A First Project Final Report on

Image Steganography using LSB Method

Submitted in Partial Fullfillment of the Requirements for the degree of **BE Information Technology** under Pokhara University

Submitted by:

Dixita Poudyal, 171510

Soni Jaiswal,171530

Anita Chalaune,171538

Under the Supervision of

Dr. Roshan Chitrakar

Date:2nd January 2020

Department of Information Technology Engineering

NEPAL COLLEGE OF INFORMATION TECHNOLOGY

Balkumari, Lalitpur, Nepal

TABLE OF CONTENTS

ACKNOWLEDGEMENT

We would like to show our gratitude to our supervisor Dr. Roshan Chitrakar, Department of Engineering of Information Technology for giving us a good guideline for project. We would also like to expand our deepest gratitude to all those who have directly and indirectly guided us in

making this project.

Many people including our classmates and team members itself, have made valuable suggestions. We thank all the people for them to complete our project.

ABSTRACT

Steganography is the science of concealing a file, message, image, video etc. within the another one. This method is used to hide any secret information so that a would-be snooper is unaware about the presence of information; only dispatcher and recipient are informed about the existence of confidential information. Various ways have been proposed to encrypt and hide secret information in different cover files and a lots of researches have suggested steganography which provides the security more than the cryptography method can do which is discussed about further in this paper. However, this paper explains a GUI based application for image steganography using LSB algorithm in JAVA

Keywords: Image steganography, LSB embedding algorithm, cryptography, JAVA

INTRODUCTION

Steganography has gotten from two Greek words, steganos, which means “covered or secret”, and graphy means writing or drawing. In a simple way, steganography is copyright information hidden secretly hidden in an ancient art and young science of communication. A broad definition of the subject includes all means to communicate in a way such that the existence of the message cannot be noticed or identified.

An art and science of hiding messages to introduce secrecy in data and information security is known as cryptography. Cryptographic techniques ‘scramble’ messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether.

The main advantage of steganography algorithm is because of its simple security mechanism. Because the steganographic message is integrated invisibly and covered inside other harmless sources, it is very difficult to detect the message without knowing the existence and the appropriate encoding scheme.

The ultimate goal of this project is to implement steganography process which follows the LSB embedding process. It is a simple plan proposed; to place the embedding data at the least significant bit (LSB) of each pixel in an image. The resulting image is called stego-image.

1. Problem Statement

Security is one of the basic needs of man since creation. Security dynamics have evolved over the years according to the researches which has become a main issue these days in technical as well as non-technical fields such as bank, schools, offices and agencies, etc. So, it is found that this process can be one of the vital security factor for secure transmission of data over the network. Steganography is most often linked with the high-level technology variety that ensures the information security. For example, a word document might be hidden inside an image file, as in the preceding story.

2. Project Objectives

In this project, data security issues are primarily concentrated upon for its further transmission over a network using steganographic technique.

- To create a complete module for hiding text information behind an image file.
- To avoid drawing suspicion to the existence of hidden message
- To test the accuracy and efficiency of the module.

3. Significance of The Study

1. The main significance of the project is to limit unauthorized access and provide better security during message transmission. To meet the requirements, we use the simple and basic approach of steganography.
2. In this project, the proposed approach finds the suitable algorithm for embedding the data in an image using steganography i.e LSB which provides the better security pattern for sending messages through a network.

METHODOLOGY

Basic process

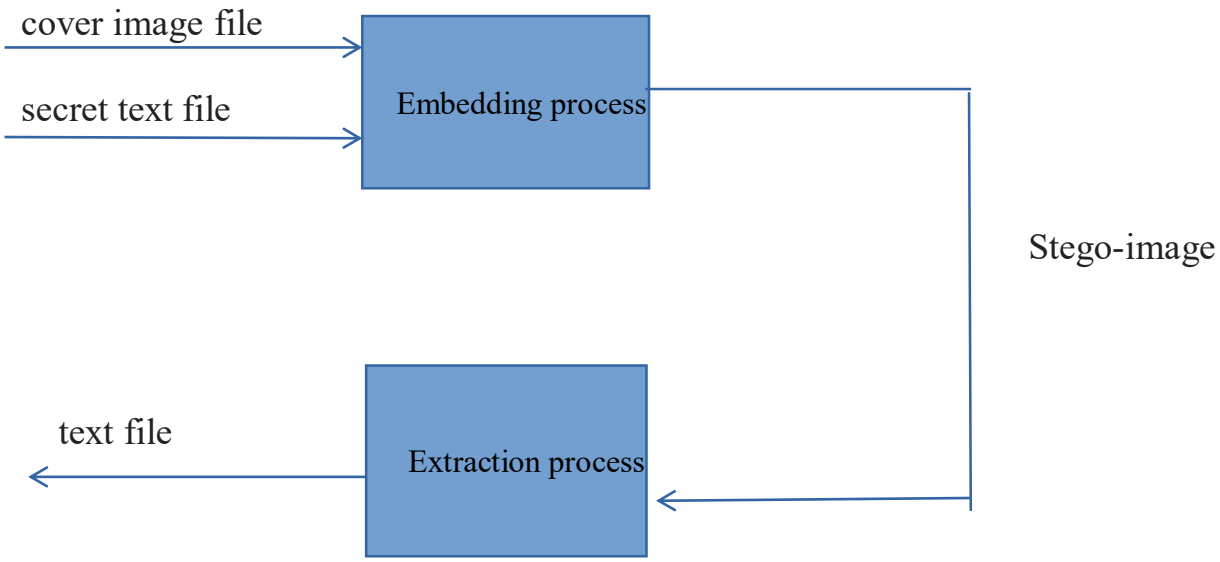

fig: block diagram of image steganography process

Here, we provide an image file i.e. a cover image, secret text to be hidden in the image and a secret key (password) which is used in both embedding and extracting process. After the embedding is done, stego-image is obtained which consists of the secret information in it. Then it is further supplied to extraction process where the image is extracted thereby accessing hidden text file using the same secret key used before.

Algorithm used:

LSB Embedding

- LSB (Least Significant Bit) substitution is the process of adjusting the least significant bit pixels of the carrier image.
- It is a simple approach for embedding message into the image.
- The Least Significant Bit insertion varies according to number of bits in an image.
- For an 8 bit image, the least significant bit i.e., the 8th bit of each byte of the image is changed to the bit of secret message.

• For 24 bit image, the colours of each component like RGB (red, green and blue) are changed.

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 its colors will be indistinguishable from the original by a human being, just by looking at it.

REVIEW

Steganography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day.

Steganography can be used for hidden communication. We have explored the limits of steganography theory and practice. We printed out the enhancement of the image steganography system using LSB approach to provide a means of secure communication. This steganography application software provided for the purpose to how to use any type of image formats to hiding any type of files inside . The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file.

Since ancient times, man has found a desire in the ability to communicate covertly. The recent explosion of research in watermarking to protect intellectual property is evidence that steganography is not just limited to military or espionage applications. Steganography, like cryptography, will play an increasing role in the future of secure communication in the “digital world”.

CONCLUSION

Finally, we approached the steganographic method to hide any text message in an image which makes a secure connection.

Steganalysis is the technique to detect Steganography.

Our method is general and can be easily extended to other LSB based steganographic method.

RECOMMENDATION

This project was made with the group effort, facing a lot of ups and downs. We had discussed what we were going to do, but due to some limitations and other factors, there are some things that we couldn't include. But whatever the outcome maybe, we are satisfied with the output and as mentioned we will definitely make a better version in near future. We have planned the following for new versions in the future.

- To hide the text in an image first of all we have to write a message and choose a cover image and encrypt it.

Secondly we open that encrypted image and decrypt it and we get the original text.

- The design seems simple, but we will try to make it more eye grabbing and attractive.

BIBLIOGRAPHY

- Amirthanjan, R.Akila, R & Deepika Chowdavarapu P., A Comparative Analysis, of ImageSteganography, *International Journal of Computer Application, 2015*
- B. Dunbar, 'A detailed look at Steganographic Techniques and their use in an Open-Systems Environment', *Sans Institute: Information Security Reading Room*, 2002.
- E. Kawaguchi, 'Applications of Steganography', *Datahide.org*, 2015.

Reference

- **https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=2ahUKEwjAnv2sweTmAhVa7HMBHeoJAfEQFjABegQIBBAB&url=https%3A%2F%2Fgithub.com%2Faagarwal1012%2FImage-Steganography-Library-Android&usg=AOvVaw3sici_4gKjBB9u8x5EFHUr**