A Novel Approach of Encoding for Image Steganography with Reduced Data Content

Ashadeep Kaur
Research Scholar
Sachdeva Engg. College for Girls, Gharuan (Mohali)

Rakesh Kumar
Dept. of CSE
Sachdeva Engg. College for Girls, Gharuan (Mohali)

Nidhi Bhatla
Dept. of CSE
Sachdeva Engg. College for Girls, Gharuan (Mohali)

ABSTRACT
Image Steganography is the technology that is being used to provide secure communication between the sender and the receiver. As the technology enhances, security becomes the important concern. Thus, image Steganography helps in embedding the data behind the image with the original image so that unauthorized user cannot access the data. In this paper, different techniques of image Steganography are discussed. This paper also concludes the comparison of the proposed technique with the existing techniques. Encoding of the data will reduce the risk of data tampering by unauthorized user and increase the security of the system. So the image format conversion is also used that will provide additional security to the data. Experiments have been performed with the proposed and existing technique and result proves that the efficiency of the proposed method is better in terms of security.

Keywords
Steganography; Stego Image; YcBcr; Run Length Encoding; Data hiding

1. INTRODUCTION
With the advancement in the technology, the risk of data tampering and theft also increases. Hence security becomes an important issue .The data needs to be kept secure and safe so that it could be accessed by the authorized personnel. In today's era most of the data travels through the internet. The protection of data is prime concern of the sender. The need is that correct data should be sent but in a secret way that only the receiver should be able to reveal the message. The first technique of cryptography was invented to send secret messages over places. In cryptography the message was encoded in the form of another message in a covered way such that only the sender and receiver knew that how to decrypt it [24]. A cryptographic key was used to decode the message that was known only by the authorized persons.

The word Steganography is a Greek word. In Greek language, it stands for "cover writing". The concept of Steganography was firstly found in Greece. First of all the Steganography was done by hiding the text behind wax on a wooden tablet. Steganography is much better than the cryptography. In Greece, the other way of implementing the concept of Steganography was that the content was hidden by shaving the head of messenger and then letting his hair grow back and hence the message was sent to the destination along with the messenger. The advantages of Steganography are that the data is hidden behind the image and it is only known to sender and receiver.

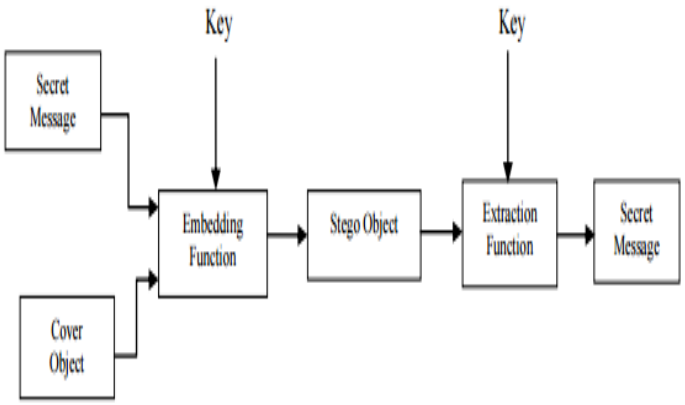


Figure 1.A model of Steganography process with cryptography

1.1 Applications of Steganography
Steganography is applied in various fields for the purpose of security and confidentiality. Following is the list of fields where Steganography is applied:

- Copyright Protection
- Feature Tagging
- Secret Communication
- Use by terrorists
- Digital Watermarking

1.2 Types of Steganography
1.2.1 Text Steganography
i) Format Based Method
ii) Random and Statistical Method
iii) Linguistics Method

1.2.2 Image Steganography

1.2.3 Audio Steganography
i) Low Bit Encoding
ii) Phase Coding
iii) Spread Spectrum

1.2.4 Video Steganography

1.2.5 Network or Protocol Steganography

1.3 Factors that affect the Image Steganography

1) Robustness
2) Imperceptibility
3) Payload Capacity
4) PSNR (Peak Signal to Noise Ratio)
5) MSE (Mean Square Error)
6) SNR (Signal to Noise Ratio)

2. STEGANOGRAPHY TECHNIQUES

2.1 Spatial Domain

In this technique only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in resisting even simple attacks such as compression, transforms [25].

2.1.1 Least Significant Bit (LSB)

This is the most common, simple approach for embedding data in a cover image. The least significant bit (8th bit) of one or all of the bytes inside an image is changed to a bit of the secret message. When we use 24-bit image, three colour bit components are used which are red, green, blue, each byte store 3 bits in every pixel. In this method of spatial domain, least significant bit of image pixel has replaced with the bit of secret data. Thus embedding has done like this with the whole data and acquired image looks similar to the original image as LSB do not make huge difference in the image. This technique does not distort the actual image during embedding of data. Large amount of data can be encrypting behind an image.

Advantages of using LSB

- Robust in nature
- Free from distortion
- Can hide large amount of data.

Drawbacks

- Changes in an image can lose data.
- Hidden data can be restored easily.
- Less secure.

All in all it can send data to the receiver without allowing the intruder to access the encrypted data.

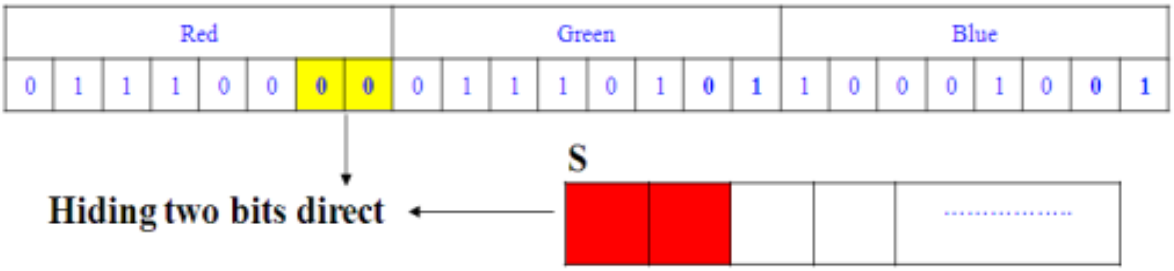


Figure 2 example of LSB in RGB format

Above image shows the LSB in image format where secret data is replaced with the LSB bits of three layers i.e. red, green and blue.

2.1.2 Pixel Value Differencing

It provides both high embedding capacity and outstanding imperceptibility for the stego-image; this segments the cover image into non overlapping [25] blocks containing two connecting pixels and it modifies the pixel difference in each pair for data embedding.

2.1.3 Pixel Indicator

This method gives the stego images of better quality than the traditional method while maintaining a high embedding capacity and it also uses concept of hiding the data using the difference between the pixel values [34]. It's more complex way of hiding information in an image. Transformations are used on the image to hide information. Transform domain embedding can be termed as a domain of embedding techniques in frequency domain; image is represented in terms of its frequencies.

2.2 Frequency Domain

2.2.1 Discrete Cosine Transformation

This method is used for converting the uncompressed image into the format of JPEG compressed image [15]. It is based on data hiding used in the JPEG compression algorithm to transform successive 8x8-pixel blocks of the image from spatial domain to 64 DCT coefficients each in frequency domain [25].The main advantage of this method is its ability to minimize the block like appearance resulting when boundaries between the 8x8 sub-images become visible (known as blocking artefact).

2.2.2 Discrete Wavelet Transformation

It gives the best result of image transformation. It splits the signal into set of basic functions. There are two types of wavelet transformation one is continuous and other is discrete [28]. This is the new idea in the application of wavelets. In this the information is stored in the wavelet coefficients of an image, instead of changing bits of the actual pixels. It also performs local analysis and multi-resolution analysis. DWT transforms the object in wavelet domain and then processes the coefficients and performs inverse wavelet transform to show the original format of the stego object [17].

3. PROBLEM FORMULATION

Steganography is word taken from the two Greek words as "steganos" and "graphie" which mean "concealed" and "writing" respectively. Jointly it referred as concealed (hidden or covered) the message. Steganography is the process of hiding the message before transmit it to the receiver. Data can be hidden within another digital medium such as text, image, audio or video. There are numerous methods of

Steganography available. Various Steganography techniques have been proposed earlier but still the required results were not achieved. So there is a need to propose a new technique of the steganography that is better than the traditional techniques that could increase the security of the system so that the data that is transferred is protected from the unauthorized access.

4. PROPOSED SYSTEM

As steganography is the practice of hiding the data in the image, various techniques have been proposed but still the security of the data that is one of the major concerns while the data is transferred in not achieved. So by studying various techniques a new method is proposed in which the security of the data is increased. Before the data is hided into the image it's encrypted. By encrypting the data, its security level is increased and is not easily detectable. In addition to this, the Image format is also changed from RGB to YcBcR. This will also increase the security of the data.

The main objectives of the proposed work are:

1) To propose a LSB based efficient technique of image steganography.
2) To increase the security of the data by applying RLE encoding and RLE decoding respectively.
3) To generate the stego image by converting RGB format into YCBCR format at the sender side, contrary at the receiver side.

5. METHODOLOGY

This section describes the methodology and block diagram of proposed technique for image Steganography. The working of the technique is divided into two parts: encoding and decoding respectively. The block diagram of proposed technique is as follows:

5.1 Encoding

1. First step is to read the image from database for the purpose of embedding data on it. This selected image is used as cover image for data hiding.
2. In this step the selected image is converted into YcBcr format from RGB.
3. After image conversion the text to be hidden is entered from user.
4. An encoding technique is applied to the text for making it much secure from data tampering. RLE is applied to encode the data.
5. In this step the text is hidden behind cover image.
6. After data hiding, the image is generated that is observed after hiding the data. This image is referred as Stego image.
7. Now the Stego image is converted to the RGB format.
8. In last step the performance parameters such as MSE and PSNR etc are calculated.

5.1.1 Block Diagram of Encoding

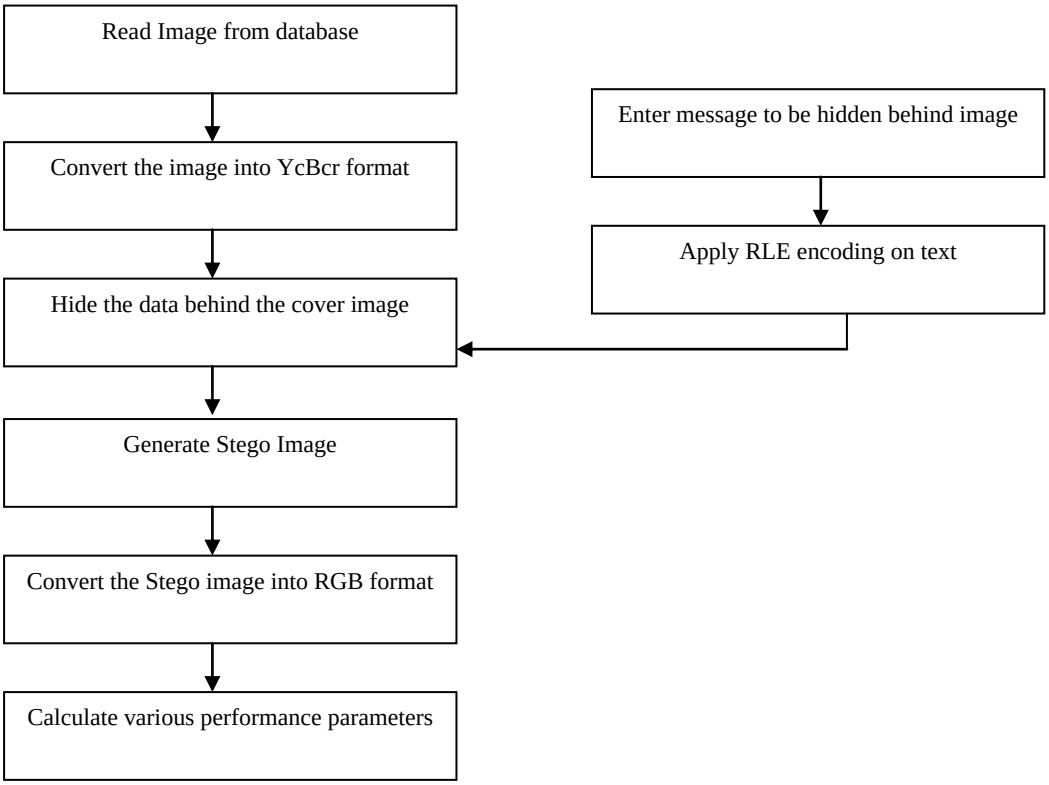


Figure 3.Block diagram of encoding in proposed technique.

5.2 Decoding

1. For decoding first of all select the Stego image.
2. Now conversion is performed from RGB to YcBcr format.
3. Then the extraction is performed on image. In this phase the hidden text is separated from the image.
4. After extraction, RLE technique is applied on observed image for decoding it.
5. In last step, the actual text is observed which is same as the original text or message before encryption.

5.2.1 Block Diagram of Decoding

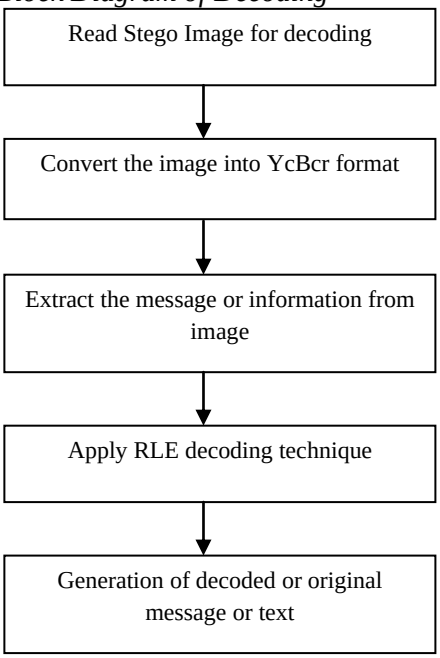
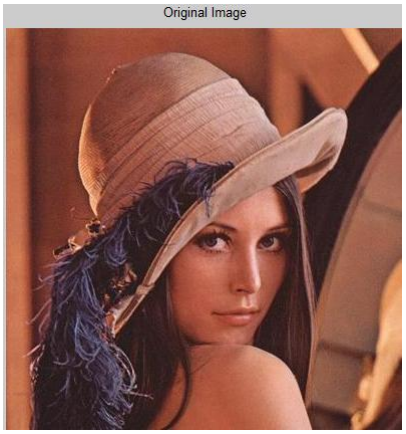


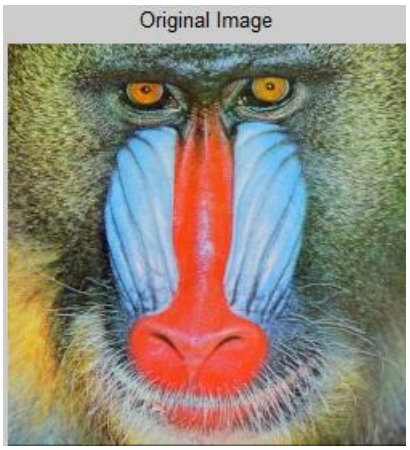
Figure 4.Block diagram of decoding in proposed technique

6. RESULTS AND DISCUSSIONS

In this section the output of the proposed technique is represented. This section describes the obtained results after applying the proposed technique. It also includes the comparison with the existing techniques. In our proposed technique we have used LSB-YcBcr which makes our technique more efficient as compared to others. The performance of the proposed technique is proved by the following results:



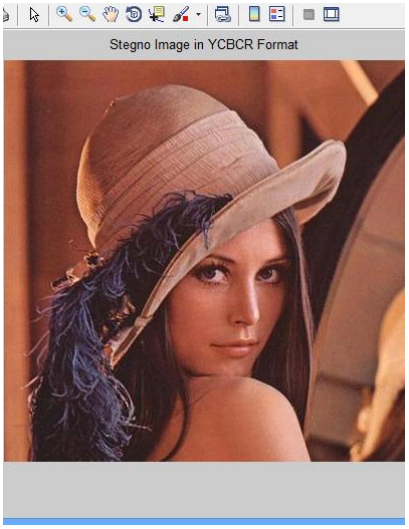
(A)



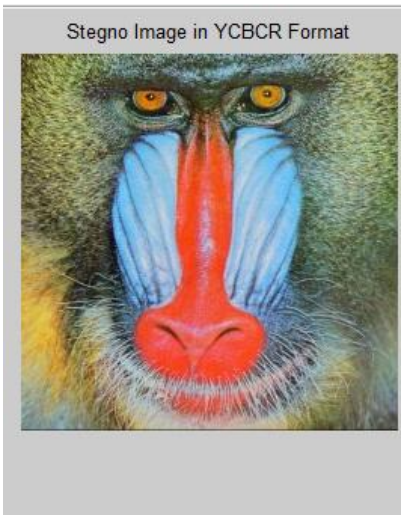
(B)

Figure 5.Sample of images before encoding the data on it.

Figure 5 represents the original images. These images are used for hiding the data. These images are referred as original images because these images are before implementing the encoding techniques.



(A)



(B)

Figure6.Acquired images after performing Steganography.

Figure 6 represents the images after performing encoding. Text that has been hidden under the original images and obtained images after performing Steganography is same.

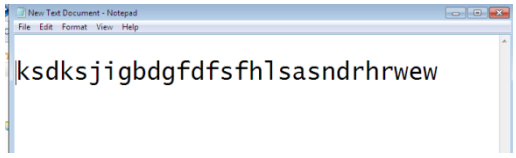


Figure 7.Original message before encoding or hiding.

Figure 7 represents the original message which is encrypted or hidden behind the image. This message is before applying the encryption technique.

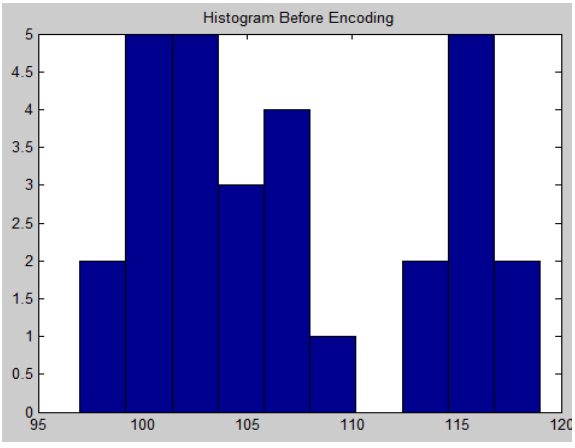


Figure 8.Histogram before encoding the data or message.

Figure 8 represents a Histogram graph which is obtained before encoding the data or message.

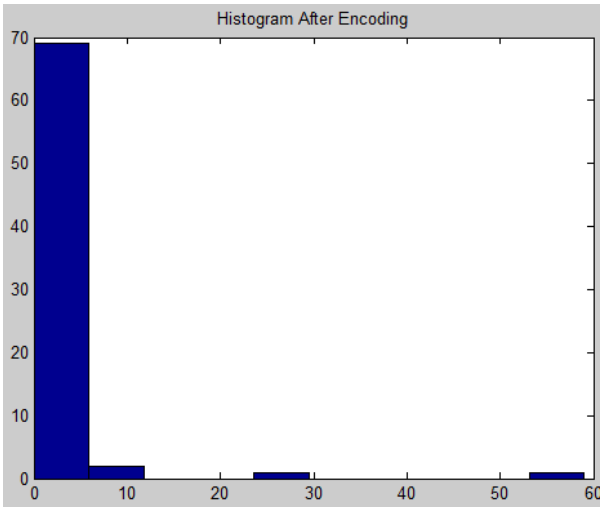


Figure 9.Histogram after encoding the data or message.

Figure 9 represents a Histogram graph which is obtained after encoding the data or message.

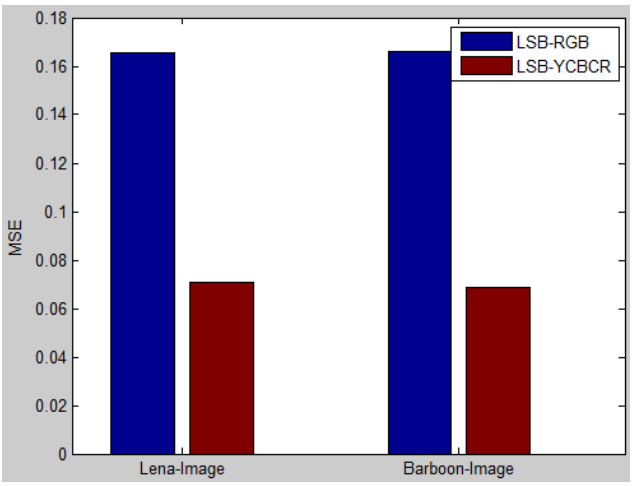


Figure 10.Comparison of MSE between proposed and LSB-RGB technique with respect to both images.

In figure 10 Graph shows the comparison between MSE of proposed and traditional technique in case of both images. MSE is Mean Square Error which should be low. Hence from above image it is observed that the MSE of proposed technique is low in both of the images as compared to LSB-RGB technique.

The following equation can be used in order to check the quality of the technique.

$$\text{MSE (t)} = \frac{1}{n}\sum_{i=1}^{k} f_i(x_i - t)^2 = \sum_{i=1}^{k} p_i(x_i - t)^2 \quad \text{.....(1)}$$

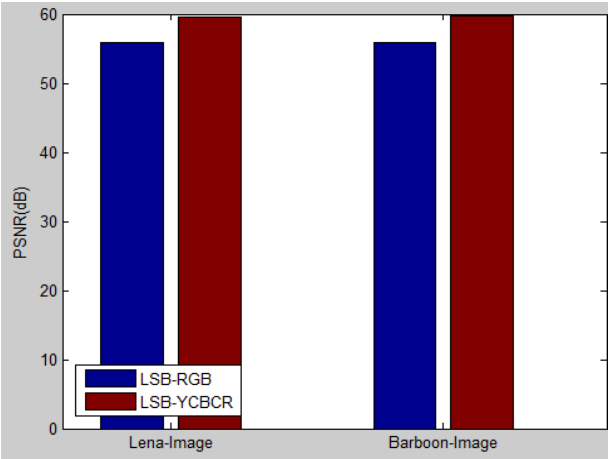


Figure 11.Comparison of PSNR between proposed and LSB_RGB technique with respect to both images.

In figure 11 Graph shows the comparison between PSNR of proposed and traditional technique in case of both images. PSNR stands for Peak Signal to Noise Ratio, it should be high. Hence from above image it is observed that the PSNR of proposed technique is high in both of the images as compared to LSB-RGB technique.

Equation 2 and 3 mentioned below can be used for calculation of PSNR.

$$PSNR=10\log_{10}\frac{(L-1)^2}{RMS} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Where

$$RMS=\frac{1}{m.n}\sum_{i=1}^{\infty}\sum_{j=1}^{n}(x_{i,j}-x'_{i,j})^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

Table 1. Performance of existing and proposed technique based on two parameters using image1

Techniques	MSE	PSNR
Existing	0.17	55
Proposed	0.07	60

Table 2. Performance of existing and proposed technique based on two parameters using image2

Techniques	MSE	PSNR
Existing	0.17	55
Proposed	0.065	60

Above tables represent the comparison of old and proposed technique using two different images. Resultant values show that proposed technique outperforms. As PSNR of both images in the proposed technique is high i.e. 60 MSE is less i.e. 0.07 and 0.065 respectively.

7. CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

Image Steganography is the technique that is being used to provide security to the system. In this process, image is hidden into another image (Stego image) for the security purpose. Text is embedded in the image. It can be visible or invisible depending on the type of technique. Image Steganography does not change the actual meaning of the data. It just hides the data into another data or image. This paper concludes that the proposed technique is much efficient than the techniques used before. In this method, first format of the image is changed. Then encoding technique is applied to the embedded data. Thus, proposed work and the experiments applied on both the images show the efficiency of the techniques. It concludes that the proposed technique is more secure and efficient than the existing techniques.

7.2 Future Scope

There are numerous techniques that have been used in the Steganography process. But in this proposed method, first data is encoded before it is embedded into the image. Thus, this method is more secure and efficient than the traditional methods. This technique can be enhanced with the help of other conversion techniques. Security of the network can be enhanced with the combination of two or more techniques to prevent unauthorized access.

8. REFERENCES

[1] M. Kameswara Rao (2015). *Security Enhancement in Image Steganography a MATLAB Approach*. Journal of scientific research, Vol 23(2), Pp 357-361.

[2] Parmar Ajit Kumar Maganbha (2015). *A Study and literature Review on Image Steganography*. IJCSIT, vol 6(1), Pp 686-688.

[3] Shikha Mohan (2015). *Image Steganography: Classification, Application and Algorithms*. IJCEM, Vol 1(10), Pp 93-97.

[4] A Rashi Singh (2014). *Review on Image Steganography*. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Volume 4, Issue 5,Pp 686-689.

[5] Chaitali R. Gaidhani (2014). *Image Steganography for Message Hiding Using Genetic*. IJCSE, vol 2(3), Pp 67-70.

[6] Chin-Chen Chang (2014). *Meaningful Shadows for Image Secret Sharing with Steganography and Authentication Techniques*. Journal of information hiding and data processing, vol 5(3), Pp 342-352.

[7] Jasleen Kour (2014). *Steganography Techniques –A Review Paper*. International Journal of Emerging Research in Management &Technology ,Volume-3, Issue-5, pp 132-135.

[8] Mamta Juneja (2014). *Improved LSB based Steganography Techniques for Color Images in Spatial Domain*. IJNS, vol 16(6), Pp 452-462.

[9] Mohammad Sajid Khan (2014). *Encryption Based Steganography- Modern Approach for Information Security*. IJCSIT, Vol. 5 (3) , Pp 2914-2917.

[10] Prof.Pramod Khandare (2014). *Data Hiding Technique Using Steganography*. IJCSIT, Vol. 5 (2) , Pp 1785-1787.

[11] Sabyasachi Pramanik (2014). *Image Steganography Using Wavelet Transform And Genetic Algorithm*. IJIRAE, vol 1(1), Pp 17-20.

[12] Shemi P B (August-2014). *An Enhanced Image Steganography Technique in Art Images*. IJCSMC, Vol.3 Issue.8, pg. 613-621.

[13] Shrutika Suri (2014). *Comparative Analysis of Steganography for Coloured Images*. JCSE, vol 2(4), Pp 180-184.

[14] Takashi Mihara (2014). *A New Framework of Steganography Using the Content of Cover Data*. Journal of information hiding and multimedia signal processing, Vol 5(2), Pp 117-123.

[15] AL-Shatnawi, Atallah M.,and Bader M. AlFawwaz (2013). *An Integrated Image Steganography System with Improved Image Quality*. Applied Mathematical Sciences 7.71 : 3545-3553.

[16] Anil Kumar (2013). *A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique*. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, Pp 363-372.

[17] Banik Bamali Gupta and Samir K Bandvopadhvay (2013). *A DWT Method for Image Steganography*. International Journal 3.6.

[18] C.P.Sumathi (2013). *A Study of Various Steganographic Techniques Used for Information Hiding*. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, 9,Pp 9-25.

[19] Goel, Arun Rana, and Stuti Manpreet Kaur (2013). *A Review of Comparison Techniques of Image Steganography*. Global Journal of Computer Science and Technology 13.4.

[20] Mehdi Hussain (2013). *A Survey of Image Steganography Techniques.* International Journal of Advanced Science and Technology Vol. 54,Pp 113-124.

[21] Stuti Goel (2013). *A Review of Comparison Techniques of Image Steganography*. Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 , pp 8-14.

[22] Swati malik, Ajit (May 2013). *Securing Data by Using Cryptography with Steganography.* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5.

[23] Soni, A., Jain, J., Roshan, R. (March 2013). *Image Steganography using discrete fractional Fourier transform*. Intelligent Systems and Signal Processing (ISSP), International Conference, vol., no., pp.97,100.

[24] Atallah M (2012). *A New Method in Image Steganography with Improved Image Quality*. Applied Mathematical Sciences, Vol. 6, no. 79, 3907 – 3915.

[25] Bhattacharyya, Souvik, and Gautam Sanyal (2012). *A Robust Image Steganography using DWT Difference Modulation (DWTDM).* International Journal of Computer Network & Information Security 4.7.

[26] J. K. Mandal (2012). *Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain.* International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, Pp 83-93.

[27] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat (July 2012). *Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique.* International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197.

[28] Saddaf rubab and M Younus (February 2012). *Improved Image Steganography Technique for Colored Images using Wavelet Transform*. International Journal of Computer Applications 39(14):29-32, Published by Foundation of Computer Science, New York, USA.

[29] Masud Karim, S.M.; Rahman, M.S.; Hossain, M.I. (December 2011). *A new approach for LSB based image Steganography using secret key.* Computer and Information Technology (ICCIT), 14th International Conference, vol., no., pp.286,291.

[30] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU. (2007). *A new Steganographic method for color and gray scale image hiding*. Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194.

[31] Deshpande Neeta, Kamalapur Snehal, DaisyJacobs (2007). *Implementation of LSB Steganography and Its Evaluation for Various Bits*. Digital Information Management, 1st International conference.pp 173-178.

[32] Komal Hirachandani. *New Approach of Information Security through Steganography by using Wavelet Transformation and Symmetric Encryption*. IJCSIT, vol 5(5), Pp 6253-6260.

[33] R.Poornima**.** *An Overview of Digital Image Steganography*. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1, Pp 23 -31.

[34] Sohag, Saeed Ahmed, Md Kabirul Islam, and Md Baharul Islam. *A Novel Approach for Image Steganography Using Dynamic Substitution and Secret key.*