Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 3, March-2017

A Study of Various Image Steganography Technology.

1. Makwana Varsha p 2.Prof.Dr. Kalpesh Wandra

PG student, Computer Engineering, C.u.shah collage of engineering & technology, Gujarat,
Dean, Faculty of Tech. & Eng. C.U. Shah University, Gujarat, India

ABSTRACT

The evolving internet technology has led to the necessity of high level of information security throughout transformation. For this determination cryptography and steganography is used. It allows the security of information but it different to each other in working manner. The cryptography it provide security using the encryption-decryption of information it means it change the information in way that not identify by third person. Steganography is basically the art of secretly hiding data or message in any cover object. Confidential information has always been a major issue from past times to the present time.it has always been inserted topic for researcher to develop secure method to send data without reveling it to any other receiver. In this paper we provide a brief overview on steganography and its method used for hiding data in cover image to obtain stego object.

Keyword: Steganography; Image, Audio, Video, Cover Media LSB; Cover Writing; Frequency Domain, Spatial Domain.

1. INTRODUCTION

In our daily life almost all the method of communication become digital and for transferring and sharing information we mainly depend on the internet. So data transmission are became important and necessity now days. Today the people it is use the internet and telephonically to transfer and sharing the information. Whether you transfer your business secrets with your employees, your private message with your relative or close friend, your personal detail like bank details, personal documents on internet so everybody wants to keep this information secure and safe form unapproved person .But we live in an not secure world where the unwanted person can access the personal information (like personal document or email) and use this details for their benefit. So for prevention of this confidential data form hackers we required high security protection from unauthorized access.

There are various methods for information security was introduced from time to time and had undergone variations based on the need of it to user. This method involve to converting the secret information into nod readable from (caser cipher) using the different algorithm and operation, code making and breaking is also use to protect information ,or replacing of data is also used to provide security. Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties. It mainly focused on to secure the information from unauthorized access, use, disclosure, disruption, modification and providing integrity, confidentiality and availability.

2. METHOD OF INFORMATION SECURITY

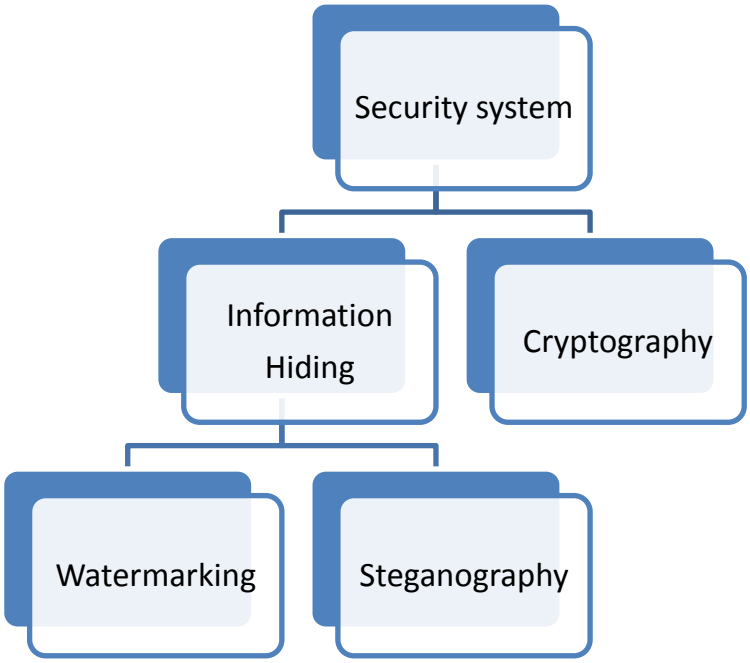

Fig 1: Different method for information security

The information security means protecting information or information system from unauthorized use, access, modification. For the information security the different method like cryptography, digital watermarking, Steganography is used to provide information security. The main purpose of security system is Data Confidentiality, Access Control, and Data Integrity, Authentication, Non Repudiation.

- **Digital Watermarking :** If any user use any of data that provide some authority to access right or provide some security to access it but any other user does not access particular information that is invisible from of watermarking.

- **Cryptography:** Cryptography is an important element of message transmission security requirement.it is the practical art of converting message or data into a different form, such that no one can read them or scramble message so no buddy can understood the message [1, 3].

- **Steganography:** Steganography is the art of undetectable communication. The steganography word is combination of two words which is derived from Greek word Steganos, which means hidden or covered and graphy means writing or drawing. So the meaning of the steganography is "covered drawing" or "hiding Writing" [1, 2, 3] .Steganography is the art of the undetectable communication. Steganography is one such pro-security mechanism that implanted in way so that the occurrences of secret data are not view (hidden). Steganography systems use multimedia objects like Image, audio, video to hide the secret information. [1, 3, 4].

Table 1: Comparison of different information security method.

Technique	Steganography	Cryptography	Watermarking
Objective	Secret communication	Data protection	Copyright preservation
What it does	Hides secret information	Replaces the secret data with its unreadable from	Hide the details of author
Carrier	Any digital media	Usually text based	Mostly images/audio files
Secret data	Payload	Plaintext	Watermark
Result	Stego-file	Cipher text	Watermarked file
Purpose	To hide message in suitable cover	To make data unreadable.	To hide owner information in their work
Visibility	Never	Always	Sometimes
Attacks	Steganalysis	Cryptanalysis	Image processing
Use	To transmit Secret information over open system	To transmit secret information over open system	To protect copyright information of inventor
Authentication	Full recovery of data	Full recovery of data	Usually achieved by cross correlation
Relation to cover	Not necessarily related to the cover. The message is more important than the cover.	N/A	Usually becomes an attributes of the cover image. The cover is more important than data
Failure	It is detected	De-ciphered	It is removed or replaced

3. STEGANOGRAPHY SYSTEM.

3.1: What is Steganography?

Steganography is going to achieve its importance due to the exponential growing and secret communication of potential computer users over the internet. It can also be defined as the study of invisible communication that usually deals with the ways of hiding the existence of the communicated message [1, 3, 5].Generally steganography is known as "invisible" communication[3,4,5] . Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today's steganography systems use multimedia items like image, audio, video etc. as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information [1].

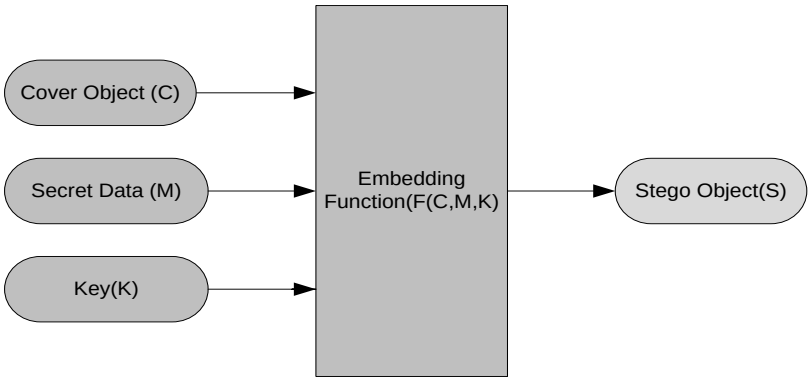

Fig 2: Basic process of steganography

In fig 2 we see the basic model of the steganography [6]. This model is giving the idea about the steganography process. The steganography is containing the four part cover object, secret Data, key and Stego object [4]. Cover object is known as Carrier objet it is used to put the hidden information on it. The secret data may be any digital media like (text message, image, audio, and video) the communication creator wants to send and secured form unauthorized person [1, 2, 4]. Key is also known as password, it is used to rises the security of steganography process. This decoding key is known only by the receiver so it is able to extract the secret data form object. The output of this process is stego object which is the cover object with the secret message. After receiving stego-image hidden message can simply be extracted with or without stego-key (depending on embedding algorithm) by the receiving end.

There should be minimum error difference between the stego-image and the original image in order to retain the quality of the image that is obtained after the data hiding process using various steganography techniques i.e. LSB technique, pixel value difference etc.

Cover medium + message + secret key (use or not use) = stego-medium

3.2 Rule of Steganography

The steganography is the technique of hiding the information inside the cover object using the steganography principal and the result is the stego- object that is send to the receiver. The receiver is taking out the secreted information from stego object using extract algorithm [6].

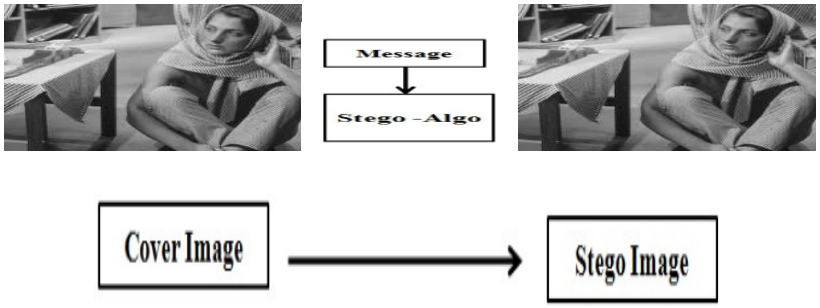

Fig 3: The Rule of Steganography

The rule of steganography method is shown in Fig.3. The principal is saying that the implanting process is done in this way that try to keep the sharp properties of the cover image [7]. The privet information is embedded inside cover image in a way that does not variant properties of cover image in a person's visualization system. The output is new image called stego-image that is looks same l as the cover image.

3.3 Key Properties of Steganography system.

As we seen the rule of the steganography is say that the output image is look same like cover image. It means that it work on the imperceptible property. A few key properties that must be considered when creating a digital data hiding system.

- **Embedding Capacity:** The amount of secret information is can be embedded without humiliation of quality of image. The amount of data that i embedded it lesser as possible because more information more the image has changed. It is easier to Steganalyst to discover the cover image is modified [6].

- **Imperceptibility:** It is also called as invisibility. It is the things in which a person should be unable to differentiate the original and stego object. The stego object that is generated it not be different such that it is visualized by human eye. Always try that the output image (stego-image) is very much similar to cover image [6].

- **Robustness:** It is main aim is that the Steganalyst it have difficulty to determine that the image conations the hidden information or not. To the degree of difficulty required to destroy embedded information without destroying the cover object. A good steganography method is exposed to many attacks that is demonstrates unfounded [6].

- **Independent of file format:** The algorithm it should be intelligent to use different file format for the used as a cover object [7].

- **Temper Resistance**: It should be difficult to alter the message once it has been embedded into stego-image [5].

- **Computation Complexity**: How much expensive it is computationally for embedding and extracting a hidden message?[5]

4. STEGANOGRAPHY IN DIGITAL MEDIUMS

Steganography is divided in the different type according to the carrier object is used to hide the secret information. [1, 2, 6].Multimedia is used as the cover object. The cover object is chosen that give the high degree of redundancy [6]. There are four category file format like image, text, audio, video use for information hiding [1, 2, 3, 4, 6].

- **Image Steganography:** Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information [1, 5, 6].

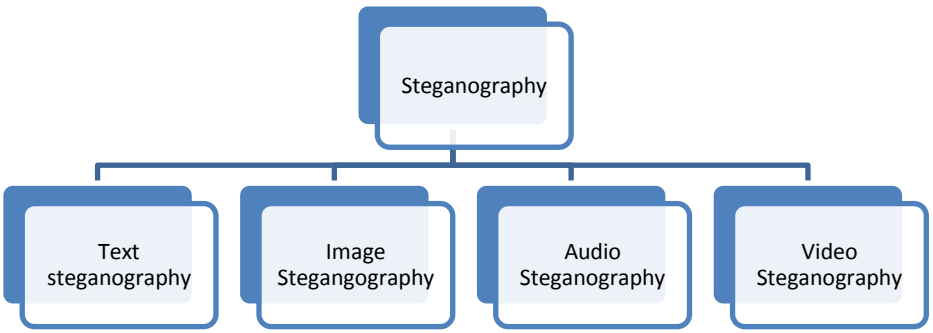

Fig 4: Type of Steganography

- **Text Steganography:** General technique in text steganography, such as number of tabs, white spaces, capital letters, just like line shift code, word shift code is used to achieve information hiding [5].

- **Audio Steganography:** When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MPEG for steganography. *LSB Coding, Phase Coding, Spread Spectrum it is method use in this method [1,5]*.

- **Video Steganography:** Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information [5].

Today the large amount of people use image as the data in the internet so image use as carrier object and image is the numerical representation of data so we can say one image is contain the more number of data so it provide the more hiding capacity. It also takes the advantages of the human visualization system.

In image Steganography it is dividing in the two type's spatial Domain steganography and transforms domain steganography [8]

5. CLASSIFICATION OF IMAGE STEGANOGRAPHY TECHNIQUES

There are numerous stenographic algorithms that can be used to embed secret information in a carrier medium. The algorithms can be categorized in following groups: spatial domain and frequency domain techniques.

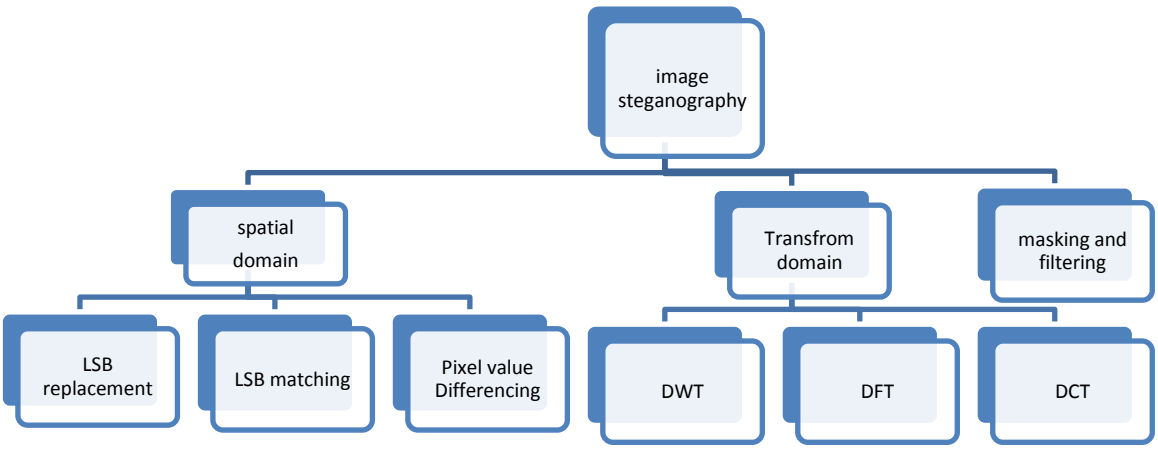

Fig 5: Type of image Steganography

5.1: Spatial Domain method:

In spatial domain scheme the secret message are inserted directly. Here the most common and simplest method is LSB insertion method. Modulating the least signification bit does not result in human perceptible differences because the amplitude of the change is small [1,4]. For our human eye, variations in the LSB are unnoticeable. Embedding of bits of data can be carried out either simply or randomly.

5.1.1: *LSB Replacement*

Least significant bit (LSB) insertion is a communal, simple approach to embedding information in a cover image. The least significant bit of the bytes inside an image is changed to a bit of the secret message. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In this steganography, the cover pixel LSBs is substituted with a bit of the message that has to be embedded. Prior to embedding, the message is transformed into a sequence of bits which are then inserted sequentially where the LSBs are located [1,2,3,4,8].
For example a bit pattern for 9 pixels of an 8-bit color image can be as follows:

Suppose the first three pixels of the original image have the following values:

[1 1 0 0 1 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 1 0 0 1]

[1 0 1 0 0 1 1 0 1 1 0 0 0 1 0 0 0 0 0 0 1 1 0 0]

[1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 1 0 0 0 1 0]

And that of secret image first three pixels is having the following values.

[1 1 1 0 0 1 0 1 1 0 1 1 0 1 1 0 1 1 1 1 0 0 0 1]

The first pixel of secret image is 167 its binary representation 11100101, is embedded into the LSBs of this part of an image, the resulting bit pattern will be as follows:

[1 1 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 1 1 0 1 0 0 1]
[1 0 1 0 0 1 1 0 1 1 0 0 0 1 0 0 0 0 0 0 1 1 0 1]

[1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 1 0 0 0 1 0]

Although the 8 bits were inserted in first 8 pixels from trace of an image, only the 2 underlined (highlighted) bits need to be modified. On an average, simply half of the pixel values in an image need to be modified while embedding the secret information. We have 256 possible intensities of 8 bit color image, changing the LSB of a pixel results in small changes in this intensity value. Such modifications cannot be identified by the human eye, thus the secret information is hidden into the carrier successfully [8].

General benefits of spatial domain LSB technique are:
1. There is less chance for humiliation of the original image.
2. More information can be stored in an image.
Weaknesses of LSB technique are:
1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

5.1.2: LSB Matching:

This category is much improved over LSB replacement method. In this LSB replacement is either randomly summed up or subtracted from the value of the cover pixel in case the bit of the confidential message is not equivalent to the LSB that come from the cover pixel [3,4] As compared to LSB Replacement method it is hard to detect LSB matching.

5.1.3: Pixel Value Differencing

This method is different when compared to the LSB replacement and LSB matching steganography methods. The Pixel-value differencing steganography technique uses the difference value between two consecutive pixels in a block to determine how many bits of text could be embedded [9].

5.2: Transform Domain Method:

This is also known as frequency domain method. This is a more difficult way of hiding information in an image. Various procedures and transformations are used on the image to hide information in it. Transform domain techniques hide data in the specific areas of the original image. Here the data is generally set into altered coefficients of an image giving much more capacity for information hiding and robustness against attacks. A number of algorithms are available for this. These techniques are better than LSB methods due to the fact that they embed information in particularly those areas of actual image which are not much exposed to processing of images. The 2-D DCT converts image blocks from spatial domain to frequency domain. The carrier image is divided into non overlapping blocks of size 8×8 and applies DCT on each of blocks of cover image using forward DCT [2].

5.2.1: *Discrete Wavelet transformation*

This transformation is an extremely necessary way to be used for signal investigation as well as image processing, mainly for multi-resolution demonstration. The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. It may crumble a signal into a number of constituents in frequency domain [11]. 1-D DWT segments a cover image further into two major components known as approximate component and detailed component . A 2-D DWT is used to segment a cover image into mainly four sub components: one approximate component (LL) and the other three include detailed components represented as (LH, HL, and HH) [10].

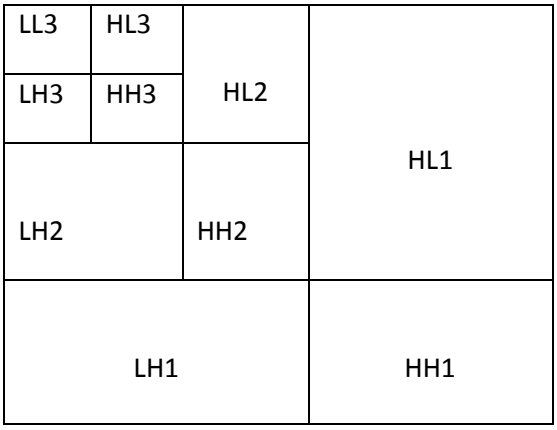

Fig 6: Three phase decomposition using DWT.

5.2.2: Discrete Cosine Transformation

This transformation technique is useful for separating an image into different parts of differing significance (which is associated with the image's quality). It resembles the Fourier Transform Technique as it converts an image from its spatial domain into frequency domain. It separates the image into spectral sub-bands according to its visual quality, i.e. high, middle and low frequency components [2, 4, 11].

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

The definition of 2d-DCT is given by:

$$DCTij = \alpha i \alpha j \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} Cmn \ cos \frac{\pi(2m+1)i}{2m} \ cos \frac{\pi(2n+1)j}{2n}$$

Where, i = 0, 1, 2……m-1 and j = 0, 1, 2……n-1

$$\alpha i = \begin{cases} 1/\sqrt{m}, & i = 0 \\ \sqrt{2/m}, & 1 \le i \le m-1 \end{cases} \qquad \alpha j = \begin{cases} 1/\sqrt{n}, & j = 0 \\ \sqrt{2/n}, & 1 \le j \le n-1 \end{cases}$$

5.2.3: Discrete Fourier transformation:

This technique is important as it separates an image into the sine and cosine values. It converts space and time dependent information into the frequency based information. It is useful for a number of applications including image filtering and reconstruction as well as image compression. It does not include all frequencies that result to form an image but constitutes of only the set of those samples which are sufficient to describe the original image [2].

5.3: ***Masking and filtering***

Masking and Filtering is a steganography technique which can be used on gray- scale images. Hiding is similar to placing watermarks on a printed image. This method embeds the secret information particularly in more significant areas rather than hiding it only into the noisy section [4]. This can be achieved for example by modifying the luminance of parts of the image. While masking does change the visible properties of an image, it can be done in such a way that the human eye will not notice the anomalies. Since masking uses visible aspects of the image, it is more robust than LSB modification with respect to compression, cropping and different kinds of image processing. The information is not hidden at the "noise" level but is inside the visible part of the image, which makes it more suitable [1].

Advantages of Masking and filtering Techniques:
1. This method is much more robust than LSB replacement with respect to compression since the information is hidden in the visible parts of the image.

Disadvantages of Masking and filtering Techniques:
1. Techniques can be applied only to gray scale images and restricted to 24 bits.

6. ANALYSIS

Table 2: Analysis of image steganography method

Domain	Method	Target to				Advantage	Disadvantage
		Capacity	Robustness	Perceptual	Temper		
Spatial	LSB	yes	no	no	no	High capacity	Hide extra bit signature with hidden message.
Spatial	LSB Matching	yes	no	no	no	High hidden capacity and good visual quality	Data set is limited.
Spatial	PVD	yes	no	no	no	High hidden capacity and good visual	Computational complex

						quality	
Transform	DCT	no	yes	no	yes	High psnr	Noticeable artifact of hidden data.
Transform	DWT	no	yes	no	yes	Invisibility high and high psnr	Less hiding capacity

6. CONCLUSION

Although only some of the main image steganography method is discussed in this paper, one can see that there exists a large selection of approaches to hiding information in image. All the method has different strong and weak point respectively. The study concludes that many approaches have been available for embedding data in images. Least Significant Bit method is the most common technique but it is less robust as it can be destroyed by simple attacks. The transform domain method it has low hiding capacity and high robust it is. Thus for an agent to decide on which stenographic algorithm to use, he would have to decide on the type of application he want to use the algorithm for and if he is willing to compromise on some features to ensure the security of others.

8. REFERENCES

1. Masour nosrati ,Ronak karimi ,and Mhedi Hariri, "An introduction to steganography methods", World Applied Programming, *World Applied Programming, Vol (1), No (3) ISSN: 2222-2510, 191-195* August 2011.

2. Kanzariya Nitin k, Rathod kirit R, Nimavat Ashish V, Jadeja Vijaysinh K "A Novel Technique for Image Steganography Techniques Based on LSB and DCT Coefficients", International Jouranal for Scientific Researc & Development, *ISSN (online): 2321-0613 ,2405-2508,*Vol-1,Issues 11,2014

3. Kanzariya Nitin k, Nimavat Ashish V, Jadeja Vijaysinh K , "highly secure images steganography techniques based on LSB,X-BOX Mapping and Huffman encoding", International Journal of Computer Science Engineeringand Information Technology Research (IJCSEITR) ISSN(P): 2249-6831; ISSN(E): 2249-7943, 23-34 , Vol. 4, Issue 6, Dec 2014

4. Amandeep Kaur, Rupinder Kaur, Navdeep Kumar" A Review on Image Steganography Techniques" *International Journal of Computer Applications (0975 – 8887),20-24,* ISSN-0975 -8887 *Volume 123 – No.4, August 2015*

5. Mehdi Hussain and Mureed Hussain," A Survey of Image Steganography Techniques", international Journal of Advanced Science and Technology Vol. 54 -ISSN 2249-9954,113-123, May, 2013

6. C.P.Sumathi, T.Santanam, G.Umamaheswari "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4 ISSN-0976-2760, No.6, 9-25, ,December 2013.

7. Kanzariya Nitin k,Nimavat Ashish v,"Comparision of Various image steganography Techniques",International journal of computer science and management research,vol 2- ISSN 2278-733X,1213-1217, Issue 1,janury 2013,

8. Himanshu Gupta , Dr Soni changlani, and prof Ritesh Kumar , "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 , 212-214, June 2013.

9. Rejani. R, Dr DMurugan,deppu V Krishanan , "Comparative study of spatial domain image steganography techniques", Int J Advanced networking and application,volume -07- ISSN: 0975-0290, 2650-2657 , issue:02,2015.

10. Sunil malviya,neelesh gupta,vibhanshu shirvastava "2D-Discrete Walsh Wavelet Transform for Image Compression with Arithmetic Coding" IEEE-31661, July 4 - 6, 2013

11. Nilanjan Dey, Tanmay Bhattacharya, S. R. Bhadra Chaudhuri " A Session based Multiple Image Hiding Technique using DWT and DCT" International Journal of Computer Applications (0975 – 8887) Volume 38– No.5 ISSN-0975 – 8887,18-21, , January 2012