# Analysis of Digital Image Data Hiding Techniques

S. Mangayarkarasi
Research Scholar, Vels University, Chennai, India.

Dr.P.Sujatha
Associate Professor, Vels University, Chennai, India.

**Abstract – The main objective of Steganography is to communicate securely in such a way that the true message is not visible to the observer. Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security. The steganographic techniques can be classified as audio, video, text, image and network steganography. In this paper we have analyzed various data hiding techniques in encrypted images.**

**Index Terms – Steganography, Data Hiding, Security.**

## 1. INTRODUCTION

In modern time data hiding is associated with digital forms such as cryptography, steganography and watermarking.

Cryptography is obscure the content of the message, but not the communication of the message. Watermarking is a pattern of bits inserted into a digital image, audio or video file that identifies the files copyright information. The word Steganography combines the Greek word "steganos means Covered, concealed or protected" and "Graphein means writing". Steganography means "covered writing", is hiding the very communication of the message. 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, image, program or protocol. Media files are ideal for steganographic transmission because of their large size. Basically embedding data based on three different facts i.e. capacity, security, and robustness. Capacity means

Within the medium the amount of data is hidden, So that the complexity of the medium should not be disturbed [6]. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks. Finally, robustness means the amount of manipulation a cover image (original image) can handle without drawing any attention that a change has taken place. Steganography and cryptography have to guarantee any of the requirements [1]. A Steganography concept is represented in Fig 1.

A piece of secret data is communicated between sender and receiver. For Secure communication a secret key is used for encrypting and decrypting the data. This reduces the risk of hacking data or third party attacks.

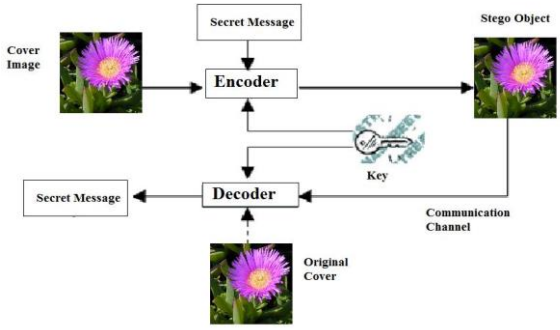


Fig 1. Block diagram of Steganography

## 2. CLASSIFICATION OF STEGANOGRAPHY TECHNIQUES

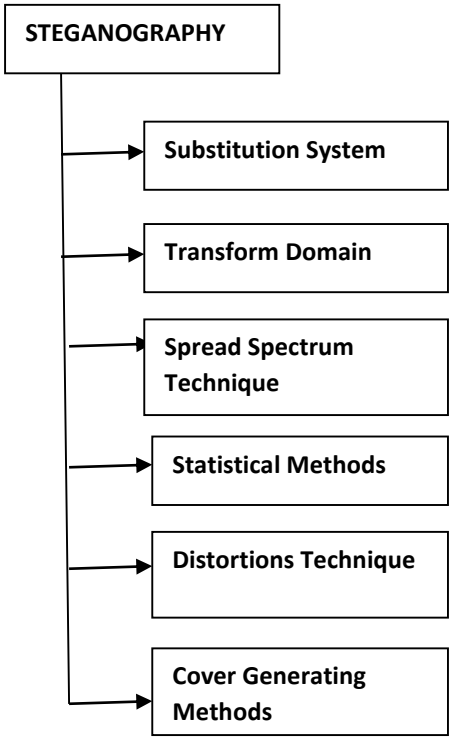


Fig 2. Steaganographic Techniques

Steganography techniques can be classified according to two approaches i) Type of covers used for secret communication or ii) according to the cover modifications applied in the embedding process. From the second approach steganography methods are grouped in to six categories, Represented in Fig 2.

**i)** Substitution systems to encode secret information by substituting insignificant parts of the cover by secret message bits.

**ii)** Transformation domain methods hide message in a significant area of the cover image. Most commonly used transform domain methods are DCT and Wavelet Transform.

**iii)** Spread Spectrum Techniques are widely used in military radio communications, due to their high robustness and to detection and correction.

**iv)** Statistical Methods

**v)** Distortions Technique

**vi)** Cover Generating Methods

Different file format can be used for different domains. Such as Audio, Video, Image, Text and Image files. In this paper we focused image stegnography method.

## 3. IMAGE STEGANOGRAPHY METHODS

Image steganography has been widely studied by researchers. There are a variety of methods used in which information can be hidden in images. In the following section, we present the most common methods. There are three common methods of steganography: Replacing Moderate Significant Bit, Transformation Domain Techniques, and Replacing Least Significant Bit [4].

In this paper we will be presenting the survey of various data hiding techniques in image steganography to facilitate the secure data transmission over the communication channels.

### 3.1. LITERATURE SURVEY

Shamin Ahmed Laskar et.al [1] proposed, to encrypt a message using transposition cipher method and then embed the encrypted message inside an image using LSB embedding method. Data hiding using LSB Steganography is described,

$$y_i = 2\left|\frac{xi}{2}\right| + m_i$$

Where xi,mi and yi are the i-th message bit, and the i-th selected pixel value before and after embedding, respectively. Let $\{p_m(x=0), p(x=1)\}$ denotes the distribution of the least significant bits in the cover message and $\{p_m(m=0), p(m=1)\}$ denotes the distribution of the secret binary message bits. The advantage of the LSB based data hiding method is simple and secure data communication.

Gurmeet Kaur et.al [2] proposed a method Discrete Cosine Transform (DCT). In this method first the DCT transforms the signal from an image representation into a frequency representation, then grouping the pixels into

8 × 8 pixel blocks and transforming the pixel blocks into 64 DCT.

Da-Chun Wu et.al [9] proposed the embedding method is pixel value differencing. In this method divide the cover images into a number of non-overlapping two-pixel blocks. Each block is categorized according to the difference of the gray scale values of the two pixels. The small difference indicates the block is in smooth area, the large difference indicates is in edge area. In this method proposed, to embed more data in edged area than smooth area.

Hsien-Wen Tseng et.al [10] proposed the method the new quantization range table is based on the perfect square number, embedding procedure and extraction procedure. For each pixel value $p \in [0, 255]$, choose the nearest perfect square number $n^2$, then we have range $n^2 - n \leq n^2 < n^2 + n$ for $n \in [1, 16]$. The width of this range is $(n^2 + n) - (n^2 - n) = 2n$, and the embedding bit length is $m = \lfloor \log_2 2n \rfloor$. For each range $[n^2 - n, n^2 + n)$, if the width of this range is larger than $2m$, then we divide this range into two subranges: $[n^2 - n, n^2 + n - 2m]$ and $[n^2 + n - 2m + 1, n^2 + n - 1]$.

J. K. Mandal and Debashis Das [11] proposed pixel value differencing method, every pixel in a colour image is composed of RGB colours. Every pixel contains 24 bits where 8 each bit is allocated for Red , Green and Blue component.

V.Nagaraja et.al [5] proposed pixel value modification method (PVM), divides the cover image into three color planes Red, Green and Blue. Each color component from a pixel is separated and three separate M*N matrix is obtained.

Y.Kumari et.al[13] proposed try-way pixel value difference(TPVD), in this method 4-pixels represented as p(x,y), p(x,y+1), p(x+1,y), p(x+1,y+1) , x& y are the pixels in the given picture.

## 4. PERFORMANCE METRICS

Steganography technique is reliable when it embeds secret message with little distortion. So that the quality of the host file cannot be affected. The secret message should be truly unnoticeable, so that the host file cannot be distinguished from the Stego file. After embedding distortion occurs normally it affects the stego file [14]. Some of the performance metrics are used for measure difference between host file and the stego file.

1. Mean Square Error (MSE)
2. Peak Signal Noise Ratio (PSNR)
3. Root Mean Square Error (RMSE)

4. Structural Similarity
5. Normalized Absolute Error

The MSE is the cumulative squared error between the compressed and the original image.

$$\mathbf{MSE} = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[\mathbf{I}(x,y) - \mathbf{I}'(x,y)]\mathbf{2}$$

Where I (x,y) is the original image, I' (x,y) is the approximated version ( the compressed image) and M, N are the dimensions of the images. A lower value of the MSE means lesser error

PSNR is the measure of the peak error.

**PSNR= 20 * log 10 (255 / Sqrt (MSE))**

The higher value of the PSNR is good because the ratio of signal to noise is higher.

The Root Mean Square Error (**RMSE**) (also called the root mean square deviation, RMSD) is a frequently used measure of the difference between values predicted by a model and the values actually observed from the environment that is being modelled. These individual differences are also called residuals, and the RMSE serves to aggregate them into a single measure of predictive power.

The RMSE of a model prediction with respect to the estimated variable $X_{model}$ is defined as the square root of the mean squared error:

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n}(X_{obs,i} - X_{model,i})^2}{n}}$$

where $X_{obs}$ is observed values and $X_{model}$ is modeled values at time/place *i*.

SSIM is used for measuring the similarity between two images. The SSIM index is a full reference metric, in other words, the measurement or prediction of image quality is based on an initial uncompressed or distortion-free image as reference.

SSIM is designed to improve on traditional methods such as peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which have proven to be inconsistent with human visual perception.

The SSIM index is calculated on various windows of an image. The measure between two windows x and y of common size $N \times N$ is:

$$\mathbf{SSIM(x,y)} = \mathbf{(2\mu_x\mu_y + c_1)\ (2\sigma_{xy} + c_2)/(\ \mu^2x + \mu^2y + c_1)\ (\ \mu^2x + \mu^2y + c_2)}$$

Where $\mu^2\mathbf{x}$ and $\mu^2\mathbf{y}$ are variance of x and y and $\mu_x$ and $\mu_y$ are average of x and y.

## 5. CONCLUSION

This comparative analysis has presented a discussion on the major data hiding methods of steganography used within digital images. The standard techniques of spatial domain such as LSB as well as transform domain techniques, DCT, PVD and PVM. Some of the performance metrics also discussed.

## REFERENCES

[1] Shamin Ahmed Laskar and Kattamanchi Hemachandran " High Capacity data hiding using LSB steganography and Encryption" International Journal of Database Management Systems ( IJDMS ) Vol.4, No.6, December 2012.
[2] Gurmeet Kaur and Aarti Kochhar, "Transform Domain Analysis of Image Steganography" International Journal for Science and Emerging ISSN No. (Online):2250-3641 Technologies with Latest Trends" 6(1): 29-37 (2013).
[3] Navneet Kaur, Sunny Behal," A Survey on various types of Steganography and Analysis of Hiding Techniques", International Journal of Engineering Trends and Technology (IJETT) – Volume 11 Number 8 - May 2014.
[4] Harshavardhan Kayarkar," A Survey on various Data Hiding Techniques and their Comparative Analysis", Jul-Sep2012, Vol. 5 Issue 3.
[5] V.Nagaraja , Dr. V. Vijayalakshmib and Dr. G. Zayaraz ," Color Image Steganography based on Pixel Value Modification Method Using Modulus Function", 2013 International Conference on Electronic Engineering and Computer Science.
[6] Laskar, S.A. and Hemachandran, K. (2012), "An Analysis of Steganography and Steganalysis Techniques", Assam University Journal of science and Technology, Vol.9, No.II, pp.83-103, ISSN: 0975-2773.
[7] https://en.wikipedia.org/wiki/Covert_channel
[8] Rajan , Muhammad Tauheed Khan," Data Hiding In Digital Image Processing Using Steganography: A Review" ,IJEDR | Volume 2, Issue 3 | ISSN: 2321-9939.
[9] Da-Chun Wu, Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters 24 (2003) 1613–1626.
[10] Hsien-Wen Tseng, Hui-Shih Leng ," A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", Hindawi Publishing Corporation Journal of Applied Mathematics Volume 2013.
[11] J. K. Mandal , Debashis Das," Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain" , International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.
[12] P. Rajkumar , R. Kar , A. K. Bhattacharjee , H. Dharmasa "A Comparative Analysis of Steganographic Data Hiding within Digital Images", International Journal of Computer Applications (0975 – 8887) Volume 53– No.1, September 2012.
[13] Mrs.Y.Kumari, Mr. G.V. Ramanaiah," A Novel Method Avoids the Fall - Off Boundaries by Using Try - Way Pixel Value Difference and Modulus Function in Image Steganography", International Journal Of Computer Science & Mechatronics,Vol.1.Issue 2. 2015.
[14] Akram M. Zeki1, Adamu A. Ibrahim Azizah A. Manaf And Shahidan M. Abdullah," Comparative Study of Different Steganographic Techniques", Recent Researches in Applied Informatics and Remote Sensing, ISBN: 978-1-61804-039-8 52.