# SPATIAL DESYNCHRONIZATION IN IMAGE STEGANOGRAPHY

Aakanksha Upadhyaya[1], Brajesh Patel[2]
[1]Department of Computer Sc. & Engineering, SRIT, RGPV University, Jabalpur, India
[2]Head of Computer Sc. & Engineering Department,
SRIT, RGPV University, Jabalpur, India.

## *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, Cover Image, Stego Image, Cipher Text, Image Format, Desynchronization.*

## 1. INTRODUCTION

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 [2].

The protection of sensitive information against unauthorized access or fraudulent changes has been of prime concern throughout the centuries. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. 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 [17].

With Secret key cryptography, a single key is used for both encryption and decryption. Because a single key is used for both functions, secret key cryptography is also called *symmetric encryption*. Public-key cryptography has been said to be the most significant new development in cryptography in the last 300-400 years [11]. One more cryptography technique is Hash functions. Hash functions, also called message digests and one-way encryption, are algorithms that, in some sense, use no key. Instead, a fixed-length hash value is computed based upon the plaintext that makes it impossible for either the contents or length of the plaintext to be recovered.

## 2. ABOUT STEGANOGRAPHY

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). Many different digital cover file formats can be used such as text, audio, image and video [3]. The steganography process may be defined as follows:

Cover medium + Hidden information + Stegokey = Stego_medium

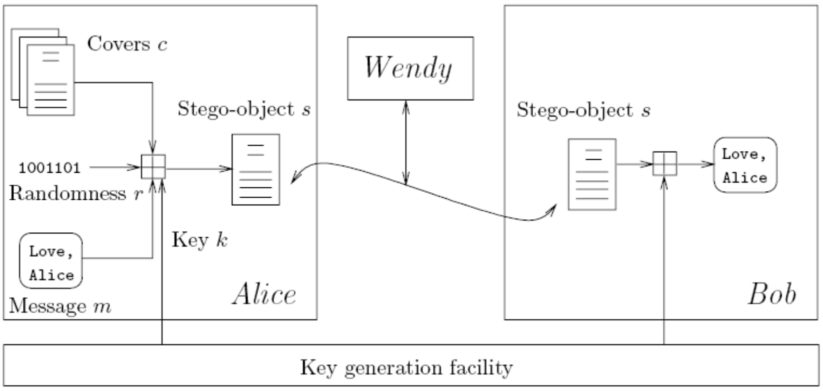

**Figure 1:** View of Steganography

## 2.1 Types 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. Image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. Figure 2 shows the four main categories of file formats that can be used for steganography.

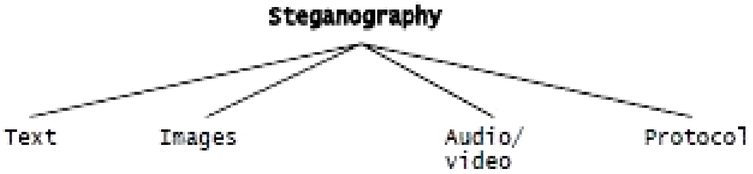

**Figure 2:** Categories of Steganography

## 2.2 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 [3].

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).

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 systems". The image formats that are most suitable for image domain steganography are lossless and the techniques are typically dependent on the image format [3].

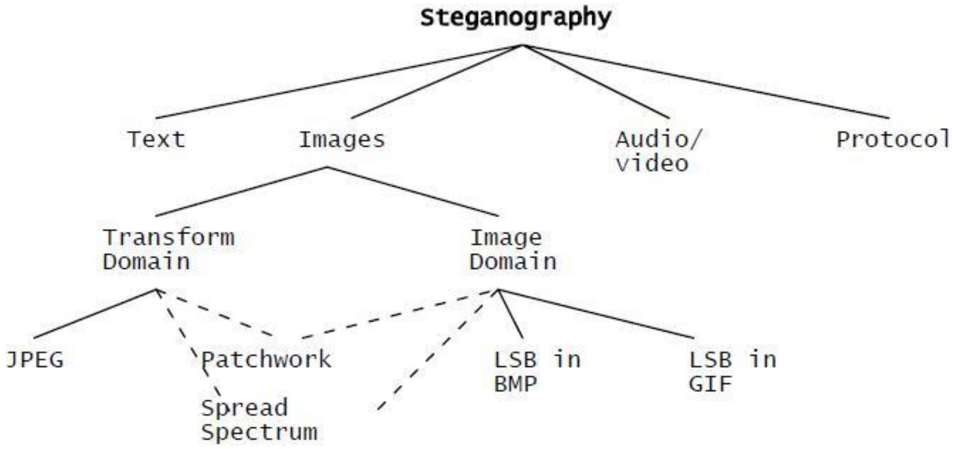

**Figure 3:** Categories of image Steganography

## 3. 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 [11]. 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 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 [8]. 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.

## 4. Spatial Desynchronization

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 [12]. 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 [13].

## 5. PROPOSED WORK

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, encryption, and hashing to perform complete algorithm.

### 5.1 Steganography Algorithm

Let I is the cover image. We can describe the proposed steganography algorithm in following steps:

**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 ($I_c$) and remaining portion of image $I_{cr}$ as output.

**Step 2:** Apply Hash function to perform randomized cropping on cropped image ($I_c$). Get hashed cropped image ($I_{ch}$) and remaining portion of image $I_{chr}$ as output.

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

**Step 4:** Now the hashed cropped version of the image ($I_{ch}$) is used for embedding cipher text ($M_e$) using steganographic. Get stego image ($I_{s1}$) as output.

**Step 5:** Stitch the stego image ($I_{s1}$) with $I_{chr}$ to obtain the embedded image $I_{s2.}$

**Step 6:** Stitch the image ($I_{s2}$) with $I_{cr}$ to obtain another embedded image $I_{s.}$

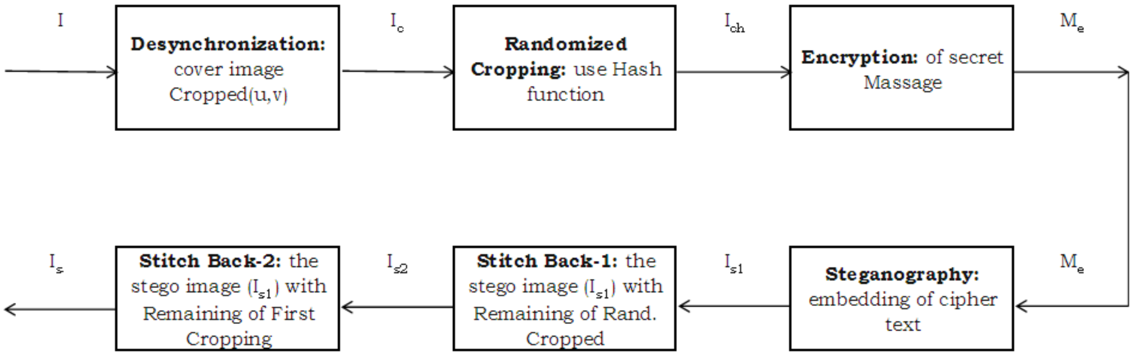
I
Desynchronization: cover image Cropped(u,v)
I_c
Randomized Cropping: use Hash function
I_ch
Encryption: of secret Massage
M_e
M_e
Steganography: embedding of cipher text
I_s1
Stitch Back-1: the stego image (I_s1) with Remaining of Rand. Cropped
I_s2
Stitch Back-2: the stego image (I_s1) with Remaining of First Cropping
I_s

**Figure 4:** Block Diagrams of Proposed Steganography Method

### 5.2 Algorithm to Extraction of stego-bits

Let $I_s$ is the stego image. The extraction of stego bits is rather simple, nearly reverse process of above algorithm. This algorithm can be described in following steps:

**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 ($I_s$) is by the image cropping scheme, i.e by removing *u* topmost rows and *v* leftmost columns. Get cropped image ($I_{sc}$) and remaining portion of image $I_{scr}$ as output.

**Step 3:** Apply Hash function to perform randomized cropping on cropped image ($I_{sc}$). Get hashed cropped image ($I_{sch}$) and remaining portion of image $I_{schr}$ as output.

**Step 4:** Now the hashed cropped version of the image ($I_{sch}$) is used for bit extraction procedure. Get cipher text of secret information ($M_e$) as output.

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

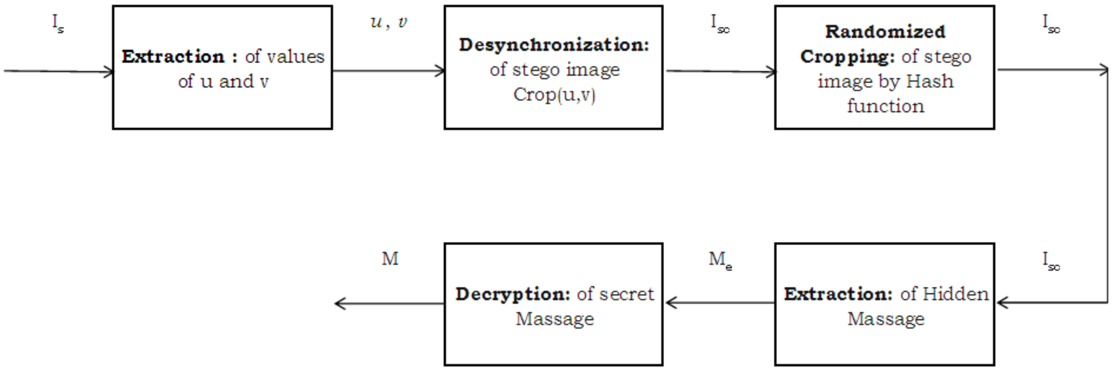
$I_s$
Extraction : of values of u and v
$u, v$
Desynchronization: of stego image Crop(u,v)
$I_{sc}$
Randomized Cropping: of stego image by Hash function
$I_{sc}$
$I_{sc}$
Extraction: of Hidden Massage
$M_e$
Decryption: of secret Massage
M

**Figure 5:** Block Diagrams of Proposed Message Extraction Method

## 6. 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 (refer section 6.2 for details). 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.

## ACKNOWLEDGEMENTS

I feel pleasure in conveying my profound thanks to my supervisor Prof. Brajesh Patel Head of Department Computer Science & Engineering, SRIT, Jabalpur, for his constant Support, valuable Guidance and Encouragement. I also thankful to all staff members of Computer Engg for their time to time supports. I am also very thankful to my family members especially to my husband and my little son for their cooperation and motivation.

## REFERENCES

[ 1] Pierre Richer, Steganalysis: Detecting hidden information with computer forensic analysis,Version 1.4b, , SANS Institute 2003.

[ 2] Jessica Fridrich and Miroslav Goljan, Practical Steganalysis of Digital Images – State of the Art, Department of Electrical Engineering, Binghamton, NY 13902-6000, 2003.

[ 3] 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.

[ 4] Che-Wei Lee and Wen-Hsiang Tsai, A New Steganographic Method Based on Information Sharing via PNG Images, National Chiao Tung University, Hsinchu, Taiwan, IEEE, 2010.

[ 5] Wai Wai Zin, Message Embedding In PNG File Using LSB Steganographic Technique, University of Computer Studies, Mandalay, Myanmar, International Journal of Science and Research (IJSR), India Online ISSN: 2319-7064, Volume 2 Issue 1, January 2013.

[ 6] R. Chandramouli, A Mathematical Approach to Steganalysis Multimedia Systems, Networking and Communications (MSyNC) Lab, Department of Electrical and Computer Engineering, Stevens Institute of Technology, Jan. 2002.

[ 7] Andreas Westfeld, F5—A Steganographic Algorithm High Capacity Despite Better Steganalysis, Technische University Dresden, Institute for System Architecture, Dresden, Germany, Springer-Verlag Berlin Heidelberg 2001.

[ 8] 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.

[ 9] Babloo Saha and Shuchi Sharma, Steganographic Techniques of Data Hiding using Digital Images, Defence Science Journal, Vol. 62, No. 1, January 2012.

[ 10] Lisa M. Marvel and Charles T. Retter, A Methodology For Data Hiding Using Images, U.S. Army Research Laboratory, APG, MD 21005, Charles G. Boncelet, Jr., University of Delaware Newark, IEEE, 1998.

[ 11] 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.

[ 12] 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.

[ 13] 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.

[ 14] http://en.wikipedia.org/wiki/Image_file_formats.

[ 15] Tao Zhang and Xijian Ping, A Fast and Effective Steganalytic Technique against JSteg-like Algorithms, Department of Information Science, University of Information Engineering, Zhengzhou, 2003.

## AUTHORS

**Aakanksha Upadhyaya** received his B. E. degree in Computer Science and Engineering from Department of Computer Science and Engineering, from Shri Ram Institute of Technology, Jabalpur under RGPV University Bhopal (M.P.). She is currently a student of Master of Engg (M.E.) in same institute. She has 4 years teaching experience of under graduate engineering students.