Comparative Study of Spatial Domain Image Steganography Techniques

Rejani. R
Department of Computer Science and Engineering, Manonmanium Sundarnar University, Tirunelveli
Email: rejani@gmail.com
Dr. D. Murugan
Department of Computer Science and Engineering, Manonmanium Sundarnar University, Tirunelveli
Email: dhanushkodim@yahoo.com
Deepu.V.Krishnan
Technical Architect, Infosys Limited, Technopark, Karyavattom Campus.
Email: deepu_vk@hotmail.com

ABSTRACT

Steganography is an important area of research in information security. It is the technique of disclosing information into the cover image via. text, video, and image without causing statistically significant modification to the cover image. Secure communication of data through internet has become a main issue due to several passive and active attacks. The purpose of stegnography is to hide the existence of the message so that it becomes difficult for attacker to detect it. Different steganography techniques are implemented to hide the information effectively also researchers contributed various algorithms in each technique to improve the technique's efficiency. In this paper we do a brief analysis of different spatial domain image stegnography techniques and their comparison. The modern secure image steganography presents a challenging task of transferring the embedded information to the destination without being detected.

Keywords – **Cover image, Embedding, LSB, MSB, RGB, Steganography, Stego-image.**

Date of Submission: July 20, 2015 Date of Acceptance: Aug 12, 2015

1. INTRODUCTION

Today information technology has developed to a great extent which was not imaginable in earlier years. These days almost all the methods of communication has become digital and for the exchanging of information we are mainly dependent on the internet. Through different locations across the globe we can exchange a variety of information. However there is also a possibility that these information may be sometimes illegally gathered, transferred and used by some malicious users or organizations for their use. This results in confidential and private data being used by another person without consent which could lead to dangerous consequences. These issues features that data protection has become an important point to consider during data communication. The main challenge faced in data privacy is the need to share data while protecting personally identifiable information from hackers and other malicious attacks. We have seen that steganography and cryptography together can protect data effectively.

Different steganography techniques have been developed to hide the message in an image. Steganography method hides the textual information in such a way that only sender and receiver can identify that a message is hidden within the image. Steganography on images can be broadly classified as spatial Domain Steganography and Frequency Domain Steganography. This paper does a comparison between some of the spatial Domain steganography techniques.

1.1 LSB Steganography

The simplest and most popular image Steganography method is the least significant bit (LSB) substitution. In this method the messages are embedded into cover image by replacing the least significant bits of the image directly. The hiding capacity can be increased by using up to 4 least significant bits in each pixel which is also quite hard to detect [16, 18, 3].

1.2 MSB Steganography

This method is a slight modification of the LSB steganography. In this method instead of changing the least significant bit the most significant bit is changed. In this case the embedded value is stored in the most significant bits of the image.

1.3 RGB Steganography

A Digital image is an array of numbers that represent light intensities at various points or pixels. Digital computer images can be normally stored as 24-bit (RGB) or 8-bit (Grayscale) files. A 24-bit file can be quite large however it provides more space for hiding information. As we know all colors are essentially a combination of three primary colors: red, green, and blue. Every primary color is represented by one byte ie every pixel represents a combination of (R,G,B).

Paper [11] is based on the manipulation of the least significant bits of pixel values [3][4] or the rearrangement of colors to create least significant bit or also called as parity bit patterns. The parity bit patterns can correspond to the message being hidden. RGB Steganography method attempts to overcome the problem of the sequential fashion and the use of stego-key for the selection of pixels. In paper [3] some least significant bit based RGB steganography method is implemented.

1.4 Pixel Value Differencing Steganography

This method is different when compared to the LSB and RGB based 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 Wu and Tasi's method has the two quantization range tables. As per that the first table using the range of widths (8, 8, 16, 32, 64 & 128) to provide large capacity and the second table uses the range widths of (2, 2, 4, 4, 4, 8, 8, 16, 16, 32, 32 & 64) which meanwhile provides a high imperceptibility [23].

2. RELATED WORK

Let us see some of the related work done in each of these area. In [3] one type of lsb based RGB intensity steganography technique proposes an improved LSB (least significant bit) based Steganography technique for images. This paper deals with an embedding algorithm for hiding encrypted messages in nonadjacent and random pixel locations in edges and smooth areas of images. At first it encrypts the secret message, then detects edges in the cover-image by using improved edge detection filter. After that the message bits are embedded in the least significant byte of randomly selected edge area pixels and 1st 3rd and 4th LSBs of red, green, blue combinations respectively across randomly selected pixels across smooth area of image. Some other types of LSB steganography techniques based on least bits are explained on [18]. And some similar technique is implemented in [16] MSB based steganography.

In RGB Intensity Based Variable-Bits Image Steganography [4] describes new algorithm for RGB image based steganography. This algorithm introduces the concept of storing variable number of bits in each channel (R, G or B) of pixel based on the actual color values of that pixel: lower color component stores higher number of bits. Secure RGB Image Steganography method from Pixel Indicator to Triple Algorithm-An Incremental Growth [1] introduces two methods of RGB image steganography one is pixel indicator technique and other is triple-A algorithm. They uses the same principle of LSB, As the secret is hidden in the least significant bits of the pixels, but also offer a better randomization while selecting of the number of bits and color used. This randomization increase the security of the system and it also increase the capacity. Some other types of RGB based steganography techniques are implemented in [1, 2, 11, and 14]. These techniques can be applied to RGB images where each pixel is represented by three bytes to indicate the additive values of red, green, and blue.

Paper [5] designs a steganography algorithm which not only hide the message behind the image but also provide more security than others. For the purpose of security, encryption technique is used with a user-defined key. In that paper, message is hide into an image in the form of an image that is using image generation method message is converted into the image of predefined format and then by using designed algorithm that image will hide into the cover image. RGB image format is used to improve the quality of the stego image. Finally this RGB image is saved as BMP image file so that no lossy compression can occur and the original message do not destroy and can be extract as it is.

In the Pixel Indicator High Capacity Technique for RGB Image Based Steganography [6] give the ideas from the random pixel manipulation methods and the stego key ones techniques are merged, which uses the least two significant bits of one of the channels to indicate existence of data in the other two channels.

In [24] the method of Wang et al. uses Pixel-Value Differencing (PVD) and their modulus function provides high capacity and good image quality. In this method the embedding process creates a number of artifacts like abnormal increases and fluctuations in the PVD histogram, thereby revealing the existence of the hidden message. To enhance the security of the algorithm it makes use of a turnover policy that prevents abnormal increases in the histogram values and a novel adjusting process is devised to remove the fluctuations at the border of the subrange in the PVD histogram. This method therefore eliminates all the weaknesses of the PVD steganography methods thus far proposed and guarantees a secure communication. Paper [25] the PVD approach is where the cover image is first partitioned into small squares. After this each square is rotated by a random degree of 0, 90, 180 or 270. The resulting image is again divided into non-overlapping embedding units with three consecutive pixels, and the mid one is used for data embedding. The number of embedded bits in this method is dependent on the differences between the three pixels. In order to preserve the local statistical features, the three pixel values will have the same sort order after data hiding. Also the new method can first use sharper edge regions for data hiding adaptively, thereby helping to preserve other smoother regions by adjusting a parameter.

3. VARIOUS STEGANOGRAPHY TECHNIQUES

We have by now seen the various methods used to hide data using steganography. The usual and most popular among these methods is the LSB or the Least Significant Bit Steganography. Different modifications of LSB techniques are familiar like LSB1 Steganography and LSB2 steganography. Likewise different variable algorithms are implemented for RGB and PVD steganography. Here we are investigates some of the algorithms of these techniques.

3.1 LSB Steganography

This is the simplest of the steganography methods based in the use of least significant bit and therefore is also the most exposed. In this technique the embedding process is quite simple and consists of the sequential substitution of each Least Significant Bit (LSB-1) of the image pixel for the bit message [18]. Even though this method is simple, It can disclose a large volume of data. The LSB1 algorithm procedures describes below:

Step 1: The data bits are changed from decimal to binary.

Step 2: The Cover image is read.

Step 3: The cover image is converted from decimal to binary format.

Step 4: The text to be disclosed inside the image and is broken into bits.

Step 5: Take the first 8 bytes of data from the cover Image. (This step will be looped)

Step 6: Embed the data bit to be hide in the least significant bit of the cover image one by one.

Let us took the first byte of original data from the Cover image be:

E.g.:- 1 1 0 1 1 0 0 0

First bit of the data to be hidden: 1

Replace the least significant bit

1	1	0	1	1	0	0	0

1	1	0	1	1	0	0	1

This process will be continued for first 8 byte of data and conceal the first byte of data.

step 7: Continue the step 6 for all pixels in the file.

Image after the disclosing process of data using the LSB-1 Steganography.

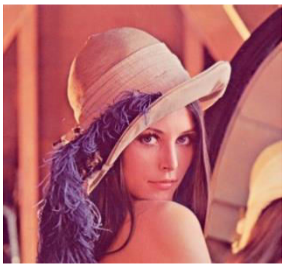


Fig. 1 Cover image

Fig. 2 Stego image

3.2 MSB Steganography

This is another common and simple approach to embedding information in an image. In this method the most significant bit (or the 1st bit) of some or all of the bits inside an image is changed to a bit of the message to be disclosed. Consider an example - a grid of 3 pixels of a 24-bit image can be follows:

(00101101 00011100 01011110)

(10100110 11100100 00001100)

(11011010 10101101 01101011)

When the number 200, whose binary representation is 11001000, is kept in the least significant bit of this part of the image the grid will become as follows:

(00101101 **0**0011100 01011110)

(10100110 **1**1100100 00001100)

(11011010 **1**0101101 01101011)

The number was embedded into the first 8 bits of the grid however only the 5 underlining bits need to be changed according to the disclosed message. Usually half of the bits in an image will need to be modified to hide a secret message using the maximum cover size on an average. As a consequence there are 256 possibilities of varying intensities of each primary color, altering the most significant bit of a pixel results in only a small change in the intensity of the color. These small changes cannot be perceived by the human eye and thus the message is successfully hidden.

Fig.4 Cover image

Fig.5 Stego image

3.3 RGB Steganography

RGB based algorithms are another method of steganography which can be used for hiding text into images. In this method [11] it uses to change the least significant bits of pixel values (3) or sometimes (4) of the rearrangement of colors to create parity bit patterns or least significant bit which correspond to the message being hidden. Along with this variable bit steganography technique is also used in RGB based steganography.

Image after embedding the data using modulus RGB steganography technique.

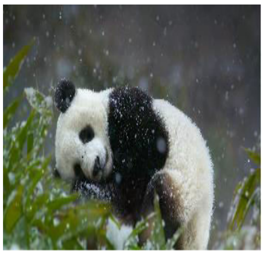


Fig. 5 Cover image

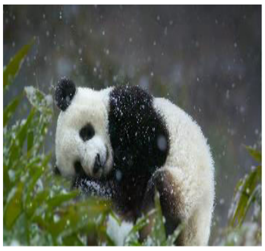


Fig. 6 Stego image

3.4 Pixel Value Differencing Steganography

In this method capacity of each pixel is determined by using the PVD technique. Then password is combined with 5th bit of that pixel to hide the properties of data. On the assumption that the password matches the data is inserted directly and otherwise inverted data is inserted into the pixel. Therefore at some places the data is inserted inverted and at other places it is hidden directly into the image. In case a hacker who does not have the knowledge of secret key tries to extracts the data it is of no use. Another inspection is that size of embedded bit is unknown without key. So with the fault key, the message cannot be resumed. The data disclosing steps are as following:

1) Open the cover image, read the pixels and create the RGB matrixes for color images and gray matrix for gray scale images.

2) Insert the secret key after converting it into bit stream.

3) Determine gray level variation near target pixel and thus determine capacity of that pixel say „n‟.

4) Employ the XOR function on the 5_{th} bit of cover image pixel with one bit taken from the secret key.

5) If password matches, "n‟ bits of message data are embedded in cover pixel.

6) Otherwise data is inverted before embedding.

7) Repeat the steps from 3 to 6 until the whole data is stored into the image.

8) After this the Size of message file is embedded into last 100 bytes using same procedure.

9) Then the data is disclosed into the cover image along with the normal image is saved to get the stego image.

4. EVALUATION CRITERIA OF TECHNOLOGIES

Human Vision cannot identify the small differences in the pictures when comparing a normal image and a stego image which has the embedded text. However there are various evaluation techniques which can be used to find out the differences between original picture and the stego image. When we are inserting message into the picture the image data will be changed slightly. In most cases it will not be noticeable to human eyes but it will affect the size, image quality, and picture information. Correspondingly with the size of content and technique used for steganography the image's noise may be increased. Here we are discussing about some of the available techniques used to find out the changes of digital images.

4.1 PSNR (Peak-Signal to Noise Ratio)

PSNR value of the encoded image (Peak Signal to Noise Ratio) is normally calculated to find the noise of the image.

MSE (Mean Squared Error) is the first value to be calculate using the formula:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

The PSNR is defined as:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

MAX_1 = Maximum possible pixel value of the image.

The minimum value of MSE denotes that both the given images are having almost same kind. Higher the PSNR value denotes the reconstruction is of higher quality. For all type of color images with RGB values per pixel the definition of PSNR is the same except the MSE is the sum over all squared value differences divided by image size and by three. Meanwhile, for color images the image is converted to a different color space and PSNR is reported against each channel of that color space.

The embedding capacity of the image can be tested using the PSNR ratio.

4.2 Root Mean Square Error

The root-mean-square deviation (RMSD) or root-mean-square error (RMSE) is a frequently used measure of the differences between values predicted by a model or an estimator and the values which are actually observed. The root-mean-square deviation will provide us a view of the sample standard deviation or the differences between the predicted values and the observed value. The differences are also called as residuals when the calculations are performed over the data samples that are used for estimation. They are also called prediction errors when computed out-of-sample. The RMSD value helps to collate the magnitudes of the errors in calculations for various times into a single measure of predictive power.

As of these factors the RMSD is generally considered as a good measure of accuracy.

In some disciplines, the RMSD is used to compare differences between two things that may change, no more which is accepted as the "standard". When measuring the average of the difference between two time series ($x_{1,t}$) and ($x_{2,t}$) this formula becomes:

$$\mathrm{RMSD} = \sqrt{\frac{\sum_{t=1}^{n}(x_{1,t} - x_{2,t})^2}{n}}.$$

4.3 Mean Squared Error

The mean squared error (MSE) of an estimator which represents the average of the squares of the "errors", i.e is, the difference in between the estimator and what is estimated. Mean square error is similar to the risk function, which is equivalent to the expected value of the squared error loss or also called as quadratic loss. This distinction comes because of randomness or because the estimator doesn't account for information that could produce a more accurate estimate.

If $\hat{Y}\blacktriangleright$ vector of n predictions and

$Y\rightarrow$ is the vector of examined values corresponding to the inputs to the function which generated the predictions,

$$\mathrm{MSE} = \frac{1}{n}\sum_{i=1}^{n}(\hat{Y_i} - Y_i)^2$$

This is a known value which is a calculated value given for a particular sample (and hence is sample-dependent).

The MSE of estimator $\hat{\theta}$with respect to the unknown parameter $\theta$is defined as

$$\mathrm{MSE}(\hat{\theta}) = \mathrm{E}\left[(\hat{\theta} - \theta)^2\right].$$

The MSE is calculated as the sum of the variance and the squared bias of the estimator or of the predictions. For MSE of an estimator,

$$\mathrm{MSE}(\hat{\theta}) = \mathrm{Var}(\hat{\theta}) + \left(\mathrm{Bias}(\hat{\theta},\theta)\right)^2.$$

4.4 Structural Similarity Index

The structural similarity (SSIM) index is another method for measuring the similarity between two images. SSIM method is a full reference metric because the measuring of image quality is actually based on an initial uncompressed or distortion-free image as a reference. This calculation is designed to improvement over the traditional methods like peak signal-to-noise ratio (PSNR) and mean squared error (MSE), which are proven to be inconsistent with human eye perception.

The difference with respect to other techniques mentioned previously such as MSE or PSNR is that these approaches estimate perceived errors. After all SSIM the image degradation is considered as a perceived deviation in the structural information. Structural information means that the pixels have strong inter-dependencies especially when they are spatially close. These dependencies has important information about the structure of the objects in the visual scene.

The SSIM metric is calculated on various windows or sections of an image. To compute between two positions x and y of common size N×N is:

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

With μ_x the average of x;

μ_y the average of y;
σ^2_x the variance of x;
σ^2_y the variance of y;
σ_{xy} the covariance of x and y;
$c_1=(k_1L)^2$, $c_2=(k_2L)^2$ two variables to stabilize the division with weak denominator;
L the dynamic range of the pixel-values (this is $2^{\#\text{bits per pixel}}-1$);
k_1=0.01 and k_2=0.03 by default.

5. TEST RESULTS

Till now we have discussed about the various Steganography methods as well as the different evaluation criteria to test these methods. Here we are evaluating the above mentioned steganography techniques and analyzing the techniques.

Test1:
The sample image used for testing is image of penguins below. The size of this image is 1.5 MB and the format of the image is .bmp. As part of our tests a standard text message of 445 byte was inserted into the image and then the PSNR, MSE and SSIM value was calculated.

The value of the test images are show below:

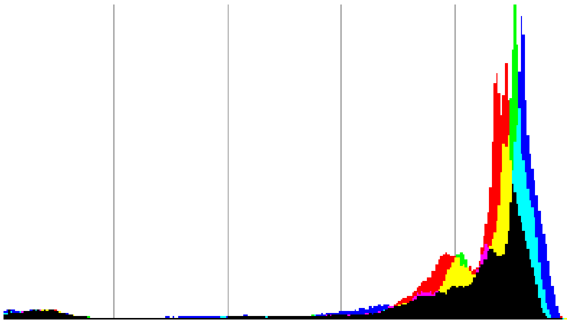
Size of the Cover image	1.5 MB
Format	BMP
Number of Pixels	1614600

Below table depicts the results for each of the steganography methods after embedding the message into the cover image by comparing the original image and the stego image.

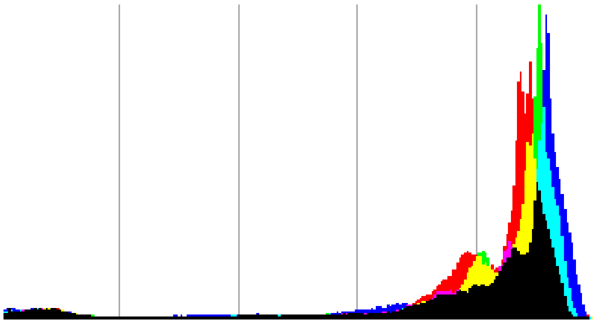
	LSB	MSB	RGB	PVD
PSNR	93.07	92.9	94.2	92.1
MSE	0.00003	0.00003	0.00003	0.00029
SSIM	1.00	1.00	1.0	1.0

Once the message has been embedded in cover image the change in the pixel value will not be noticed to human eyes in the stego image. It is quite hard to find the very minor color changes in the cover and stego image by human eye. To identify this a histogram comparison is used by steganalyst to identify the stego image by comparing the histogram of cover image and stego image.

Based on these tests that have been conducted separate histograms are drawn for cover and stego image.



Histogram – Cover image (Penguin)



Histogram of Penguin image after embedding message
Mean:2014 Median:223 Standard deviation:56.2

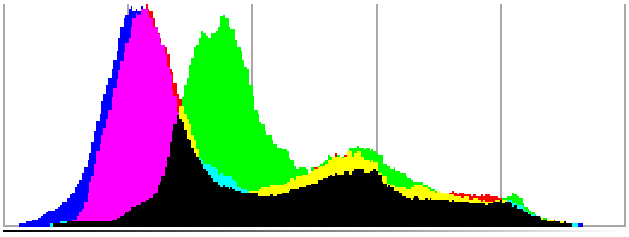
Test2:
The sample image used for test2 is image of squirrel below.

The size of this image is 2.5 MB and format is BMP. As part of the tests a standard text message of 500 byte was inserted into the image and then the PSNR, MSE and SSIM value was calculated.

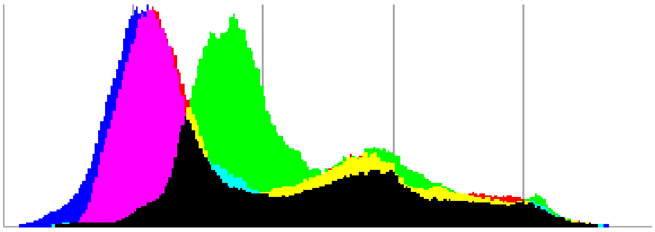
Size of the Cover image	2.5 MB
Format	BMP
Number of pixels	2399296

Below table depicts the results for each of the steganography methods after embedding the message into the cover image by comparing the original image and the stego image.

	LSB	MSB	RGB	PVD
PSNR	92.77	92.5	94.0	92.4
MSE	0.00004	0.00003	0.00003	0.00022
SSIM	1.00	1.00	1.0	1.0



Histogram – Cover image (squirrel)



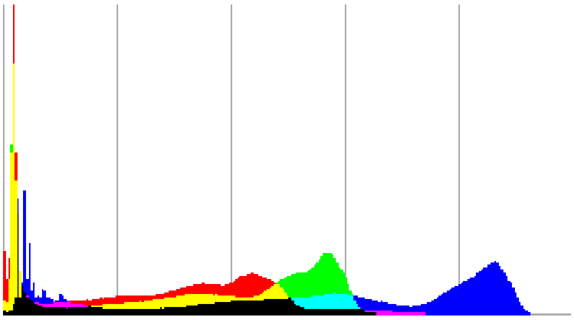
Histogram of squirrel after embedding text
Mean: 100.2 Median:87 Standard deviation:48.5

Test3:
The sample image used for testing is image of Tajmahal below. The size of this image is 5.5 MB and format is BMP. As part of the tests a standard text message of 1000 byte was inserted into the image and then the PSNR, MSE and SSIM value was calculated.
Mean: 96.3 Median: 100 Standard deviation: 67.2

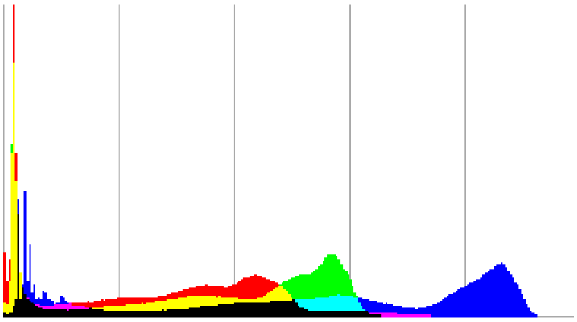
Size of the Cover image	5.5 MB
Format	BMP
Number of pixels	5760000

Below table depicts the results for each of the steganography methods after embedding the message into the cover image by comparing the original image and the stego image.

	LSB	MSB	RGB	PVD
PSNR	90.11	89.9	92.24	90.02
MSE	0.00005	0.00004	0.00004	0.00033
SSIM	1.00	1.00	1.0	1.0



Histogram – Original image (Taj Mahal)



Histogram of Taj Mahal After embedding text

6. CONCLUSION

Steganography method is used to hide data into images without evoking suspicion to hackers as well as other attackers. There is different classification of steganography based on the algorithm used internally. In this paper we have compared LSB, MSB, RGB and PVD methods of steganography and also tested each one of them. The tests were done to identify which one of these methods is better from the other in terms of noise produced and changes made to the pixels. From our tests we could find out that the RGB based steganography method out performs the other methods in terms of PSNR and MSE calculation while SSIM calculation remained the same for all methods. It is also more difficult to identify by hackers when compared with LSB and MSB methods. Hence it is more advantageous over the other two methods for use of steganography.

REFERENCES

[1] Namita Tiwari1, Madhu Shandilya “Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth” International Journal of Security and Its Applications Vol. 4, No. 4. Oct. 2010

[2] Koyi Lakshmi Prasad , Dr. T.Ch.Malleswara Rao “A Novel Secured RGB LSB Steganography with Enhanced StegoImage Quality” *Int. Journal of Engineering Research and Applications* pp.1299-1303.

[3] Mamta Juneja, and Dr. Parvinder S. Sandhu “An Improved LSB based Steganography Technique for RGB Color Images “ 2nd International Conference on Latest Computational Technologies (ICLCT'2013), pp. 10-14, 2013.

[4] Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub “RGB Intensity Based Variable-Bits Image Steganography *IEEE*, pp. 1322-1327, 2008.

[5] Babita, Mrs. Ayushi “Secure Image Steganography Algorithm using RGB Image Format and Encryption Technique” *IJCSET*, pp. 758-762 Jun 2013.

[6] Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi "Pixel Indicator Technique for RGB Image Steganography" http://faculty.kfupm.edu.sa/COE/gutub/Publications/J_m_paper.pdf

[7] Hassan Mathkour and atool Al-Sadoon, Ameur Touir "A New Image Steganography Technique" *IEEE,* pp. 1-4 Oct. 2008.

[8] Qingzhong Liu, Andrew H. Sung, Zhongxue Chen and Xudong Huang "A JPEG-Based Statistically Invisible Steganography "*ICIMCS'11 ACM*, 978-1-4503-0918-9/11/08 2011.

[9] Sheng Dun Hu, & KinTak U "A Novel Video Steganography based on Non-uniform Rectangular Partition" Proceedings of IEEE International Conference on Computational Science & Engineering, pp. 57-61, 2011.

[10] D. R. L. Prasanna, L. Jani Anbarasi and M. Jenila Vincent "A Novel Approach for Secret Data Transfer using Image Steganography and Visual Cryptography" ACM ICCCS pp. 596-599 February 2011

[11] Mandep Kaur, Surbhi Gupta, Parvinder S. Sandhu, Jagdeep Kaur "A Dynamic RGB Intensity Based Steganography Scheme" *World Academy of Science, Engineering and Technology*, pp. 630-633, 2010.

[12] P.Thiyagarajan, G.Aghila and V.Prasanna Venkatesan, "Dynamic Pattern Based Image Steganography "Journal of computing, volume 2, issue 8, august 2010, ISSN: 2151-9617

[13] Ankit Chaudhary, Jaldeep Vasavada, J.L. Raheja. S. Kumar and M. Sharma, "A Hash Based Approach for Secure Keyless Image Steganography in Lossless RGB Images", *The 22nd International Conference on Computer Graphics and Vision*, pp. 80-83, 2012

[14] K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R and L M Patnaik, "Authentication of Secret Information in Image Steganography", *IEEE Region 10 Conference TENCON*, pp. 1-6, 2008.

[15] N Sathisha, Madhusudan G N , Bharathesh S , K Suresh Babu, K B Raja and Venugopal K R "Chaos based Spatial Domain Steganography using MSB" *IEEE International Conference*, pp. 177 - 182 2010.

[16] Chen Ming, Zhang Ru, Niu Xinxin & Yang Yixian "Analysis of Current Steganography Tools: Classifications & Features", *IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp.384 - 387, 2006.

[17] A.E.Mustafa, A.M.F.ElGamal, M.E.ElAlmi, and Ahmed.BD, "A Proposed Algorithm for Steganography In Digital Image Based on Least Significant Bit",*Research Journal Specific Education Faculty of Specific Education Mansoura University*, pp. 752-767, 2011.

[18] Tao Zhang, Wenxiang Li, Yan Zhang, & Xijian Ping "Detection of LSB Matching Steganography Based on Distribution of Pixel Differences in Natural Images" *Proceedings of International Conference on Image Analysis and Signal Processing*, pp. 548-552, 2010.

[19] Lisa M. Marvel, Charles G. Boncelet & Charles T. Retter, "Spread Spectrum Image Steganography", *IEEE Transactions on Image Processing*, pp. 1075-1083, VOL. 8, NO. 8, AUGUST 1999.

[20] B.Padmasri and M.Amutha surabi "Spread Spectrum Image Steganography with Advanced Encryption Key Implementation",*International Journal of Advanced Research in Computer Science and Software Engineering,* pp. 713-720, Volume 3 , Issue 3 , March 2013.

[21] Maria Gkizeli, Dimitris A. Pados and Michael J. Medley, "Optimal Signature Design for Spread-Spectrum Steganography",*IEEE Transactions on Image Processing*, pp. 391- 405, VOL. 16, NO. 2, FEBRUARY 2007.

[22] K. Satish, T. Jayakar, Charles Tobin, K. Madhavi and K. Murali "Chaos Based Spread Spectrum Image Steganography", *IEEE Trans. Consumer Electronics, pp. 587-590,* 2004.

[23] Hsien-Wen Tseng and Hui-Shih Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number", *Journal of Applied Mathematics, Volume 2013 (2013)*, Article ID 189706, pp. 1-8 . http://dx.doi.org/10.1155/2013/189706.

[24] Jeong-Chun Joo, Hae-Yeoun Lee, and Heung-Kyu Lee1 "Improved Steganographic Method Preserving Pixel-Value Differencing Histogram with Modulus Function" , *Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing* Volume 2010, Article ID 249826, 13 pages, doi:10.1155/2010/249826

[25] Weiqi Luo, Fangjun Huang and Jiwu Huang, "A more secure steganography based on adaptive pixel-value differencing scheme", *Multimedia Tools and Applications*, pp. 407-430, Vol. 52 Issue 2-3, April 2011.