ANALYSIS OF STEGANOGRAPHY FOR GRAY-SCALE AND COLORED IMAGES USING LSB SUBSTITUTION TECHNIQUE

[1]Girish Mahajan, [2]Prof. Makrand Samvatsar
[1]M.Tech Scholar, [2]Associate Professor
[1]Department of Computer Science Engineering,
[1]Patel College of Science & Technology, Indore, M.P.

Abstract - As the escalation of internet is one of the major traits of information technology, data hiding techniques has taken a significant role for the transmission of multimedia content. One of the essential properties of digital information is that it is in principle very simple to create and share out unlimited number of its duplicates. The fact that an unlimited number of perfect copies of text, image, audio and video records can be illegally created and distributed requires studying ways of embedding copyright information and serial numbers in image, audio and video data. Steganography brings a variety of very substantial technique how to conceal key information in an imperceptible and/or irremovable way in data like image, audio and video. Steganography is most important part of the fast emerging area of information hiding. In this work, we have deliberated steganography methods using LSB substitution for gray scale image also for colored images. Approaches for image steganography always focus on retaining the visual quality of an image while scrambling a secret message in it. The simulation results of our work indicates that this method achieves well especially when embedding secret data at higher LSB bit positions. There are few procedures that try to improve the quality of stego image by embedding secret data only in the channels of least importance. Our work also describes frequency domain techniques to achieve the enhancement in confidential and authenticated data storage and secured transmission. Performances of all these transform are compared according to application of data hiding technique. Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) is used as a performance index to show the quality of steganographic image.

Index Terms – Steganography, LSB, Color Images, Data Hiding

In this modern world, internet offers great convenience in transmitting large amounts of data in different parts of the world. However, the safety and security of long distance communication remains an issue. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. In order to solve this problem has led to the development of steganography schemes.

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

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 [1]. Steganography and cryptography are both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [1]. The strength of steganography can thus be amplified by combining it with cryptography.

In this paper, we have studied spatial domain technique is used in image processing for application like data hiding i.e. steganography. It is observed that data hiding using image is more useful than data hiding through text. The objectives of thesis are:

1. To hide the data like text and image, cover selection is important.
2. To achieve steganography in spatial domain LSB substitution method is used. Also this chapters suggested types of steganography and various attacks.
3. To compare the performance of all these methods with each other.
4. To study the effect of variation of parameter on Power Signal to Noise Ratio (PSNR) and Mean Square Error (MSE).
5. Comparison of performance parameters, i.e. PSNR for different images.

This paper is organized as follows. Section II discusses the basic idea of steganography technique and literature review involved in this paper. Section III describes performance parameters of images. Section IV shows implementation of these methods and their results. Finally section V gives the conclusion.

I. STEGANOGRAPHY

Steganography is a branch of information hiding in which secret information is camouflaged within other information. The word steganography in Greek means “covered writing” (Greek words “stegos” meaning “cover” and “grafia” meaning “writing”) [2]. The main objective of steganography is to communicate securely such a way that the true message is not visible to the observer. That is unwanted parties should not be able to distinguish any sense between cover-image (image not containing any secret message) and stego-image (modified cover-image that containing secret message). Thus the stego-image should not deviate much from original cover-image. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. The schematic representation of the steganography is given in Fig. 1:

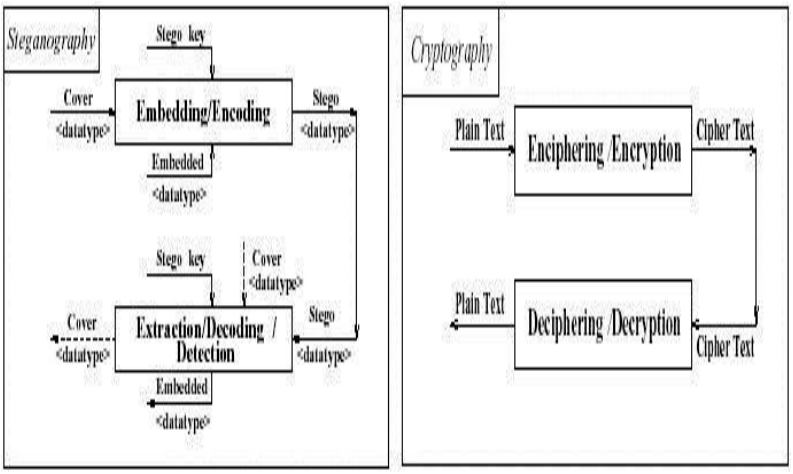


Fig. 1: Steganography versus Cryptography

The techniques of data hiding i.e. steganography, watermarking and cryptography are interlinked. The first two are quite difficult to tease apart especially for those coming from different disciplines. Table 1 summarizes the differences and similarities between steganography, watermarking and cryptography.

Table 1: Comparison of steganography, watermarking and crytography

Creterion/ Method	**Steganography**	**Watermarking**	**Cryptography**
Carrier	Any digital media	Mostly image/audio files	Usually text based
Secret Data	Payload	Watermark	Plain text
Key	Optional		Necessary
Inputt files	Atleast two unless in self-embedding		One
Output files	Stego-file	Watermarked-file	Cipher-text
Objective	Secrete communication	Copyright preserving	Data protection
Visibility	Never	Sometimes	Always
Flexibilty	Free to choose any cover	Cover choice is restricted	N/A
Fails When	It is detected	It is removed/replaced	De-ciphered

On the basis of the image formats i.e. Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), and to a lesser extent- Portable Network Graphics (PNG), image steganography are of three types:

- Steganography in the image spatial domain
- Steganography in the image frequency domain
- Adaptive steganography

Steganography in the image spatial domain: Here spatial features of image are used. This is a simplest steganographic technique that embeds the bits of secret message directly into the least significant bit (LSB) plane of the cover image. In a gray-level image, every pixel consists of 8 bits. The basic concept of LSB substitution is to embed the confidential data at the rightmost bits (bits with the smallest weighting) so that the embedding procedure does not affect the original pixel value greatly [3]. The mathematical representation for LSB is as equation 1:

$$x'_i = x_i - x_i \, mod \, 2^k + m_i \qquad \textbf{(1)}$$

In Equation (1), x'_i represents the i^{th} pixel value of the stego-image and xi represents that of the original cover-image. m_i represents the decimal value of the i^{th} block in the confidential data. The number of LSBs to be substituted is k. The extraction process is to copy the k-rightmost bits directly. Mathematically the extracted message is represented as in equation (2):

$$m_i = x_i \, mod \, 2^k \qquad \textbf{(2)}$$

Hence, a simple permutation of the extracted mi gives us the original confidential data [4]. This method is easy and straightforward but this has low ability to bear some signal processing or noises. And secret data can be easily stolen by extracting whole LSB plane. A general framework showing the underlying concept is highlighted in Fig. 2.

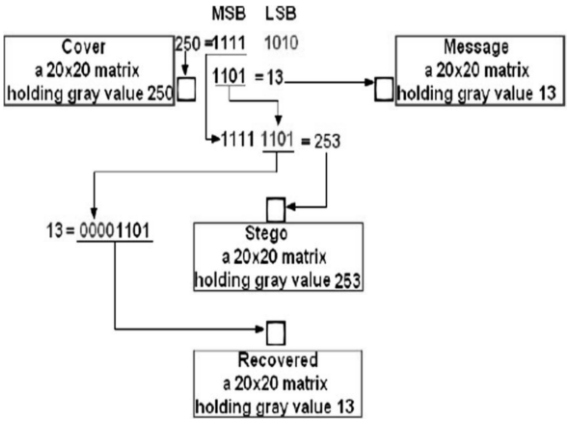


Fig. 2: Steganography in spatial domain. The effect of altering the LSBs up to the 4th bit plane

In the case of steganography, the reconstructed image is only an approximation to the original. Although many performance parameters exist for quantifying image quality, it is most commonly expressed in terms of mean squared error (MSE) and peak signal to noise ratio (PSNR). For a good steganography, MSE should be less. PSNR is provided only to give us a rough approximation of the quality of steganography. PSNR should be more for good perception of received image.

Princymol Joseph et *al.*, describes a brief study on steganography in their research paper. In steganography, information can be concealed in carriers such as text files, images, audio and video. Based on features such as carrying file, type of message to be rooted, methods of compression used etc., the technique used in steganography can contrast. The power of a steganographic technique lies in its capacity to retain the message, as secret as potential and also the amount of data that can be hidden, as large as possible. In malice of the point that numerous methods already exist in steganography, researches are going on in this field [5].

Amritpal Singh et *al.*, suggested enhanced LSB based image steganography methods for RGB images. There are number of steganography techniques projected to hide data like LSB, DCT, pixel-value differencing, DFT etc. into images with accuracy level. But these techniques grief from some problems like less hiding capacity lower the quality of image and security of hidden data after hiding more data into it. To overwhelm these problems they proposed an improved LSB technique for color images by embedding the information into three planes of RGB image in a way that increases the quality of image and attains high embedding capacity [6].

Dilpreet Kaur et *al*, discussed about hybrid approach of cryptography, data compression and steganography has been proposed in their paper. Inspiration behind their work is to provide a smart image steganographic technique which must be skilled enough to offer better quality stego-image with a high data hiding capability. Projected method is a LSB based approach and enthused with the invention of H. B. Kekre in the field of image steganography. Maximum data hiding capability of proposed method will be assessed from kekre's algorithm [7].

II. PERFORMANCE PARAMETER

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Image quality measures are of excessive significance in various image processing applications. In the case of steganography and watermarking, the recreated image is only a guesstimate to the original. Although many recital parameters exist for measuring image quality, basically these two classes are objective eminence assessment approaches, viz Mean square error (**MSE**), peak signal to noise ratio (**PSNR**), and signal to noise ratio (**SNR**).

Mean Square Error: This parameter is demarcated as the mean square of difference of corresponding pixel values in the original image and stego-image. Likewise root mean square can be defined as the root mean square of variance of corresponding pixel values in the original image and stego-image. For a good data hiding techniques, MSE should be less. Further, the root mean square can be intended by taking square root of MSE. The mean square error can be expressed as in equation:

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[f'(i,j) - f(i,j)]^2$$

Peak Signal to Noise Ratio (PSNR): The PSNR is the only scrupulously defined metric. The main motive for this is that no good rigorously defined metrics have been projected that take effect of the Human Visual System (HVS) into interpretation. PSNR is provided only to give us a rough approximation of the quality of steganography. The PSNR in mathematical form can be given as equation:

$$PSNR = 10\ log_{10}\left[\frac{256 \times 256}{MSE}\right]$$

III. RESULTS & SIMULATION

A. Steganography using Text:

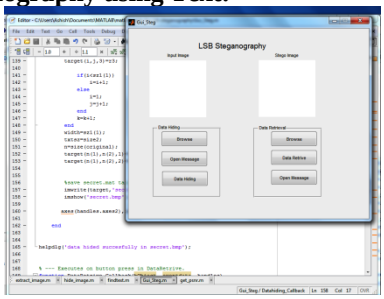
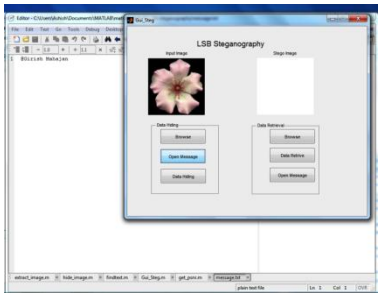
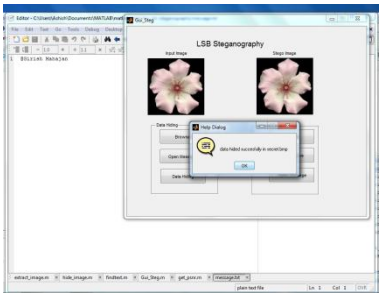
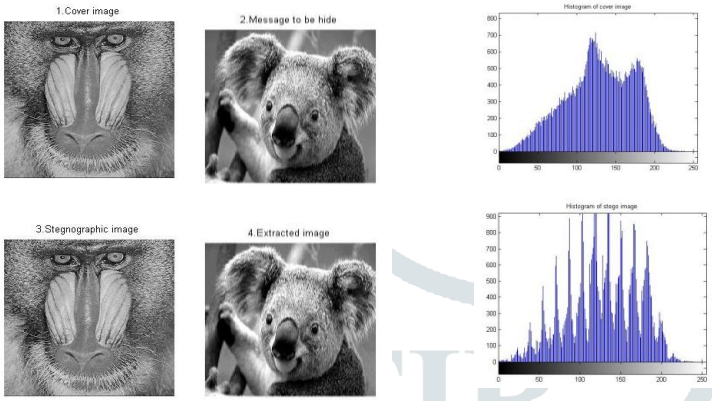




Fig 3: Illustration of various steps involves in steganography using text

B. Steganography in Gray Scale Image:



PSNR between message and extracted image is 29.25 dB
PSNR between cover and stegangraphic image is 32.57 dB

Fig 4: Illustration of Steganography using LSB substitution (n=4) and histogram of cover, extracted image

C. Steganography using DFT and DCT of Cover Image:

PSNR between message and extracted image is 23.29 dB
PSNR between cover and stegangraphic image is 5.49 dB

Fig 5: Illustration of Steganography using DFT of cover image

PSNR between message and extracted image is 29.01 dB
PSNR between cover and stegangraphic image is 4.79 dB

Fig 6: Illustration of Steganography using DFT of cover image

D. Steganography in Colored Image

Fig 7: I[st] row: Cover and message image, II[nd] row: Steganographic image and extracted image

IV. CONCLUSION

It is witnessed form the simulation images and PSNR values acquired in the case of steganography; discrete cosine transform (DCT) is effective than spatial domain method because transform makes the steganographic image more robust. These methods are more composite and gentler than spatial domain methods; however they are more protected and lenient to noises. Frequency domain transformation can be realistic in discrete Fourier transform i.e. DFT, discrete cosine transform i.e. DCT. Also by using LSB substitution method in color image we can achieve more robust steganography [5].

The data hiding technique that is given in this paper can be further improved to increase the hiding capacity of images without affecting the imperceptibility of the images. The other future scope is that our technique can be enhanced to embed colored nested messages in colored image. In addition, we will optimize and improve the spread spectrum algorithm to become faster and more intelligent.

REFERENCES

[1] Wang, H and Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004

[2] Moerland, T. "Steganography and Steganalysis". Leiden Institute of Advanced Computing Science, www.liacs.nl/home/tmoerl/privtech.pdf

[3] Anjali A. Shejul and Umesh L. Kulkarni, "A Secure Skin Tone based Steganography Using Wavelet Transform", International Journal of Computer Theory and Engineering, Vol.3, No.1, February, 2011,

[4] Ashish Soni, Rakesh Roshan, Jitendra Jain, "Image Steganography in Discrete Fractional Fourier Transform Domain", International Conference on Intelligent System and Signal Processing 2013, ISBN no: 978-1-4799-0316-0©IEEE.

[5] Princymol Joseph, Vishnukumar S., "A Study on Steganographic Techniques", Proceedings of 2015 Global Conference on Communication Technologies (GCCT 2015), 2015 IEEE

[6] Amritpal Singh, Harpal Singh, "An Improved LSB based Image Steganography Technique for RGB Images", International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE

[7] Dilpreet Kaur, Harsh Kumar Verma, Ravindra kumar Singh, "A Hybrid Approach of Image Steganography", International Conference on Computing, Communication and Automation (ICCCA), 2016 IEEE.