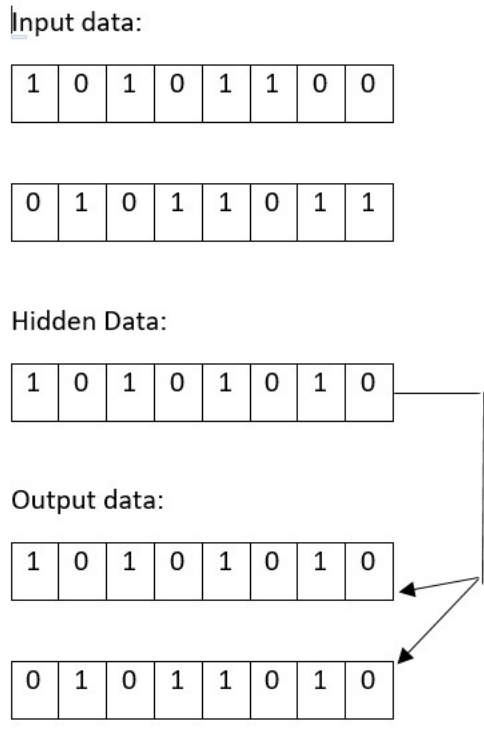


Figure 2.

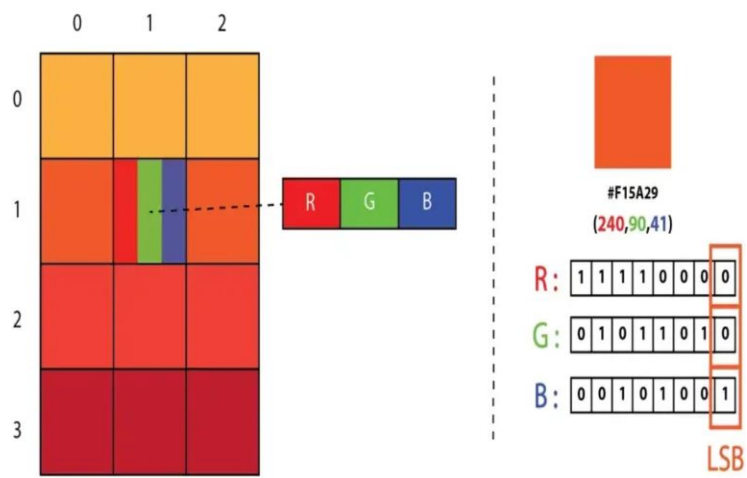


Figure 3.

After the encryption process the stego image will be sent to the receiver. Receiver can decrypt the image with a secret key that means, reverse the process. The final bits of

each pixel should be collected, stored and divided into groups of 8 before being converted back. The algorithm used in the method is given below.

Embedding algorithm:

Step 1: Get the input cover image and secret image.

Step 2: Accept the stego-key from the user and calculate the average value of them.

Step 3: Convert each character of secret message and each LSB bit of cover image from the position of average of stego-key.

Step 4: Substitute the LSB bit of cover image with binary values of secret message with respect to the starting point until the end of secret message.

Step 5: Insert the starting point until the end of secret message.

Step 6: Calculate the PSNR of original and resulting images.

Step 7: Send a stego-image to the receiver.

Extracting algorithm:

Step 1: Get the input stego calculate average value.

Step 2: Load the stego-image that is sent from the sender.

Step 3: Extract each of LSB bit from the stego image until to find out the end bit.

Step 4: Reconstruct the collecting LSB bits from the stego-image.

Step 5: Transform the LSB bits to correspondent characters.

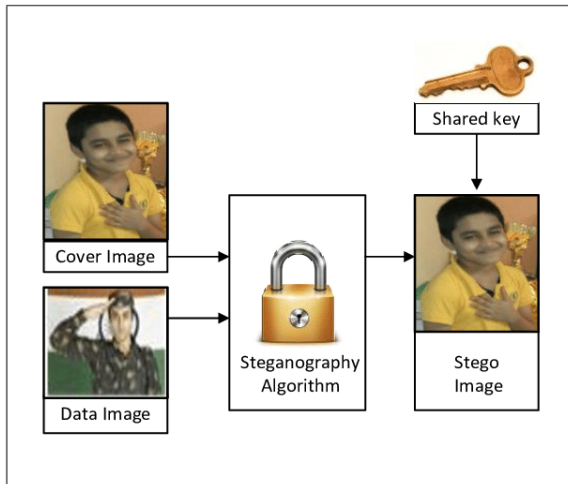


Figure 4.

DISCUSSION

The efficiency of the proposed method for merging one image into another is assessed by metric pick signal-to-noise ratio (PSNR). This ratio is used to compare the quality of an original image to one that has been compressed. The quality of the reconstructed image increase with increasing PSNR. If we don't use the LSB method for image steganographic communication the capacity of image will change, which will be suspicious to any 3rd party viewer. Suppose if a cover image is 512 Kb and we add an image into that the capacity will increase. So it viewer can easily suspect the image. That's why LSB method is proposed in this paper. By using LSB steganography we modify and remove the pixel value of a cover image and replace the value with secrete data. So the capacity will remain the same which will not visible by open eyes of 3rd party viewers when transporting it through internet. No one will suspect anything could be inside in the image.

CONCLUSION AND FUTURE WORK

In this paper, the author tried to provide a method for effectively incorporating data into an 8-bit color image. Using the LSB based technique the cover image and the secret image are first combined in the proposed technique. The proposed method can conceal image with the fewest distortions and information losses. In future a tool will be developed that will work exactly the same as the proposed method in this paper. The software is still under development.

REFERENCES

- [1]. Kahn, D. (1996, May). The history of steganography. In *International workshop on information hiding* (pp. 1-5). Springer, Berlin, Heidelberg.
- [2]. Tyagi, V. (2012). Image steganography using least significant bit with cryptography. *Journal of global research in computer science*, 3(3), 53-55.
- [3]. Judge, J. C. (2001). Steganography: past, present, future. *SANS white paper*, 30.
- [4]. Raja, K. B., Chowdary, C. R., Venugopal, K. R., & Patnaik, L. M. (2005, December). A secure image steganography using LSB, DCT and compression techniques on raw images. In *2005 3rd international conference on intelligent sensing and information processing* (pp. 170-176). IEEE.
- [5]. Elharrouss, O., Almaadeed, N., & Al-Maadeed, S. (2020, February). An image steganography approach based on k-least significant bits (k-LSB). In *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)* (pp. 131-135). IEEE.

- [6]. Arun, C., & Murugan, S. (2017, April). Design of image steganography using LSB XOR substitution method. In *2017 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0674-0677). IEEE.
- [7]. Sutaone, M. S., & Khandare, M. V. (2008, January). Image based steganography using LSB insertion technique. In *2008 IET International Conference on Wireless, Mobile and Multimedia Networks* (pp. 146-151). IET.
- [8]. Ali, U. A. M. E., Sohrawordi, M., & Uddin, M. P. (2019). A robust and secured image steganography using LSB and random bit substitution. *American Journal of Engineering Research (AJER)*, 8(2), 39-44.
- [9]. Joshi, R., Gagnani, L., & Pandey, S. (2013). Image steganography with LSB. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 2(1), 228-229.
- [10]. Pradhan, A., Sekhar, K. R., & Swain, G. (2018). Digital image steganography using LSB substitution, PVD, and EMD. *Mathematical Problems in Engineering*, 2018.
- [11]. Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In *14th international conference on computer and information technology (ICCIT 2011)* (pp. 286-291). IEEE.
- [12]. Tyagi, V. (2012). Image steganography using least significant bit with cryptography. *Journal of global research in computer science*, 3(3), 53-55.
- [13] ALabaichi, A., Al-Dabbas, M. A. A. A. K., & Salih, A. (2020). Image steganography using least significant bit and secret map techniques. *International journal of electrical & computer engineering (2088-8708)*, 10(1).

[14]. Astuti, Y. P., Rachmawanto, E. H., & Sari, C. A. (2018, March). Simple and secure image steganography using LSB and triple XOR operation on MSB. In *2018 International Conference on Information and Communications Technology (ICOIACT)* (pp. 191-195). IEEE.

[15]. Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M.

(2017). CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. *Multimedia Tools and Applications*, 76(6), 8597-8626.