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

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

Image Steganography Combined with TSFS using LSB

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: 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.

In this thesis a process to Increase security of hidden data in Image and Prevent data extraction has been presented. We will encrypt data by use key1 and hide data using LSB technique using key2. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. By using the key, the chance of getting attacked by the attacker is reduced.

Keywords: TSFS, LSB (Least Significant Bit), Hidden message.

I. INTRODUCTION

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 cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. In this article we discuss image files and how to hide information in them, and we discuss results obtained from evaluating available steganographic software.

Steganography is the method of unobservable communication. This is practiced through hiding data in other data. In Steganography, we use carriers to conceal the data. The carriers may be image, audio, text, video, etc. The confidential information is reserved in some carrier and then transported. The message in steganography is of two types – one is Envelop and other is confidential message .The envelop is used as carrier which envelops the message to be send.
The confidential message is wrapped inside the envelope. Steganography can be applied in numerous regions:

1. Validation: The process of justifying the oneness
2. Solitude: This confirms message reached to accurate receiver.
3. Integrity: This confirms message will not be modified in anyway.
4. Non-repudiation. : It proves that message is authentic.

Image definition

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap. An image map is a file containing information that associates different locations on a specified image with hypertext links. An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture element). Grayscale images use 8 bits for each pixel and are able to display 256 different colours or shades of grey. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour variations for the pixels of a 24-bit image are derived from three primary colours: red, green and blue, and each primary color is represented by 8 bits. Thus in one given pixel, there can be 256 different quantities of red, green and blue.

To a computer, an image is an array of numbers that represent light intensities at various points (pixels). These pixels make up the image's raster data. A common image size is 640 x 480 pixels and 256 colors (or 8 bits per pixel). Such an image could contain about 300 kilobits of data. Digital images are typically stored in either 24-bit or 8-bit files. A 24-bit image provides the most space for

DOI 10.17148/IJARCCE.2015.4854

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

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

hiding information; however, it can be quite large (with the exception of JPEG images).

Figure 1 Data Hiding in Image

Embedding Data

Embedding data, which is to be hidden, into an image requires two files. The first is the innocent-looking image that will hold the hidden information, called the cover image. The second file is the message—the information to be hidden. A message may be plain text, ciphertext, other images, or anything that can be embedded in a bit stream. When combined, the cover image and the embedded message make a stego image. 2 A stego-key (a type of password) may also be used to hide, then later decode, the message. Most steganography software neither supports nor recommends using JPEG images, but recommends instead the use of lossless 24-bit images such as BMP. The next-best alternative to 24-bit images is 256-color or gray-scale images. The most common of these found on the Internet are GIF files.
In 8-bit colour images such as GIF files, each pixel is represented as a single byte, and each pixel merely points to a colour index table (a palette) with 256 possible colours. The pixel's value, then, is between 0 and 255. The software simply paints the indicated colour on the screen at the selected pixel position.

Steganography

Steganography is the art of hiding information imperceptibly in a cover medium. The word "Steganography" is of Greek origin and means "covered or hidden writing". The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganographic techniques try to exploit the digital media images, audio files, video files etc.

Steganography and cryptography are cousins in the spy craft family. Cryptography scrambles a message by using certain cryptographic algorithms for converting the secret data into unintelligible form. On the other hand, Steganography hides the message so that it cannot be seen. A message in cipher text might arouse suspicion on the part of the recipient while an "invisible" message created with steganographic methods will not. Anyone engaging in secret communication can always apply a cryptographic algorithm to the data before embedding it to achieve additional security. In any case, once the presence of hidden information is revealed or even suspected, the purpose of steganography is defeated, even if the message content is not extracted or deciphered.

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. Steganography and watermarking differ in a number of ways including purpose, specification and detection/extraction methods.

The most fundamental difference is that the object of communication in watermarking is the host signal, with the embedded data providing copyright protection. In steganography the object to be transmitted is the embedded message, and the cover signal serves as an innocuous disguise chosen fairly arbitrarily by the user based on its technical suitability. In addition, the existence of the watermark is often declared openly, and any attempt to remove or invalidate the embedded content renders the host useless. The crucial requirement for steganography is perpetual and algorithmic undetectability. Robustness against malicious attack and signal processing is not the primary concern, as it is for watermarking.

Image steganography

Image steganography Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego-image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego- image unauthentic persons can only notice the transmission of an image but can't see the existence of the hidden message.

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

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

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

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 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 nonexpert 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.OBJECTIVES

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

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

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

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.

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 TSFS algorithm using key1 and then cipher text will be hidden 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.
3. Implement proposed work in MATLAB.

IV. PROPOSED METHODOLOGY

The Steganalytic attacks developed till date can be classified into visual and statistical attacks.

The statistical attacks can further be classified as

1. Targeted Attacks
These attacks are designed keeping a particular steganographic algorithm in mind. These attacks are based on the image features which get modified by a particular kind of steganographic embedding. A particular steganographic algorithm imposes a specific kind of behaviour on the image features.

2. Blind Attacks
The blind approach to steganalysis is similar to the pattern classification problem. The pattern classifier, in our case a Binary Classifier, is trained on a set of training data. The training data comprises of some high order statistics of the transform domain of a set of cover and stego images and on the basis of this trained dataset the classifier is presented with images for classification as a non-embedded or an embedded image. Many of the blind Steganalytic techniques often try to estimate the cover image statistics from stego image by trying to minimize the effect of embedding in the stego image.

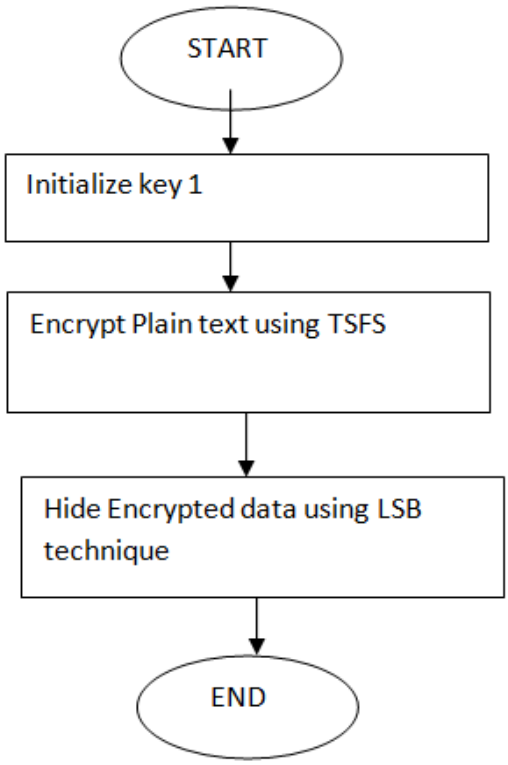

Figure 2 Flow Chart

V. CONCLUSION AND FUTURE WORK

All the algorithms study the behaviour of the cover image while ignoring the message bit stream. It may be possible to design some encoding functions, which given a cover image and an embedding algorithm can modify the message stream such that it becomes more suitable for embedding than the original bit stream. This kind of steganography can be useful even in the "Active Warden Framework" of steganography because firstly the modified message stream will be introducing less artifacts in the cover. Secondly, even if the embedding algorithm is known to the attacker, the exact message sequence cannot be reconstructed unless the attacker has the knowledge of the encoding function.

Another possible direction of research can be formulated as a problem of "Image Retrieval". It is based on searching for a suitable cover image given a message sequence and the embedding algorithm. This may be possible through

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

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

maintaining a huge image database and given any message sequence and a pseudo-random key for generating embedding locations, we search for a cover image from the database that will generate a stego image with minimum amount of changes. The change criterion considered for searching can be dependent on the features used by the corresponding Steganalytic attacks. Some other possible ideas can be borrowed from the field of "Visual Cryptography" which encrypts a message by distributing the decoding key into different images such that the message can be broken only by a proper combination of these images

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"