STEGANOGRAPHY

[1]Nilesh N Bhoi, [2]Prem Prakash Gupta, [3]Pradeep Sharma, [4]Rahul Yadav, [5]Ms. Priyanka Singh
Department of Information Technology
ADGITM, New Delhi, India

Abstract- A Steganography is the practice of hiding a secret message inside of (or even on top of) something that is not secret. That something can be just about anything you want. These days, many examples of steganography involve embedding a secret piece of text inside of a picture. Or hiding a secret message or script inside of a Word or Excel document. The purpose of steganography is to conceal and deceive. It is a form of covert communication and can involve the use of any medium to hide messages. It's not a form of cryptography, because it doesn't involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways. Where cryptography is a science that largely enables privacy, steganography is a practice that enables secrecy – and deceit.

Keywords: Image Steganography, Data Hiding, Image Steganography Techniques, Data Embedding and Extracting

1. INTRODUCTION

Steganography is a Greek word which means concealed writing. The word steganos means covered and graphial means writing . Thus, steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the secret data in another file in such a way that only the recipient knows the existence of message. In ancient time, the data was protected by hiding it on the back of wax, writing tables, and stomach of rabbits or on the scalp of the slaves. But today's most of the people transmit the data in the form of text, images, video, and audio over the medium. In order to safely transmission of confidential data, the multimedia object like audio, video, images are used as a cover sources to hide the data. Steganography is defined as the study of invisible communication. Steganography usually deals with the ways of hiding the existence of the communicated data in such a way that it remains confidential. It maintains secrecy between two communicating parties. In image steganography, secrecy is achieved by embedding data into cover image and generating a stego-image. There are different types of steganography techniques each have their strengths and weaknesses. In this paper, we review the different security and data hiding techniques that are used to implement a steganography such as LSB, ISB, MLSB etc.

In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attackers suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed. Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of data so that no one can detect its presence.

Figure 1.1: Process Of Steganography

In steganography the process of hiding information content inside any multimedia content like image , audio, video referred as a Embedding. For increasing confidentiality of communicating data both techniques may combined. Application of Steganography:

- Confidential Communication
- Protection of Data Alteration
- Access Control System for Digital Content Distribution
- E-Commerce
- Database Systems.
- Digital watermarking.
- Secret Data Storing

2. CRYPTOGRAPHY

Cryptography: Cryptography can be used to provide message confidentiality and integrity and sender verification. The basic functions of cryptography are encryption, decryption and cryptographic hashing. In order to encrypt and decrypt messages, the sender and recipient need to share a secret. Typically this is a key, like a password, that is used by the cryptographic algorithm. The key is used by the sender to encrypt the message (transform it into cipher text) and by the recipient to decrypt the message (reverse the cipher text back to clear text). This process can be done on a fixed message, such as an e -mail, or a communications stream, such as a TCP/IP connection. Cryptographic hashing is the process of generating a fixed-length string from a message of arbitrary length. If the sender provides a cryptographic hash with the

message, the recipient can verify its integrity. Modern cryptographic systems are based on complex mathematical relationships and processes. Let's focus on the common cryptography standards used to secure computer communications and how they are used.

A compiler can be divided broadly into two phases based on their functioning: Analysis Phase and Synthesis Phase. The three basic types of cryptography in common use are symmetric key, asymmetric (public) key systems and cryptographic hash functions. Typically, the strength of a cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement. The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography.

The Least Significant Bit (LSB) is one of the main techniques in spatial domain image Steganography. The concept of LSB Embedding is simple. It exploits the fact that the level of precision in many image formats is far greater than that perceivable by average human vision. Therefore, an altered image with slight variations in crypto system is directly related to the length of the key. This assumes that there is no inherent weakness in the algorithm and that the keys are chosen in a way that fully utilizes the key space (the number of possible keys). There are many kinds of attacks that can be used against crypto systems, but these are beyond our scope here.

If you use public algorithms with no known vulnerabilities, use reasonable key lengths (most defaults

its colors will be indistinguishable from the original by a human being, just by looking at it. In conventional LSB technique, which requires eight bytes of pixels to store 1byte of secret data but in proposed LSB techniques are fine) and choose good keys (which are normally chosen for you), your communications will be very secure.

Steganography: Steganography aims to hiding information in a cover data in such a way that non-participating persons are not able to detect the presence of this information by analysing the information detection. Unlike watermarking, steganography does not intended to prevent the hidden information by opponents of removing or changing the hidden message, which is embedded in the cover data but it emphasizes on remains it undetectable. Steganography is particularly interesting for applications in which the encryption cannot used to protect the communication of confidential information.

3. STEGANOGRAPHY WITH LSB ALGORITHM

Bytes of pixels are sufficient to hold one message byte. Rest of the bits in the pixels remains the same. Steganography is the art and science of communicating in a way which hides the existence of the communication. Steganography plays an important role in information security. It is the art of invisible communication by concealing information inside other information. The term steganography is derived from Greek and literally means covered writing. A Steganography system consists of three elements: cover image (which hides the secret message),the secret message and the stegano-image(which is the cover object with message embedded inside it). A digital image is described using a 2-D matrix of the color intestines at each grid point (i.e. pixel). Typically gray images use 8 bits, whereas colored utilizes 24 bits to describe the color model, such as RGB model. The Steganography system which uses an image as the cover, there are several techniques to conceal information inside cover-image. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement.

4. STEGANOGRAPHY PROCESS

Encoding Process: The steganography technique used is LSB coding. The offset of the image is retrieved from its header. That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process. For encoding, we first take the input carrier file i.e. an image file and then direct the user to the selection of the text file.

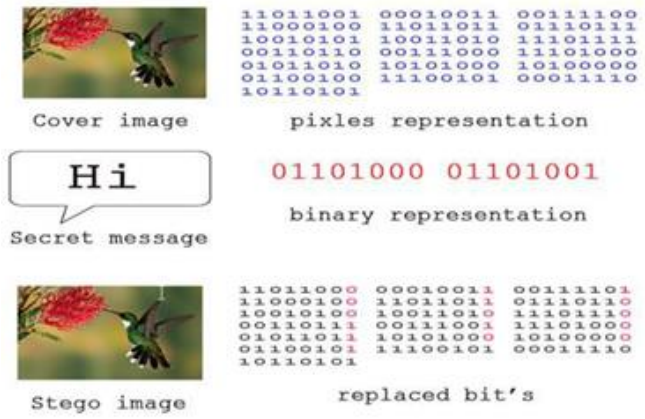

Figure 4.1 LSB Operation

Decoding Process: The offset of the image is retrieved from its header. Create the user space using the same process as in the Encoding. Using getRaster() and getDataBuffer() methods of Writable Raster and DataBufferByte classes. The data of image is taken into byte array. Using above byte array, the bit stream of original text file is retrieved into the another byte array

5. RESULT

The figure 5.1 is the image of steganography system as soon as the user runs the project. The Apache Net beams imports all the modules and after the building the project, the project starts with the below starting screen.

Figure 5.1 Starting App Screen

After the project is successfully build and run, user is shown with two button in figure 5.2:

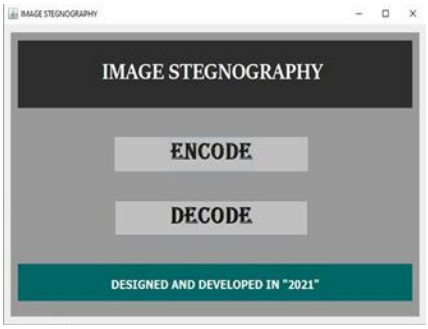

Figure 5.2 Home Page

i.e. encode and decode button. On Clicking on encode button a dialog box opens. User can type the message which the user wants to hide into the image. Click on open button and choose the image in which the message to hide.

Figure 5.3

In figure 5.3 after clicking on embed a Stenographic image is generated. The user can click on save button to share the encrypted image with hidden message over any communication network.

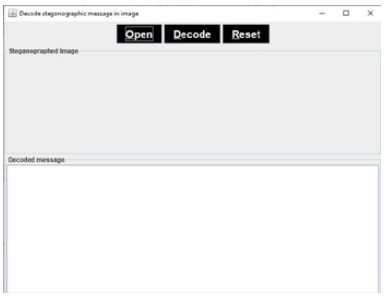

Figure 5.4 Decoding Process

On receiving the encrypted image, user has to click on decode button and open the encrypted image and click on decode button. The hidden message will be shown to the user in Decoded message dialog.

6. CONCLUSION

It is observed that through LSB Substitution Steganographic method, the results obtained in data hiding are pretty impressive as it utilizes the simple fact that any image could be broken up to individual bit-planes each consisting of different levels of information. It is to be noted that as discussed earlier, this method is only effective for bitmap images as these involve lossless compression techniques But this process can also be extended to be used for colour images where, bit plane slicing is to be done individually for the top four bit-planes for each of R, G, B of the message image.

REFERENCES

[1] Subramanian, N., Elharrouss, O., Al-Maadeed, S. and Bouridane, A., 2021. Image Steganography: A Review of the Recent Advances. IEEE Access.

[2] Liu, J., Ke, Y., Zhang, Z., Lei, Y., Li, J., Zhang, M. and Yang, X., 2020. Recent advances of image steganography with generative adversarial networks. IEEE Access, 8, pp.60575-60597.

[3] Ansari, A.S., Mohammadi, M.S. and Parvez, M.T., 2019. A comparative study of recent steganography techniques for multiple image formats. International Journal of Computer Network and Information Security, 11(1), pp.11-25.

[4] Kadhim, I.J., Premaratne, P., Vial, P.J. and Halloran, B., 2019. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, pp.299-326.

[5] Ahmed, O.M. and Abduallah, W.M., 2017. A Review on Recent Steganography Techniques in Cloud Computing. Academic Journal of Nawroz University, 6(3), pp.106-111.

[6] Luo, Y., Huang, Y., Li, F. and Chang, C., 2016. Text steganography based on ci-poetry generation using Markov chain model. KSII Transactions on Internet and Information Systems (TIIS), 10(9), pp.4568-4584.

