ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

An Efficient Data Hiding in Digital Colour Image by Sparse Representation

Prof. Rohini Nipanikar, Pratibha More

Assistant Professor, Dept. of ECE, PVPIT, Pune, Maharashtra, India[1]

PG Student [VLSI & EMBEDDED SYSTEM], Dept. of ECE, PVPIT, Pune, Maharashtra, India[2]

ABSTRACT: Steganography is one form of cryptography where we hide data within images. Reversible data hiding is a form of steganography in which we hide data within images, audio, video form. In reversible data hiding the original cover can be recovered without loss after the embedded messages are extracted. The project proposes the improvement of security system for secret data communication through multi plane image data embedding in Colour images or gray-scale images. A given input image is converted to any one plane of RGB colour image. After completion of plane separation, the secret data will hide into the image pixels. The data hiding technique uses the LSB algorithm for hiding the secret message bits into the input cover image. In the data extraction, the secret data will be extracted by using relevant key for choosing the image pixels STEGO image to get the information about the data. The performance of this technique in Colour Image and data hiding will be analysed based on image and data. This paper presents a result of LSB method with sparse representation and chaos algorithm. Another RDH technique, histogram shifting is compared with LSB method, both methods displays result with sparse representation.

KEYWORDS: RDH, LSB, chaos algorithm, Sparse representation, Histogram Shifting.

I.INTRODUCTION

Data hiding is a technique used to put a secret data in a host media like images with small changes in host. In most of the data hiding techniques the cover image becomes distorted due to data hiding process and it cannot be retrieved back to the original form. Thus the cover media due to the data embedding. In some applications, such as medical applications and military applications, recovery of the original cover image without any damage is a must, since these images have too process further. The process of recovering the cover or host image without any damage after the secret data extraction is known as reversible data hiding. LSB technique is supported by manipulating the least-significant-bit (LSB) planes by directly substituting the LSBs of the cover-image with the secret message bits. LSB method achieve high capacity. Now a day's advancement in computer networks, signal processing and digital multimedia are spread widely through the internet. This causes security issues of exposing transmitted digital data on the network with high risk of being copied or intercepted illegally. In order to safeguard the privacy of data, various data hiding techniques have been proposed to encrypt the data before data transmission.

II.SYSTEM MODEL AND ASSUMPTIONS

An efficient data hiding in digital colour image by sparse representation uses the following aspects:

1) Sparse representation
2) Chaos encryption
3) Embedding using LSB
4) Histogram Shifting

This proposed method is based on the LSB substitution. Here input image is 24-bit colour image. We can take any format of the image like BMP, GIF, JPEG, and PNG. We use colour image so next part is to separate the R, G, and B plane with each of 8-bit plane. After plane separation the sparse coding is applied to each plane of the RGB image. The secret data is hidden in each R, G and B plane in same manner.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Data embedding:

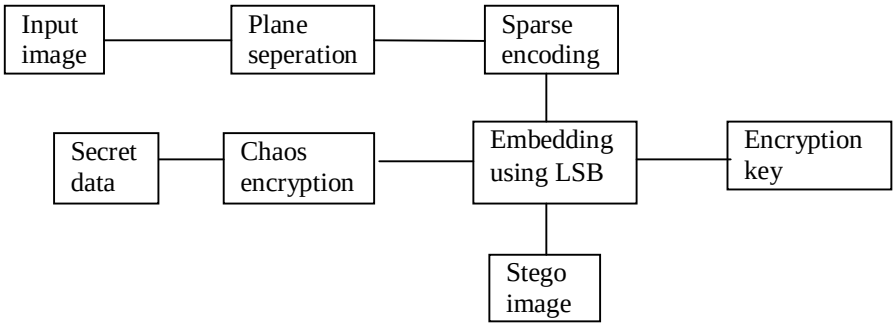

Fig.1 data embedding

In the data embedding process, first we have to take any high quality colour image. In this image we have to hide our secret data. After that the colour image is separated into the different planes like R, G, and B. The sparse encoding is applied to all separated planes and after the sparse encoding encryption we get stego image. The secret data is encrypted by using chaos encryption, which is converted into the ASCII format. Then LSB algorithm is used for the embedding process. Final output is the sparse encoded stego image.

Data Extraction:

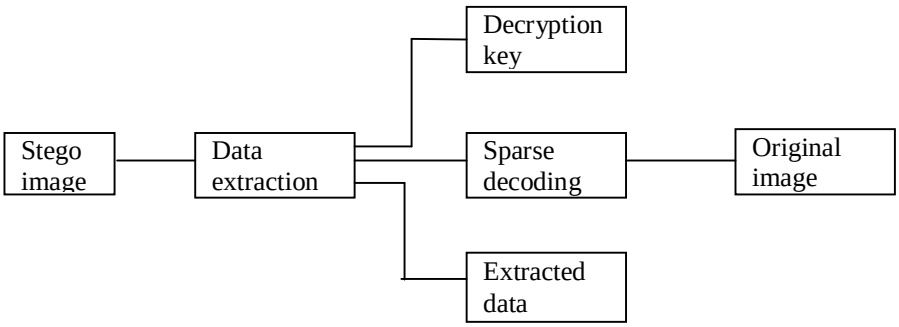

Fig.2 data extraction

The stego image generated at the end of the data embedding part is the input of the data extraction process. The data is extracted by using the chaos decryption. Here the reverse process of the embedding part is used. Sparse decoding is used to decode the image and get the extracted data. After the sparse decoding we can get the original image with high quality. This is the brief idea related to the proposed method. Following section gives us details about the whole process.

A) Sparse representation

Signals carry overwhelming amounts of data in which applicable information is often more difficult to find. Processing is faster and simpler in a sparse representation where few coefficients disclose the information we are looking for. Such representations can be established by decomposing signals over elementary waveforms selected in a family called a dictionary. Given a cover image, we first divide it into small patches that are then represented according to an dictionary via sparse coding. The dictionary contains number of images for the sparse representation. Here, the dictionary contains 10 sample images. By using the dimension of that images the dictionary is created. For the creating dictionary, first we have to take the dimension of the small patches.

B) Chaos encryption

Chaos encryption is one of the advanced encryption standard to encrypt the image for secure data transmission. It encrypts the indigenous image pixel values with encryption key value caused from chaotic sequence with threshold

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

function by bit x-or operation. Logistic map is used for generation of chaotic map sequence. It is very useful to transmit the secret image through unsecure channel securely which stops data hacking chance. The chaotic systems are based on a complex or real number space called as boundary continuous space. Chaos theory generally aims that to understand the asymptotic activities of the iterative progression the properties essential for chaotic systems designed for cryptography is sensible to an initial condition with topology transitivity. Following fig.3 shows the process flow of chaos algorithm.

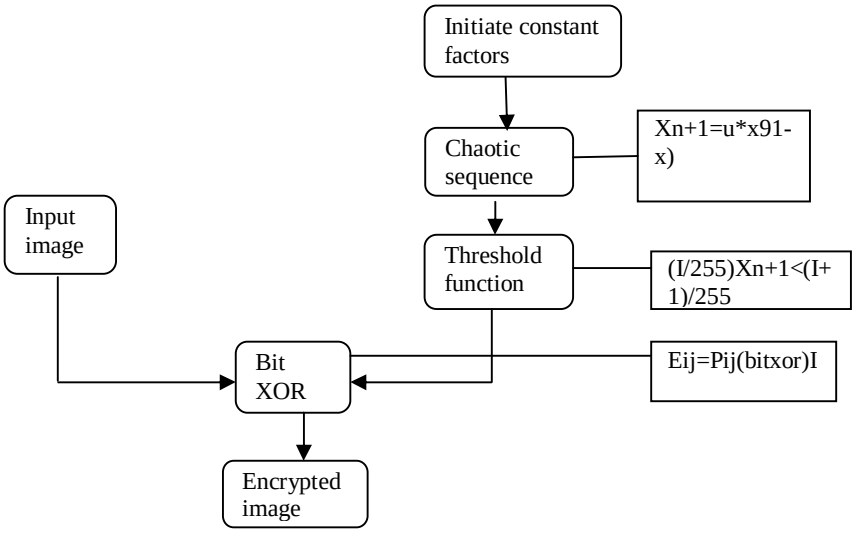

Fig.3 chaos process flow

In that the two initiate constant factors are fixed for each evaluation. By using the equation, Xn+1=u*x(1-x) chaotic sequence is generated. Threshold function is calculated by using equation (I/255)<Xn+1<(I+1)/255. Then threshold point and input image compared by bit xor operation Eij=Pij(bitxor) I. Finally, we get the encrypted image

C)LSB embedding

The most widely used stenography method is the technique of LSB substitution. In a gray-scale image, every pixel consists of 8 bits. One pixel can hence display 28=256 variations. Here we use the color image having 24 bits. The weighting configuration of an 8-bit number with MSB and LSB bits is as shown in Figure.

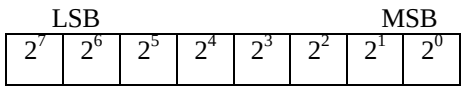

Fig.4 weighting of an 8-bit pixel

The simple idea behind of LSB substitution is to embed the secret data at the rightmost bits, so that the embedding procedure does not affect the original pixel value. The mathematical representation for LSB method is:

x represents the i th pixel value of the stego-image, i x represents that of the original cover-image, and i m represents the decimal value of the i th block in secret data. The number of LSBs to be replaced is denoted as k. The extraction process is same the k-rightmost bits directly. Furthermore, the secret data might be easily captured by extracting the k-rightmost bits directly.

In LSB substitution method, a pseudo-random number generator is used to randomly issue and hide the bits of a secret message into the least significant bits of the pixels within a carrier image, called the cover image. A popular approach to achieve this is the random interval method. Both communication parties allocate a stego-key, k able to use as a seed for a random number generator. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. This is usually accomplished with two complementary techniques:

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

The LSB is the simplest spatial domain watermarking technique to embed secret data in the least significant bits of the cover image. Example of least significant bit is:
Image:
10010101 00111011 11001101 01010101….
Watermark:
0 1 0 1…..
Watermarked Image:
1001010 **0** 0011101**1** 1100110**0** 0101010**1**…..

The steps used to embed the watermark in the original image by using the LSB:
1) Convert RGB colour image to grey scale image.

2) Make double precision for image.

3) Shift most significant bits to low significant bits of cover image.

4) Make LSB bit of host image zero.

5) Add shifted version (step 3) of cover image to modified (step 4) host image.
The advantage of this method is that it is easily performed on images. And it provides high perceptual transparency. When we embed the watermark by using LSB the quality of the image will not devalue. The main drawback of LSB technique is its poor robustness to common signal processing operations because by using this technique watermark can easily be destroyed by any signal processing attacks. It is not vulnerable to attacks and noise but it is very much invisible. A major advantage of the LSB algorithm is it is quick and easy. There has also been steganography software expanded which work around LSB colour alterations.LSB insertion also works well with gray-scale images.

C) Histogram Shifting
An image histogram is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. Histogram based data hiding technique embeds the data in the cover media by shifting the histogram of the image. Histogram technique finds peak or zero points in the histogram and data embeddingis done by shifting these peak and zero points. This technique yields higher data hiding capacity with low distortion. Histogram based reversible data hiding method was introduced by Niet al., where message is embedded within the histogram. Embedding is done by shifting the peak and zero points of the histogram.

III. RESULT AND DISCUSSION

The Quality of the reconstructed image is measured in terms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image and the reconstructed image at decoder is defined as:

$$\text{MSE} = \sigma_q^2 = \frac{1}{N} \sum_{j,k} (f[j,k] - g[j,k])^2$$

Where the sum j, k shows the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is defined as:

$$\text{PSNR} = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are not virtually seperable by human eyes.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

Correlation Coefficient: It is used to indicate the similarity between two different images with their intensities. It will be defined as, Cor_coef = [sum (sum (u1.*u2))] / [sqrt (sum(sum(u1.*u1))*sum(sum(u2.*u2)))];

Fig. 5 and 6 shows the results of both the method LSB substitution and Histogram shifting. These figs includes the sparse encoding, stego image, sparse encoding encryption image, plane seperation etc.

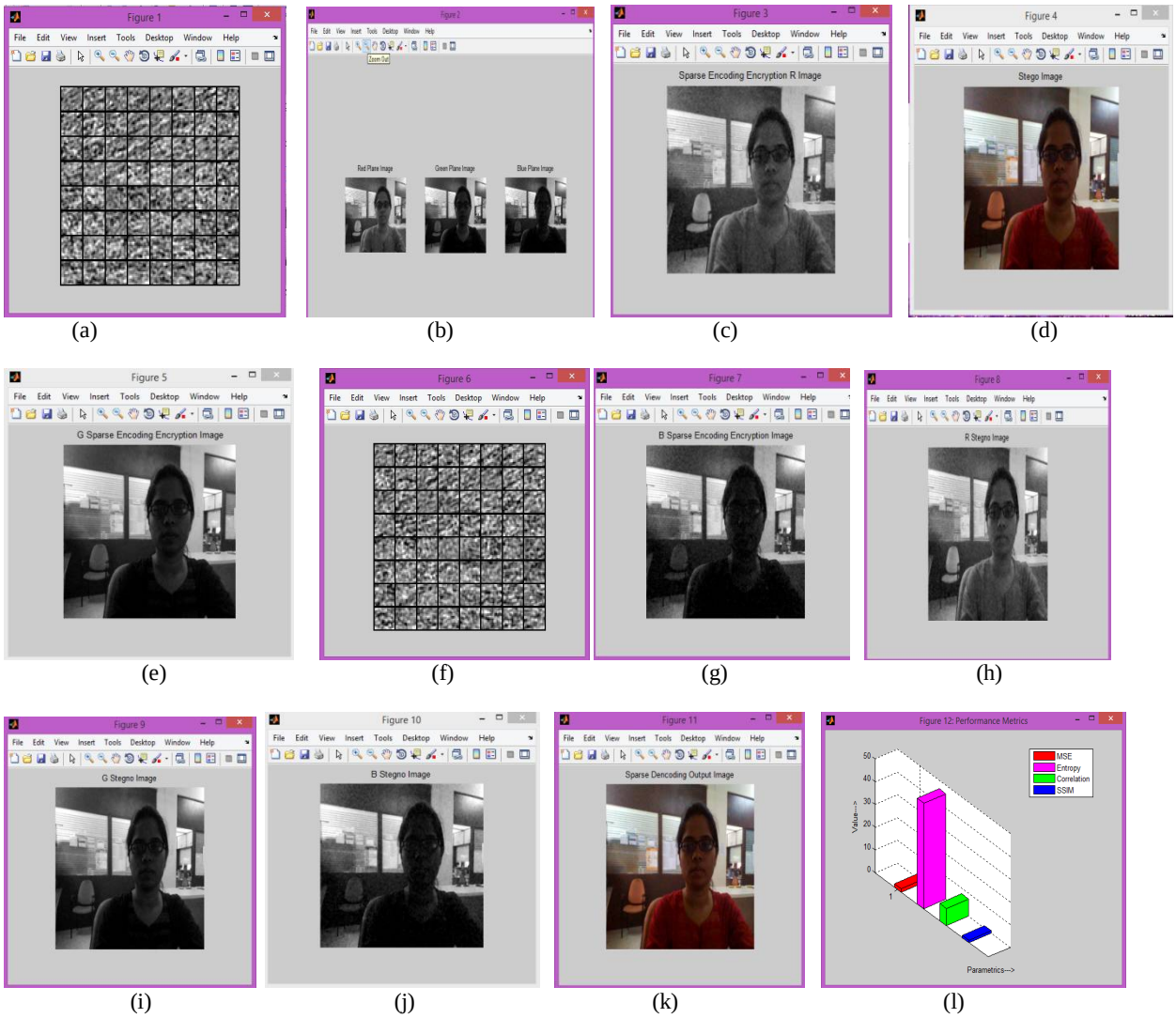

Fig.5 Result of LSB method with sparse encoding a) R plane sparse encoding b) plane separation c) sparse encoding encryption R image d) stego image e) G sparse encoding encryption image f) B plane sparse encoding g) B stego image encryption image h) R stego image) G stego image j) B stego image k) sparse decoding output image l) performance metrics.

The result of the LSB method indicated by the above images. Fig (a) shows the R plane sparse encoding while fig (b) indicate the plane separation. After that sparse encoding encryption is done which shows in fig (c). In this way we get the three separate plane B and G in fig (e) and (f) respectively. At the last the image (k) indicates the sparse decoding output image. Finally fig (l) indicates the performance parameters. In this way we can get the LSB methods test result.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

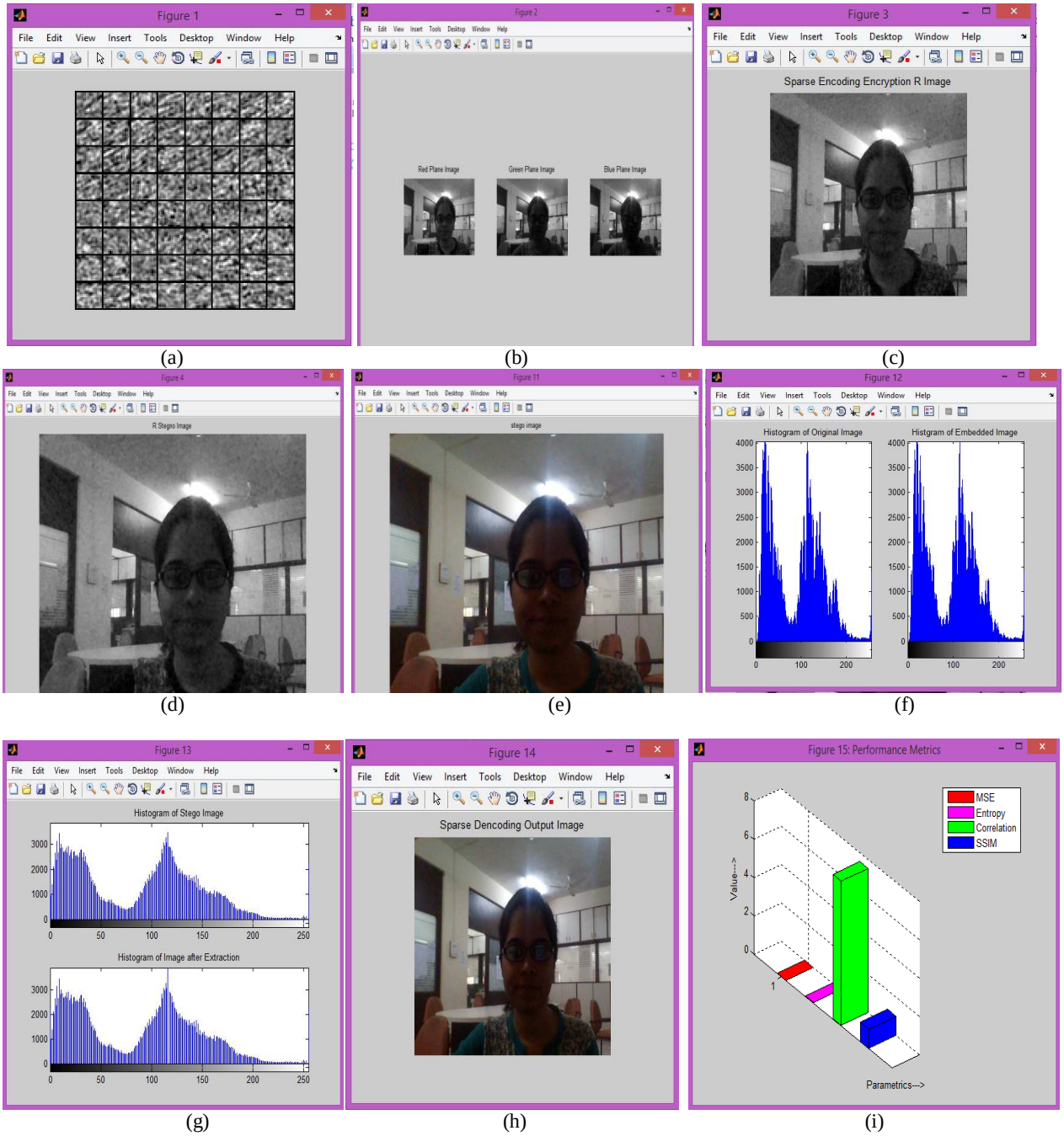

Fig.6 Results of histogram shifting method a) sparse encoding b) plane sepearation c) sparse encoding encryption R plane d) R stego image e) stego image f) histogram output imagesg) histogram images h) sparse decoding output image i) performance matrics.

The above fig, indicates the result of the histogram shifting method, in that fig (a) shows the sparse encoding, fig (b) shows the plane separation, fig (c) shows the sparse encoding encryption of R plane, fig (d) shows the R stego image. In this way we can get three separate stego image of each plane. By adding these three separate plane we get one stego image which indicates the image (e). Fig (f) shows the histogram of the original image and the embedded image while fig (g) shows the histogram of the stego image and the histogram of stego image after encryption. Fig (h) shows the

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijareeie.com

Vol. 6, Issue 5, May 2017

sparse decoding output image. Finally the image (i) indicates the performance metrics such as, MSE, Entropy, Correlation, and SSIM. In this way, the data hide in cover image by using the histogram shifting method.

IV.CONCLUSION

This paper has proposed a method of embedding through LSB substitution which is more beneficial because of the sparse representation. Compared to another data hiding for colour images our method is much larger used. The data hider simply adopts the bit replacement to substitute the secret data. The data extraction and cover image recovery are seperable, and are error free. The experimental results on the colour image by LSB have demonstrated that our MSE is 1.4563, PSNR is 46.4982 and entropy is 7.7189. On the other hand by using the Histogram Shifting, our MSE is 0.0032, PSNR is 73.0734. Hence we can say that the PSNR of Histogram Shifting is greater.

V. ACKNOWLEDGMENT

This work was supported by PVPIT, Bvdhan, Pune. This work is based on LSB Substitution method and Histogram Shifting method.

REFERENCES

[1] R.Rathna Krupa, “An Overview of Image Hiding Techniques in Image Processing”, The SIJ Transactions on Computer Science Engineering & its Applications (CSEA) Vol. 2, No. 2, March-April 2014.
[2] Preeti Parashar and Rajeev Kumar Singh, “A Survey: Digital Image Watermarking Techniques”, International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp.111-124.
[3] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Steganography", In Proceedings of the Fifth Annual Information Security South Africa Conference,(ISSA2005), Sandton, South Africa, June/July 2005.
[4] Prabhishek Singh, R S Chadha, “A Survey of Digital Watermarking Techniques, Applications and Attacks”, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 9, March 2013.
[5] Rathika R, Prof.S.Kumaresan,” Survey on Reversible Data Hiding Techniques”, 2016 3rd International Conference on Advanced Computing and Communication Systems (ICACCS -2016), Jan. 22 – 23, 2016, Coimbatore, INDIA.
[6] Manu Devi, Nidhi Sharma, "Improved Detection of Least Significant Bit Steganography Algorithms in Color and Gray Scale Images", In: Proc.IEEE Raecs UIET Panjab University Chandigarh, March 2014.
[7] Mehdi Hussain, Mureed Hussain, "A Survey of Image Steganography Techniques", International Journal of Advanced Science and Technology (/JAST), Vo1.54 pp.113- 123, May 2013.
[8] Mamta Juneja, Dr. Parvinder S. Sandhu, "An Improved LSB based Steganography Technique for RGB Color Images", 2nd International Conference on Latest Computational Technologies (lCLCT), London (UK), June 2013.
[9] Xin Zhang, Weibin Chen, “A New Chaotic Algorithm for Image Encryption”, pp 889-892 IEEE ICALIP2008.
[10] Xiaochun Cao, ” High Capacity Reversible Data Hiding in Encrypted Images by Patch-Level Sparse Representation”, IEEE Transactions on Cybernetics, vol. 46, NO. 5, May 2016.