ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 8, August 2015

An Improved LSB Image Steganography using TSFS

Ruchi[1], Mr. Vipul Goyal[2]

Student, CSE, JCDM College of Engineering, Sirsa, India [1]

Asst Professor, CSE, JCDM College of Engineering, Sirsa, India [2]

Abstract: This paper proposes steganalysis methods for extensions of least-significant bit (LSB) overwriting to both of the two lowest bit planes in digital images: there are two distinct embedding paradigms. The author investigates how detectors for standard LSB replacement can be adapted to such embedding, and how the methods of “structural steganalysis,” which gives the most sensitive detectors for standard LSB replacement, may be extended and applied to make more sensitive purpose-built detectors for two bit plane steganography. The literature contains only one other detector specialized to detect replacement multiple bits, and those presented here are substantially more sensitive. The author also compares the detectability of standard LSB embedding with the two methods of embedding in the lower two bit planes: although the novel detectors have a high accuracy from the steganographer’s point of view, the empirical results indicate that embedding in the two lowest bit planes is preferable (in some cases, highly preferable) to embedding in one.

Keywords: Steganography, Cryptography, Image, LSB (Least significant bit).

I. INTRODUCTION

Replacement of least-significant bits (LSBs) in digital images is an extremely simple form of information hiding. For the non expert steganographer, its ease of embedding, high capacity, and visual imperceptibility may prove attractive. However, it is now known that there are particular flaws which make steganalysis (detection) of this embedding method much easier than that of other additive steganography. The aim of this paper is to consider the extension to replacement of the two LSBs. Such embedding is still visually imperceptible, of even higher capacity, and still extremely simple. But there exist parallel “structural” weaknesses of such embedding, which allows us to extend the most sensitive detectors for LSB replacement to detect embedding in two bit planes; we will develop and benchmark such detectors. One might ask why a steganographer would want to extend the weak LSB embedding method to ore bit planes. It will be shown that, at least as far as the detectors presented here are concerned, it is actually somewhat better (harder to detect) to embed in two bit planes than in one.

Steganography is the art of hiding information in ways that prevent the detection of hidden messages. Steganography, derived from Greek, literally means “covered writing.” It includes a vast array of secret communications methods that conceal the message’s very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications.

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message so it cannot be understood. Steganography hides the message so it cannot be seen. A message in cipertext, for instance, might arouse suspicion on the part of the recipient while an “invisible” message created with steganographic methods will not.

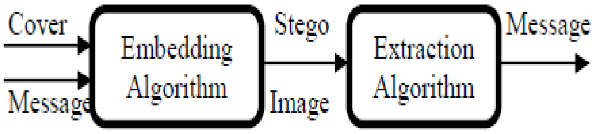


Fig 1 Basic components of Steganography

Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points.

PAST

The word Steganography technically means covered or hidden writing. Its ancient origins can be traced back to 440 BC. Although the term steganography was only coined at the end of the 15th century, the use of steganography dates back several millennia. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on

DOI 10.17148/IJARCCE.2015.4853

the scalp of slaves. Invisible ink has been in use for centuries for fun by children and students and for serious undercover work by spies and terrorists.

PRESENT

The majority of today's steganographic systems uses multimedia objects like image, audio, video etc as cover media because people often transmit digital pictures over email and other Internet communication. Modern steganography uses the opportunity of hiding information into digital multimedia files and also at the network packet level.

Least significant bit insertion

Least significant bit (LSB) insertion4 is a common, simple approach to embedding information in a cover file. Unfortunately, it is vulnerable to even a slight image manipulation. Converting an image from a format like GIF or BMP, which reconstructs the original message exactly (lossless compression) to a JPEG, which does not (lossy compression), and then back could destroy the information hidden in the LSBs 24-bit images. To hide an image in the LSBs of each byte of a 24-bit image, you can store 3 bits in each pixel. A 1,024 ´ 768 image has the potential to hide a total of 2,359,296 bits (294,912 bytes) of information. If you compress the message to be hidden before you embed it, you can hide a large amount of information. To the human eye, the resulting stego-image will look identical to the cover image.

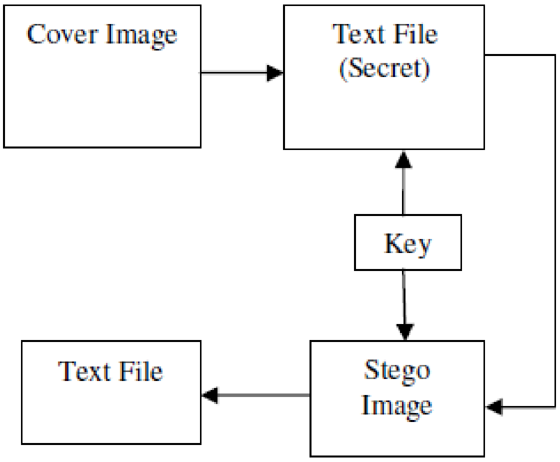


Fig 2 Steganography process

TSFS Encryption

A. Transposition
Transposition transformation changes the location of the data matrix elements by using diagonal transposition that reads the data matrix in the route of zigzag diagonal starting from the upper left corner after getting the data and pads it with *s if it is less than 16 digits.

B. Substitution
The second algorithm is substitution transformation. It replaces one data matrix element with another by applying certain function. If the element represents an alphabetic character, it then will be replaced with another character. If the element represents a number, it will be replaced with a number and if it represents a symbol, it will be replaced with a symbol.

C. Folding
The third algorithm is folding transformation. It shuffles one of the data matrix elements with another in the same entered data, like a paper fold. The data matrix is folded horizontally, vertically and diagonally. The horizontal folding is done by exchanging the first row with the last row. The vertical one is done by exchanging the first column with the last column. The diagonal fold is done by exchanging the inner cells, the upper-left cell with the down-right cell and the upper-right cell with the down-left cell

D. Shifting
The last part of the algorithm is the shifting transformation, which provides a simple way to encrypt.

II. LITERATURE REVIEW

N. F. Johnson explained in images there are two types of compression: lossy compression and lossless compression. In Lossless compression, with lossless compression, every single bit of data that was originally in the file remains after the file is uncompressed. All of the information is completely restored. The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and BMP (bitmap file). lossy compression reduces a file by permanently eliminating certain information, especially redundant information. When the file is uncompressed, only a part of the original information is still there. In this case the resulting image is expected to be something similar to the original image, but not the same as the original.
The most common algorithm belonging to this class of techniques is the Least Significant Bit (LSB) Replacement technique in which the least significant bit of the binary representation of the pixel gray levels is used to represent the message bit.
LSB manipulation is a quick and easy way to hide information but is vulnerable to small changes resulting from image processing or lossy compression. Such compression is a key advantage that JPEG images have over other formats. High color quality images can be stored in relatively small files using JPEG compression methods; thus, JPEG images are becoming more abundant on the Internet. One steganography tool that integrates the compression algorithm for hiding information is Jpeg-Jsteg. Jpeg-Jsteg creates a JPEG stego-image from the input of a message to be hidden and a lossless cover image. According to the Independent JPEG Group, the JPEG software we tested has been modified for 1-bit steganography in JFIF output files, which are composed of lossy and non lossy sections. The software combines the message and the cover images using the JPEG algorithm to create lossy JPEG stego-images [1]

Piyush Goel present a study on the Steganographic paradigm of data hiding has been presented. The problem

DOI 10.17148/IJARCCE.2015.4853

of data hiding has been attacked from two directions. The first approach tries to overcome the Targeted Steganalytic Attacks. The work focuses mainly on the first order statistics based targeted attacks. Two algorithms have been presented which can preserve the first order statistics of an image after embedding. Experimental Results reveal that preserving the image statistics using the proposed algorithm improves the security of the algorithms against the targeted attacks. The second approach aims at resisting Blind Steganalytic Attacks especially the Calibration based Blind Attacks which try to estimate a model of the cover image from the stego image. A Statistical Hypothesis Testing framework has been developed for testing the efficiency of a blind attack. A generic framework for JPEG steganography has been proposed which disturbs the cover image model estimation of the blind attacks. This framework has also been extended to a novel steganographic algorithm which can be used for any JPEG domain embedding scheme. Experimental results show that the proposed algorithm can successfully resist the calibration based blind attacks and some non-calibration based attacks as well.

In this thesis approach was aimed at preservation of the marginal statistics of a cover image. The preservation of marginal statistics helps in defeating the targeted attacks designed for specific steganographic algorithms. We covered two kinds of algorithms under this approach. The first algorithm was designed to inherently preserve the first order statistics of the cover image while embedding itself. It has been shown that this approach is able to resist first order statistics based targeted attacks while maintaining an acceptable quality of the stego image. The second algorithm was an attempt at explicitly restoring the marginal statistics of the image after data has been embedded in the image. It was found that under a specified constraint the suggested algorithm is optimal in terms of the noise added due to the restoration procedure. It was also observed that although the restoration of the image statistics can resist targeted attacks, it does not improve the security of an embedding algorithm against blind attacks. This observation was attributed to the fact that the restoration process acts as an additional source of noise in the cover signal which can be captured during feature extraction and classification. This factor limits the applicability of this approach to only targeted attacks. [2]

A. Ker proposes steganalysis methods for extensions of least-significant bit (LSB) overwriting to both of the two lowest bit planes in digital images: there are two distinct embedding paradigms. The author investigates how detectors for standard LSB replacement can be adapted to such embedding, and how the methods of “structural steganalysis,” which gives the most sensitive detectors for standard LSB replacement, may be extended and applied to make more sensitive purpose-built detectors for two bit plane steganography. The literature contains only one other detector specialized to detect replacement multiple bits, and those presented here are substantially more sensitive. The author also compares the detectability of standard LSB embedding with the two methods of embedding in the lower two bit planes: although the novel detectors have a high accuracy from the steganographer’s point of view, the empirical results indicate that embedding in the two lowest bit planes is preferable (in some cases, highly preferable) to embedding in one.

Replacement of least-significant bits (LSBs) in digital images is an extremely simple form of information hiding. For the non expert steganographer, its ease of embedding, high capacity, and visual imperceptibility may prove attractive. However, it is now known that there are particular flaws which make steganalysis (detection) of this embedding method much easier than that of other additive steganography. The aim of this paper is to consider the extension to replacement of the two LSBs. Such embedding is still visually imperceptible, of even higher capacity, and still extremely simple. But there exist parallel “structural” weaknesses of such embedding, which allows us to extend the most sensitive detectors for LSB replacement to detect embedding in two bit planes; we will develop and benchmark such detectors. One might ask why a steganographer would want to extend the weak LSB embedding method to more bit planes. It will be shown that, at least as far as the detectors presented here are concerned, it is actually somewhat better (harder to detect) to embed in two bit planes than in one. Therefore, if one must embed by replacement of bits. [3]

III.PROPOSED METHODOLOGY

1. Problem Statement

Steganography deals with hiding of information in some cover source. On the other hand, Steganalysis is the art and science of detecting messages hidden using steganography; this is analogous to cryptanalysis applied to cryptography. The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload. Hence, the major challenges of effective steganography are:-

1. Security of Hidden Communication: In order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically.

2. Size of Payload: Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory. Depending on the specific application scenarios, a trade off has to be sought.

Another form of data hiding in digital images is Watermarking. Digital watermarking is the process of embedding auxiliary information into a digital cover signal with the aim of providing authentication information. A watermark is called robust with respect to a class of transformations if the embedded information can reliably be detected from the marked signal even if degraded by any transformation within that class. Typical image degradations are JPEG compression, rotation, cropping, additive noise and quantization.

DOI 10.17148/IJARCCE.2015.4853

Image Steganalysis can extract data from an Image. To prevent data extraction, we can store data in encrypted form so that extracted data will be unused full until encryption key will be provided.
We have two keys, one for data encryption and another is for Image steganography. It will increase security.

2. Objective
1. Increase security of hidden data in Image and Prevent data extraction. This can be done using two keys. Plain text will be encrypted using DES algorithm using key1 and then cipher text will be hidded in Image using key2 with help of LSB Technique.
2. To hide the message or a secret data into an image which acts as a cover medium using LSB technique and use of TSFS Encryption.
3. Implement proposed work in MATLAB.

IV.RESULTS

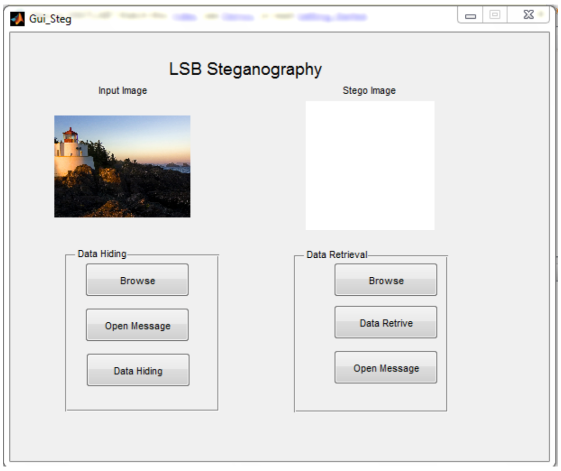
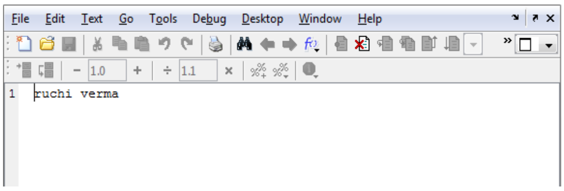
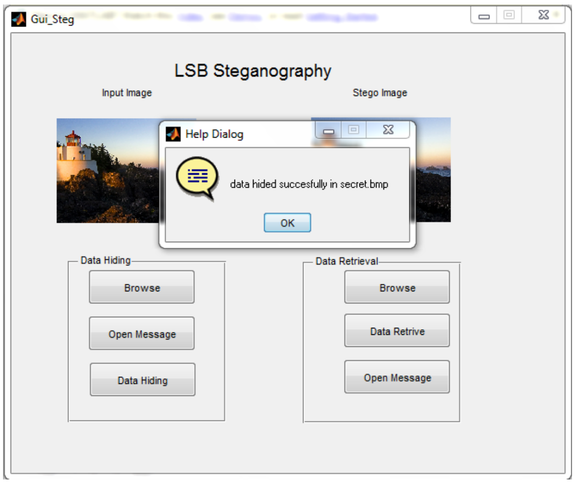


Fig 3 LSB Steganography GUI



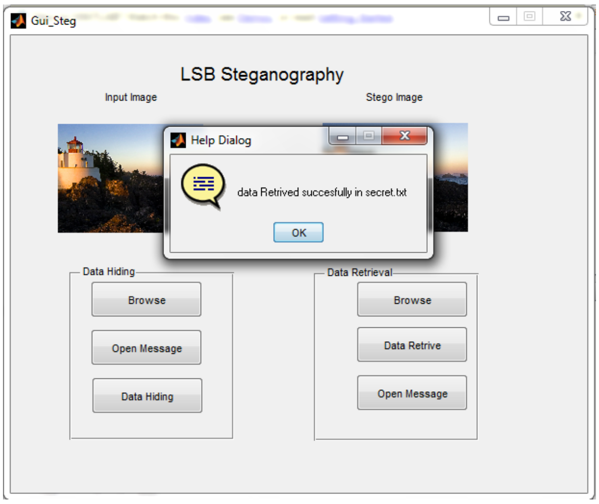
```
ruchi verma
```

Fig 4 Input Data



data hided succesfully in secret.bmp

Fig 5 Data Hiding



data Retrived succesfully in secret.txt

Fig 6 Data Extraction

V. CONCLUSION

This paper mainly probes the steganography carried by image, which combines TSFS encryption with LSB algorithm, and implements dual protect of hidden information, making the hidden information incomprehensible and invisible. Besides, the TSFS encryption algorithm changes the statistical characteristics of the secret information, and improves the lowest matching degree of its bit stream and carrier image, leading to a better imperceptibility of steganographic algorithm.

REFERENCES

[1] N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen”, 1998, IEEE Computer.
[2] Piyush Goel, “Data Hiding in Digital Images: A Steganographic Paradigm, 2008
[3] A. Ker, “Steganalysis of Embedding in Two Least-Significant Bits”, 2007, IEEE Trans. on Information Forensics and Security.
[4]Kshetrimayum Jenita Devi, “A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique”, 2013.
[5] Philip Bateman, “Image Steganography and Steganalysis”, 2008
[6] Hengfu YANG, “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”
[7] Xin Liao, “Embedding in Two Least Significant Bits with Wet Paper Coding”
[8] R M Goudar, “Compression Technique Using DCT & Fractal Compression– A Survey”
[9] J. K. Mandal, “Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images Through Exclusion of Overflow/Underflow”
[10] Rita Chhikara, “Concealing Encrypted Messages using DCT in JPEG Images”
[11] T. Morkel, “AN OVERVIEW OF IMAGE STEGANOGRAPHY”
[12] Andrew D. Ker, “Improved Detection of LSB Steganography in Grayscale Images”

DOI 10.17148/IJARCCE.2015.4853