Image Steganography Techniques in Spatial Domain, their Parameters and Analytical Techniques: A Review Article

Kamaldeep
UIET, M.D.University, Rohtak
Kamalmintwal@gmail.com

Dr. Rajkumar
UIET, M.D.University, Rohtak
Rajyadav76@rediff.com

***Abstract*— In this paper we will discuss various image steganography techniques in spatial domain. Their parameter and the method of analyzing the difference between the stego image and cover media. Steganography is defined as the art and science of hiding data as well as information in a carrier file in such a way that an intruder is unable to find out the data inside the carrier file. Text file, image file, audio file and video file are the possible carrier files. The main objectives of steganography are undetectability, robustness, temper resistance and hiding capacity of the hidden data. These are the main factors which make it different from other techniques further there are two popular schemes used for image steganography: spatial domain embedding and transform domain embedding. Most of the steganographic techniques discussed in literature either use spatial domain or transform. In the spatial domain the data is embedded directly into pixels of the image, which involves less complex computation whereas in transform domain, the data is embedded into the transform coefficients of the image.**

***Keywords*— Steganography, spatial domain, LSB Method, parameters, analytical technique**

I. INTRODUCTION

Steganography comes from Greek words Steganos (Covered) and Graptos (Writing. The term "steganography" came into use in 1500's after the appearance of Trithemius' book on the subject "steganography" [1]. In ancient time, people use wooden tablets, invisible ink, microdots etc. for steganography purpose. Usually the secret information is concealed by the use of an innocuous cover as to not arouse suspicion if hostile agents discover the cover. As an example, the cover text:

I'm feeling really stuffy. Emily's medicine wasn't strong enough without another febrifuge.

hides the sentence "Meet me at nine" if the reader retains the second letter of each word in sequence [2].Steganography can also be achieved by embedding secret data in an unsuspecting medium like image, video or audio, in such a way that the human-perceived quality of the unsuspecting medium is not altered [3]. The idea was first described by Simmons in 1983 [4]. More comprehension theory of steganography is given by Anderson [5]. Steganography is different from Cryptography which is about concealing the content of the message whereas steganography is about concealing the existence of the message itself [6]. Images provide excellent carriers for hidden information and many different techniques have been introduced [7]. In case of image steganography [8,9,10], if the secret data could be encrypted first and then embedded into a cover image then we get the better results. The image into which the encrypted data is embedded is called stego image. The difference between original image and stego image is very small that the human eye cannot distinguish the difference [6, 11]. The steganographic model is given in fig. 1.

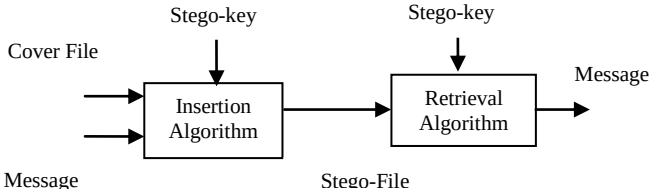

Fig. 1: Steganography Model

II. TYPES OF STEGANOGRAPHY ON THE BASES OF COVER-MEDIA

The most of the steganography system uses mainly four kind of cover media namely text, image, audio, video etc. On the bases of cover media steganography can be categories into four categories

- Text Steganography
- Image Steganography
- Audio Steganography
- Video Steganography.

A. Text steganography

This type of steganography uis also called linguistic steganography. One major category, perhaps the most difficult kind of steganography is text steganography or linguistic steganography because due to the lack of redundant information in a text compared to an image or audio [12], [13]. The text steganography is a method of using written natural language to conceal a secret message as defined by Chapman et al. [14]. The advantage to prefer text steganography over other media is its smaller memory occupation and simpler communication. For a more thorough knowledge of steganography methodology the reader may see [15], [16].Some Steganographic model with high security features has been presented in [17], [18], [19] ,[20]and [21].

B. Image steganography

Image is one of the best cover media for hiding the message. In image steganography [22] [23] [24] [25]and [26] the message is hidden into the an image. The message can be hidden in two ways : those in the Image Domain and those in the Transform Domain [27]. Image – also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency– domain, images are first transformed and then the message is embedded in the image [28].

C. Audio Steganography

In audio steganography the data is hidden into the audio file. Steganography of audio signals is more challenging compared to the steganograaphy of images or video sequences, due to wider dynamic range of the HAS in comparison with human visual system (HVS) [28]. The HAS perceives sounds over a range of power greater than 109:1 and a range of frequencies greater than 103:1. The sensitivity of the HAS to the additive white Gaussian noise (AWGN) is high as well; this noise in a sound file can be detected as low as 70 dB below ambient level [29]. Some commonly used methods of audio steganography are listed and discussed below in brief [30]

D. Video Steganography

In video steganography[31],[32],[33]and [34] the message is hidden into the video file. In the video steganography first the video file is taken as cover media. Then the cover media is broken down into the frame. After that the message is hidden into these frame using any video steganographhic algorithm for example LSB.

III. IMAGE STEGANOGRAPHY ON THE BASES OF DOMAIN

An image is defined as an arrangement of numbers and such numbers usually stand for different light intensities in different parts of the image [35]. The numeric description takes the form of a lattice where the individual points given the name 'pixels'. Pixels are displayed horizontally, row by row. In a color scheme, the number of bits is known as the bit depth and this basically refers to the number of bits assigned to each pixel [36]. Image is the most popular cover objects used for steganography Message is embedded into the original image in spatial-domain or in transform domain. Image steganography techniques can be divided into two groups: those in the Image Domain and those in the Transform Domain [37]. Image also known as spatial – domain techniques embed messages in the intensity of the pixels directly, while for transform – also known as frequency – domain, images are first transformed and then the message is embedded in the image [38]. Figure 2 shows the classification of steganography based on the domains.

IV. PARAMETERS OF IMAGE STEGANOGRAPHY TECHNIQUES

There are many parameters which tell about the goodness of the steganography algorithms.These parameters include hiding capacity, perceptual transparency (or security), robustness, complexity, survivability,capability and detectability [39, 40, 41, 42].

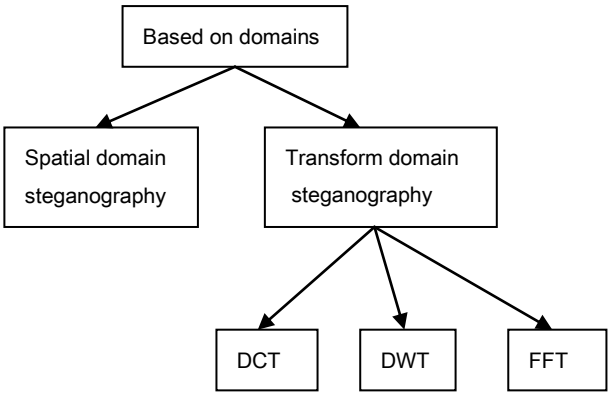

Fig. 2 Classification of Steganograaphy based on domain

A. Hiding Capacity

Hiding capacity is the size of information that can be hidden relative to the size of the cover. A larger hiding capacity allows the use of a smaller cover for a message of fixed size, and thus decreases the bandwidth required to transmit the stego-image.

B. Perceptual Transparency

The act of hiding the message in the cover necessitates some noise modulation or distortion of the cover image. It is important that the embedding occur without significant degradation or loss of perceptual quality of the cover. In a secret communications application, if an attacker notices some distortion that arouses suspicion of the presence of hidden data in a stego-image, the steganographic encoding has failed even if the attacker is unable to extract the message.

C. Robustness

Robustness refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression, and conversion back to digital form (such as in the case when a hard copy of a stego-image is printed and then a digital image is formed by subsequently scanning the hardcopy.

D. Tamper Resistance

Beyond robustness to destruction, tamper-resistance refers to the difficulty for an attacker to alter or forge a message once it has been embedded in a stego-image, such as a pirate replacing a copyright mark with one claiming legal ownership. In a copyright protection application, achieving good tamper resistance can be difficult because a copyright is effective for many years and a watermark must remain resistant to tampering even when a pirate attempts to modify it using computing technology decades in the future.

E. Other Characteristics

Computational complexity of encoding and decoding is another consideration and individualapplications may have additional requirements. For example, for a copyright protection application, a watermark should be resistant to collusion attacks where many pirates work

V. APPLICATIONS OF STEGANOGRAPHY

Steganography, in general, have many applications including copyright protection, Feature Tagging and secret communications etc. [43, 44].

A. Copyright Protection

Hiding capacity is the size of information that can be hidden relative to the size of the cover. A larger hiding capacity allows the use of a smaller cover for a message of

B. Feature Tagging

Captions, annotations, time stamps and other descriptive elements can be embedded inside an image, such as the name of the individuals in a photo or location in a map. Copying the stego image also copies all of the embedded features and only parties who possess the decoding stego key will be able to extract and view the features.

C. 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 used steganography does not advertise covert communication and therefore, avoid scrutiny of the sender, message and recipient.

D. Digital Watermark

The objective of a digital watermark is to place an indelible mark on an image. Usually, this means encoding only a handful of bits, sometimes as few as one. This "signature" could be used as a means of tracing the distribution of images for an on-line news service and for photographers who are selling their work for digital publication. One could build a digital camera that places a watermark on every photograph it takes. Theoretically, this would allow photographers to employ a "web-searching agent" to locate sites where their photographs appear [44].

E. Tamper Proofing

The objective of tamper-proofing is to answer the question, "Has this image been modified?" Tamper-proofing techniques are related, but distinct from the other data-hiding technologies. What differentiates them is the degree to which information is secured from the host signal. Most data-hiding techniques attempt to secure data in the face of all modifications. Tamper-proofing techniques must be resilient to small modifications (e.g., cropping, tone scale or gamma correction for images or balance or equalization for sounds) but not to large modifications (e.g., removing or inserting people from an image or taking words out of context in an audio recording [44].

VI. ANALYZING TECHNIQUES OF STEGO IMAGE AND COVER MEDIA

For measuring the quality of reconstructed image that is stegao image as compared to the original image, the metric needs to be define [45, 46]. There are three common error metrics used for estimating noise on images are RMSE, PSNR, and NCC.

A. Psnr

The PSNR [1] (Peak Signal to Noise Ratio) measures the similarity between two images (how two images are close to each other). Peak Signal to Noise Ratio (PSNR): The PSNR is evaluated in decibels and is inversely proportional the Mean Squared Error. It is given by the equation [47] it can be given by the following equation.

$$PSNR = 10\ Log10\ [\frac{(I)^2}{MSE}] \quad S$$

where:

- I is the dynamic range of pixel values, or the maximum value that a pixel can take, for 8-bit images: I=255.
- MSE is the mean square error.

B. Rmse

The Root mean square error measures the difference between these two images. Since the computing of these two metrics is very easy and fast, they are widely-used and very popular [48].

$$MSE = \frac{1}{(N*M)^2} \sum_{i=1}^{N} \sum_{j=1}^{M} (Xij - Yij)^2$$

Here,

- N, is the noumber of rows in the cover image.
- M, is the number of column in the vover image
- Xij, intensity of pixelij in cover image
- Yij, intensity of pixelij in stego image

Assuming pixel values in the range [0,255], The following observations are mentioned as:

- RMSE of zero which means an identical image results in infinite or undefined PSNR
- RMSE of 255 result in PSNR of zero
- RMSE greater than 255 results in negative PSNR.

C. Ncc

Normalized cross correlation (NCC) has been commonly used as a metric to evaluate the degree of similarity (or dissimilarity) between two compared images. The main advantage of the normalized cross correlation over the cross correlation is that it is less sensitive to linear changes in the amplitude of illumination in the two compared images. Furthermore, the NCC is confined in the range between –1 and 1. [49] to evaluate the performance the Normalized Cross- Correlation (NCC) which is given by the following equation

$$NCC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (Xij * Yij)}{\sum_{i=1}^{N} \sum_{j=1}^{M} (Xij)2}$$

Here,

- N, is the noumber of rows in the cover image.
- M, is the number of column in the vover image
- Xij, intensity of pixelij in cover image
- Yij, intensity of pixelij in stego image

VII. EXISTING METHODS OF IMAGE STEGANOGRAPHY IN SPATIAL DOMAIN

In Spatial Domain of an image, we can directly access any pixel in that image without involving any mathematics. The information bit is inserted directly in the pixel by using various algorithms. There are various techniques of image steganography in spatial domain which are given below:

- LSB Method
- 6th, 7th Bit Method
- Gray Level Modification Method
- Pixel Value Difference Method
- Parity Checker Method
- Pixel Value Differencing Method
- Cover Region and Parity Bits Method
- Optimum Pixel Adjustment Procedure

A. LSB (Least Significant Bit) Method

The popular and oldest method for hiding the message in a digital image is the LSB method [50]. In LSB method we hide the message in the least significant bits (LSB's) of pixel values of an image. In this method binary equivalent of the secret message is distributed among the LSBs of each pixel.

For example data bits 01100101 are tried to hide into an 8 bit color image. According to this technique 8 consecutive pixels from top left corner of the image are selected. The binary equivalent of those pixels may b like this

00100101 11101011 11001010 00100011
11111000 11101111 11001110 11100111

Now each bit of data 01100101 are copied serially (from left hand side) to the LSB's of equivalent binary pattern of pixels, resulting the bit pattern would become

00100100 11101011 11001011 00100010
11111000 11101111 11001110 11100111

The problem with this technique is that it is very vulnerable to attacks such as image compression and quantization of noise.

1) Advantages of LSB:

- 100 % chances of insertion.
- Easy to implement

2) Disadvantages of LSB:

- One of the major disadvantage associated with LSB method is that intruder can change the least significant bit of all the image pixels. In this way hidden message will be destroyed by changing the image quality, a little bit, i.e. in the range of +1 or -1 at each pixel position.
- Not immune to noise and compression technique.
- One of the basic techniques so more vulnerable to Steganalysis.

B. 6th, 7th Bit Method

Parvinder et al [51] obtained an algorithm to hide the message in 6th and 7th bit of pixel value. Here instead of LSB bits 6th and 7th bit of pixel values are used to hide the secret data within an image. This novel proposed method overcomes the all disadvantages of LSB insertion method .However it has its own disadvantage that is the chance that the message bit will be inserted at pseudorandom location at first instance is less as compared to LSB.

1) Algorithm for insertion of message bit 'b'

i. Find the pseudo – random location 'L' in image using secret key to insert the message bit b.
ii. Check whether at location 'L' pixel value is 00000000 or 11111111, called boundary values. If yes, ignore this location and go to step (i). Here it has to ignore these boundary values because the change may be +2 or _2 in pixel values, which is to be avoided.
iii. Check whether at location 'L'
   a) 6th and 7th bits are b, b? If yes, then no change at 'L' is required. Message bit is already there. Go to end.
   b) 6th and 7th bits are b, bc or bc ? If yes, then see that whether it is possible to make 6th and 7th bits as b, b by adding or subtracting 1 to pixel value? If yes, do it and go to End. Otherwise ignore the location 'L' and go to step (i).
iv. 6th and 7th bits are bc, bc ? If yes, then see whether it is possible to make 6th and 7th bits to b, b by adding or subtracting 1? If yes ,do it go to End. Otherwise change them to b,b or b, b by adding or subtracting 1 and go to (i).
v. End

2) Algorithm for retrieval of message bit 'BS

i. Trace out the location 'L' for the same secret key as used in insertion algorithm.
ii. Pixel value is equal to of the boundary values i.e., 00000000 or 11111111? If yes, then it is invalid address. Go to step (i).
iii. Check whether at location 'L'
   a. 6th and 7th bits are different i.e. if bc or b ,bc? If yes, then it is invalid location at first chance.
   b. 6th and 7th bits are same i.e. b,b then b is the message bit.
iv. End

3) Advantages

- 49% chances, that when message bit is inserted, no change in pixel value is required.
- 12.5% chances, that change in pixel value is required, when it is ignoring the location.

4) Disadvantages

- Not optimal chances of insertion.
- If intruder change LSB, secret data may be affected.
- Not immune to compression and noise.

C. GLM (Gray Level Modification) Method

Gray level modification Steganography [52] is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM Steganography uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

For example, by taking the bit stream 1001010101. The first element of the bit stream is 1, so it has to modify our selected pixel to represent 1. It propose to decrement the value of the selected pixel by one so as to make them odd; and now this odd pixel would represent a bit stream equivalent to 1. The message insertion and extraction process can be shown by figure 3 and figure 4.

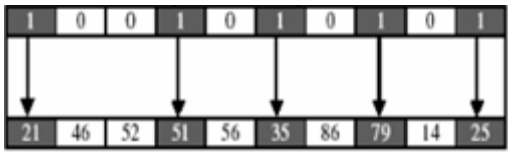

Fig 3: Data Embedding Process in GLM

Fig 4: Data Extraction Process in GLM

1)Algorithm for Embedding Process of GLM

i. Select pixels according to an arbitrary function g (x, y).
ii. Modify the gray level values of the selected pixels to make them even by adding one. These even gray levels will represent 0 in a bit stream.
iii. To represent 1, modify the appropriate pixel by decrementing its gray level value by 1
iv. Thus, we can represent both 1s and 0s using pixels, which satisfy the condition of being odd or even.

2) Algorithm for Retrieval of Data

i. Now there is a modified image and the secret function (which is used to find pixel location). Using this function, those pixels that have been used to embed data are identified.
ii. The receiver knows the algorithm logic that an even value of gray level represents 0 while an odd value represents 1. Knowing this, the receiver can acquire the hidden data.
iii. The receiver first picks up the selected pixels and map them to the respective binary data.
iv. Odd number is mapped to one while even number is mapped to zero.

3)Advantages of GLM

- Chances of insertion of data are optimal.
- Easy to implement.

4) Disadvantages of GLM

- Vulnerable to Steganalysis.
- Not immune to noise and compression.

D. Hiding Data In 6th, 7th & 8th Bit of Pixel Values

Rajkumar et al [53] proposed a novel approach to hide the data 6^{th}, 7^{th} and 8^{th} bit of pixel values. In this method 6th, 7th and 8th bits of the image pixels are used to hide the message. Since this method involves 8th bit for hiding the message, intruder can easily change 8th bit of all image pixels and this may result in the loss of message. To avoid this, time factor has been introduced, i.e. at some time t1, sender sends the cover object with message and at some other time t2 sender sends the cover object without message. Sender and recipient agree on this time factor initially before starting any communication. The advantage of introducing time factor (slot) is that if least significant bits of all pixels are changed by the intruder even then the message can be retrieved by comparing the two cover bjects, i.e. one containing the message and the other not containing the message.

1) Algorithm For Insertion of Message Bit 'b'

Let b^c denote the complement of b, i.e. if b=0 then b^c=1 and if b=1 then b^c=0.

i. Find pseudo- random location (*l*) in the cover object using secret key for inserting the message bit 'b' (i.e. 0 or 1)
ii. Check whether at location (*l*) pixel value is, 00000000, 00000001, 11111110 or11111111. If yes, then this is an invalid location and therefore goes to (i).
iii. Check whether at location (*l*);
   a) 6th, 7th and 8th bits are b b b, b b b^c or b^c b b? If yes, no change at (*l*) is required. Message bit is already there, go to end.
   b) 6th, 7th and 8th bits are b b^c b^c, b^c b^c b or b^c b^c b^c ?If yes, then make these b b b, b b b^c or b^c b b by adding or subtracting 1. However, if it is not possible to make these as b b b, b b b^c or b^c b b by adding or subtracting 1, then make these b^c b b^c or b b^c b and go to end.
   c) 6th, 7th and 8th bits are b^c b b^c or b b^c b? If yes, then make these b b b, b b b^c, or b^c b b by adding or subtracting 1, Otherwise go to end.
iv. End.

2) Algorithm for Retrieval of Message Bit B As bbb or bbBc Or bcbb:-

i. Trace out the location "l" from the same secret key which was used during insertion process by the sender.
ii. Check whether pixel value is equal to 00000000, 00000001, 11111110 or 11111111? If yes, then it is an invalid address. Go to (i)

iii. Check whether at location (*l*);

a) 6th, 7th and 8th bits are b^c b b^c or b b^c b? If yes, then no message bit has been inserted and therefore go to (i)
b) 6th, 7th and 8th bits are b b b , b b b^c or b^c b b. then 'b' is the message bit.

iv. End.

3) Advantages

- The probability that the message bit will be inserted at the pseudorandom location at first chance is 85.93%.
- The advantage of introducing time factor(slot) is that if LSBs of all pixels are changed by intruder even then the message can be retrieved.
- It can be easily detected if intruder makes some changes because changes will be of +2/-2 range

4) Disadvantages

Chances of insertion are not optimal (100 %) at first instance.As discussed in this section regarding the message insertion at 6^{th} ,7^{th} and 8^{th} bit pixel values it conclude that even this method is not optimal. But it has almost achieved a solution nearly close to optimal solution. In upcoming section Parity Checker Method proposed by Rajkumar et al has been discussed.

E. Parity Checker Method [53]

In this method, Rajkumar et al gives the concept of odd and even parity. According to this method, 0 can be inserted at a pixel location if that pixel has odd parity i.e. the number of 1's in the binary value of the pixel should be odd. Similarly, 1 can be inserted at a pixel location if that pixel has even parity i.e. the number of 1's in the binary value of pixel should be even. If the corresponding parity does not exist at a pixel location either for 0 or 1, then we make corresponding parity at that pixel location (odd parity for 0 and even parity for 1) by adding or subtracting 1 to the pixel location such that the change in the image quality should not be visible to the human visual system (HVS). In the next section PVD Method has been discussed.

F. PVD (Pixel Value Differencing Method) [55]

The pixel value differencing (PVD) method proposed by Wu and Tsai can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification. In the next section, Cover Region and Parity Bits Method has been discussed.

G. Cover Region and Parity Bits Method [56]

In this technique, the image is divided in a minimum of L (m) contiguous and disjoint regions and their use are defined by a pseudo-random number generator (PRNG). The parity of the region is calculated by using equation given below.

$$P(I) = \sum_{j \in I} LSB(C_j) MOD_2$$

It is necessary only one LSB flipping of any pixel of the region to change the parity region value. In the coming section, Optimal Pixel Adjustment Method has been discussed.

H. Optimum Pixel Adjustment Procedure [56]

The proposed Optimal Pixel adjustment Procedure (OPAP) reduces the distortion caused by the LSB substitution method. In OPAP method the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden.

1) PROCEDURE FOR HIDING

- First a few least significant bits are substituted with the data to be hidden.
- Then in the pixel, the bits before the hidden bits are adjusted suitably if necessary to give less error.
- Let n LSBs be substituted in each pixel.
- Let d= decimal value of the pixel after the substitution.
- d1 = decimal value of last n bits of the pixel.
- d2 = decimal value of n bits hidden in that pixel.
- If (d1~d2) <= (2^n)/2 then no adjustment is made in that pixel.
- Else

  If(d1<d2)

  d = d – 2^n .

  If(d1>d2)

  d = d + 2^n .

This d is converted to binary and written back to pixel.

2) Retrieval

The retrieval follows the extraction of the least significant bits (LSB) as hiding is done using simple LSB substitution.

3) Advantages

- 1. Simple methodology.
- 2. Easy retrieval.
- 3. Improved stego-image quality than LSB substitution.

VIII. CONCLUSIONS

In this paper we have reviewed various steganographic techniques, different parameters and different methods for analyzing of original image and stego image. Each of these steganographic techniques tries to satisfy the various steganographic parameters such as imperceptibility, capacity and robustness which have been discussed in this paper. For example The LSB technique in spatial domain has 100% chances of insertion hence high payload capacity of data etc, but they often fail to prevent statistical attacks and are thus easily detected. In future we will try to devolve a technique which covers maximum parameter of the steganography

REFERENCES

[1]. Bandopadhyay, S.K., BhattaCharya, D., Ganguly, D., Mukherjee, S. and Das, P. (2007),"A Tutorial Review on Steganography".

[2]. Eugene, T.L. and Edward, J.D.(2006), "A Review of Data Hiding in Digital Images", Video and Image Processing Laboratory (VIPER), Indiana.

[3]. Amirtharajan, R., Ganesan, V., Jithamanyu, R. and Rayappan, J.B.B. (2010), "An Invisible Communication for Secret Sharing against Transmission Error", Universal Journal of Computer Science & Engineering Technology, 1 (2), 117-121.

[4]. Simmons, G. J. (1983), "The Prisoners Problem and the Subliminal Channel", Proceedings of crypto '83, Plenum Press, pp 51-67.

[5]. Anderson, R. J. (1996), "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48.

[6]. Anderson, R.J. and Petitcolas, F.A.P. (1998), "On the Limits of Stegnography", IEE Journal on selected Areas in Communications, Vol. 16 No 4, pp 474-481

[7]. Johnson, N.F., Duric, Z. and Simmons, G. J. (2001)," Information hiding : steganography and watermarking - attacks and countermeasures (advances in information security, volume 1)". Kluwer academic publishers, february 15.

[8]. Amirtharajan, R., Akila, R. and Chowdavarapu, P.D. (2010), "A Comparative Analysis of Image Steganography". International Journal of Computer Applications 2(3): 41–47.

[9]. Cheddad, A., Condell, J., Curran, K. and Kevitt, P.M. (2010), "Digital image steganography: Survey and analysis of current methods Signal Processing 90 :727–752.

[10]. Bender, W. and Gruhl, D. (1996), "Techniques for data hiding", Ibm Systems Journal, Vol 35, Nos 3&4.

[11]. Anderson, R. J. (1996), "Stretching the Limit of Steganography", In Information Hiding, Springer Lecture Notes in Computer Science, Vol. 1174, pp 39-48.

[12]. N.F. Maxemchuk J.T. Brassil, S. Low and L. O.Gorman. Electronic marking and identification techniques to discourage document copying. IEEE Journal on Selected Areas in Communications, 13:1495–1504, 1995.

[13]. N.F.Johnson. and S. Jajodia. Steganography: seeing the unseen. IEEEComputer, 16:26–34, 1998.

[14]. G. Davida M. Chapman and M. Rennhard. A practical and effective

[15]. N.F.Johnson. and S. Jajodia. Steganography: seeing the unseen. IEEE Computer, 16:26–34, 1998. approach to large-scale automated linguistic steganography. In Proceedings of the Information Security Conference, pages 156–165, October 2001.

[16]. JHP Eloff. T Mrkel. and MS Olivier. An overview of image steganography. In Proceedings of the fifth annual Information Security South Africa Conference., 2005.

[17]. Souvik Bhattacharyya. and Gautam Sanyal. Study of secure steganography model. In Proceedings of International Conference on AdvancedComputing and Communication Technologies (ICACCT-2008), Panipath,India, 2008.

[18]. Souvik Bhattacharyya. and Gautam Sanyal. An image based steganography model for promoting global cyber security. In Proceedings of International Conference on Systemics, Cybernetics and Informatics, Hyderabad,India, 2009.

[19]. Souvik Bhattacharyya. and Gautam Sanyal. Implementation and design of an image based steganographic model. In Proceedings of IEEE International Advance Computing Conference, Patiala ,India, 2009

[20]. Avinash Prasad Kshitij. Souvik Bhattacharyya. and Gautam Sanyal. A novel approach to develop a secure image based steganographic model using integer wavelet transform. In Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing (Indexed by IEEE Computer Society), Cochin ,India, 2010.

[21]. B.Souvik , B.Indradip and S.Gautam, " A Novel Approach of Secure Text Based Steganography Model using Word Mapping Method(WMM)" International Journal of Computer and Information Engineering 4:2 2010.

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

[23]. Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areasin Communications, May 1998

[24]. Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999

[25]. Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002

[26]. Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001

[27]. Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001

[28]. Lee, Y.K. & Chen, L.H., "High capacity image steganographic model", Visual Image Signal Processing, 147:03, June 2000

[29]. Nedeljko Cvej, Algorithms for audio watermarking and steganography, Oulu 2004, ISBN: 9514273842.

[30]. Sos S. Agaian, David Akopian, Sunil A. D'Souza1, Two algorithms in digital audio steganography using quantized frequency domain embedding and reversible integer transforms, USA.

[31]. Hussein A. Aly, "Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error", Ieee Transactions On Information Forensics And Security, Vol. 6, No. 1, March 2011

[32]. J. Zhang, J. Li, and L. Zhang, "Video watermark technique in motion vector," in Proc. XIV Symp. Computer Graphics and Image Processing, Oct. 2001, pp. 179–182.

[33]. C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in Proc. Int. Conf. Innovative Computing, Information and Control (ICICIC'06), 2006, vol. II, pp. 803–806.

[34]. P.Wang, Z. Zheng, and J. Ying, "A novel videowatermark technique in motion vectors," in Int. Conf. Audio, Language and Image Processing (ICALIP), Jul. 2008, pp. 1555–1559.

[35]. N.F. Johnson and S. Jajodia. (1998, Feb.). "Exploring steganography: seeing the unseen." IEEE Computer Journal. [On line]. 31(2), pp. 26-34. Available: http://www.jjtc.com/pub/r2026.pdf [Jun. 2011].

[36]. T. Morkel, J.H.P. Eloff, and M.S. Oliver. "An overview of image steganography." in Proc. ISSA, 2005, pp. 1-11.

[37]. Silman, J., "Steganography and Steganalysis:An Overview", *SANS Institut*e, 2001

[38]. Simmons, G., "The prisoners problem and the subliminal channel", *CRYPTO*, 1983

[39]. Titchener, M.R. (1984), "Technical note:Digital encoding by way of new T-codes", IEE Proc. E. Comput. Digit Tech, 131, (4), pp. 151-153.

[40]. Bender, W. and Gruhl, D. (1996), "Techniques for data hiding", Ibm Systems Journal, Vol 35, Nos 3&4.

[41]. Chandramouli, R. and Memon, N.D. (2003), "Steganography capacity: A steganalysis perspective", Proc. SPIE Security and Watermarking of Multimedia Contents, Special Session on Steganalysis.

[42]. Parvez, M. T. and Gutub, A.(2008), "RGB Intensity Based Variable-Bits Image Steganography", APSCC 2008-Proceedings of 3rd IEEE Asia-Pacific Services Computing Conference, Yilan, Taiwan, 9-12.

[43]. Johnson, N. and Jajodia, S. (1998), "Exploring steganography: seeing the unseen," *IEEE Computer*, pp. 26-34.

[44]. Bender, W. and Gruhl, D. (1996), "Techniques for data hiding", Ibm Systems Journal, Vol 35, Nos 3&4.

[45]. Le Phu Dung, Srinivasan Bala, Mohammed Salahadin, Kulkarni Santosh and Wilson Campbell, "A Measure for Image Quality", ACM, pp. 513-519, 1998.
[46]. Z. Wang and A. C. Bovik, A universal image quality index, IEEE Signal Processing Letters, vol. 9, no. 3, pp.81-94, March 2002
[47]. Ahmet M. Eskicioglu, Paul S. Fisher, "Image Quality Measures and Their Performance" IEEE Transactions on Communication, Vol. 43, No. 12, pp. 2959-2965, December 1995.
[48]. Wang, Z., Sheikh, H. R. & Bovik, A. C. (2003) Objective Video Quality Assessment. The Handbook of Video Databases: Design and Applications.CRC Press.
[49]. D. M. Tsai and C. T. Lin "Fast normalized cross correlation for defect detection"Department of Industrial Engineering and Management, Yuan-Ze University, Chung-Li, Taiwan, R.O.C.
[50]. Johnson, N. and Jajodia, S. (1998), "Exploring steganography: seeing the unseen," *IEEE Computer*, pp. 26-34.
[51]. Singh, P., Batra, S. and Sharma, H.R. (2005), ""Evaluating the Performance of Message Hidden in First and Second Bit Plane", WSEAS Transaction on Information Science and Technology, vol. 2, no 8, pp 1220-1222.
[52]. Potdar, V. and Chang, E. (2004), "Gray Level Modification Steganography for Secret Communication", IEEE International Conference on Industrial Informatics, Berlin, Germany.
[53]. Yadav, R., Rishi, R. and Batra, S.(2010), "A new Steganography Method for Gray Level Images using Parity Checker", International Journal of Computer Applications (0975-8887) Volume 11-No. 11.
[54]. Wu, D.C. and Tsai, W.H. (2003), "A steganographic method for images by pixel-value differencing. Pattern Recognition Letters", 24: 1613-1626.
[55]. Manchanda, S., Dave, M. and Singh, S.B. (2004),"Customised and secure Image Steganography Through Random number Logic".
[56]. Krenn, R. (2004)," Steganography and steganalysis".Internet Publication,http://www.krenn.nl/univ/cry/steg/article.pdf,(2004)March