Appraise Of Multifarious Image Steganography Techniques

Dr. Sudeep Thepade*, Smita S. Chavan**

*(Dean (R & D) & Professor, Pimpri Chinchwad College of Engineering, University of Pune, Pune)
** (Assistant Professor, Department of Computer Engineering, Dr. D.Y.Patil School of Engg. Academy, University of Pune)

ABSTRACT

This paper presents a review of multifarious methods available for image steganography. The steganography is an art and science of invisible communication. The image steganography is divided into four basic terminologies viz. cover image, message, stego image, embedding and extracting algorithm. In this paper comparison of steganography with other security techniques is done. Image steganography technique is widely used technique to secure information utilized for covert communication, featured tagging, copyright protection, military agencies and for many more applications related to secure communications. Image steganography is divided into two domains, spatial and transform. For Spatial domain techniques like Least significant bit replacement and PVD based methods , the embedding capacity is more but sustainability against attacks on stego image is very less, so this technology need more attention to overcome the disadvantage of existing algorithms. The current research is going on transform domain techniques which provide good robustness against attacks. Here, comparative analysis of various image steganography methods is done considering various performance evaluation parameters like invisibility, payload capacity, robustness against attacks etc.

Keywords - LSB, PVD, DCT, Walsh transform, Steganography.

I. INTRODUCTION

A wide variety of systems require invisible communication to hide existence of the secret message for secure exchange of information. Internet is the most used and fastest medium for communication but it faces many security related problems like hacking, copyright, eavesdropping etc. Cryptography is the technique which was created to secure the secrecy of communication. There are many different methods to encrypt & decrypt data in order to keep the message secret. Unfortunately, it is not enough to keep the content of a message secret, it is also important to keep the existence of message secret. The technique in which the existence of hidden message is kept secret is called as Steganography.

Steganography is the art and knowledge of unseen communication. The word Steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing”. This can be achieved by hiding information in other information visually plausible and thus the existence of communicated information is kept hidden.

Steganography is mainly classified into four categories that are Text, audio/video, Image and Protocol. The categorization of steganography is shown in figure 1.

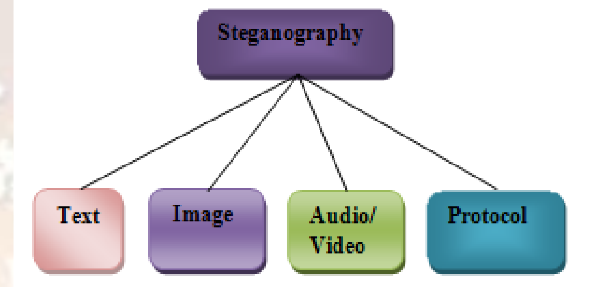


Fig.1: Categorization of Steganography

In text, audio/video, Image steganography message is kept hidden in text, image, audio/video formats, where the term protocol steganography refers to the technique of embedding information within messages and network control protocols used in network transmission. In the OSI network model there exist covert channels where Steganography can be used. In image steganography, the secret message is hidden in digital images with various hiding methods. In Histories the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was dispatched with the hidden message [1].

First section of the paper includes the introduction, need, categories and various applications of Image Steganography. Further sections include various similarity measurement criteria used for performance evaluation of image steganography methods. End part consists of comparative analysis of various Image steganography methods from spatial and frequency domain followed with conclusion.

II. LITERATURE SURVEY

The steganography is an emerging research area where it encompasses various applications, in [6, 10], authors have been proposed a data hiding scheme with simple LSB substitution. By applying optimal pixel adjustment process to the stego –image which is obtained by the simple LSB substitution method, the image quality greatly improved with low extra computational complexity. In [11], a novel data hiding method based on the least significant bit substitution and multi pixel differencing method is presented on the proposed to improve the capacity of hidden secret data and to provide imperceptible visual quality. In [12], the steganographic method proposed by Chang and Tseng is reviewed and the problem related to the Chang-Tseng scheme is described. A modified scheme is proposed to overcome the problem in which the embedded data cannot be extracted correctly. That is in order to enhance the image quality of stego image and enlarge the embedding capacity of the host image, a novel method to embed secret data into the host image by adaptive LSB substitution based on the pixel value differencing is proposed. In [13], authors has expand the LSB matching revisited image Steganography and proposed an edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image. Authors also discussed about, for lower embedding rates only sharper edge regions are used while keeping the other smoother regions as they are. When the embedding rate increases, more edge regions can be released adaptively for data hiding by adjusting just a few parameters.

Cheng-Hsing Yang has proposed a new LSB based method, called the Inverted Pattern (IP) LSB substitution approach is proposed to improve the quality of stego- image .Each section of secret images is determined to be inverted or not inverted before it is embedded. These decisions are recorded by IP for the purpose of extracting data and the pattern can be seen as a secret key or an extra data to be re-embedded [14]. Where, in [2], authors have proposed a technique which is a combination of PVD modulus and LSB method. By showing the experimental results it is concluded that hiding capacity increases enormously. In [26], author has used last two bits of pixel for insertion and retrieval of message. This method is an improvement over earlier methods like Least Significant Bit (LSB) method, 6th and 7th bit method and 6th, 7th and 8th bit method. In [27] paper, presents a comparison between the basic LSB technique which involves replacement of least significant bits in order to hide the colored message image behind the colored cover image, with the other technique for increased capacity of hiding information using an advanced LSB methodology wherein the bit replacement takes place in accordance to range specified for the color images. There have been many techniques for hiding messages in images in such a manner that the alterations made to the images are perpetually indiscernible. This paper proves experimentally that the technique for increased capacity of information hiding in LSB‘s method gives better performance in all the parameters and is a safe technique for embedding secret messages [25].

Generally DCT based image Steganography hides the text messages in least significant bits of the Discrete Cosine (DC) coefficient of the image. For JPEG or video compression, DCT is a part of compression. In [4], paper authors has presented an image based Steganography that combines LSB, Discrete Cosine Transform (DCT) and Compression techniques on raw images to enhance the security of the payload. Initially, the LSB algorithm is used to embed the payload bits into the cover image to derive the stego –image. The stego image is transformed from spatial domain to the frequency domain using DCT. Finally Quantization and run-length coding algorithms are used for compressing the stego image to enhance its security. In [15], paper a new steganographic system is introduced for message embedding by inverting the LSB of DCT coefficients of JPEG image. This algorithm offers high capacity compared to existing steganographic system. In [16,17,18] paper, block based Steganography algorithm with minimum MSE is presented, an algorithm that embed data in the least significant bit (LSB) of the discrete cosine transform (DCT) coefficients of JPEG image blocks. Block Based Steganography (BBS) algorithm offers high capacity with statistically minimal changes compared to current steganographic algorithms. The wavelet transform is a transformation to basis functions that are localized in frequency. The wavelet compression methods are better at representing transients such as image of stars on a night sky. In [19, 20], a method is proposed that uses Discrete Walsh transform. DWT is applied to cover image to obtain the Walsh coefficients. Similarly DWT is applied to each of the message images as well to obtain their Walsh coefficients.

The cover image coefficients are divided into 4 quadrants 1st quadrant – Left Top, 2nd right Top, 3rd left bottom and 4th right bottom. In [21], Information hiding is done in frequency domain using the DCT and Walsh transform. The DCT and Walsh transform are applied to cover image, which results in DCT and Walsh coefficients and then used for secret message embedding. A threshold is used for carrying out the secret message Embedding. From the experimental results the embedding capacity which is based on the number of coefficients obtained for a threshold value is more for DCT transform as compared to Walsh Transform.

In [23] paper, authors have proposed hybrid Steganography (HDLS) which is an integration of both spatial and transform domains. The cover image as well as the payload is divided into two cells each. The RGB components of cover image cell I are separated and then transformed individually from spatial to transform domain using DCT/DWT/FFT and embedded in a special manner, the components of cell II retained in spatial domain itself.

III. APPLICATIONS

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography. All these applications of information hiding are quite diverse. Steganography is well known and widely used technique to secure information utilized for:

Copy right Protection: A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property. This is the watermarking scenario where the message is the watermark. The “watermark” can be a relatively complicated structure. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified. Detection of an embedded watermark is performed by a statistical, correlation, or similarity test, or by measuring other quantity characteristic to the watermark in a stego-image. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent surge of interest in digital Steganography and data embedding.

Covert Communication is possible by the use of Steganography. Therefore the inspection of the sender, message and recipients can be avoided.

A secret copyright notice or watermark can be embedded inside an image to identify it as intellectual property. Featured tagging: Captions, annotations, time stamps and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or location in the map.

Secret Communication: In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use Steganography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers or eavesdroppers [28].

There are many more applications of steganography like Authentication, Bank transactions, Credit cards codes, Multimedia content copyrights, Companies’ safe circulation of secret data, TV broadcasting ,Enhancing robustness of image search engines and smart IDs where individual’s details are embedded in their photographs.

Due to property of obsceneness in Steganography, it is more effective for Military and intelligence agencies, because they required unobtrusive communication mode.

There are some contemporary applications, one of which was in Medical Imaging Systems where a separation is considered necessary for confidentiality between patients’ image data or DNA sequences and their captions, e.g., physician, patient’s name, address and other particulars. A link however, must be maintained between the two. Thus, embedding the patient’s information in the image could be a useful safety measure and it helps in solving such problems [8, 9].

IV. METHODS OF IMAGE STEGANOGRAPHY

Image steganography methods can be mainly classified into Spatial Domain and Frequency Domain Techniques as shown in the Fig 2. Spatial domain methods can be sub classified in LSB methods which are of variable or fixed type. Further frequency domain methods can be sub classified into orthogonal transform based like DCT, Walsh etc and wavelet transform based methods such as DCT wavelet, Walsh wavelet, kekre’s wavelet etc.

1. Spatial Domain techniques

Spatial domain techniques are also known as Image domain techniques. Spatial technique embeds messages in the intensity of the original image pixels directly. Spatial domain techniques include bit-wise methods that apply bit insertion & noise manipulation. A simple and well known approach is directly hiding secret data into the least significant bit (LSB) of each pixel in an image. LSB can be of variable bit or fixed bit.

2. Frequency Domain Techniques

Frequency domain is also known as transform domain. In this method, images are first transformed then the message is embedded in the image. The simple orthogonal transforms like DCT, Walsh etc are used for image steganography. Discrete cosine transformation (DCT) technique is used for image steganography in transform domain due to its energy compaction property. DCT is a lossy compression transform where the cosine values cannot be generated as original, because DCT alter values (example 8.667 to 9) to hide the information.

DCT domain embedding is the most popular one, mostly because of the fact that DCT based image format are widely available in public domain as well as the common output format of digital cameras. Embedding in DCT domain is simply done by altering the DCT coefficients. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components.

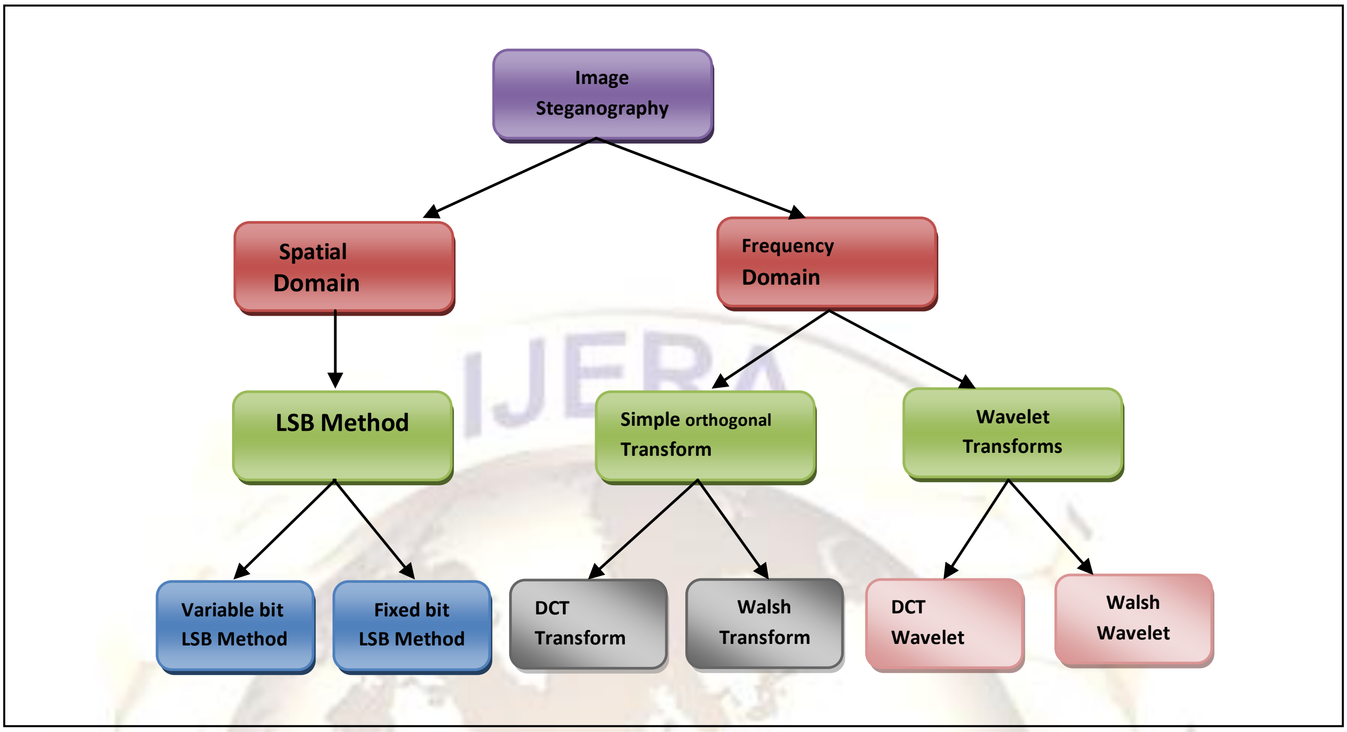


Fig. 2: Image Steganography methods

The general equation for a 2D (N by M image) DCT is defined by the following equation:

$$C(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

….. (1)

for u, v = 0, 1, 2, . . . , N-1. Here, the input image is of size N X M. c (i, j) is the intensity of the pixel in row i and column j; C(u, v) is the DCT coefficient in row u and column v of the DCT matrix. Signal energy lies at low frequency in image; it appears in the upper left corner of the DCT.

V. IMAGE STEGANOGRAPHY SYSTEM

Image Steganography is nothing but hiding information exclusively in images. Image Steganography has the following terminology.

Cover-Image: It refers to the image used as a carrier to embed message into.

Message: It can be plain text or image as a message.

Stego- Image: refers to the generated image which is carrying a hidden message.

In Image Steganography a process embeds the message into cover image and generates a stego image. That stego image is then sent to the receiver without anyone else knowing that it contains the hidden message. The receiver can then extract the message with or without stego key depends on the hiding scheme. Basic diagram of Image Steganography is shown in Figure 3.

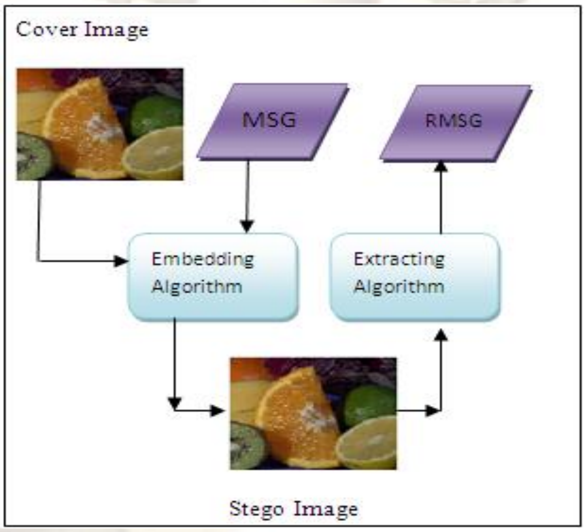


Fig.3: Basic diagram of Image steganography

VI. ATTACKS ON STEGANOGRAPHY

Attacks on Images can be possible in Image Steganography like Image Manipulation attacks, Statistical attacks, visual attacks etc. The well known attacks on Stego images are compression attack, cropping of stego, resizing the stego, noise addition for example salt and pepper noise addition, brightness attack can be possible in Steganography.

Attacks are mainly categorized in six types. They are:

(i) Stego-only attack: only the stego-image is available for analysis.
(ii) Known cover attack: the original cover-image and stego- image are both available.
(iii) Known message attack: at some point, the hidden message becomes known to the attacker. Analyzing the stego-image for patterns that correspond to the hidden message may be beneficial for future attacks against that system. Even with the message, this may be very difficult and may even be considered equivalent to the stego-only attack.
(iv) *Chosen stego attack:* the steganography tool (algorithm) and stego-image are known.
(v) *Chosen message attack:* the stego analyst generates a stego image from some steganography tool or algorithm from a chosen message. This goal in this attack is to determine corresponding patterns in the stego-image that may point to the use of specific steganography tool or algorithms.
(vi) *Known stego attack:* the steganography algorithm is known and both the original and stego-image are available [7].

VII. Performance Evaluation Measures for Image Steganography Methods

The quality of steganographic technique can be evaluated with the help of evaluation parameters like Mean Square Error, Peak to signal noise ratio, capacity, bit error rate etc.

A. Mean Square Error (MSE):

It is defined as the square of error between cover image and stego image. The distortion in the image can be measured using MSE and is calculated using equation no.(2).

$$MSE = \left[\frac{1}{N*N}\right]^2 \sum_{i=1}^{N}\sum_{j=1}^{N}(X_{ij} - \bar{X}_{ij})^2$$

…... (2)

Where:

X_{ij} : The value of the pixel in the cover image.

$\bar{X}_{ij}$: The value of the pixel in the stego image.

N : Size of Image.

Lower Mean square error is preferable, as it considered that lower the MSE better performance of steganography technique.

B. Peak Signal to Noise Ratio (PSNR):

It is the measure of quality of the image by comparing the cover image with the stego image, i.e. it measures the percentage of the stego data to the image percentage. PSNR is calculated using equation (3)

$$PSNR = 10\log_{10}\frac{255^2}{MSE}db$$

.

............(3)

Higher the peak signals to noise ratio, better the performance of steganography technique.

C. Capacity:

It is the size of the data in a cover image that can be modified without deteriorating the integrity of the cover image. The steganographic embedding operation needs to preserve the statistical properties of the cover image in addition to its perceptual quality. Capacity is represented by bits per pixel (bpp). Maximum embedding capacity is considered.

D. Bit error rate (BER):

Here we compute the BER for two equal size images that is cover image and stego-image. BER is more accurate for error analysis when compared to MSE, because in BER we compute the actual number of bit positions which are replaced in the stego image. Lower bit error rate is preferable.

E. Entropy:

Entropy is a measure of security for steganographic system which is computed as follows. Let el, e2,... em be m possible elements with probabilities P(el), P(e2), ... P(em); the entropy is given by,

$$H(e) = -\sum_{i=0}^{m-1} P(e_i)\log_2 P(e_i)$$

….. (4)

The above equation provides an estimate of the average minimum number of bits required to encode a string of bits based on the frequency of the symbol [4, 5].

VIII. Comparison of Methodologies Discussed

In this section comparison of various methodologies of Image Steganography is done based on various criteria like invisibility, payload capacity, robustness against attacks, files are unsuspicious or not , imperceptibility criteria’s etc.[1],similarity measurement done using cover image, and stego images, retrieved image with hidden message. In the first methodology a PVD modulus image steganography technique is discussed [02]. Here authors have proposed a method which is combination of PVD modulus and LSB method. This combination is having high embedding capacity as compared to other techniques like LSB etc. here the method uses LSB method for smooth areas and PVD modulus method for edge area pixel pairs. A threshold is defined to determine whether a pixel pair falls in smooth area or edge area. Though this method embeds more data into cover image it is not that much robust against attacks.

In the second methodology the inverted pattern approach is used to improve image quality of information hiding by LSB substitution [03]. Here, a new LSB-based method, called the inverted pattern (IP) LSB substitution approach, is proposed to improve the quality of the stego-image. Each section of secret images is determined to be inverted or not inverted before it is embedded. The decisions are recorded by an IP for the purpose of extracting data and the pattern can be seen as a secret key or an extra data to be re-embedded. This method has high embedding capacity; it retains the high quality of the image, and embeds secret messages into the cover image needing only a short computation time. So, this method is simple and efficient with better image quality than LSB substitution In the third method a secure image steganography using LSB, DCT and compression technique is done on raw images [4]. The combination of this methods is used to enhance the security of the payload are presented. Initially, the LSB algorithm is used to embed the payload bits into the cover image to derive the stego-image. The stego-image is transformed from spatial domain to the frequency domain using DCT. Finally quantization and run-length coding algorithms are used for compressing the stego-image to enhance its security. It is observed that secure images with low MSE and BER are transferred without using any password, in comparison with earlier works.

In the fourth method [22, 29], author's are comparing the results of steganography using simple orthogonal transforms (Walsh and DCT) with steganography using wavelet (Walsh wavelet and DCT Wavelet) on the basis of their hiding capacity, imperceptibility and robustness against various attacks. The wavelet transform is applied on full cover image and the secret information is embedded into lower energy blocks of the transformed cover image. Before embedding, the system applies pre-processing step on the secret information. Secret information is first normalized and then embedded in to the cover. This will reduce the embedding error. In a normalized version, the pixel components take on values that span a range between 0.0 and 1.0 instead of integer ranges of [0-255].

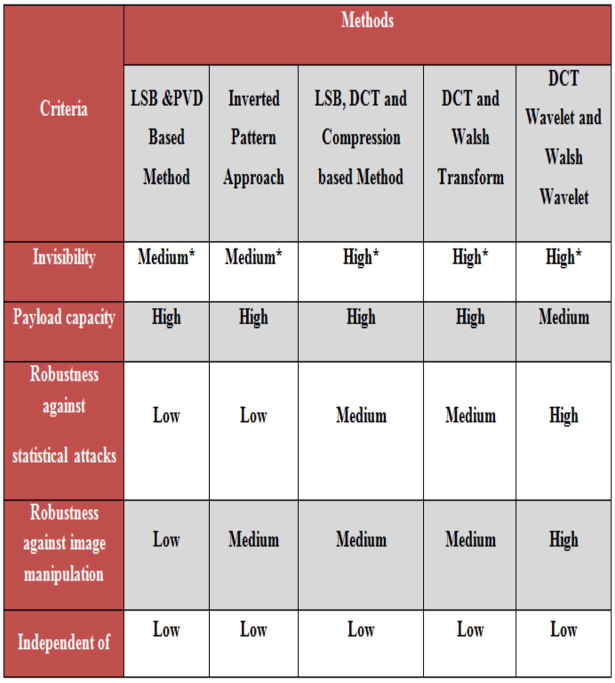
The table no.1 shows the comparison of various methods based on imperceptibility criteria's.

VII. CONCLUSION

The combination of LSB and PVD modulus method produces images with acceptable quality and embeds more data into the cover image than the PVD modulus method. In second paper, a new LSB based approach called the IP LSB substitution approach, requires short computing time and achieves result of high capacity and high quality. In third paper, the combination of LSB algorithms, DCT transformation and compression using quantization and run-length coding on raw images have been used to obtain secure stego images. This approach enables secure transfer of payload with low BER and MSE. This method is more robust against attacks such as compression, cropping etc as compared to spatial domain techniques.

In fourth paper, Comparison of DCT and Walsh transform with DCT Wavelet and Walsh Wavelet is done for image steganography. From comparison it is concluded that steganography using DCT and Walsh achieve good embedding capacity but provide poor robustness to attacks such as changing brightness of stego image, cropping the stego, and adding noise to stego, and Steganography using DCT wavelet and Walsh wavelet achieves slightly lesser embedding capacity than DCT and Walsh transform but provide excellent robustness against attacks.

Table No.1. Comparison of image steganography techniques.



Criteria	Methods				
	LSB &PVD Based Method	Inverted Pattern Approach	LSB, DCT and Compression based Method	DCT and Walsh Transform	DCT Wavelet and Walsh Wavelet
Invisibility	Medium*	Medium*	High*	High*	High*
Payload capacity	High	High	High	High	Medium
Robustness against statistical attacks	Low	Low	Medium	Medium	High
Robustness against image manipulation	Low	Medium	Medium	Medium	High
Independent of	Low	Low	Low	Low	Low

*Depends on cover image used

REFERENCES

[1] T. Morkel, J.H.P.Eloff, M.S.Oliver, "An Overview of Image Steganography", Published in *Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa*, 2005.

[2] M. Gadiparthi, K.Sagar, D.Sahukari, R.Chowdary, "A High Capacity Steganographic Technique based on LSB and PVD Modulus Methods*", International Journal of Computer Applications ISSN: 0975-8887*, Volume 22- No.5, May 2011.

[3] C.H. Yang, "Inverted Pattern Approach to improve image quality of information hiding by LSB Substitution", Pattern Recognition 41, 2008, pp. 2674-2683.

[4] K. B. Raja, C. R. Chowdary, K.R Venugopal and L.M. Patnaik , "A Secure Image Steganography Using LSB, DCT and Compression Techniques on Raw Images", *Proceedings of IEEE 3rd International Conference on Intelligent Sensing and Information Processing, ICISIP'05,Bangalore,India, Dec*. 2005, pp.170-176.

[5] Wang. C-M. et al. , "A High Quality Steganography Method with Pixel-Value Differencing and Modulus Function", J. Syst. Software (2007), doi:10.1016/j.jss.2007.01.049

[6] Chi-Kwong Chan, L.M. Cheng, "Hiding Data in Images by Simple LSB Substitution", Pattern Recognition 37, 2004, pp. 469-474.

[7] Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis based on Digital Image*", 4th IEEE International Congress on Image and Signal Processing,2011*, doi: 978-1-4222-9306-7/11.

[8] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and analysis of current methods", Signal Processing 90(3), 2010, pp.727- 752.

[9] Sara Natanj, Seyed Reza Taghizadeh, "Current Steganography Approaches: A survey", *International Journal of Advanced Research in Computer Science and Software Engineering, Volume 1,Issue-1,December*-2011,ISSN:2277 128X.

[10] Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern recognition 37, 2004, pp.469-474.

[11] Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo, "Image Data Hiding Method based on Multi-pixel Differencing and LSB Substitution Methods" , *International conference convergence and Hybrid Information Technology*, 2008.

[12] Suk-Ling Li, Kai-Chi Leung L.M Cheng, "Data hiding in Images by Adaptive LSB Substitution Based on the pixel value Differencing", in the *Proceedings of the First IEEE International Conference on Innovative Computing, Information and Control(ICICIC'06),* 2006,doi: 0-7695-2616-0/06.

[13] S.T.V.S Kumar, S.S. Panda, "A new approach to Image Steganography", published in: *International Journal of Electronics and Computer Engineering, Volume 3, Issue -1 NCRTCST,* ISSN 2249-071X.

[14] Cheng-Hsing Yang, "Inverted Pattern approach to improve image quality of information hiding by LSB Substitution", Published in *The Journal of Pattern Recognition Society, Pattern Recognition* 41,2008, pp. 2674-2683.

[15] M. Gadiparthi, K.Sagar, D. Sahukari, "A high Capacity Steganographic Technique based on LSB and PVD Modulus Methods", *International Journal of Computer Applications,ISSN:0975- 8887, Volume 22-No.5*, May2011.

[16] Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, Fathy Z. Amer, "JPEG Steganography System with Minimal Changes to the Quantized DCT Coefficients", *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6*, January 2012.

[17] Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, and Fathy Z. Amer, "Utilizing Image Block Properties to Embed Data in the DCT Coefficients with Minimum MSE", *International Journal of Computer and Electrical Engineering*, Vol. 3, No. 3, June 2011.

[18] Dr. H. B. Kekre, Dr. Tanuja K. Sarode, Sudeep Thepade, "Inception of Hybrid Wavelet Transform using two Orthogonal Transforms and its use for image Compression", *International journal of computer science and information Security (IJCSIS),Volume no. 9, Issue -6*, ISSN 1947-5500, 2011, pp.80-87.

[19] Dr. H. B. Kekre, Dr. Tanuja K. Sarode, Sudeep Thepade, Sonal Shroff, "Instigation of Orthogonal Wavelet Transforms using Walsh, Cosine, Hartley, Kekre Transforms and their use in Image Compression", *International journal of computer science and information*

Security (IJCSIS),Volume no. 9, Issue -6, ISSN 1947-5500, 2011,pp.125-133.

[20] Dr. H. B. Kekre, A.A Athawale, U. A. Athawale, "Increased capacity for information hiding using Walsh transform" *International Conference and Workshop on Emerging Trends in Technology (ICWET 2010) – TCET, ISBN: 978-1-60558-812-4* doi :10.1145/1741906.1741923 ,pp. 96-101.

[21] Dr. H. B Kekre, A Athawale, P.N Halarnkar, V.K Banura, " Performance comparison of DCT and Walsh Transform for Steganography", *International Conference and Workshop on Emerging Trends in Technology (ICWET 2010) – TCET*, ISBN: 978-1-60558-812-4, doi>10.1145/1741906.1741921, pp. 81-88.

[22] Dr. H. B. Kekre, Archana B.Patankar, Dipali Koshti, " Performance comparison of Simple Orthogonal Transforms and Wavelet Transforms for Image Steganography", *International Journal of Computer Applications(0975-8887), Volume 44- No.6*, April 2012

[23] K .B Raja, K. B. Shivakumar, K.B Raja, "Hybrid domain in LSB Steganography" *International Journal of Computer Applications (0975 – 8887), Volume 19– No.7*, April 2011

[24] M.M Kazi, Najran N.H. Al_Dawala, K.V.Kale, "Steganography Enhancement by combining text and image through Wavelet Technique" *International Journal of Computer Applications (0975 – 8887), Volume 51– No.21*, August 2012

[25] Yambem Jina Chanu, Themrichon Tuithung, " Image Steganography and Steganalysis: A Survey" *International Journal of Computer Applications (0975 – 8887), Volume 52– No.2*, August 2012

[26] Rajkumar Yadav, Ravi Saini ,Gaurav Chawla, "A Novel Approach For Image Steganography In Spatial Do-Main Using Last Two Bits of Pixel Value" *International Journal of Security (IJS), Volume (5) :* Issue (2) : 2011

[27] H.B.Kekre, Dhirendra Mishra, Rhea Khanna, Sakshi Khanna & Aadil Hussaini, "Comparison between the basic LSB Replacement Technique and Increased Capacity of Information Hiding in LSB's Method for Images", *International Journal of Computer Applications (0975 – 8887), Volume 45– No.1*, May 2012

[28] Dr. H. B. Kekre, Archana Athawale, Dipali Sadavarti , "Algorithm to Generate Kekre's Wavelet Transform from Kekre's Transform" Dr. H.B. Kekre et al. / *International Journal of Engineering Science and Technology Vol. 2(5)*, 2010, pp. 756-767.

[29] Dr. H.B. Kekre, Ms. Archana Athawale and Ms. Dipali Sadavarti, "Algorithm to Generate Wavelet Transform from an Orthogonal Transform", *International Journal of Image Processing (IJIP), Volume (4): Issue (4)* 444, 2009.