ISSN: 0975-766X
CODEN: IJPTFI
Available through Online *Review Article*
www.ijptonline.com

STEGANOGRAPHY: A COMPARATIVE STUDY, ANALYSIS OF KEY ISSUES AND CURRENT TRENDS

Vanmathi C*, Prabu S
School of Information Technology and Engineering, VIT Universtiy, Vellore, Tamilnadu, India.
School of Computing Science and Engineering, VIT Universtiy, Vellore, Tamilnadu, India.
Email: vanmathi.c@vit.ac.in

Received on 22-07-2016 *Accepted on 30-08-2016*

Abstract

Information security is the one of the most important, crucial part of any digital communication and one of the largest issues faced in the digital world. Securing information from unauthorized access, modification and destruction, maintain the confidentiality and integrity of the data. Though many security techniques exist to secure information, well known and widely used is a cryptography and steganography. Cryptography is the art of changing the text into an unintelligible content at the sender and it is changed again into readable content at the receiver end. Steganography is hiding the content to the any digital media like image, video and audio which cannot be seen. The ultimate goal of steganography rather than robustness is that the adversary, not even able to identify that the media contains the secret message. The strength of steganography applications depends on the result of the stego object. The difference between the original object and stego object should not be more in terms of visual and statistical properties. This paper provides the review of various steganography techniques in different domains, performance evaluation metrics, key issues, discussion on the latest methods and future directions in this field. This article also provides the strength and weakness of the each technique.

Keywords: Data hiding, Review, Steganography, Psnr , Stego.

1. Introduction

The steganography [1] is the art of hiding information in ways that prevent the detection of hidden messages. It is derived from the Greek, means “covered writing”. Steganography hides data for various purposes, including secret data storing, confidential communication, and authentication. The main goal of the steganography is to make the secret communication insensible; it conceals the very existence of the secret message. Steganography is applied in many private communication where the secrecy has to be maintained. The various fields like military [2] and

intelligence agencies [3], healthcare industry and in, specific medical imaging systems use the benefit of information hiding. [4], checksum embedding [5], radar systems and remote sensing.

1.1 A framework for secret communication

Steganography applications follow a general working principle given in fig1. A is the sender wants to transmit the secret message to the receiver B. A is choosing a cover object to embed and hide the secret message into it using steganographic algorithm. The cover object may be any image, audio or video similarly the secret message may be text or an image. At the receiver end the reverse steganographic algorithm is applied to extract the secret message from the cover object. Stego key may be used to control the embedding process.

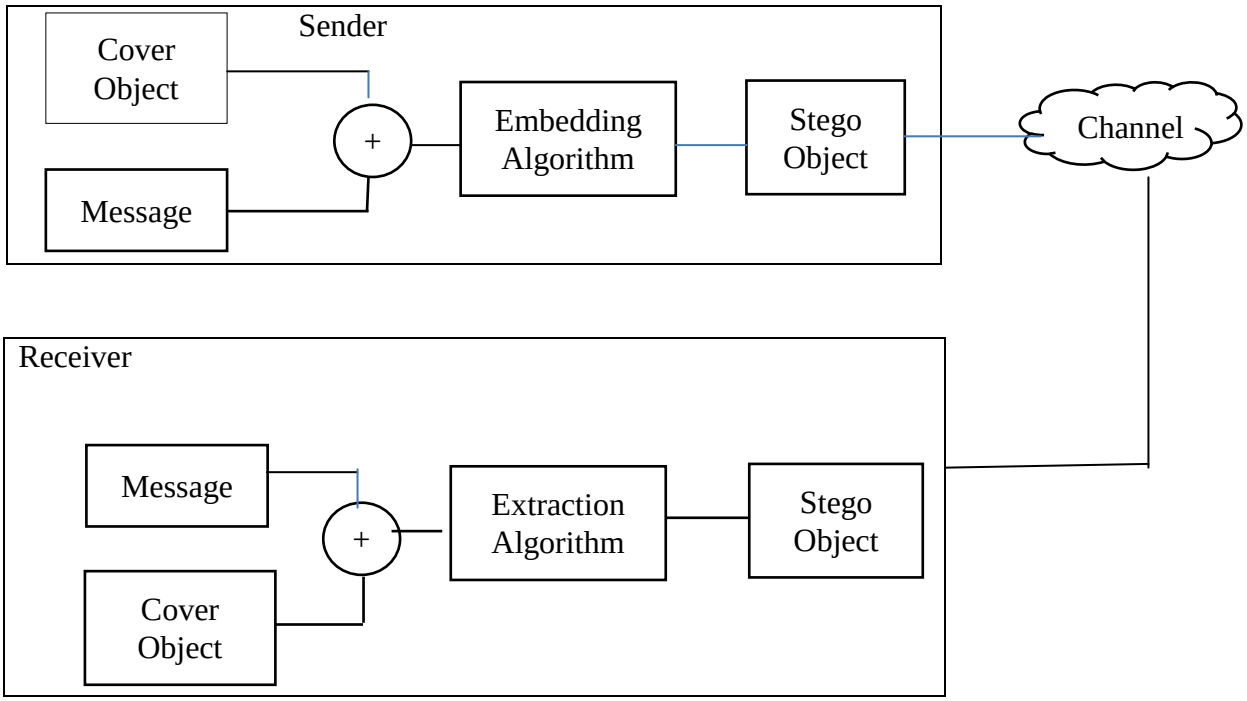

Fig1. Framework for Steganography.

1.2 The key terms and characteristics

The key terms used in steganography are

Cover object – The object which is used to hide the secret message

Message – The secret message that is the actual information to be hidden in the cover object.

Stego object – The cover object after embedding the secret message.

Embedding algorithm – Procedure to hide the message into cover object.

Extraction algorithm – Procedure to extract the secret message from the stego object.

The embedding process can be described as

E: C X M -> C, where C is the cover and M is the message, and satisfies the condition |C|>=|M|

The Extraction process can be described as D: C -> M where C is the cover and M is the message. The private steganographic algorithm is shared by both sender and receiver for embedding and extracting the secret message. The characteristic of a steganographic system can be measured by three important factors

a. Imperceptibility – Which is the most important property of the data which shows how difficult to determine the presence of the data existence.A true steganographic system should not be detectable neither by system or by human being.
b. Data Capacity – Which is the possible amount of secret data to be hidden and retrieved successfully on the cover image without degrading the cover image quality. The human eye cannot detect the small amount of data hidden. The statistical tests reveal the presence of large amounts of data is hidden
c. Robustness - Refers how well the stego system withstands the various attacks like cropping, rotating, compressing and filtering to extract or remove the hidden data. Watermarking is an example of the robust steganographic system.

2. Types of Steganography

There are two types of Steganography Fig2.Linguistic and technical steganography. Linguistic steganography hides the data in a non obvious way so that is not visible to others [6]. There are different ways which use the linguistic structure of a text as a place to hide the information.

It is divided into two types semagrams and open codes. In semagrams the message is hidden using symbols and signs. In open codes the secret data are hidden using legal paraphrases of the text so that it is not suspected by the observer

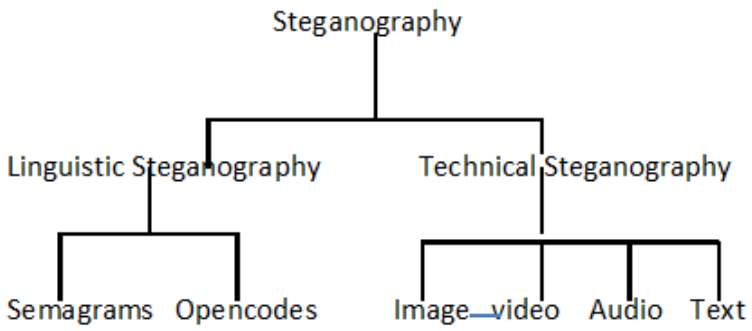

Fig2. Types of Steganography.

Technical steganography uses the various systematic methods like invisible ink, microdots and computer based algorithms to hide the secret message. It uses digital images, audio , video and text as a cover medium to hide the message. Image Steganography becomes more popular compared to others due to its wide use of images over the

internet and other applications. It involves hiding the information which naturally present in 'noise' within the image. Noise can be defined as unwanted or unimportant information present in the image signal. Audio Steganography hides the message in 'audio noise'. Audio noise is the frequencies which is not heard by humans. Changing the actual audio signal to hide the secret message affects the statistical properties of audible signals and it is easily identified by sound engineers, audiophiles and musicians. So care must be taken while modifying the audio signal. Steganography is broadly classified into various domains spatial, transform, spread spectrum, statistical and cover generation technique [2]. This paper provides the detailed review of spatial and transform domain techniques on the image. The most popular image formats on the internet are Graphics Interchange Format, Joint Photographic Experts Group (JPEG), and the Portable Network Graphics (PNG). Most of the techniques are developed to exploit the structures of these .

2.1 Spatial domain steganography

Spatial domain techniques are also called as substitution techniques. In this the actual pixel values of the image are changed to hide the secret data. In substitution technique the secret message bits is encoded in the insignificant parts of the cover image generally in LSBs. Since there are only minor changes in the image the sender assumes the attacker will not notice the changes in the original image. But it is vulnerable to signal processing attacks and also it loses the total information for lossy compression techniques. Fig 3 shows the common methods used in spatial domain.

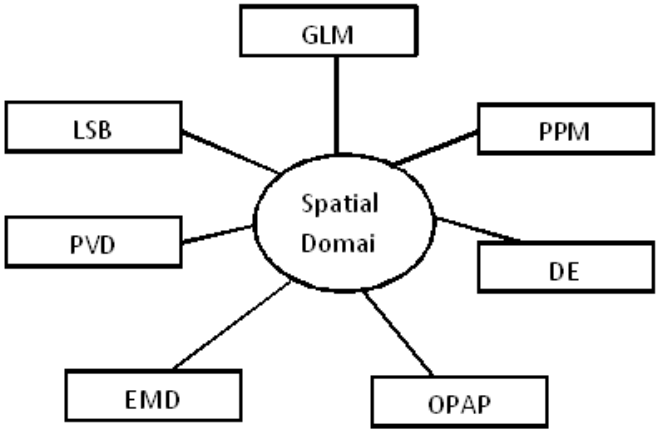

Fig 3. Existing methods of Spatial Domain Technique.

LSB – least Significat Bit

PVD – Pixel Value Differencing

PPM – Pixel Pair Matching

GLM – Gray Level Modification

EMD- Exploiting Modification Direction

DE – Diamond Encoing

2.1.1 LSB method

The LSB replacement [7] is the general spatial domain techniques which are used in spatial domain, in which the secret data is hidden in Least Significant Bits of the image so that the modification is not noticeable by the human eye. The best result is achieved if the 1st to 4th LSB bits are replaced by the secret bits. It can be applied to 8 bit grey or 24 bit color images. In 24 bits each 3 bits of a secret image can be hidden in each red, blue and green components if one LSB is replaced.

The following fig 4 shows LSB replacement in 8 bit image formats.

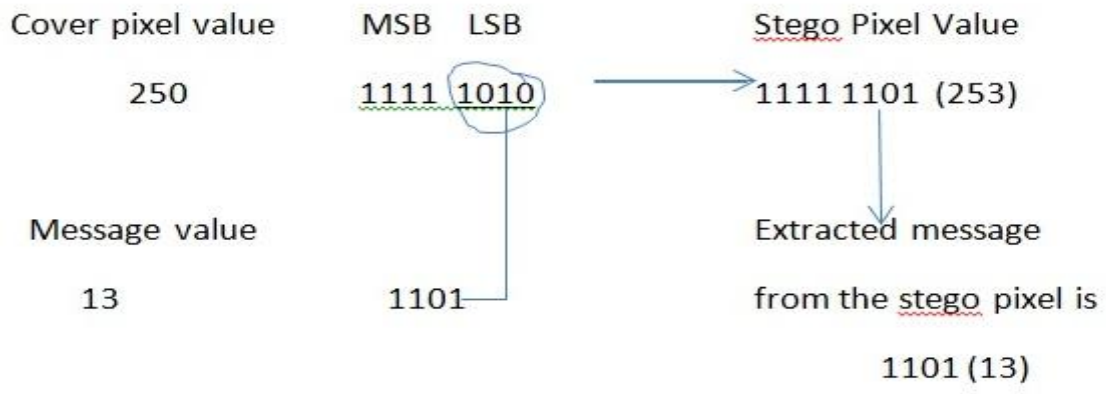

Fig4. Example of 8 bit LSB replacement.

The following figure 5 shows LSB replacement in 24 bit image formats

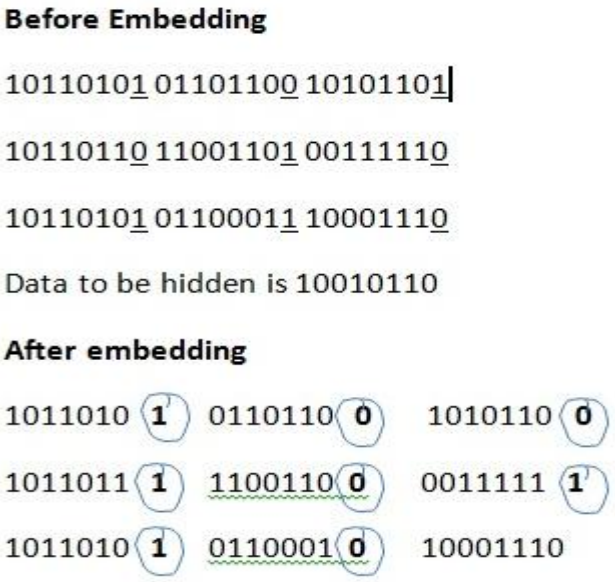

Fig5. Example of 24 bit LSB replacement.

LSB+ algorithm [8] embed the secret bits based on the unit frequencies. The unit frequencies are identified by two adjacent pixels. The extra bits 0 and 1s are embedded to maintain the histogram of the image. This method reduces the additional distortion caused by the normal LSB method.

Kazem et all [9] proposed method for improving LSB++ by identifying the sensitive pixels which is having more impact on the stego image.histogram attacks doesnot affect the stego image. The elimination of the extra bits improves the visual quality of the stego image.

2.1.2 Pixel Value Differencing (PVD)

Wu, Tsai [10] first proposed pixel value differencing method which gives stego images with better quality than the LSB embedding and maintains high embedding data capacity . It uses the difference between the pixel values, the cover image is divided into non overlapping blocks of two connected pixels and modifies the pixel values of the block based on the difference. The number of secret bits to be embedded is decided by the range table given below.

0 8 16 32 64 128 255

0~7	8~15	16~31	32~63	64~127	128~255

Table 1. Range Table.

Assume the pixel values of the gray scale image is 95 and 114. The difference between these pixel values is 19, which lies in the lower bound 16 and upper bound 31. Assume that the secret bit values are 1001 1000.

The embedding process is done based on the following

Step1: Find the difference between the two consecutive pixels result is 19.

Step2: The lower bound value is chosen based on the range table, so 16 is chosen as the low bound for 19. The secret message bits 1001 value 9 and it is added to the lower bound value 16, results 25.

Step 3: Calculate the difference between the secret bit value and the actual pixel difference 25 – 19 = 6 and divide the value by 2 and the computed value is subtracted and added to the target pixel values. The Final stego pixel values comeat 92 and 117.

2.1.3 PVD with Optimal Pixel Adjustment Process

Han-ling Zhnag [11] Instead of using a fixed range of values used in PVD uses an original PVD method by applying it surrounding 3 pixel values.

f(x-1,y-1) top left pixel	f(x-1,y) top pixel
f(x,y-1) left pixel	f(x,y) target pixel

The embedding capacity of the target pixel value is calculated from other surrounding pixel difference values. PVD can be applied to the edge pixels to increase the embedding capacity.

Honsinger et. al [12] used the spatial domain for data hiding. They used 256 modulo addition for embedding in the original image, hash function and secret key used while embedding the secret data. The reversibility is done by using of modulo addition and prevents the overflow and underflow condition It produces salt and pepper noise during modulo addition.

Wein Hong et.al [13] [14] used pixel differencingmethod, in this the nearest neighboring pixels to predict the visited pixel value and calculates the variance value from those pixels. Message bits are embedded by adjusting the difference value found in the pixels. They proved the proposed algorithm with existing methods in terms of payload. H.Y. Leung et al. [15] [16]]partition the cover image two divisions, onestore the secret information and the second stores the details like block type map and location maps which is the information about the plan of the data is hidden in the image. Data is hidden in the smooth regions rather than non-smooth regions and used accurate gradient selection predictor method is used for embedding. They increased the payload by utilizing the prediction error values of the previous methods. Kekre [17] combined PVD with a multiple LSB algorithm to achieve better capacity. The image is divided into non overlapping pixels, if the pixel is between the range 0-191 then the PVD method is applied else multiple LSB method is followed.

The embedding process is done using quantization and falling of boundary check technique [18]. Secret bits are embedded in zigzag fashion fig 6 and identifies the blocks which comes with boundary and those blocks are ignored during embedding.

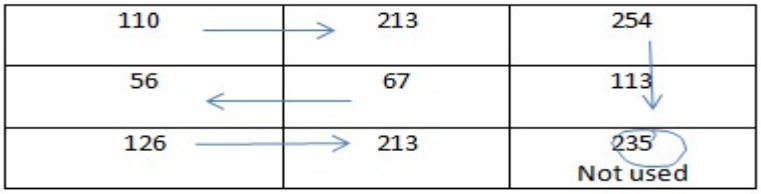

Fig. 6 Zig Zag PVD.

Xinpeng Zhang [19] proposed PVD using pseudo random parameter to defeat the histogram steganalysis. Wen-Jan Chen [20] used hybrid edge detector along with LSB replacement method. Their method not only increases the capacity and and also improves the visual quality of the image. The experimental results also shown by comparing the number of edge pixels obtained by the hybrid edge detector. Wein Hong et.al [21] [22] used pixel differencing method, in this the nearest neighboring pixels to predict the visited pixel value and calculates the variance value from those pixels. Message bits are embedded by adjusting the difference value found in the pixels. They proved the proposed algorithm with existing methods in terms of payload. Yifeng Sun [23] improves the steganographic system by selecting the best cover based on Gauss Markov process. The smaller correlation cover has been chosen for data hiding based on the KL divergence and Bhattacharyya distance. The least square estimator and exponential model of correlation is used for spatial domain cover selection.

In this approach [24] the image is partitioned into smaller segments and allow embedding only within the segment. Randomization technique is applied to preserve histogram of the image.

Potter et al. [25] proposes Gray level modification techniques where the gray pixel values are changed based on the odd and even values. One to one mapping is done between the gray values and the secret binary data bits for embedding. Tung-Shou Chen [26] introduced a new method based on pixel pair matching (PPM) uses the values as the reference coordinate and find the pixel values suitable for secret data bit. The distortion of the stego image is reduced by fining the more compact neighbourhood and allowing any notational system.

Zhang [27] proposed Exploiting Modification Direction for increasing the embedding capacity of the nary notaional system. Instead of increasing or decreasing the pixel values by 1 , used 2n+1 possible values of secret digit. The secret digits are represented in 2n+1 ary notational system. Ruey Ming [28] proposed Diamond encoding based method where instead of using 2n+1 ary digit into n cover pixels , $2k^2+2k+1$ ary digit into a cover pixel where k is the parameter for embedding.

2.2 Transform Domain Steganography

In spatial domain the secret data are embedded directly in the pixel values. In Transform domain first the image is transformed into frequency domain and the secret data is embedded on the frequency values. [29]. Spatial domain embeds more data compare to transform domain, but increases the robustness Hence the data is hidden in the more robust area of the image. Transform domain data hiding provides more resistance to image processing attacks. It is vulnerable to unauthorized users. There are several techniques available for converting the image from the spatial

domain to frequency domain. The most common frequency domain technique is Discrete Cosine Transform (DCT), Fourier Transform (FT) and Discrete Wavelet Transform (DWT). The most popular technique widely used is DCT.

2.2.1 Discrete Cosine Transform

DCT is important is wide range applications in science and engineering from lossy compression of audio and JPEG images. [30] . DCT divides the image into different frequencies with respect to image visual quality, low, middle and high frequencies fig. 7. Thus, it gives flexibility to choose regions to hide the message. The low frequency component contains the most visual parts of the image. The high frequency components are suppressed through image processing attacks [31]. So The middle frequency coefficient's are modified to for data hiding. So the imperceptibility and robustness are increased.

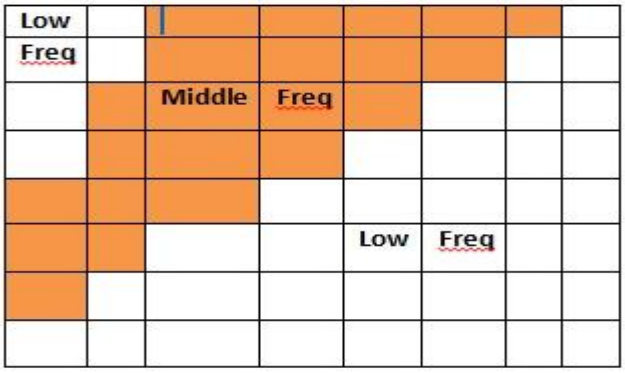

Fig 7. Freqency Regions of DCT.

In DCT domain steganography the image is divided into 8X8 block of pixels and DCT is applied to each block. The general equation for 2D DCT is given in equation 1 and equation 2 [32]. Inverse DCT is applied after the secret data is embedded in the frequency values of the image to convert back to the spatial domain.

DCT

$$F(u,v) = \frac{1}{4}C(u)C(v) \sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)cos\left[\frac{\pi(2x+1)u}{16}\right] cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (1)$$

for x =0,….,7 and y = 0,…..,7

where C(k) = $\begin{cases} 1/\sqrt{2} & for\ k = 0 \\ 0 & otherwise \end{cases}$

IDCT

$$f(x,y) = \frac{1}{4}C(u)C(v) \sum_{u=0}^{7}\sum_{v=0}^{7} F(u,v)cos\left[\frac{\pi(2x+1)u}{16}\right] cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (2)$$

for u =0,….,7 and v = 0,…..,7

F5 Algorithm is developed by Westfeld [33], instead of using LSB quantized DCT coefficient, the absolute value of the coefficient is reduced by 1 using F5 algorithm. Chi square attacks not able to identify this type of steganography. Matrix embedding is used to determine the number of modification to be carried out for the cover image for data embedding. [34] used Differential Phase Shift Keying, Pseudo Random Number Generator and DCT for data hiding. Chaotic method is applied to the RGB planes separately to ensure more security so that an attacker cannot steal the data. Hideki Noda et al [35] proposed JPEG steganography using Quantization index modulation and DCT. It preserves histograms characteristic and provides more data capacity. Hossein [36] used JSTEG algorithm as a base work and they tested the algorithm for middle and high frequencies for LSB data embedding. The boundaries of middle and high frequencies are not followed and achieved better results than JSTEG. Chin –Chen [37] proposed reversible data hiding scheme where the two successive zero DCT coefficient of middle frequencies are used for data embedding. Modified the quantization table to maintain the image quality of the stego image. A pair of 2X2 DCT coefficients, mod 4 is applied for data embedding.

The data path to embed the secret message from the coefficients is chosen based on Shortest route modification with some constraint. The embedding capacity is better than the DCT method for JPEG images [38]. In [39] used Fresnelet Transform Method in frequency domain for data hiding. The embedding capacity is more compared with other transform methods. They used LSB by the high frequency sub bands of the image for QR code secret message. Adaptive histogram equalization is applied to control the overflow.

2.2.2 Discrete Wavelet Transform

It is the most popular transformation technique for steganography. DWT converts the image in the spatial domain to transform domain. DWT is widely used and has more performance than DCT because it separates low frequency and high frequency components clearly on a pixel by pixel basis. The high frequency components are the edges in the image. These edges are used for steganography since the human eye is less sensitive to edges.The low frequency components are not altered to preserve image quality.

Fig 8 shows the various partitions of the image in the horizontal direction at various levels.At each level the LL subbands of previous level is used as an input. There are different types of wavelet exists Haar Wavelet, Daubechies, Fast wavelet and Dual complex wavelet transform [40]. Various steganography methods have been developed by using different wavelet transforms.

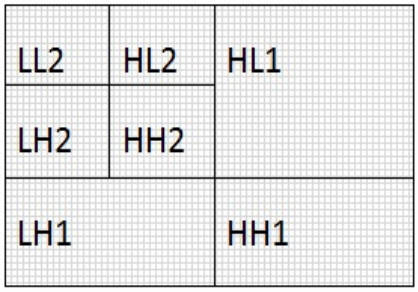

Fig 8 Three Phase Decomposition using DWT.

[41] authors proposed steganographic scheme using Discrete Wavelet transform and provides more data capacity and more security.Alpha and beta parameters are used to merge the data and cover images wavelet coefficients for embedding.The cover and the data are preprocessed in order to improve the decoding of the secret data. The proposed algorithm improves the acceptable PSNR ratio and MSE.

Yong-Kuan et al [42] proposed a reversible data hiding method base on Harr Discrete Wavelet Transform. Before embedding the secret data into the high frequency component of the image , compress the secret data using Huffman coding , which ensures the recovery of the data without any distortion. The results gives better PSNR value and improved system performance.

Elham Ghasemi et. Al [43] Proposed a GA based Discrete Wavelet Transform Steganography, which improves robustness and minimizes bit rate error. Optimal Pixel Adjustment Process is used after data embedding to achieve minimal bit error between the stego image and the cover image. The algorithm improves the hiding capacity and better PSNR ratio compared to the existing methods. [44] applied Discrete Wavelet Transform for data hiding and the secret image data is pre-processed by some mathematical operations.

[45] Discussed two different DWT techniques one is three level wavelet and another one is single level wavelet. The results of the methods improved the PSNR ratio is better than previous.[46] Described a method using DWT and IWT various combinations with the secret image and the cover image. Only one channel is used to hide the secret image either R, G, B so thereby maintaining the better imperceptibility.

[47] Uses a DWT difference based steganographic method, the four seed embedding pixel values are selected for each 8x8 block based on the 3X3 neighbourhood. For each seed block the difference between the DWT coefficients is calculated which decides the embedding rate for each block. The system is proved against steganalysis.[48] described DWT based data hiding where the cover image is decomposed into N levels. The secret data of the multiple images are hidden in the different R, G, B DWT coefficients of the cover image. The frequency values of some components

are combined for secret data embedding. [49] used 2D DWT Haar Transform. The secret data are embedded using 5LSB model. Inverse DWT is applied twice.

2.3 Spread Spectrum Steganography

Spread Spectrum Steganography [50] deals with either cover image as a noise or tries to add pseudo random noise to the cover image. It transmits the data for the given frequency below the noise level. The data is added as a noise so it is difficult to detect. It is more robust against statistical attacks. The resistance to the noise is high using spread spectrum and hence the data can be received correctly. Spread Spectrum spreads the bandwidth of narrow band frequency into a wide range of frequencies. After spreading if any one frequency band is low it is not easily detectable. It embeds the binary data in White Gaussian Noise. The noise is finally combined with cover image to get the stego image. The observer is not able to distinguish the cover image from the stego image.

[51] The system adds a single value message below the noise level of the cover image and treats the cover image as a noise. The value is the real number, so it is difficult to recover so it decreases the value ofsingle bits. The cover image is divided into sub images if more than one bit wants to transmit. There are different techniques exist, they are Direct Sequence Spread Spectrum, Frequency Hopping spread spectrum. [52] In Pseudo random Noise the secret data is spread over the cover image so it becomes difficult to detect. [53] combined Spread Spectrum with error control coding gives more robust system. Pseudo Random Number is added to the original secret data, since the data after adding the random number is a very less value which is not imperceptible to the human eye as well as by the computer system. [54] used block spread spectrum and duplicate spreading methods instead of spread spectrum technique. [55] authors proposed signature vector based spread spectrum and proved the algorithm provides more data hiding capacity with an increase Signal to Interference plus noise ratio.

Altuki [56] used the advantage of error control coding and combined the Discrete Fourier Transform to the Spread Spectrum increases the transform coefficients for secret data embedding. Widadi [57] et al. Proposed blind image steganography using direct sequence and frequency hopping spread spectrum techniques. The secret data are retrieved without using the original cover image. [58] used Spread Spectrum and Code Division Multiple access for spatial domain and transform domain. The experimental results show the spread spectrum is highly robust for signal manipulation.

[59] Proposed Audio steganography, where audio signals are embedded into the image. Integer wavelet transform is used to hide the secret data in Cb and Cr high frequency components of third and second bit planes. Shown better

psnr and squared pearson correlation coefficient values. Frequently used audio formats are WAV and AIFF. The various audio steganographic methods [60] are Low-Bit Encoding, Polarity Inversion, Echo Hiding, Phase Coding, Cepstral Hiding, Perceptual Masking

2.4 Statistical Steganography and Cover Generation technique

It is also called as model based techniques. It modifies the statistical characteristic of the cover to embed the data . The modification is very less and hence luminance variation is not detectable by the human eye [1]. [61] It checks for binary 1 in the cover file and the corresponding bit is used for data embedding . It makes significant changes in the statistical characteristic if 1 is transmitted. Considers the arbitrary property of the cover signal for data hiding [62].

This model based steganography [63] Preserves global DCT histogram. Steghide embeds data by swapping DCT coefficients and avoids changes in the histogram[64]. However statistical methods are simple , but it is more vulnerable to rotating, cropping, scaling and compressing image processing attacks .

In Cover Generation secret data is generated as a cover image, where the secret data are converted into various picture elements finally combined to create a cne cover image. This cover image is the stego image. This image is not affected by cropping, rotating and scaling. This techniques uses pseudo random images. It is predisposed by third parties because a group of messages is passing without any reason [1].

3. Steganography Performace Measure

The following are the metrics used for evaluating the steganographic system. These metrics provides some measures and statistical distribution of the pixel between two digital images, ie between the cover image and the stego image.

3.1 Mean Square Error (MSE)

It is defined as the square of the difference between pixel values of the cover image and the stego image divided by the size of the image. The following formula specified in the equation 3 gives MSE value between X and Y image of size MxN

$$\text{MSE} = \frac{1}{NxM}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}[X(i,j) - Y(i,j)]^2 \qquad (3)$$

3.2 Peak Signal to Noise Ratio (PSNR)

It is a well known and commonly used performance measure for finding the image distortion between the images. PSNR finds the quality of the stego image compared with stego image. The mathematical formula is given in equation 4 for calculating the PSNR value is as follows.

$$PSNR = 20\log_{10}\left(\frac{MAXf}{\sqrt{MSE}}\right) \quad (4)$$

Where MAX_f – Maximim pixel value , usually the value is 255

3.3 Structural Similarity Index Metric (SSIM)

It is used to measure similarity between the stego image and the original image. The following equation 5 is designed based on the three factors luminance distortion, contrast distortion and loss of correlation .

$$SSIM(x,y) = l(x,y)).c(x,y).s(s,y) \quad (5)$$

$$l(x,y) = \frac{2\mu x\mu y + C1}{\mu x^2\mu y^2 + C1}$$

$$c(x,y) = \frac{2\partial x\partial y + C2}{\partial x^2\partial y^2 + C2}$$

$$s(x,y) = \frac{2\partial xy + C3}{\partial x\partial y + C2}$$

Where

l(x,y) is lumincance comparision

c(x,y) is the contrast comparision

s(x,y) is the structure comparision

∂x, ∂y – Standard Deviation

∂xy – Covariance between x and y

C1, C2, C3 – positive constants

4. Evaluation of Different Techniques

There are several parameters to measure the steganographic algorithm. Depends on the purpose, it is important to decide the suitable algorithm. The below table summarizes the evaluation of different techniques based on the parameters of the survey. Spatial Domain Techniques hides large amount of data, but it is vulnerable to small changes. It is more affected by the compression and the image processing operations like cropping, rotating and scaling. Thus, it is low robust.

Transform Domain hides a significant amount of data through DCT and DWT techniques. It has not been likely to attack if the message size is small. Since data are embedded in the transform domain, the distortion made in the stego

image is very small. These techniques are less prone to statistical attacks. Spread Spectrum Techniques are spreading the secret message throughout the image and hence less prone to statistical attacks.

This type of steganographic applications is widely used in military communications since it is more robust against detection. It provides maximum data capacity and robustness so it is best suitable steganography for secret communication. Statistical techniques are more vulnerable to image processing attacks, and any attack which works against watermarking. The payload and imperceptibility depend on the selection of the cover image.

Table 2. Evaluation of Different Steganographic Algorithms.

Steganographic Method	Imperceptibility	Robustness	Data Capacity
Spatial Domain			
LSB	LOW	LOW	HIGH
PVD	HIGH	MEDIUM	HIGH
GLM	HIGH	MEDIUM	HIGH
OPAP	HIGH	MEDIUM	HIGH
Transform Domain			
DCT	HIGH	MEDIUM	MEDIUM
DWT	HIGH	HIGH	MEDIUM
Spread Spectrum			
	HIGH	MEDIUM	HIGH
Statistical Methods (Depends of cover image selction)			
	MEDIUM	LOW	LOW

5. Conclusion

Steganography provides covert communication for transmitting secret information. Each techniques are tries to improve the three important factors of the steganographic system imperceptibility ,robustness and capacity . The above discussed methods conclude a trade off between image quality and the capacity of the data to be embedded. If the capacity increases, it decreases the quality of the image and vice versa. OPAP and PVD can be used to provide more data capacity, but same time it is very robust. DCT and DWT techniques can be used to provide more robustness and imperceptibility with acceptable data capacity. Spatial domain techniques are less robust against lossy compression and frequency domain is best choice for the lossy compression technique. By looking at the table measures each and every methods has their own weakness and strengths. Depends on the purpose one can choose the most appropriate steganograhic method.

References

1. I. Cox, M. Miller, J. Bloom, J.Fridrich, and. Kalker. "Digital Watermarking and Steganography (Second Edition)", Morgan Kaufmann Publishers, 2007, ISBN: 978-0-12- 372585-1.

2. Rebecca T. Mercuri, The many colors of multimedia security. Communications of the ACM, , 2004, 47:25-29.
3. P. Wayner. Disappearing cryptography. Morgan Kaufmann Publishers, San Francisco, CA, USA, second edition, 2002. ISBN 1-55860-769-2.
4. R Rodriguez-Colin, F.-U. Claudia, and G. de J. Trinidad-BIas. Data hiding scheme for medical images. In 17th IEEE Inti. Conference on Electronics, Communications and Computers, February 2007 pages 33-38.
5. Y. Li, C. T. Li, and C. H. Wei. Protection of mammograms using blind staganography and watermarking. In 3rd Inti. Symposium on Information Assurance and Security, August 2007
6. Singh, Nanhay, Bhoopesh Singh Bhati, and R. S. Raw. "Digital image Steganalysis for computer forensic investigation." Computer Science and Information Technology (CSIT) (2012): 161-168.
7. A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems" 3rd International Workshop on Information Hiding ,vol. 1768 pp. 61--76, Oct. 1999
8. Hung-Min Sun, Yao-Hsin Chen, King-Hang Wang, An image data hiding scheme being perfectly imperceptible to histogram attacks, Image Vis. Comput.New Zealand IVCNZ 2006 (2006) 27–29.
9. Kazem Qazanfari, Reza Safabakhsh ,A new steganography method which preserves histogram:Generalization of LSB++, Information Sciences 277 (2014) 90–101
10. Wu,Tsai, "A steganographic method for images by pixel-value differencing" ,Volume 24, Issues 9-10, June 2003, pages 1613-1626
11. Han-ling ZHANG, Guang-zhi GENG, Cai-qiong Xing, 2009."Image Steganography using Pixel-Value Differencing", IEEE DOI 10.1109/ISECS.2009.139), 109–112.
12. C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, "Lossless Recovery of an Original Image Containing Embedded Data," U.S. Patent 6 278 791 B1, Aug. 21, 2001
13. Wien Hong ,Tung-ShouChen , Mei-ChenWua , An improved human visual system based reversible data hiding method using adaptive histogram modification ,Optics Communications 291 87–97 , 2013
14. Hong, Wien, Tung-Shou Chen, and Mei-Chen Wu. "An improved human visual system based reversible data hiding method using adaptive histogram modification", Optics Communications, 2013.
15. H.Y. Leung, L.M. Cheng, F. Liu, Q.K. Fu , Adaptive reversible data hiding based on block median preservation and modification of prediction errors , The Journal of Systems and Software 2204– 2219 , 2013.
16. T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc.ISSA, 2005, pp. 1-11.

17. Dr H.B Kekre, Ms Pallavi Halarnkar, Kahkashan Ansari, Parakh Jindal, Yash Chaturvedi," Information hiding with increased capacity using KMLA+PVD approach", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555 Vol. 2, No.2, April 2012.
18. Leung, H.Y., L.M. Cheng, F. Liu, and Q.K. Fu. "Adaptive reversible data hiding based on block median preservation and modification of prediction errors", Journal of Systems and Software, 2013.
19. A.L.Khade. B.G.Hogde, V B Gaikwad. "Secret Communication via Image Hiding In Image by Pixel Value Differencing", ICWET?, February 2010, 437-438.
20. Xinpeng Zhang , Shuozhong Wang ,Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security, Pattern Recognition Letters 25 (2004) 331–339
21. Wen-Jan Chen,Chin-Chen Chang , T. Hoang Ngan Le, High payload steganography mechanism using hybrid edge detector , Expert Systems with Applications 37 (2010) 3292–3301
22. Wien Hong ,Tung-ShouChen , Mei-ChenWua , An improved human visual system based reversible data hiding method using adaptive histogram modification ,Optics Communications 291 87–97 , 2013
23. Hong, Wien, Tung-Shou Chen, and Mei-Chen Wu. "An improved human visual system based reversible data hiding method using adaptive histogram modification", Optics Communications, 2013.
24. Yifeng Sun, Fenlin Liu Zhengzhou, Selecting Cover for Image Steganography by Correlation Coefficient ,Second International Workshop on Education Technology and Computer Science, 2010
25. Yinan Wang, Weirong Chen, Yue Li, Wei Wang,and ChangTsun Li, HPS: Histogram Preserving Steganography in spatial domain, 978-1-4799-4370-8/14 2014 IEEE
26. Potdar V.and Chang E. Gray level modification steganography for secret communication. In IEEE International Conference on Industria Informatics., pages 355–368, Berlin, Germany, 2004.
27. Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching." IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February 2012, 176-184.
28. X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," IEEE Communications Letters, Vol. 10, No. 11, pp. 781-783, 2006.
29. Ruey-Ming Chao, Hsien-Chu Wu, Chih-Chiang Lee and Yen-Ping Chu , A Novel Image Data Hiding Scheme with Diamond Encoding , EURASIP Journal on Information Security 2009.

30. N. F. Johnson, S. Katzenbeisser. "A Survey of steganographic techniques." in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43-78.
31. https://en.wikipedia.org/wiki/Discrete_cosine_transform
32. G. Langelaar, I. Setyawan, R.L. Lagendijk, (2000) "Watermarking Digital Image and Video Data", in IEEE Signal Processing Magazine, Vol 17, pp 20-43.
33. A. Westfeld. "F5-A steganographic algorithm: high capacity despite better steganalysis." In Proc. of the 4th Information Hiding Workshop, LNCS, 2001, pp. 289-302.
34. Wen-Yuan Chen , Color image steganography scheme using DFT, SPIHT codec, and modified differential phase-shift keying techniques , Applied Mathematics and Computation 196 (2008) 40–54
35. Hideki Noda , Michiharu Niimi , Eiji Kawaguchi , High-performance JPEG steganography using quantization index modulation in DCT domain , Pattern Recognition Letters 27 (2006) 455–461
36. Hossein Sheisi, Jafar Mesgarian, and Mostafa Rahmani , Steganography: Dct Coefficient Replacement Method and Compare With JSteg Algorithm , International Journal of Computer and Electrical Engineering, Vol. 4, No. 4, August 2012
37. Chin-Chen Chang , Chia-Chen Lin , Chun-Sen Tseng , Wei-Liang Tai , Reversible hiding in DCT-based compressed images , Information Sciences 177 (2007) 2768–2786
38. KokSheik Wonga, Xiaojun Qi, Kiyoshi Tanaka , A DCT-based Mod4 steganographic method , Signal Processing 87 (2007) 1251–1263
39. S. Uma Maheswari, D. Jude Hemanth , Frequency domain QR code based image steganography usingFresnelet transform International Journal of Electronics and Communications (AEU), Int. J. Electron. Commun. (AEU) 69 (2015) 539–544
40. https://en.wikipedia.org/wiki/Discrete_wavelet_transform
41. H.S. Majunatha Reddy and K.B. Raja, "High capacity and security steganography using discrete wavelet transform." International Journal of Computer Science and Security. 2009, pp. 462-472.
42. Yung-Kuan Chan , Wen-Tang Chen , Shyr-Shen Yu , Yu-An Ho , Chwei-Shyong Tsai , Yen-Ping Chu , A HDWT-based reversible data hiding method , The Journal of Systems and Software 82 (2009) 411–421

43. Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi ,High Capacity Image Steganography Using Wavelet Transform and Genetic Algorithm Proceedings of international multiconference of Engineers and Computer Scientists , March 2011
44. Po-Yueh Chen and Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering 2006.
45. Narasimmalou, T.; Joseph, R.A., Discrete Wavelet Transform Based Steganography for Transmitting Images , IEEE-International Conference On Advances In Engineering, Science And Management , March 2012
46. Prabakaran G, Dr. Bhavani R , Sankaran S , Dual Wavelet Transform in Color Image Steganography Method, International Conference on Electronics and Communication System (ICECS -2014)
47. Souvik Bhattacharyya , Gautam Sanyal , A Robust Image Steganography using DWT Difference Modulation (DWTDM) , I.J. Computer Network and Information Security, 2012
48. Della Babya, Jitha Thomasa, Gisny Augustinea, Elsa Georgea, Neenu Rosia Michaela , A Novel DWT based Image Securing Method using Steganography , International Conference on Information and Communication Technologies , 2014
49. Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal ,Implementation of Imsage Steganography Using 2-Level DWT Technique , International Journal of Computer Science and Business Informatics , ISSN: 1694-2108 | Vol. 1, No. 1. MAY 2013
50. M. Marvel, Charles G. Boncelet, Jr.,and Charles T. Retter, Methodology of Spread-Spectrum Image SteganographyLisa Army Research Laboratory 1998
51. P. Kruus, C. Scace, M. Heyman, and M. Mundy. (2003), "A survey of steganography techniques for image files." Advanced Security Research Journal. [On line], 5(1), pp. 41-52. , 2003 Available: http://www.isso.sparta.com/documents/asrjv5.pdf#page=47
52. H. Wang and S. Wang. (2004, Oct.). "Cyber Warfare: steganography vs. steganalysis , Communications of the ACM. [On line]. 47(10), pp. 76-82.Available: www.csc.liv.ac.uk/~leszek/COMP526/week4/comp526-3.pdf Mar, 2011
53. L.M. Marvel, C.G. Boncelet Jr., C.T. Retter. (1999). "Spread spectrum image steganography." IEEE Trans. image processing. [On line]. 8(8), pp. 1075-1083. Available: http://www.mendeley.com/research/spread-spectrum-image-steganography-1/ [Apr., 2011].

54. C.L. Tsai, K.C. Fan, and C.D. Chung. "Secure information by using digital data embedding and spread spectrum techniques." IEEE 35th International Carnahan Conference on Security Technology, 2001. pp. 156-162.
55. K.C. Widadi, P.H. C.C. Wah. "Blind steganography using direct sequence/frequency hopping spread spectrum technique. in : Information, Communications and Signal Processing, 5th International Conference, 2006. pp. 1125-1129.
56. M. Gkizeli, D.A., and M.J. Medley. (2007, Feb.). "Optimal signature design for spreadspectrum steganography." IEEE Signal Processing Society. [On line]. 16(2), pp. 391-405.
57. F. Alturki and R. Merserau. "Secure blind image steganographic technique using Discrete Fourier Transform." in Proc. IEEE International Conference on Image Processing, 2001. pp.16-162.
58. R.S. Singh, M.A. Khani, and N. Singh. (2010, Dec.). "Spread spectrum image steganography in multimedia messaging service of mobile phones." International Journal of Electronics Engineering. [On line]. 2(2), pp. 365 – 369. Available: http://www.csjournals.com/IJEE/PDF%202-2/Article_29.pdf [Oct., 2011].
59. Hemalatha S, U. Dinesh Acharya, Renuka A, Wavelet transform based steganography technique to hide audio signals in image. Elsevier Procedia Computer Science 47 (2015) 272 – 281
60. Fatiha Djebbar , Beghdad Ayad , Karim Abed Meraim, Habib Hamam ,Comparative study of digital audio steganography techniques , EURASIP Journal on Audio, Speech, and Music Processing, December 2012,
61. R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. "Data masking: a secure-covert channel paradigm." in IEEE Workshop on Multimedia Signal Processing, 2002. pp. 339-342.
62. P. Moulin and Y. Wang. Statistical modeling and steganalysis of DFT-based image steganography. In E.J. Delp and P.W. Wong, editors, Proceedings of SPIE Electronic Imaging, Security, Steganography,and Watermarking of Multimedia Contents VIII,volume 6072, pages 607202–1–607202–11, 2006.
63. H. Noda, M. Niimi, and E. Kawaguchi. Application of QIM with dead zone for histogram preserving JPEG steganography. In Proceedings ICIP, Genova, Italy, September 2005.

Corresponding Author:
Vanmathi C*,
Email: vanmathi.c@vit.ac.in