An Efficient Data Hiding Technique for Steganography

P. Karthiga Lakshmi
Second year M.E – CSE
Holycross Engineering College, Tuticorin. India.

ABSTRACT- Bose Chaudhuri Hochquenghem (BCH) based data hiding scheme for JPEG steganography is presented. Traditional data hiding approaches hide data into each block, where all the blocks are not overlapping each other. Two consecutive blocks can be overlapped to form a combined block which is larger than a single block, but smaller than two consecutive non overlapping blocks in size. In order to embed more amounts of data into the combined block than a single block. A way to get a joint solution for hiding data into two blocks with intersected coefficients such that any modification of the intersected area does not affect the data hiding process into both blocks. Due to hiding more amounts of data into the intersected area, embedding capacity is increased. The nonzero DCT coefficient stream is modified to achieve better steganalysis and to reduce the distortion impact after data hiding. Reducing distortion between the cover object and stego object is an important issue for steganography.

Index Terms- BCH, Steganography, Less Detectable Data Hiding.

I. INTRODUCTION

Network security is becoming more and more important as people spend more and more time connected. Compromising network security is often much easier than compromising physical or local security, and is much more common. Security in computer networks is an extremely active and broad area of research, as networks of all sizes are targeted daily by attackers seeking to disrupt or disable network traffic.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Generally, messages will appear to be something like images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible ink between the visible lines of a private letter. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.

As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

A. OBJECTIVE

The main objective is to make the transmitted information invisible by embedding the information in the cover medium. It is used to enhance the security and robustness of the information against attacks.

II. DATA HIDING SCHEME

1. A modification to the JPEG algorithm that inserts LSB's in some of the lossless stages or pilots the rounding of the coefficients of the DCT.
2. Steganography can be said to protect both messages and communicating parties.
3. An attacker cannot usually even know if the message was embedded, and it will be very hard to extract it without knowing the right keys.

Two consecutive blocks can be overlapped to form a combined block. Hiding more amounts of data into the intersected area. Get a joint solution for intersected coefficients. 8 bits be hidden into 15 coefficients from a1 to a15 and another eight bits into the coefficients from a11 to a25.

III. SYSTEM ARCHITECTURE

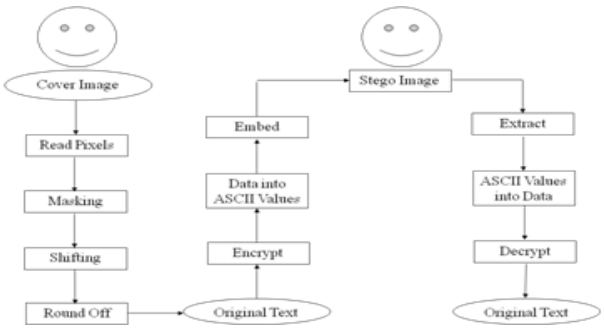

Fig. 1 Overall system architecture

The overall system architecture is given in fig 1.1 above where the secret information has been hidden in the cover images. Then read pixel by pixel, masking and shifting followed by the round off. Finally, the data would be hidden and extracted only by the intended sender and receiver.

1. Carrier File - A file which has hidden information inside of it.
2. Steganalysis - The process of detecting hidden information inside of a file.
3. Stego-Medium - The medium in which the information is hidden.
4. Redundant Bits - Pieces of information inside a file which can be overwritten or altered without damaging the file.
5. Payload - The information which is to be concealed.

A. MODULES

In order to achieve an efficient data hiding technique for the protection of confidential data from the attacker. The process has been divided into separate modules. They are as follows:

1. Reading a pixel
2. Masking
3. Shifting
4. Round off
5. Encrypt
6. Convert data into ASCII values
7. Embed data into an image
8. Extract data from image
9. Convert ASCII values into data
10. Decrypt

Divide the task of embedding hidden information in a cover medium into two steps;

1. Identification of redundant bits: Redundant bits can be modified without detectably degrading the cover medium.

2. The selection of bits in which the hidden information should be placed.

IV. PROBLEM DEFINITION

The main advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages, no matter how unbreakable will arouse suspicion, and may in themselves be incriminating. In computing, the detection of steganographically encoded packages is called steganalysis. The simplest method to detect modified files, however, is to compare them to known originals. Easy to protect the digital data and provide privacy of information transmitted across the World Wide Web. To make the transmitted information invisible by embedding the information in a cover media and try to enhance the security and the robustness of the information against attacks and image processing techniques.

A. ADVANTAGES

1. Hide more amount of data than existing system.
2. More security.
3. Hackers cannot guess about the pixel color values.

V. HIDING A MESSAGE INSIDE IMAGES

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in news groups. The use of steganography is which detects the presence of hidden messages inside images that were posted on the net. However, after checking one million images, no hidden messages were found, so the practical use of steganography still seems to be limited. To hide a message inside an image without changing its visible properties, the cover source can be altered in "noisy" areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations involve the usage of the least-significant bit (LSB).

VI. LEAST SIGNIFICANT BIT METHOD

The popular and oldest method for hiding the message in a digital image is the LSB method. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.

For example data bits 01100101 are tried to hide into an 8 bit color image. According to this technique 8 consecutive pixels from top left corner

of the image are selected. The binary equivalent of those pixels may be like this:

00100101 11101011 11001010 00100011
11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become:

00100100 11101011 11001011 00100010
11111000 11101111 11001110 11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise

LSB - Uses

1. Storing passwords and/or other confidential information.
2. Covert communication of sensitive data.
3. Speculated uses in terrorist activities.
4. Being widely used to hide and/or transfer illegal content.

VII. REASONS FOR USING DIGITAL IMAGES

1. It is the most widely used medium being used today.
2. Takes advantage of our limited visual perception of colors.
3. This field is expected to continually grow as computer graphics power also grows.
4. Many programs are available to apply steganography.

VIII. IMAGE ATTRIBUTES

1. Digital images are made up of pixels.
2. The arrangement of pixels make up the image's "raster data" .
3. 8-bit and 24-bit images are common.
4. The larger the image size, the more information you can hide. However, larger images may require compression to avoid detection.

IX. STEGANALYSIS

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. Unlike cryptanalysis, where it is obvious that intercepted data contains a message though that message is encrypted, steganalysis generally starts with a pile of suspect data files, but little information about which of the files, if any, contain a payload. The steganalyst is usually something of a forensic statistician, and must start by reducing this set of data files which is often quite large; in many cases, it may be the entire set of files on a computer to the subset most likely to have been altered.

The problem is generally handled with statistical analysis. A set of unmodified files of the same type, and ideally from the same as the set being inspected, are analyzed for various statistics. Some of these are as simple as spectrum analysis, but since most image and audio files these days are compressed with lossy compression algorithms, such as JPEG and MP3, they also attempt to look for inconsistencies in the way this data has been compressed. This distortion is predictable, and simple steganographic encoding algorithms will produce artifacts that are detectably unlikely.

One case where detection of suspect files is straightforward is when the original, unmodified carrier is available for comparison. Comparing the package against the original file will yield the differences caused by encoding the payload and thus the payload can be extracted.

X. CONCLUSION

Image Steganography as a whole has existed in many forms throughout much of history. Lossless compression of images with a great deal of color variation work best as a cover image to embed a message. Image Steganography can be used as beneficial tool for privacy

The project "Steganography" after being tested and was found to be achieving what is meant for. But this system never provides a full proof solution for all their problems in the user point of view. The system has been designed in such a way that it can be modified with very little effort when such a need arises in the future. The system has been found to work efficiently and effectively. Due to its higher user friendliness, others may use these documents as a prototype for developing similar application.

By using the properties of the DCT and the frequency domain developed the zeros hiding method. Zeros hiding proved to be easier to analyze than bit-o-stego and can hide significantly more data. Bit-o-stego can only hide data in coefficients that were not dropped, thus limiting the amount of data can hide. It greatly enhances the effectiveness of the steganography since it uses a key, making it much more challenging to detect. It is more effective, but the complexity of bit-o-stego makes

it more promising. The methods and accompanying detection schemes developed broadened of steganography which unlike encryption allows secret data to be traded hands without raising an eyebrow.

XI. FUTURE ENHANCEMENT

Due to time and computing limitations, could not explore all facets of steganography and detection techniques. The method which is unable to explore was to analyze the noise of the pictures. Adding hidden data adds random noise, so it follows that a properly tuned noise detection algorithm could recognize whether or not a picture had steganographic data or not.

Future enhancements and plans which are envisioned for the system are the following:

1. The stego image which contains the confidential data is visible as it is the cover image.
2. Going to hide the data in an image after encrypt the confidential information and extract the data but which must be decrypt by the same key that was used to encrypt the data.
3. The development of a system that will utilize the Steganographic Obliterator on incoming and email messages and attachments.

ACKNOWLEDGEMENT

First and foremost, I would like to thank "The Almighty", the lord of all creations who is by His abundant grace sustained me to work on this project successfully. The work on this paper was guided by Mr. R. Resington Director of Research and Development (CanDo Automation) and Mr. A. Jeyamurugan M.E., Assistant Professor, for being instrumental in the completion of our project with his complete guidance.

I also thank all of my family and friends for their help in making this project a successful one.

REFERENCES

[1] Sachnev and Kim, Modified BCH data hiding scheme for JPEG Steganography,in Proc of 10th USENIX Security Symposium, Washington, DC, 24–24(2012).

[2] R Zhang, V Sachnev, HJ Kim, Fast BCH syndrome coding for steganography. Lect Notes Comput Sci. 5806, 48–58 (2009).

[3] V Sachnev, HJ Kim,R Zhang,Less detectable JPEG steganography method based on heuristic optimization and BCH syndrome coding, in Proc of ACM Workshop on Multimedia and Security, Princeton, NJ, 131–139 (September 7–8,2009).

[4] J Fridrich, T Filler, Practical methods for minimizing embedding impact in steganography, in Proc EI SPIE, San Jose, CA, 6505,2–3 (2007).

[5] K Solanki, A Sakar, BS Manjunath, YASS: Yet another steganographic scheme that resists blind steganalysis. Lect Notes Comput Sci. 2939, 154–167 (2007).

[6] J Fridrich, Minimizing the embedding impact in steganography, in Proc of ACM Multimedia and Security workshop, Geneva, Switzerland, 2–10 (September 26–27, 2006).

[7] H Noda, M Niimi, E Kawaguchi, Application of QIM with dead zone for histogram preserving JPEG steganography, in Proc of ICIP, Geneva, Italy,(2005).

[8] J Fridrich, M Goljan, D Soukal, Wet paper coding with improved embedding efficiency. IEEE Trans Inf Secur Forensics. 1(1),102–110 (2005).

[9] J Fridrich, M Goljan, D Soukal, Perturbed quantization steganography using wet paper codes, in Proc of ACM Workshop on Multimedia and Security, Magdeburg, Germany, Z–15 (September 20–21, 2004).

[10] J Eggers, R Bauml, B Girod, A communications approach to steganography, in Proc of EI SPIE, San Jose, CA, 4675, 26– 37 (2002).

[11] N Provos, Defending against statistical steganalysis, in Proc of 10th USENIX Security Symposium, Washington, DC, 24–24 (2001).