Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.55 – 61

IMAGE STEGANOGRAPHY USING DESYNCHRONIZATION

Suchitra Sinha[#], Prof. Prateek Gupta[*]

[#]Department of Computer Sc & Engg, SRIST, RGPV University, Jabalpur, MP, India
suchitrasinha884@gmail.com

[*]Head of Department, Computer Sc. & Engg, SRIST, RGPV University, Jabalpur, MP, India
pguptace@yahoo.com

Abstract— Steganography is the art and science of hidden communication. There are two important aspects of the steganography system: capacity and security. Steganography and cryptography share the objective of protecting secret information. Cryptography encrypts the secret information prior to communication, whereas steganography hides the existence of the secret information. Steganography leaves behind detectable traces in the stego object and modifies the statistical properties. Detecting the presence of distorted statistical properties is called statistical steganalysis. The spatial de-synchronization operation is used to hide the embedding domain from the attacker by randomizing the embedding domain. This paper is based on the application of spatial de-synchronization in image Steganography.

Keywords— Steganography, Cryptography, Steganalysis, Image Processing, Cover Image, Stego Image, Cipher Text, Image Format, Desynchronization.

I. INTRODUCTION

Steganography is an art of sending a secrete message under the camouflage of a carrier content. The goal of steganography is to mask the very presence of communication, making the true message not discernible to the observer. It aims to embed secret data into a digital cover media, such as digital audio, image, video, etc., without being suspicious.

Steganography hides the existence of a message by transmitting information through various carriers. Its goal is to prevent the detection of a secret message. A typical steganography system consists of three objects: cover object (which hides the secret message), the secret message and the stego object (which is the cover object with message embedded inside it). Refer Figure-1 for general view of steganography.

The term steganography literally means ―covered writing‖.
The objective of steganography is to communicate information in an undetectable manner such that when the messages are observed by unintended recipient there will not be enough evidence that the messages conceal additional secret data [4].

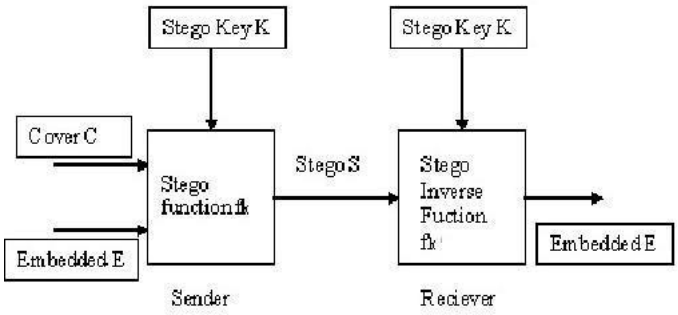

Figure 1: View of Steganography

The protection of sensitive information against unauthorized access or fraudulent changes has been of prime concern throughout the centuries. Modern communication techniques, using computers connected through networks, make all data even more vulnerable for these threats. Also, new issues have come up that were not relevant before, e.g. how to add a (digital) signature to an electronic document in such a way that the signer cannot deny later on that the document was signed by him.

Cryptology addresses the above issues. It is at the foundation of all information security. The techniques employed to this end have become increasingly mathematical of nature. Figure-2 shows the major branches of cryptology.

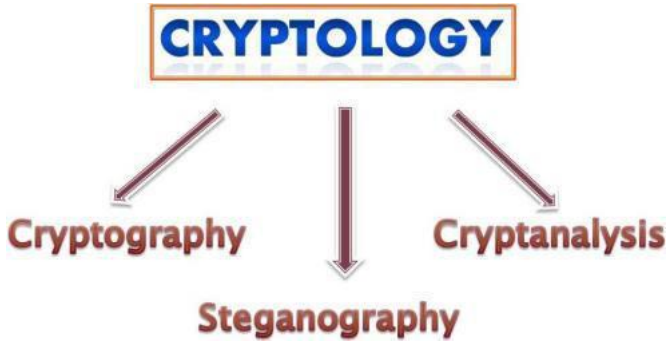

Figure 2: Branches of Cryptology

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription.
Cryptography systems can be broadly classified into symmetric-key systems that use a single key that both the sender and recipient have, and public-key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses.

II. CLASSIFICATION OF STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the object‟s use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. There are four main categories of file formats that can be used for steganography as shown in Figure-3 [1].

Following section gives a brief description of these categories of steganography.

Image Steganography: JPEG compression is a commonly used method for reducing the size of an image, without reducing the aesthetic qualities enough to become noticeable by the naked eye. Broadly speaking, it extracts all the information from an image that the human eye is not perceptible to and would therefore not miss should it not be there [2].

Audio Steganography: Audio Steganography is the technology of embedding information in an audio channel. It is used for digital copyright protection. Watermarking is the technique which hides one piece of information [message] in another piece of information [carrier]. It is widely used for applications such as audio clip etc [2].

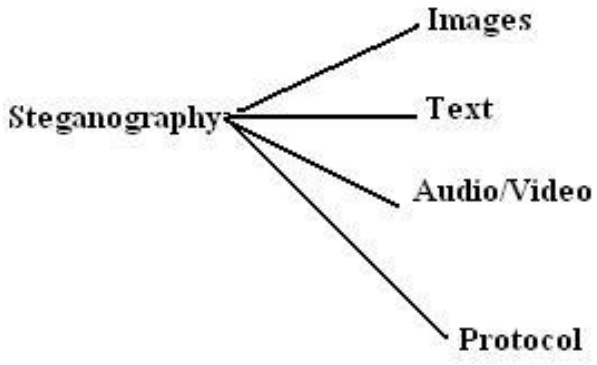

Figure 3: Categories of Steganography

Video Steganography: Video files are generally a collection of images and sounds, so most of the presented techniques on images and audio can be applied to video files too. The great advantages of video are the large amount of data that can be hidden inside and the fact that it is a moving stream of images & sounds. Therefore, any small out otherwise noticeable distortions might go by unobserved by humans because of the continuous flow of information [2].

Protocol Steganography: The term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the layers of the OSI network model there exist covert channels where steganography can be used. An example of where information can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never used.

Text Steganography: One major category, perhaps the most difficult kind of Steganography is text Steganography or linguistic Steganography because due to the lack of redundant information in a text compared to an image or audio. The text Steganography is a method of using written natural language to conceal a secret message. The advantage to prefer text Steganography over other media is its smaller memory occupation and simpler communication [2].

III. IMAGE COMPRESSION

When working with larger images of greater bit depth, the images tend to become too large to transmit over a standard Internet connection. In order to display an image in a reasonable amount of time, techniques must be incorporated to reduce the image's file size. These techniques make use of mathematical formulas to analyze and condense image data, resulting in smaller file sizes. This process is called compression [8].

In images there are two types of compression: lossy and lossless. Both methods save storage space, but the procedures that they implement differ.

Lossy compression creates smaller files by discarding excess image data from the original image. It removes details that are too small for the human eye to differentiate, resulting in close approximations of the original image, although not an exact duplicate. An example of an image format that uses this compression technique is JPEG (Joint Photographic Experts Group).

Lossless compression, on the other hand, never removes any information from the original image, but instead represents data in mathematical formulas. The original image's integrity is maintained and the decompressed image output is bit-by-bit identical to the original image input. The most popular image formats that use lossless compression is GIF (Graphical Interchange Format) and 8-bit BMP (a Microsoft Windows bitmap file).

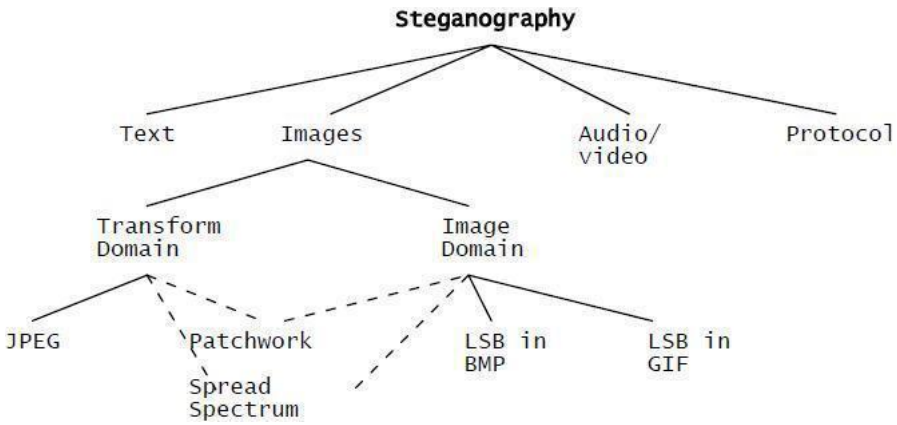

Figure 4: Categories of image Steganography

Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain. Image (or spatial) domain techniques embed messages in the intensity of the pixels directly, while for transform (or frequency) domain, images are first transformed and then the message is embedded in the image.
Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are sometimes characterized as ―simple system. The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [8].

IV. WHAT IS STEGANALYSIC?

Steganography leaves behind detectable traces (i.e., distortion) in the stego object and modifies the statistical properties. Detecting the presence of distorted statistical properties is called statistical steganalysis. Steganalysis is a relatively new research discipline with few articles appearing before the late-1990s. Steganalysis is "the process of detecting steganography by looking at variances between bit patterns and unusually large file sizes". It is the art of discovering and rendering useless covert messages [5].

The goal of steganalysis is to identify suspected information streams, determine whether or not they have hidden messages encoded into them, and, if possible, recover the hidden information.
The challenge of steganalysis is that:

- The suspect information stream, such as a signal or a file, may or may not have hidden data encoded into them.
- The hidden data, if any, may have been encrypted before inserted into the signal or file.
- Some of the suspect signal or file may have noise or irrelevant data encoded into them (which can make analysis very time consuming).
- Unless it is possible to fully recover, decrypt and inspect the hidden data, often one has only a suspect information stream and cannot be sure that it *is* being used for transporting secret information [7].

The steganalysis techniques focus on detecting the presence/absence of a secret message in observed message, to our knowledge there seems to have been no attempt in extracting the secret message. In general, extraction of the secret message could be a harder problem than mere detection [9].

Therefore, based on the ultimate outcome of the effort we classify steganalysis into two categories:

1. **Passive steganalysis**: Detect the presence or absence of a secret message in an observed message.
2. **Active steganalysis:** Extract a (possibly approximate) version of the secret message from a stego message.

However, attacks and analysis on hidden information may take several forms: detecting, extracting, and disabling or destroying hidden information. An attack approach is dependent on what information is available to the steganalyst (the person who is attempting to detect steganography-based information streams).

- **Steganography-only attack**: Only the steganography medium is available for analysis.
- **Known-carrier attack**: The carrier that is, the original cover and steganography media are both available for analysis.
- **Known-message attack**: The hidden message is known.
- **Chosen-steganography attack**: The steganography medium and tool (or algorithm) is both known.
- **Chosen-message attack**: A known message and steganography tool (or algorithm) is used to create steganography media for future analysis and comparison. The goal in this attack is to determine corresponding patterns in the steganography medium that may point to the use of specific steganography tools or algorithms.
- **Known-steganography attack**: The carrier and steganography medium, as well as the steganography tool or algorithm, are known.

There are two classes of steganalytic attacks on JPEG steganohraphy. The first is the targeted attacks where the embedding algorithm is known to the attacker. The next is the blind attacks where attack is independent of the embedding algorithms [10].

V. SPATIAL DOMAIN METHOD

In spatial domain scheme, the secret messages are embedded directly. Here, the most common and simplest steganography method is the least significant bits (LSB) insertion method. In the LSB technique, the least significant bits of the pixels are replaced by the message bits which are permuted before embedding. Most steganography software hide information by replacing only the least-significant bits (LSB) of an image with bits from the file that is to be hidden. This technique is generally called LSB encoding. One of the most common techniques used in steganography [1].

The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image [1].

Pixels:

(10101111 11101001 10101000)
(10100111 01011000 11101001)
(11011000 10000111 01011001) Secret message:
01000001

Result:

(10101110 11101001 10101000)
(10100110 01011000 11101000)
(11011000 10000111 01011001)

The three bold bits are the only three bits that were actually altered. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message. A slight variation of this technique allows for embedding the message in two or more of the least significant bits per byte. This increases the hidden information capacity of the cover-object, but the cover-object is degraded more, and therefore it is more detectable [1].

The next step is the quantization phase of the compression. Here another biological property of the human eye is exploited: The human eye is fairly good at spotting small differences in brightness over a relatively large area, but not so good as to distinguish between different strengths in high frequency brightness. This means that the strength of higher frequencies can be diminished, without changing the appearance of the image. JPEG does this by dividing all the values in a block by a quantization coefficient. The results are rounded to integer values and the coefficients are encoded using Huffman coding to further reduce the size [7].

VI. WHAT IS SPATIAL DESYNCHRONIZATION

Domain separation is an approach which prevent from calibration attack. Domain separation (or randomization) is a technique which is used for hiding the embedding domain from the attacker [7].

The separation of the embedding domain from the staganalytic domain is used to prevent cover image prediction from the stego image. In other words, if the embedding domain is kept secret from the attacker then it is not possible to mount calibration attack by predicting the cover image statistics [7].

The spatial de-synchronization operation is used to hide the embedding domain from the attacker by randomizing the embedding domain. Here spatial de-synchronization implies the embedding grid is not synchronized with the JPEG compression grid of the stego image. Due to this spatial shifting (de-synchronization), a noise (sometimes called de-synchronization noise) is added to the stego image. This noise masks the steganographic noise in such a way that the detection of steganographic embedding becomes difficult for the attackers. Thus spatial shifting operation resists calibration based attacks [6].

VII. MODIFIED ALGORITHM

In this section I am going to discuss the proposed algorithm of steganography and extraction of hidden message. I use the concept of spatial de-synchronization, randomization, encryption, and hashing to perform complete algorithm.

Let us we discuss the Steganography Algorithm first. Suppose I is the cover image then the steps of proposed steganography algorithm is as follows:

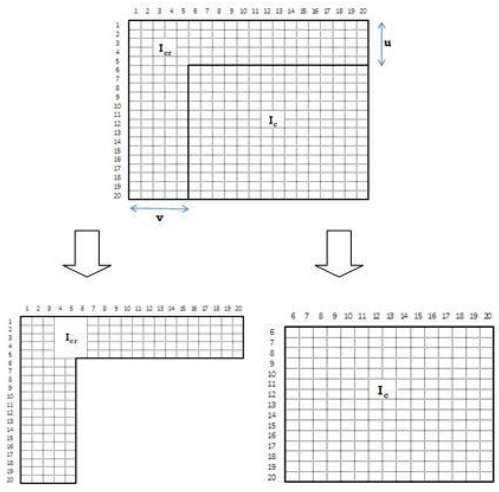

Figure 5: Cropping Of *u* Topmost Rows and *v* Leftmost Columns

Step 1: Desynchronize the cover image (I) is by the image cropping scheme, i.e by removing u topmost rows and v leftmost columns. Get cropped image (Ic) and remaining portion of image Icr as output. (As shown in Figure-5)

Step 2: Apply Hash function to perform randomized cropping on cropped image (Ic). Get hashed cropped image (Ich) and remaining portion of image Ichr as output. (As shown in Figure-6)

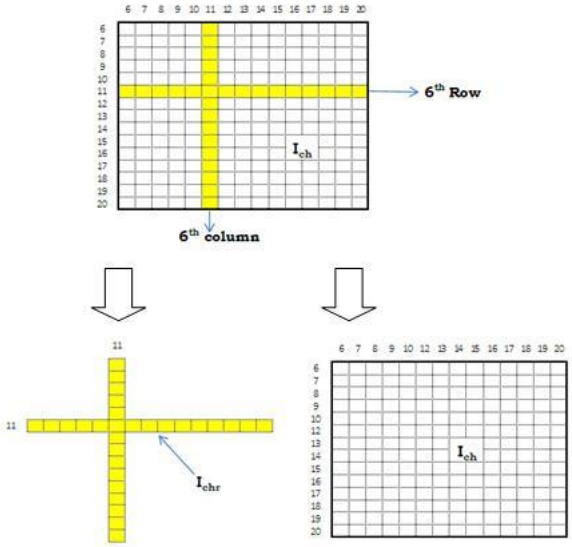

Figure 6: Randomized Cropping of Cover Image

Step 3: Encrypt the secret information (M). Get cipher text (Me) as output.

Step 4: Now the hashed cropped version of the image (Ich) is used for embedding cipher text (Me) using steganographic. Get stego image (Is1) as output.

Step 5: Stitch the stego image (Is1) with Ichr to obtain the embedded image Is2.

Step 6: Stitch the image (Is2) with Icr to obtain another embedded image Is.

Now to get the secrete message back I propose following steps by considering Is is the stego image.

Step 1: Extract the value of *u* & *v* (i.e. number of cropped rows and column) from stego image.

Step 2: Desynchronize the stego image (Is) is by the image cropping scheme, i.e by removing *u* topmost rows and *v* leftmost columns. Get cropped image (Isc) and remaining portion of image Iscr as output.

Step 3: Apply Hash function to perform randomized cropping on cropped image (Isc). Get hashed cropped image (Isch) and remaining portion of image Ischr as output.

Step 4: Now the hashed cropped version of the image (Isch) is used for bit extraction procedure. Get cipher text of secret information (Me) as output.

Step 5: Decrypt cipher text (Me) to get the secret information (M) as output.

VIII. CONCLUSIONS

I my work, a new steganographic algorithm have been proposed to resist steganalytic attacks. I tested my algorithm by taking nearly 50 different cover images of different image formats, specially JPEG and PNG image format. I found the correct working of proposed algorithm. I have applied the spatial desynchronization scheme in two stages. At first stage cropping number of rows and columns is done. In second stage I performed randomized cropping. The advantages of randomized cropping are based on the level of randomization. I also incorporate the concepts of encryption of massage just before embedding it into cover image. The concepts of randomized cropping and encryption of massage seems a better concept against steganalytic attacks. We can also perform the proposed algorithm in grayscale as well as true color images. Even I have implemented the proposed algorithm correctly and it seems a better algorithm but proper testing of proposed algorithm is needed. We can consider it as theoretical model. Because of lack of experimental setup I could not able to do it. So this is the limitation of my work and that could be done in future.

REFERENCES

[1] Shikha Mohan and Satnam Singh, Image Steganography: Classification, Application and Algorithms, International Journal Of Core Engineering & Management (IJCEM), Volume 1, Issue 10, January 2015.

[2] Sagar S.Pawar, Prof. Vinit Kakde, Review On Steganography For Hiding Data, International Journal of Computer Science and Mobile Computing, ISSN 2320–088X, IJCSMC, Vol. 3, Issue. 4, pg.225 – 229, April 2014.

[3] Tanmoy Halder, Sunil Karforma**,** and Rupali Mandal**,** E-govornence Data Security using Steganography, Concepts, Algorithms and Analysis, International Journal of Applied Sciences & Engineering (IJASE) 2(1) : April 2014, 41-54.

[4] Jessica Fridrich and Miroslav Goljan, Practical Steganalysis of Digital Images – State of the Art, Department of Electrical Engineering, Binghamton, NY 13902-6000, 2003.
[5] Satenik Bagyan, Thomas Mair, Yuri Suchorski, Marcus J. B. Hauser and Ronny Straube, Spatial desynchronization of glycolytic waves as revealed by Karhunen–Loeve analysis, September, 2008.
[6] Arijit Sur, Devadeep Shyam, Piyush Goel, and Jayanta Mukherjee, An image steganographic algorithm based on spatial desynchronization, Multimedia Tools Appl, Springer Science & Business Media New York, Nov 2012.
[7] Sur A., Goel P., and Mukhopadhyay J., Spatial Desynchronization: A Possible Way to Resist Calibration Attack, Dept. of Comput. Sci. & Eng., Indian Inst. of Technology, Guwahati, India, 2009.
[8] Andreas Westfeld and Andreas Pfitzmann, Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned, Dresden University of Technology, Department of Computer Science, D-01062 Dresden, Germany.
[9] I. Diop, S .M Farssi, O. Khouma, H. B Diouf, K .Tall, and K .Sylla, New Steganographic scheme based of Reed-Solomon codes, International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.2, March 2012.
[10] Babloo Saha and Shuchi Sharma, Steganographic Techniques of Data Hiding using Digital Images, Defence Science Journal, Vol. 62, No. 1, January 2012.

