www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 6 June 2015, Page No. 12429-12434

Image Steagnography: A Review

Priyanka Jagota

Scholar at Rayat Bahra Institute of Engineering and Biotechnology Mohali,
Punjab

jagotapriyanka.42@gmail.com

ABSTRACT: *Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Various techniques of image Steganography are explained such as spatial domain technique, Spread Spectrum Technique, Transform Domain Technique, Statistical Technique, distortion technique. In this paper various Image Steganography techniques are reviewed.*

Keywords: *Cryptography, Steganography, Image Steganography, Spatial Domain, Distortion technique, Spread Spectrum technique, Parameters.*

1. INTRODUCTION

Steganography is the art of hiding information in some media. A Steganography system thus embeds hidden content in unremarkable cover media to avoid eavesdropping. In the past, people used hidden tattoos or invisible ink to convey secret information. Today, computer and network technologies provide easy-to-use communication channels for transmission of messages. Essentially, the information-hiding process in a steganography system starts by identifying a cover medium's redundant bits (those that can be modified without destroying that medium's integrity). The embedding process creates a *stego medium* by replacing these redundant bits with data from the hidden message. Modern technique aims to keep its mere presence undetectable, but steganography systems because of their invasive nature, leave behind detectable traces in the cover medium. Even if secret content is not revealed, the modified cover medium changes its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium's statistical properties. The process of finding these distortions is called statistical steganalysis.

1.1 Types of Steganography

- **Text Steganography:** A text when taken as a carrier object is termed as text Steganography. Different formats are used in this technique. In text Steganography number of tabs, white spaces capital letters are used to achieve information or message hiding.

Er. Surbhi Gupta

Associate Professor at Rayat Bahra Institute of Engineering and Biotechnology Mohali,
Punjab

royal_surbhi@yahoo.com

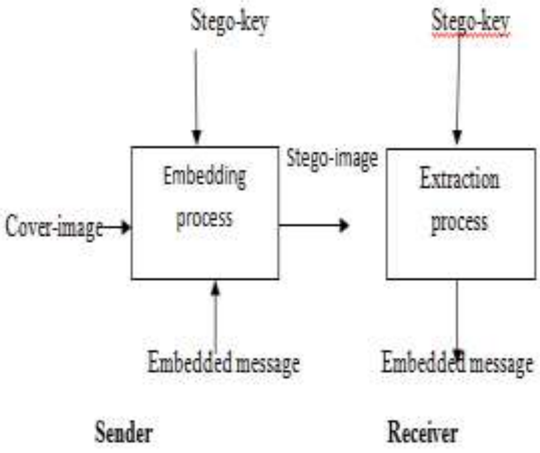


Figure [1] Data Hiding Process

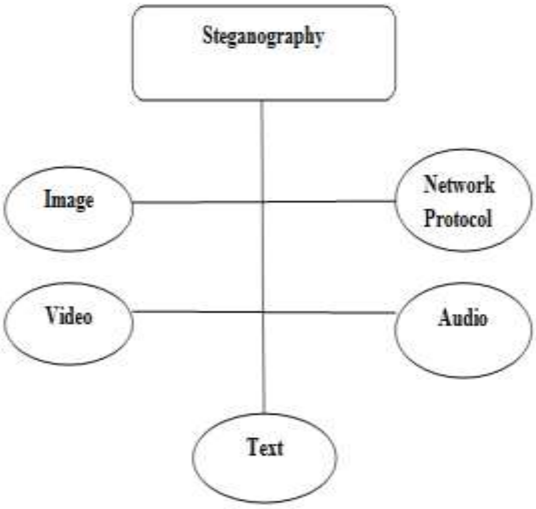
- **Image Steganography:** An image when taken as a carrier object is termed as image

Steganography .Concealing data inside images is a prominent procedure these days. A picture with a secret message inside can undoubtedly be spread over the World Wide Web or in newsgroups. In the domain of digital images many different file format exist.

- **Audio Steganography:** Audio when taken as a carrier object, then it is called audio Steganography. In this, secret message is embedded into digitized sound signal which results slight adjusting of double arrangement of the audio recorded. There have been many techniques for hiding information or message in such a manner that the changes made to the audio file are perceptually indiscernible.

- **Video Steganography:** This technique has video as its carrier object. The use of video Steganography is more eligible rather than the other multimedia files, because of its size and memory requirements. All types of formats are used.

- **Protocol steganography:** The term protocol steganography is to embed information within network protocols such as TCP/IP. We hide information in the header of a TCP/IP packet in some fields that can be either optional or are never used.



1.2. Image Steganography Terminologies

Image Steganography terminologies are as follows:-

- **Cover-Image:** Original image that is used for hiding purpose.

- **Message:** Actual information which is used to hide into images. Message could be a plaintext or some other image.

- **Stego-Image:** When we combine the secret message and cover image, then it is formed.

- **Stego-Key:** A key which is used for embedding or extracting the message from the cover image.

1.3. Image Steganography Classifications

Image Steganography is categorized in following aspects and the best Steganography measures [10].

- **High Capacity**: Maximum size of secret message which can be embedded into cover image.
- **Perceptual Transparency:** After hiding process into cover image, perceptual quality will be degraded into stego-image as compared to cover-image.
- **Robustness:** After embedding, data should stay fixed if stego-image goes into some transformation such as cropping, scaling, filtering and addition of noise.
- **Temper Resistance**: It should be difficult to alter or change the message once it has been embedded into a stego-image.
- **Computation Complexity**: How much expensive it is computationally for embedding and extracting a hidden message?

Measure	**Advantage**	**Disadvantage**
High capacity	High	Low
Robustness	High	Low
Temper Resistance	High	Low
Computational Complexity	Low	High
Perceptual Transparency	High	Low

SECTION I

1.4 Steganography Techniques

- **Spatial Domain Techniques:** There are many versions of spatial domain Steganography. This technique is based upon grey level mappings, where the type of mapping depends on criterion chosen for enhancement. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSB's of pixel values without introducing any distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labeling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

Advantages of spatial domain LSB technique are:
1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

- **Transform Domain Technique:** This is a more complex way of hiding information in an image as compared with spatial domain. Various algorithms and transformations are used on an image to hide the message. With the help of transform domain technique we can divide the image into parts. Transform domain technique has an advantage over spatial domain technique as they hide information in the area of the image that is less exposed to compression and cropping. Transform domain is more robust. Transform domain embedding is the process of embedding data in the frequency domain of a signal. It is much stronger than the time domain embedding. Transform domain techniques are broadly classified into:

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

- **Spread Spectrum Technique:** The spread spectrum technique is a data hiding communication which uses digital images. There are two approaches used: one is direct-sequence spread spectrum and second one is frequency hopping spread spectrum. Direct sequence spectrum is used in telecommunication. Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudo random sequence of 1 and −1 values, at a frequency much higher than that of the original signal, thereby spreading the energy of the original signal into a much wider band. This strategy utilizes the idea of spread range. In second method, frequency-hopping spread spectrum pseudo-randomly returns the carrier, instead of adding pseudo-random noise to the data, which results in a uniform frequency distribution whose width is determined by the output range of the pseudo-random number generator
- **Distortion Techniques:** In distortion technique, information about the original cover image during decoding process is needed. Decoder function is used to know the difference between the original cover image and the distortion image. Using this technique, a stego object is created by applying a sequence of modifications to the cover image. The encoder adds a sequence of changes to the original cover image. So, information or message is stored by signal distortion. This sequence of modifications is use to match the secret message required to transmit .The message is encoded at pseudo-randomly chosen pixels. If the stego-image is different from the cover image at the given message pixel, the message bit is "1." otherwise, the message bit is "0." The encoder can modify the "1" value pixels in such a manner that the statistical properties of the image are not affected.
- **Statistical Techniques:** In the statistical techniques, the information is encoded by changing several properties of the cover. In this technique, the existence of 1 bit is utilized, which embeds one bit of information or message into a digital carrier. This is done by modifying the cover image in such a way that statistical property changes significantly if 1 is transmitted. Otherwise the cover image is left unchanged. So the receiver can easily detect the difference between modified and unmodified image.

SECTION II

Related Work

Hussain & Hussain [1] explained that steganography is a process that involves hiding a message in appropriate carrier such as image, audio and video. The carrier can then be send to the receiver without knowing about the secret message. Various types, techniques, terminologies, classifications and applications such as military purpose, medical images were described.

Laskar & Kattamanchi et al [3] explained the high capacity data hiding approach by using LSB steganography and encryption to hide the secret data or information into cover image. They explained about the combination of encryption and Steganography. A message was first encrypted using transposition cipher text and then the encrypted message was embedded inside an image using LSB insertion method. The combination of these two increased the security of the secret message. MSE and PSNR were calculated to measure the quality of image .The main objective was to provide resistance against visual and statistical attacks as well as high capacity.

Karim & Rahman et al [4] introduced a new approach for LSB based image Steganography using secret key to hide the secret message or information into cover image. This approach enhances the existing LSB substitution technique to improve the security level of hidden information or message. Depending on secret key hidden information is stored into different positions of LSB of an image. As a result, it was difficult to extract the hidden information or message into cover image. To measure the quality of stego image two parameters PSNR and MSE were used. The value of PSNR gives better result.

Maya & Mariko et al [2] explained how data hiding was used in bit planes of sub band wavelets coefficients by using the integer wavelets transform (IWT). To increase data hiding capacity while keeping the imperceptibility of the hidden data, the replaceable IWT coefficient areas were defined by a complexity measure used in bit plane complexity segmentation steganography (BPCS). The approach had a high data hiding capacity. Error control coding was used to reduce the Bit Error Rate (BER) of extracted hidden data when stego image receive some channel distortion.

Provos & Honeyman et al [5] explained the method to hide secret data into cover image. The authors discussed the existing steganography systems and presented recent research in detecting them via statistical steganalysis. The practical application of detection algorithms and the mechanisms for getting around them were also listed.

SECTION III

RESULTS

Different parameters are used which are explaining as below:

(1) Parameters used

PEAK SIGNAL-TO-NOISE RATIO

The term peak signal-to-noise ratio (PSNR) is an expression for the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. Because many signals have wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale. The PSNR is defined as [8] :

$$PSNR = 10.\log_{10} (MAX^2/MSE)$$

$$= 20.\log_{10} (MAX_I/\sqrt{}MSE)$$

$$=20.\log_{10} (MAX_{I)} - 10.\log_{10} (MSE)$$

PSNR is most commonly used to measure the quality of reconstruction of lossy compression codes. The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codec's, PSNR is an approximation to human perception of reconstruction quality. Although a higher PSNR generally indicates that the reconstruction is of higher quality, in some cases it may not. PSNR is most easily defined via the mean squared error (MSE). Here, MAX_I is the maximum possible pixel value of the image. When the pixels are represented using 8 bits per sample, this is 255.

MEAN SQUARED ERROR:

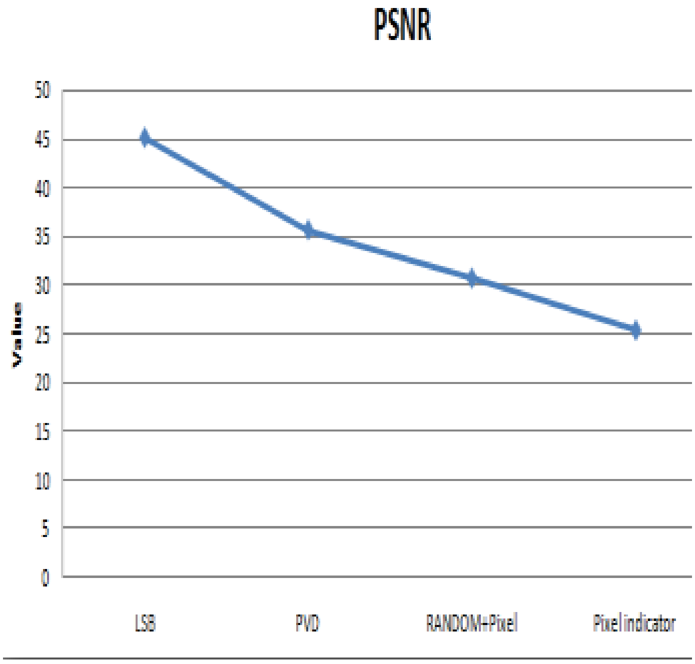
Mean squared error (MSE) of an estimator measures the average of the squares of the "errors", that is, the difference between the estimator and what is estimated. MSE is a risk function, corresponding to the expected value of the squared error loss or quadratic loss. The difference occurs because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate. The MSE is the second moment (about the origin) of the error, and thus incorporates both the variance of the estimator and its bias. For an unbiased estimator, the MSE is the variance of the estimator. Like the variance, MSE has the same units of measurement as the square of the quantity being estimated. In an analogy to standard deviation, taking the square root of MSE yields the root-mean-square error or root-mean-square deviation (RMSE or RMSD), which has the same units as the quantity being estimated; for an unbiased estimator, the RMSE is the square root of the variance, known as the standard deviation.

Parametric Values

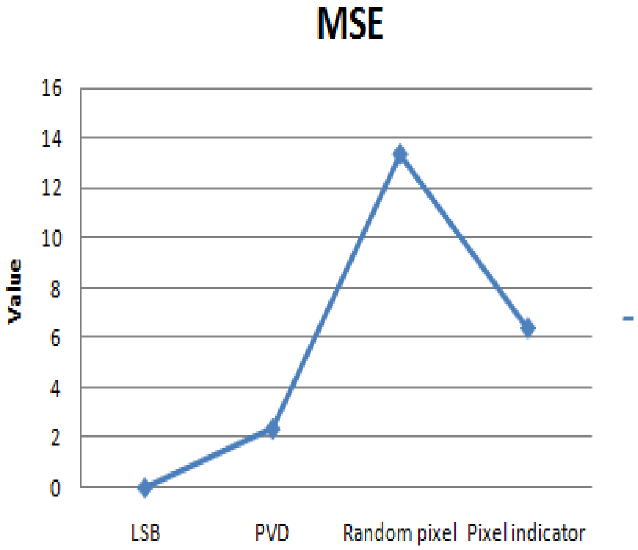
Approach	PSNR	MSE
LSB	45.05	0
PVD	35.63	2.36
Random pixel	30.69	13.36
Pixel indicator	25.36	6.396

In this table, LSB technique contains the highest value of the PSNR and lowest value of MSE as compared to the other techniques which are shown in table. Due to these values the quality of image has become better. That's why this technique has been opted.

(2) Graphs



In this graph, horizontal axis is representing the techniques and vertical axis is representing the values of PSNR. This graph shows the highest value of PSNR in case of LSB as compared to the other techniques. If PSNR attains a highest value then it contains a better quality of image.



In this graph, horizontal axis is representing the techniques and vertical axis is representing the values of MSE. This graph shows the lowest value of MSE in case of LSB as compared to the other techniques. If MSE attains a lowest value then it contains a better quality of image.

(3) Images

Original image

Pixel Indicator

Random pixel

LSB

PVD

SECTION IV

CONCLUSION

This paper gives an overview of different techniques of steganography, classification and its types. This paper also provides efficient information related to the steganography, in respect to the Techniques reviewed spatial domain technique is the best because distortions are not created and changes are not reflected.

SECTION V

REFRENCES

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

[2] Silvia Torres-Maya, Mariko Nakano- Miyatake and Héctor Perez-Meana *SEPI,"* An Image Steganography Systems Based on BPCS and IWT" 16th IEEE International Conference on Electronics, Communications and Computers

[3] Shamim Ahmed Laskar and Kattamanchi Hemachandran "High Capacity Data Hiding approach by using LSB steganography and encryption" International Journal of Database Management Systems (IJDMS), Vol. 4, No. 6, December 2012.

[4] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain "A New Approach for LSB Based Image Steganography using Secret Key" International Conference on Computer and Information Technology pp. 22-24 December, 2011.

[5] Provos, N., Honeyman, P, "Hide and seek: An introduction to steganography," IEEE Security & Privacy Magazine 1 (2003) pp. 32-44.

[6] Dr. Diwedi Samidha, Dipesh Agrawa, NRlIST "Random Image Steganography in Spatial Domain" 2013, IEEE.

[7] kaminsky, a. "An overview of cryptanalysis research for the advanced encryption standard" IEEE conf. on military communications conference, 2010, pp 1310 – 1316.

[8] Alaa A. Jabbar Altaay, Shahrin bin Sahib, Mazdak Zamani "An Introduction to Image Steganography Techniques "International Conference on Advanced Computer Science Applications and Technologies, 2013 IEEE.

[9] R. chandramouli, Nasir Memon "Analysis of LSB Based Image Steganography Techniques" 2001 IEEE.

[10] Mehdi Hussain, Mureed Hussain "Pixel Intensity Based High Capacity Data Embedding Method" 2010 IEEE.