ISSN:2229-6093

Protection through Oblivion

'An Image Based Steganography'

T Chandra Sekhara Reddy[1], D Prasad[2], B.Venkateswara Reddy[3]

Assoc.Professor, Dept. of CSE, Vikas College of Engineering & Technology, Nunna,Vijayawada, A.P., India.
Assoc.Professor, Dept. of CSE, D.V.R & Dr. H.S MIC College of Technology, Kanchikacherla, A.P., India.

Assoc.Professor, Dept. of ECE, Vikas College of Engineering & Technology,Nunna,Vijayawada, A.P., India.

chandu.tummuru@gmail.com, dprasad.vza@gmail.com, bheemireddyv@gmail.com

Abstract - *The growth of high speed computer networks and that of the Internet, in particular, has increased the ease of Information Communication. Ironically, the cause for the development is also of the apprehension - use of digital formatted data. In comparison with Analog media, Digital media offers several distinct advantages such as high quality, easy editing, high fidelity copying, compression etc. But this type of advancement in the field of data communication in other sense has hiked the fear of getting the data snooped at the time of sending it from the sender to the receiver. So, Information Security is becoming an inseparable part of Data Communication. In order to address this Information Security, Steganography plays an important role This paper includes review of existing methods and techniques for image based steganography and a new steganographic technique based on the file hybridization. In contrast to other methods of steganography where data embedded in image work on the principle of only one image file, the proposed method works on more than one image and focus on increased multilevel security.*

Keywords - Analog media, Digital media Setganography, image.

1. Introduction

Information is the wealth of any organization. This makes security-issues top priority to an organization dealing with confidential data. Whatever is the method we choose for the security purpose, the burning concern is the degree of security. Steganography is the art of covered or hidden writing [1]. The difference between Steganography and cryptography is that Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed inside a digital Picture, Video or Audio file. What Steganography essentially does is exploit human perception; human senses are not trained to look for files that have information hidden inside of them.

2. Overview of Steganography

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). The term "Steganography" came into use in 1500's after the appearance of Trithemius' book on the subject "Steganographia". The word "Steganography" technically means "covered or hidden writing". Its ancient origins can be traced back to 440 BC. In ancient times, messages were hidden on the back of wax writing tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been in use for centuries—for fun by children and students and for serious espionage by spies and terrorists [2, 3]. 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 [4]. In modern approach, depending on the nature of cover object, steganography can be divided into five types: Text Steganography, Image Steganography, Audio Steganography, Video Steganography and Protocol Steganography. So, in the modern age so many steganographic techniques have been designed which works with the above concerned objects. With respect to Steganography there is a problem of unauthorized data access, often taken as Steganalysis

[5]. Steganalysis is a process in which a steganalysis cracks the cover object to get the hidden data. It is hoped that Dual Steganography, Steganography along with Cryptography may be some of the future solution for this above mentioned problem.

3. Surveys of Methods And Experiments

Information can be hidden inside a multimedia object using many suitable techniques. In this section, we will discuss different techniques or methods which are often used in image based steganography.

3.1 Image Steganography

To hide information, straight message insertion may encode every bit of information in the image or selectively embed the message in "noisy" areas that draw less attention—those areas where there is a great deal of natural color variation. The message may also be scattered randomly throughout the image. A number of ways exist to hide information in digital media. Common approaches include

- Least significant bit insertion
- Masking and filtering
- Redundant Pattern Encoding
- Encrypt and Scatter
- Algorithms and transformations

Each of these techniques can be applied, with varying degrees of success.

3.1.1 Least significant bit insertion

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works well for image, audio and video steganography. To the human eye, the resulting image will look identical to the cover object [1, 3]. For example, if we consider image steganography then the letter A can be hidden in three pixels (assuming no compression). The original raster data for 3 pixels (9 bytes) may be

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

The binary value for A is 10000001. Inserting the binary value for A in the three pixels would result in

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

On average, LSB requires that only half the bits in an image be changed. You can hide data in the least and second least significant bits and still the human eye would not be able to discern it. The resultant image for the above data insertion and the original cover image are given below.

Fig. 1: The cover image

Fig. 2: The stego-image (after A is inserted)

3.1.2 Masking and filtering

Masking and filtering techniques are mostly used on 24 bit and grey scale images. They hide info in a way similar to watermarks on actual paper and are sometimes used as digital watermarks. Masking images entails changing the luminance of the masked area. The smaller the luminance change, the less of a chance that it can be detected. Observe that the luminance in Figure 2 is at 15% in the mask region if it was decreased then it would be nearly invisible [1, 2, 6]. Masking techniques embed information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the "noise" level. This makes it more suitable than LSB with, for instance, lossy JPEG images.

3.1.3 Redundant Pattern Encoding

Patchwork and other similar tools do redundant pattern encoding, which is a sort of spread spectrum technique. It works by scattering the message throughout the picture. This makes the image more resistant to cropping and rotation. Smaller secret images work better to increase the redundancy embedded in the cover image, and thus make it easier to recover if the stego-image is manipulated [1, 2].

3.1.4 Encrypt and Scatter

The Encrypt and Scatter technique tries to emulate white noise. It is mostly used in image steganography. White Noise Storm is one such program that employs spread spectrum and frequency hopping. It does this by scattering the message throughout an image on eight channels within a random number that is generated by

the previous window size and data channel. The channels then swap rotate, and interlace amongst each other. Each channel represents one bit and as a result there are many unaffected bits in each channel. This technique is a lot harder to extract a message out of than an LSB scheme because to decode you must first detect that a hidden image exists and extract the bit pattern from the file. While that is true for any stego-image you will also need the algorithm and stego key to decode the bit pattern, both of which are not required to recover a message from LSB. Some people prefer this method due to the considerable amount of extra effort that someone without the algorithm and stego-key would have to go through to extract the message. It is also as susceptible as straight LSB to image degradation due to image processing [1, 6].

3.1.5 Algorithms and transformations

LSB modification technique for images does hold good if any kind of compression is done on the resultant stego-image e.g. JPEG, GIF etc [7]. JPEG images use the discrete cosine transform to achieve compression. DCT is a lossy compression transform because the cosine values cannot be calculated exactly, and repeated calculations using limited precision numbers introduce rounding errors into the final result. Variances between original data values and restored data values depend on the method used to calculate DCT [8, 9, 10].

4. Evaluation

All the above mentioned algorithms for image steganography have different strong and weak points and it is important to ensure that one uses the most suitable algorithm for an application. The most important requirement is that a steganographic algorithm has to be imperceptible. Following criteria has been proposed for imperceptibility of an algorithm:

Invisibility – The invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised [11].

Payload capacity – Unlike watermarking, which needs to embed only a small amount of copyright information, steganography in other hand requires sufficient embedding capacity [12].

Robustness against statistical attacks – Statistical steganalysis is the practice of detecting hidden information through applying statistical tests on image data. Many steganographic algorithms leave a "signature" when embedding information that can be easily detected through statistical analysis.

Robustness against image manipulation – while being transmitted the image may undergo changes by an active attacker in an attempt to remove hidden Information. Image manipulation, such as cropping or rotating, can be performed on the image. These manipulations may destroy the hidden message. It is preferable for steganographic algorithms to be robust against malicious changes to the image

Independent of file format – With many different image file formats used on the Internet, it might seem suspicious that only one type of file format is continuously communicated between two parties. The most powerful steganographic algorithms thus possess the ability to embed information in any type of file.

Unsuspicious files – This requirement includes all characteristics of a steganographic algorithm that may result in images that are not used normally and may cause suspicion. Abnormal file size, for example, is one property of an image that can result in further investigation of the image by a warden.

The levels at which the algorithms satisfy the requirements are defined as high, medium and low. A high level means that the algorithm completely satisfies the requirement, while a low level indicates hat the algorithm has a weakness in this requirement. A medium level indicates that the requirement depends on outside influences, for example the cover image used. LSB in GIF images has the potential of hiding a large message, but only when the most suitable cover image has been chosen [1]. The ideal, in other words a perfect steganographic algorithm would have a high level in every requirement. Unfortunately in the algorithms that are evaluated here, there is not one algorithm that satisfies all of the requirements. Thus a trade-off will exist in most cases depending upon the need.

5. Discussion

LSB is the most popular and straight forward technique for image steganography but it is also most vulnerable to attacks. It is very easy to find data present in image using steganalysis if we are using LSB method. Also it results in image degradation if amount of data to be

hidden is more. Masking is more robust than LSB insertion with respect to compression, cropping, and some image processing. This technique actually extends an image data by masking the secret data over the original data as opposed to hiding information inside of the data. Encryption and scatter technique provides more security as it is harder to detect but as like LSB it results in degradation of the image. So the major issue while discussing the steganography is the robustness against attacks. An ideal algorithm is one that fulfills all the requirements discussed above.

6. Proposed Work

All the methods used for embedding data in an image work on the principle of one image file. A new technique can be designed based on the concept that a single image file may be divided into two or more sub image files and based on our requirements. We can embed the required data into a particular chosen sub image file which is, of course, a part of mother image file. This concept helps us in designing a methodology for both hiding and extracting information.

In contrast to the LSB scheme being used for hiding the data, our main purpose here is to consider the entire byte representing any particular pixel for storing the information. Consequently, by the process of replacing the entire byte for embedding information in the container Image, only one pixel can be used to store three characters, whereas by LSB technique one need a minimum of nine pixels to store these three characters as three pixels are required to store a single character. Further, if we replace all pixel values of an image then the entire image generally changes and may look completely like another image of suspicious. However, by the use of the concept of hybridization both the supporting file and the container file together give the impression of a normal unsuspicious image file. Again when the volume of data to be sent is comparatively less than the container image file, instead of choosing all pixels for replacement a selected number of pixels can be considered for our purpose.

Hybrid File creation and Data Extraction

Arithmetic or Logical operations can be performed on pixel-by-pixel basis between two or more images. For an example, subtraction of two images result in a new image whose pixel at co-ordinate (x, y) is the difference between the pixels as the same locations in the two images being subtracted. Depending on the hardware or software being used, the actual mechanism of implementing arithmetic, logic operation can be done sequentially. In this method, first a supporting image is selected and then based on our requirements (i.e. the size of message) we select the appropriate container file. If we consider the size of the supporting image as, M1 x N1, then we can place the container file inside the supporting file in a region defined by A(x, y) and B(x + r, y + s) for a suitable value of r and s,
where $0 \leq r \leq M1$ and $0 \leq s \leq N1$

7. Conclusion

The suitability of steganography as a tool to conceal highly sensitive information has been discussed by using a new methodology sharing the concept of hybridization and a multilevel of security of data is achieved. This suggests that an image containing encrypted data can be transmitted to any where across the world in a complete secured form. Downloading such image and using it for many times will not permit any unauthorized person to share the hidden information. Industries like music, film, publishing and organization like ministry and military will definitely be highly benefited by the use of such techniques. So the use of steganography and cryptography collectively can be used for increasing the security and robustness of the technique against the attacks.

References

[1] Johnson, N. F. and Jajodia, S. (1998). Exploring steganography: Seeing the unseen. Computer, 31(2):26–34.

[2] Robert Krenn. Steganography and steganalysis.

[3] Alain C. Brainos II. A Study Of Steganography And The Art Of Hiding Information.

[4] Niels Provos, Peter Honeyman, Hide and Seek: Introduction to Steganography (2003).

[5] Debashis Ganguly. Swarnendu Mukherjee, Mohit Mundhra (2006). Digital Watermarking: a New Approach. In Proc. 41st Annual conference, CSI'06, paper no. 11.

[6] Francesco Queirolo. Steganography in Images.

[7] Kathryn Hempstalk. Hiding Behind Corners: Using Edges in Images for Better Steganography .

[8] Westfeld, A. (2001). F5-a steganographic algorithm: High capacity despite better steganalysis. In

Proc. 4th Int'l Workshop Information Hiding, pages 289–302.

[9] W. Brown and B.J. Shepherd, Graphics File Formats: Reference and Guide, Manning Publications, Greenwich, Conn, 1995.

[10] E. Koch, J. Rindfrey, and J. Zhao, "Copyright Protection for Multimedia Data," Proc. Int'l Conf. Digital Media and Electronic Publishing, Leeds UK 1994.

[11] Zenon Hrytskiv, Sviatoslav Voloshynovskiy, Yuriy Rytsav., Cryptography and Steganography of Video information in modern communication, Electronics and Energetics, Vol 11, No. 1, 115-225.

[12] Dean Lewandowski, Mike Palmisano., Steganography.