# STUDY AND REVIEW OF DATA OBSCURING TECHNIQUES BASED ON SPATIAL IMAGE STEGANOGRAPHY

**Igloo Jain[1], P.S. Mann[2]**

[1]*Assistant Professor, Computer Science & Engineering, Chandigarh University, Punjab, India,* **igloo.j@gmail.com**
[2]*Assistant Professor, Information Technology, DAVIET, Punjab, India,* **psmann@hotmail.com**

## Abstract

*Steganography technique is an approach of data obscuring which is invisible i.e. presence of hidden data is unknown to unintended users. The secret message is embedded in a cover medium which can be an image or text file and resultant cover object is transmitted over the untrusted channel. Steganography is gaining due significance due to the enormous increase in secret communication between potential computer users over the internet. It can also be defined as the study of invisible transmission that usually deals with the ways of hiding the existence of the communicated message. Generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. Steganography is unlike cryptography in the way that cryptography obscures the contents of clandestine message whereas steganography is hiding the existence message. In this paper an overview of steganography has been elaborated. This paper studies and reviews various data obscuring techniques based on spatial domain image steganography like Least Significant Bit, Most Significant Bit, Parity check, Pixel value differencing. It elaborates an overview of steganography and illustrates the process of steganography. Various classifications of steganographic techniques are discussed. The image domain/ spatial domain techniques are discussed in detail and a relative comparison is derived between these techniques on the basis of various parameters like robustness, image quality, and compression losses.*

***Index Terms:*** *Steganography, Spatial domain, Parity Checker, Least Significant Bit, Moderate Significant Bit.*

--------------------------------------------------------------------- *** ---------------------------------------------------------------------

## 1. INTRODUCTION

In the current trends of the world, the internet is the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. However, one of the main problems with sending data over the internet is the "security threat" it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring.

Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet.

In order to improve the security features in data transfers over the internet, many techniques have been developed like: Steganography, Cryptography etc. In Greek, the word cryptography means ―secret writing. Cryptography is the process of converting the original text into an unreadable format for others by rearranging and substituting the original text.

Steganography is derived from two Greek words, which means ―covered writing. While Cryptography is a method to conceal information by encrypting it to "cipher texts" and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the text into a seemingly invisible image or other formats [21].

Steganography and cryptography are counter parts in digital security the obvious advantage of steganography over cryptography is that messages do not attract attention to themselves, to messengers, or to recipients [9]. Also, the last decade has seen an exponential growth in the use of multimedia data over the Internet. These include Digital Images, Audio and Video files. This rise of digital content on the internet has further accelerated the research effort devoted to steganography. The various applications of steganography include secure military communications, multimedia watermarking and fingerprinting applications for authentication purposed to curb the problem of digital piracy.

## 1.1 Overview of Steganography

Steganography prominence is increasing due to clandestine communication between various computer customers over internet. So by steganography we mean imperceptible communication in which the essence of covert message is unknown. Data hiding in steganography is accomplished by embedding the covert message into cover object depending on the technique of steganography used.

Steganography is derived from two Greek words Steganós (Covered), and Graptos (Writing) which means "covered or hidden writing". Intention behind using steganography is to obscure the very subsistence of the secret message in the cover medium. Now a days in steganography image, audio, video etc. are used as cover media as people send digital images over email or share them through other internet communication application. It is different from bulwarking the genuine content of a message. In simple words it would be akin to that, hiding information into other information

## 1.2Steganography process

The procedure of hiding data using steganography is shown in Figure 1.1.

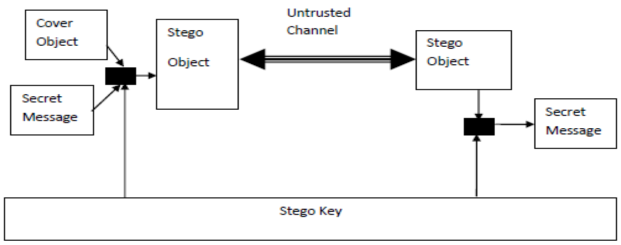

Fig 1.1: Steganography process

The cover object is the file in which we will hide the message, which may also be encrypted using the stego key. The resultant file is the stego object (which will, of course. be the same type of file as the cover object). The cover object (and, thus, the stego object) are typically image or audio files. The stego object is transmitted over the untrusted channel. At the receiver side the secret message is extracted from the stego object using stego key.

## 1.3 Classification of Steganography

Steganography is classified into following steganographic techniques on the basis of type of cover medium. It can be shown in Figure 1.2.

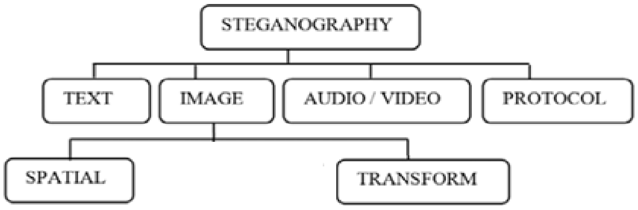

Figure 1.2: Types of Steganography [16]

**Text Steganography:** It involves altering the formatting of present text or varying words within a text etc. Text steganography is assumed to be the complicated due to absence of redundant information which is present in image, audio or a video file.

**Image Steganography:** In this clandestine message is embedded in image which acts as cover object.

**Audio/Video Steganography:** In this message is embedded in audio or digital format.

**Protocol Steganography:** In this technique data is stored in network protocols e.g. TCP, UDP etc. In these protocols unused header bits are used to store the secret message.

## 2. IMAGE STEGANOGRAPY TECHNIQUES

Image steganography techniques can be divided into following domains.

**a) Spatial Domain Methods:** In this the pixel gray levels and their color values are used for encoding the message bits. These techniques are the simplest in terms of embedding and extraction complexity.

Spatial domain techniques are broadly classified in fig 2.1.

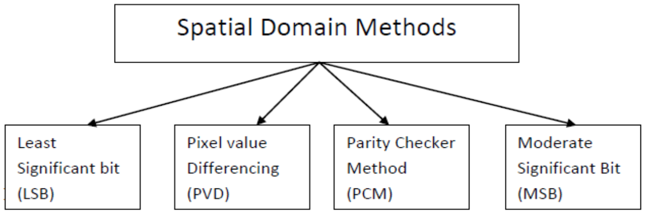
Spatial Domain Methods
Least Significant bit (LSB)
Pixel value Differencing (PVD)
Parity Checker Method (PCM)
Moderate Significant Bit (MSB)

Fig 2.1: Spatial Domain Methods

### 1. Least Significant Bit Method (LSB)

Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image in least significant bit position. The least significant bit is the 8 of the bytes inside an image. It is changed with bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 In other words; one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data.

### 2. Pixel value differencing Method (PVD)

The pixel-value differencing (PVD) [1] scheme uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. This scheme provides high imperceptibility to the stego image by selecting two consecutive pixels and designs a quantization range table to determine the payload by the difference value between the consecutive pixels.

### 3. Parity Checker Method (PCM)

The Parity Checker Method (PCM) [3] method uses the concept of odd and even parity for insertion and retrieval of message. In this method even value can be inserted at a pixel position to identify pixel has 1(odd) parity bits. It can be identical odd value insert at a pixel; if the pixel should be 0 (even) parity [3]. If the close similarity parity do not exist at a pixel position for odd or even, then the pixel location can be added and subtracted such that the change in the image quality will not be Visible (to the human visual system).

### 4. Moderate Significant Bit (MSB)

Moderate significant bit (MSB) [19] insertion is a common, simple approach to embedding information in a cover image at moderate significant bit position. Already we have Least significant bit technique in which data is stored at least significant bit position but problem arises in case when image is compressed, LSB of image is discarded. So the receiver won't be able to extract the data. To overcome this problem we have moderate significant bit technique in which secret data is embedded at 4th, 3rd or 2nd moderately-significant-bit of pixel of an image.

**b)Transform Domain Technique:** In this data is embedded in the frequency domain of a signal. It is more difficult way of hiding information in an image. Transform domain techniques hide information in areas of the image that are less exposed to compression, cropping, and image processing. E.g Discrete cosine transformation technique (DCT), Discrete Wavelet transformation technique (DWT).

## 3. BRIEF LITERATURE SURVEY

The foremost aim of this paper is to perform a survey on various spatial domain steganography techniques used in recent years. Different techniques utilized by different authors in different years were mentioned below pellucidly.

T Morkel et al. [2] provides overview of image steganography, its uses, techniques, identify the requirements of a good steganographic algorithm and briefly reflects on which steganographic techniques are more suitable for which applications.

M. Sitaram Prasad et al. [4] proposed a novel to provide more security for the key information with the combination of image compression and data encryption method. This method requires less memory space and fast transmission rate because of image compression technique is applied. This method has been implemented and tested on varies images and data. It provides better security for encrypted data and no distortion in the image quality.

Rajkumar et al. [7] presented a new steganography technique for hiding data in images using parity checker. This method uses the concept of odd and even parity for insertion and retrieval of message. This method is an improvement over earlier methods like least significant bit method and 6th, 7th bit method for hiding information in images.

Balkrishan et al. [5] offered a new scheme for concealing a piece of critical information in a gray-scale image using a separate public key designed on the concept of simultaneous encryption and embedding of data. A new type of flexible matrix is proposed to encipher the critical information more effectively and efficiently. The enciphered information is then embedded into cover image using a new concept of randomly chosen moderate-bit insertion. The enciphered data bits are extracted and then deciphered with same public key. The proposed matrix protects the hidden information from attacks besides ensuring lesser computational load for encrypting data. In addition to this, it provides the flexibility to select any type of 16x16 matrix having entries ranging from 0 to 255.

B. Jindal et al. [11] suggested a novel method for crypto data hiding within grey scale image in the spatial domain, so that the interceptors will not notice about the existence of the important data. The basic concept of the proposed method is to embed the important crypto data in the 4th moderately-significant-bit of pixel of an image. The first 3 LSB bits of image pixel is used for local pixel adjustment to reduce the effect of degradation in the cover image due to moderate bit insertion. Experimental results are performed on four different same size images and shows that the visual quality of the stego image is acceptable. This method provides a higher security and more robust to attacks such as compression, cropping and some other image processing methods than the LSB of stego-image.

B. Jindal et al. [19] reported on a new type of camouflaging in digital image for hiding crypto-data using moderate bit alteration in the pixel. In the proposed method, cryptography is combined with steganography to provide a two layer security to the hidden data. The novelty of the algorithm proposed in the present work lies in the fact that the information about hidden bit is reflected by parity condition in one part of the image pixel. The remaining part of the image pixel is used to perform local pixel adjustment to improve the visual perception of the cover image. In order to examine the effectiveness of the proposed method, image quality measuring parameters are computed. In addition to this, security analysis is also carried by comparing the histograms of cover and stego images. This scheme provides a higher security as well as robustness to intentional as well as unintentional attacks.

## 4. CONCLUSION

This paper analyzes various steganographic techniques for image in spatial Domain. Spatial Domain Steganographic methods have two sides of coin means have both advantages and disadvantages. Below mentioned table gives the relative comparison of various spatial domain steganographic methods.

| Steganographic technique | Robustness | Image Quality | Compression Loss |
|---|---|---|---|
| Moderate Bit Insertion | Moderate | Low | Less |
| LSB substitution | Low | More | More |
| Parity Check | More | Moderate | More |
| PVD | Less | High | Less |

**Table-1: Comparison of Spatial Domain Steganographic Methods**

From above table we conclude that it's difficult to find the best steganographic technique. So the choice of technique depends on various factors like payload size, cover image size etc.

## 5. ACKNOWLEDGEMENT

I am thankful to Mr. P.S. Mann for his guidance and support.

## 6. REFERENCES

[1]. C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[2]. T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography," Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically)

[3]. Hassan Mathkour, Ghazy M.R. Assassa, Abdulaziz Al Muharib, Ibrahim Kiady,"A Novel Approach for Hiding Messages in Images", International Conference on Signal Acquisition and Processing,2009

[4]. M. Sitaram Prasad, S. Naganjaneyulu, Ch. Gopi Krishna, C. Nagaraju, "A Novel Information Hiding Technique For Security By Using Image Steganography",Journal of Theoretical and Applied Information Technology, Vol 8. No. 1 – 2009

[5]. Balkrishan and Amar Partap Singh, "Hiding Encrypted Data using Randomly Chosen Moderate Bit Insertion in Digital Image Steganography," Journal of Computer Science and Engineering, vol. 1, issue 2, pp. 21-27, June 2010.

[6]. Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010

[7]. Rajkumar, Rahul Rishi and SudhirBatra, "A New Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975 – 8887) Volume 11– No.11, December 2010

[8]. V.SathyaPreiya , S.SathishKumar,M.Shanmuganathan, "Provide Secure Authenticity For Propagating", International Journal of Engineering Trends and Technology- May to June Issue 2011

[9]. PallaviKhare, Jaikaran Singh, Mukesh Tiwari, "Digital Image Steganography", Journal of Engineering Research and Studies Vol.II Issue III July- pg 101-104, September,2011

[10]. N Verma, "Review of Steganography Techniques", International Conference and Workshop on Emerging Trends in Technology (ICWET 2011)

[11]. B. Jindal, A. P. Singh, "Moderate Bit Insertion for Hiding Crypto-Data in Digital Image for Steganography", Special issues on IP Multimedia Communications (1):136-138, October 2011.

[12]. Ajit Singh and UpasanaJauhari, "A Symmetric Steganography with Secret Sharing and PSNR Analysis for Image Steganography", International Journal of Scientific & Engineering Research Volume 3, Issue 6, June-2012

[13]. RonakDoshi,PratikJain,Lalit Gupta "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER), Vol.2, Issue.6, pp-4634-4638, Nov-Dec. 2012

[14]. Kanzariya Nitin K. and Nimavat Ashish V, "Comparison of Various Images Steganography Techniques", International Journal of Computer Science and Management Research Vol 2 Issue 1, January 2013

[15]. Mehdi Hussain and MureedHussain "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology,Vol. 54, May, 2013.

[16]. C.Gayathri , V.Kalpana "Study on Image Steganography Techniques", International Journal of Engineering and Technology (IJET), Vol 5 No 2 Apr-May 2013

[17]. Bharti Ahuja, Rashmi Lodhi "Different Algorithms used in Image Encryption: A review ",International Journal of

Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 07 Jul 2013

[18]. AnubhaPrajapati "Steganography Using Lsb Technique", Proceedings Of National Conference On Recent advancements In Futuristic Technologies (Ncraft'13), 2013

[19]. B. Jindal, A. P. Singh, "Camouflaging in Digital Image for Secure Communication", Journal of The Institution of Engineers (India): Series B June 2013, Volume 94, Issue 2, pp 85-92

[20]. Mukesh Garg, A.P. GurudevJangra, "An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering , Volume 4, Issue 1, January 2014

[21]. K.B.Bini, R.Sreejith, "Secure Reversible Data Hiding with Image Encryption", International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE), Volume 3, Issue 2, February 2014

[22]. A. KajaMoideen, K. R. Siva Bharathi, "A Novel Method for Data Hiding In Encrypted Image And Video", International Journal of Emerging Technology and Advanced Engineering , Volume 4, Issue 2, February 2014

[23]. "Steganography" http://en.wikipedia.org/wiki/Steganography

[24]. "Advantages of Steganography Over Cryptography" http://steganographyandroid.blogspot.in/2013/03/advantages-of-steganography-over.html

[25]. "Steganography, hiding text inside photos and sound files" http://www.hacker10.com/tag/cryptography-vs-steganography/

## BIOGRAPHIES

**Igloo Jain** is doing Master of Technology in Computer Science & Engineering at DAVIET, Jalandhar and completed B.Tech in Computer Science & Engineering from the same college. Currently she is working as Assistant Professor at Chandigarh University, Gharuan,

**Mr. P.S. Mann** is B.Tech with Hons, M.Tech and is currently pursuing Phd. He is working as Assistant Professor in Department of Information Technology DAVIET, Jalandhar.