IMAGE ENCRYCPTION AND DECRYPTION USING RANDOM IMAGE KEY

[1]A. Vyasa Bharadwaja, [2]M. Bhuvaeswari Devi, [3]CH.Pavan kumar , [4]B.pavan sai, [5] G.Gopi Venkata Raja Reddy

[1]Assistant Professor, [2]UG Student, [3]UG Student, [4]UG Student, [5]UG Student

[1,2,3,4,5] Department of Electronics and Communication Engineering,

[1,2,3,4,5] Godavari Institute of Engineering and Technology, Rajahmundry, India.

1.ABSTRACT:

Internet plays an important role in circulating a huge amount of multimedia.To send an image over the network secretly, the sender tries to find encryption algorithm to hide image information. This project aims at designing an efficient encryption algorithm for color image using random image key generated with minimum time execution for encryption and decryption operations. XOR operation is used here to provide high level of security to the data.

2.INTRODUCTION:

Image processing involves changing the nature of an image in order to either

1. Improve its pictorial information for human interpretation
2. Render it more suitable for autonomous machine perception.

In this project, an image encryption method based on a new random key generated from the same image is going to be adopted. The previous related work takes into account to review the points of power in these studies and to see how researchers think in this field. and decryption process are as shown in the Sample encryption following figure 3.1.

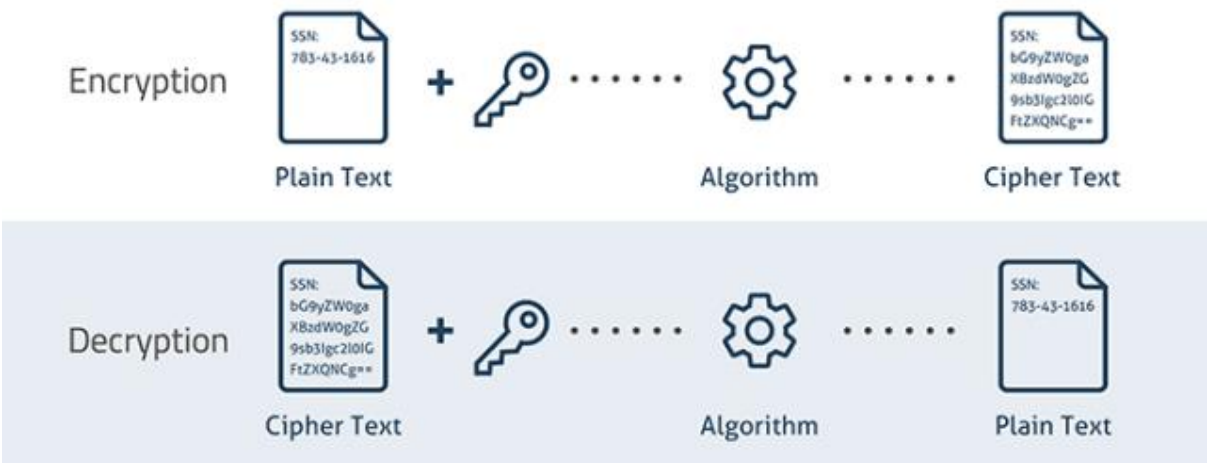

Figure 2.1: Sample Encryption and Decryption Process

Image Cryptosystem can be classified into two main sections; one for encryption and the other for decryption. The block cipher and stream cipher are two types of cryptosystem, so private key and public key are two strategies to be used in an encryption. In this paper a new algorithm is proposed to encrypt color image using symmetric key which is generated from the same image or any image can be selected. Some tests are applied here to determine performance algorithm. These are histogram, mean square error, peak signal to noise ratio, entropy, correlation coefficients, number of changing pixel rate and unified averaged changed intensity [2]. The proposed algorithm was satisfied with good results where speed of running was good for encryption and decryption algorithm.

3.LITERATURE SURVEY:

In this section many studies are summarized here to survey some ideas about the image encryption during the last years. Pratibha S. Ghode et al. [1] improved a keyless method for image cipher in lossless color images to encrypt and decrypt image without any loss of data quality. Khanzadi H. et al. [2] proposed an image encryption algorithm using bit sequence random generator based on Chaotic Logistic and Tent maps. Mirzaei et al. [3] introduced a new parallel algorithm for image encryption. First of all, the plain image is divided into 4 equal blocks and then the position of each block is shuffled.Then a total shuffling algorithm is applied to the whole image. After this, we use different values for encrypting each pixel in each of the 4 blocks of the whole image. Wei et al. [4] introduced image encryption algorithm depending on Deoxyribonucleic acid (DNA) and chaotic system. As well as using Hamming distance to generate the secret keys. However, Panduranga and Naveen [5] proposed a hybrid approach for partial image encryption to rearrange the mapping image and select a pixel value of re-arranged mapping image based on the mapping function through converting the pixel value of original image into a row and column values of mapping image. Ibrahim and Maaly [6] present a new effective approach for image encryption which employs the main Discrete Fourier Transform (DFT) followed by Differential Evolution (DE) approach.

4.PROPOSED ALGORITHM:

In this section,fast algorithm is proposed here to encrypt and decrypt color image. Proposed algorithm applies for any size of image. In symmetric image encryption, the sender and thereceiver must share the same key. In this paper, a new algorithm is designed to generate image key from the same image or any image selected with the aid of the sender. XOR logic plays the main role in this algorithm. The basic idea is cutting the picture where not everyone can recognize them, especially if it has been cut horizontally and vertically into smaller parts as much as possible. In this paper, image key is generated according to this idea by rotating the origin image to three directions. The four pictures are cut and mixed haphazardly then utilizing XOR rationale to produce picture key.The four pictures are cut and mixed haphazardly then

utilizing XOR rationale to produce picture key. The algorithm can be illustrated through the following algorithm.

Image Key Generating Algorithm Steps:

1. Input color image.
2. Rotate color image to three directions (left, right and down).
3. Cutting and random permutation each image which get from step 1 and 2.
4. Create essential key from stage 3 utilizing XOR rationale.
5. Examination essential key to three channels (R, G and B)..
6. Analysis primary key to three channels (R, G and B).
7. Flip R to three directions (left to right, up to down and right to left)
8. Rotate R and flip it to three directions (left to right, up to down and right to left)
9. For all matrixes generated in steps 6 and 7 use XOR to get new R.
10. Repeat steps from 6-8 to get new G and New B.
11. Reconstruct R, G and B to new image.
12. Use XOR between origin image in step1 and new image in step 9.
13. Examination picture in sync 11 to three channels (R, G and B).
14. Apply XOR for R, G and B to generate image key.
15. End.

5.BLOCK DIAGRAM:

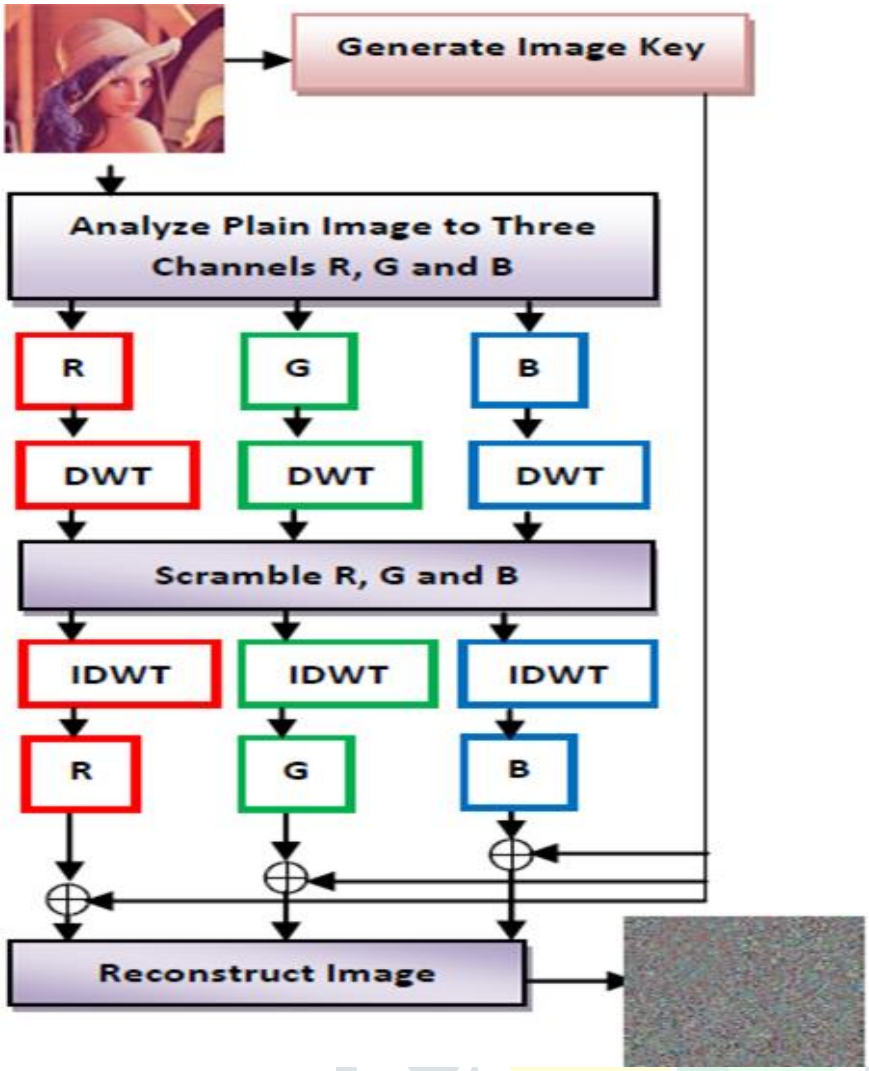

Figure 5.1: Proposed Decryption Algorithm

The steps of proposed encryption algorithm can be illustrated as below:

1. Input plain color picture or image
2. Create mystery key from the plain colour picture or colour image
3. Get R, G, and B components for color picture or colur image.
4. Extract features for R, G, and B using Wavelet Transform.
5. Scramble each R, G, and B.
6. Use Inverse Wavelet Transform to obtain new picture or image.
7. Encrypt every channel by secret key which is produced using XOR.
8. Combine R, G, and B channels to create the cipher color picture or colour image.
9. Save cipher image.
10. End.

Decryption image can be obtained by reverse algorithm where the symmetric key is the same as illustrated in figure 4.2.

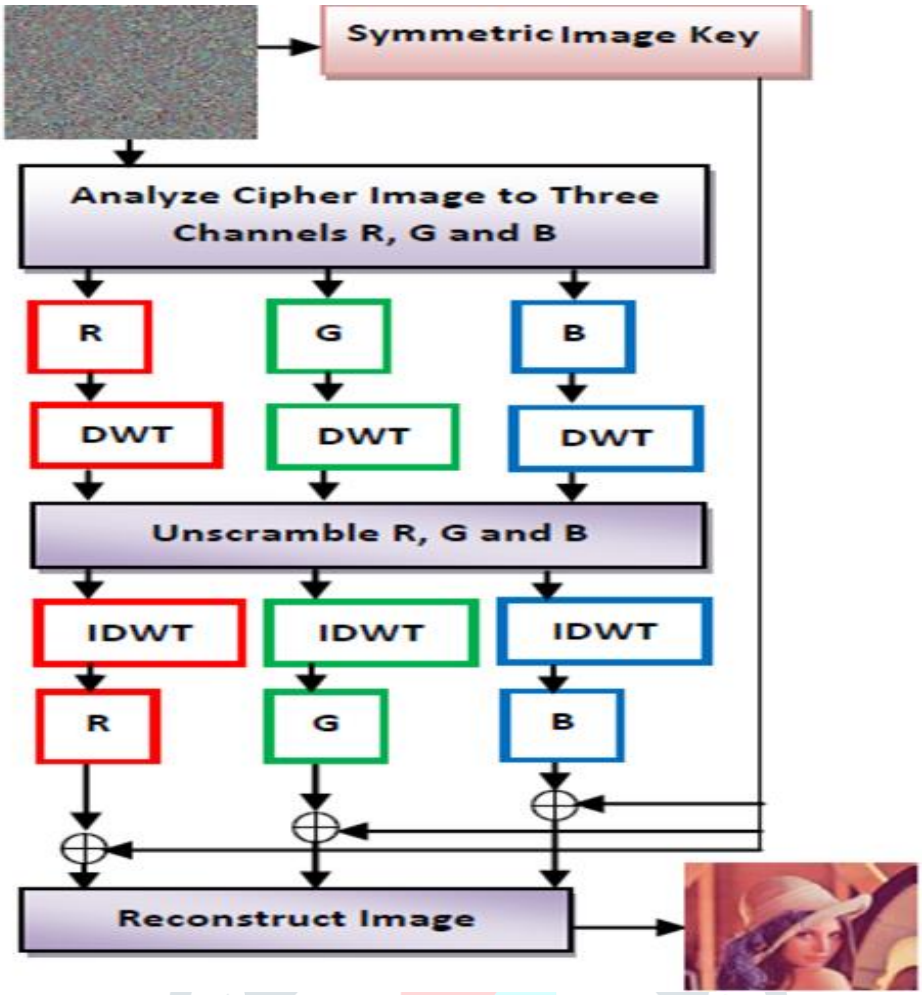

Figure 5.2: Proposed Decryption Algorithm

The steps of proposed decryption algorithm can be illustrated as below:

1. Input plain color picture or colour image.
2. Get R, G, and B components for color picture or colour image.
3. Extract features for R, G, and B using Wavelet Transform.
4. Unscramble each R, G, and B.
5. Use Inverse Wavelet Transform to get new image.
6. Decrypt every channel by using secret key which is produced using XOR.
7. Combine R, G, and B channels to recover the plain color picture or colour image.
8. Display origin image.
9. End.

6.SIMULATION RESULTS:

Proposed encryption algorithm is implemented using MATLAB R2013a on a personal computer running Windows. The color images with size 256 by 256 are used as input image through the application of the proposed algorithm. In this section, several tests are taken into account. For example, Histograms are to be considered for better understanding.

Histogram is statistics measure which is can be used to supply image statistics. It is a representation of color image by distributing the number of pixels to each value. The Figure gives us a good idea about histogram for a color image, for instance, where distributed pixels values for image encryption are equal to prevent attacker from access origin image.Red, green and blue channels of inception picture are decayed here for a similar picture or image.

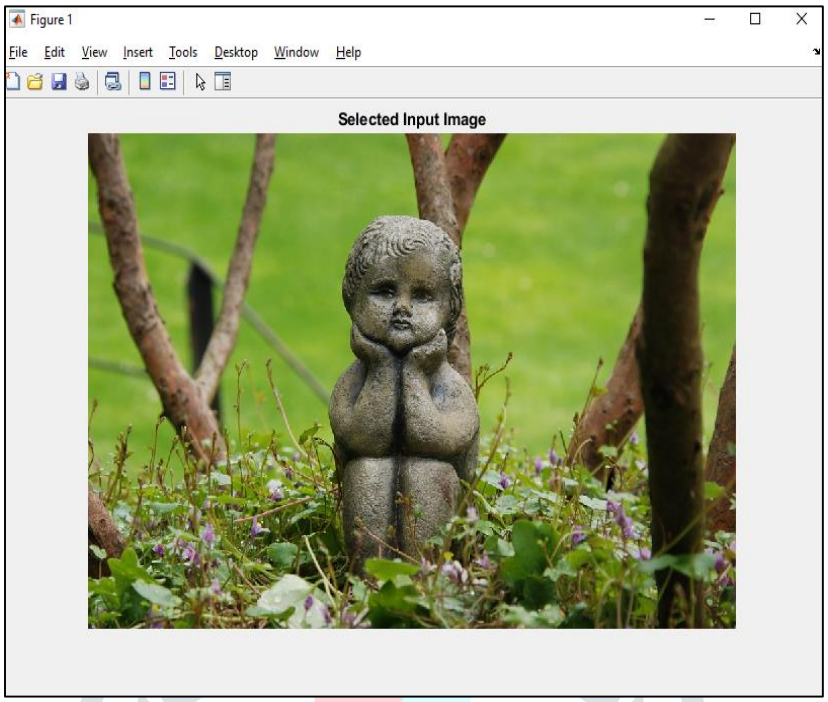

Figure 6.1: Selected Input image

Figure 6.2: R, G and B Channel extraction of input image

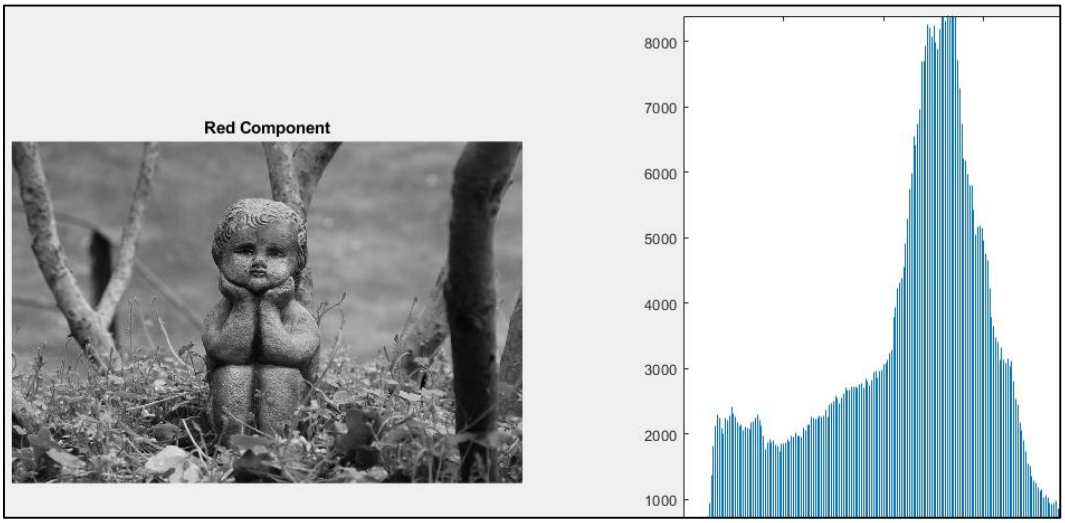

Figure 6.3: Red component of an image with its Histogram

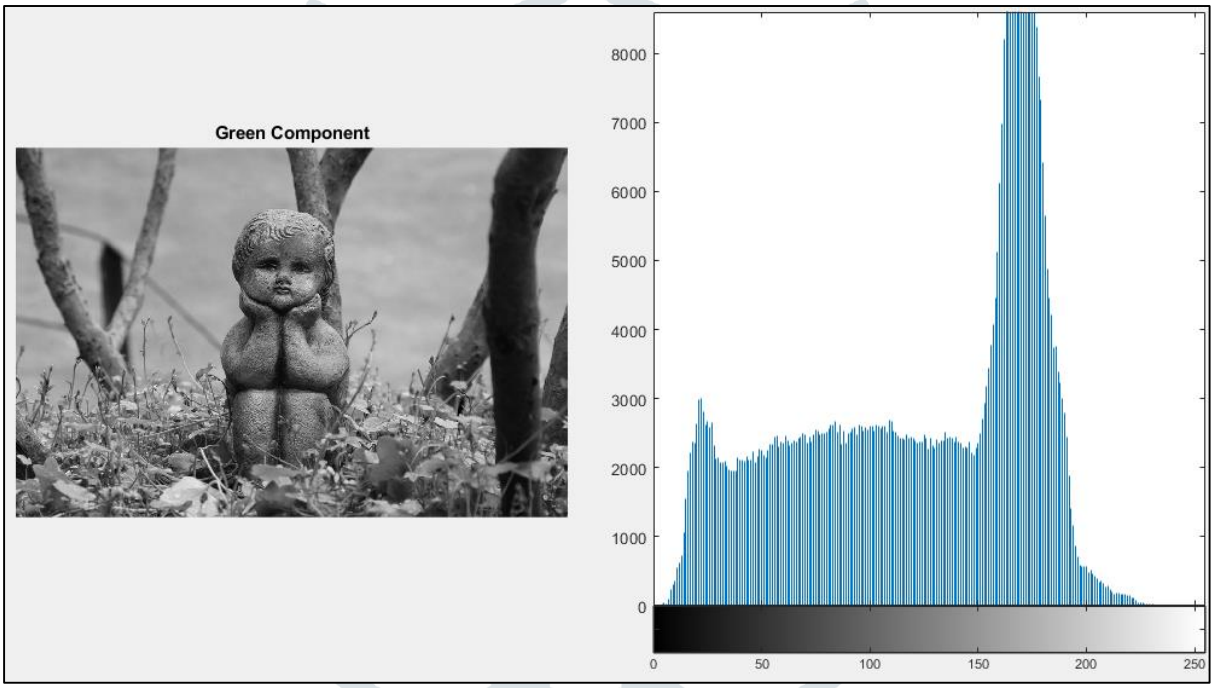

Figure 6.4: Green component of an image with its Histogram

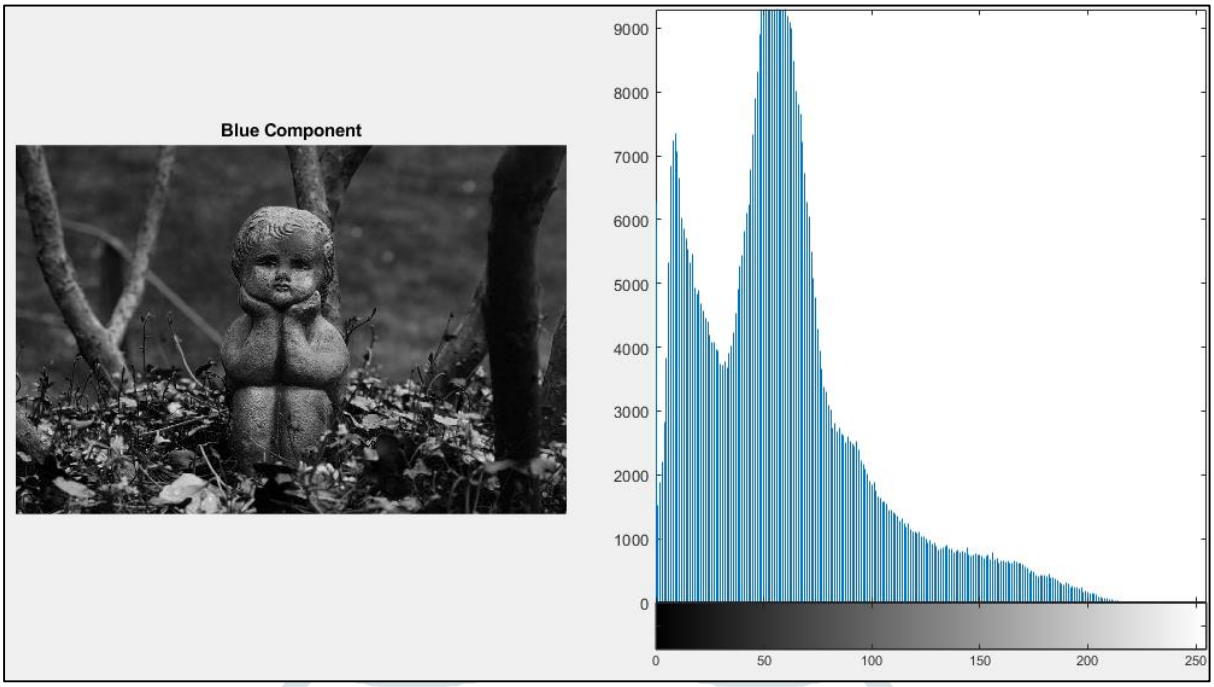

Figure 6.5: Blue component of an image with its Histogram

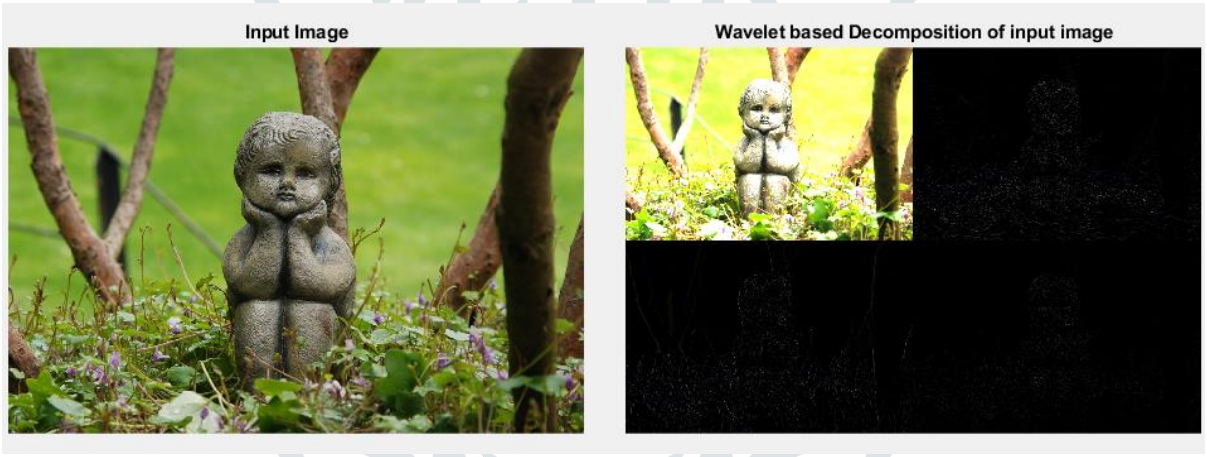

Figure 6.6: Wavelet based decomposed image

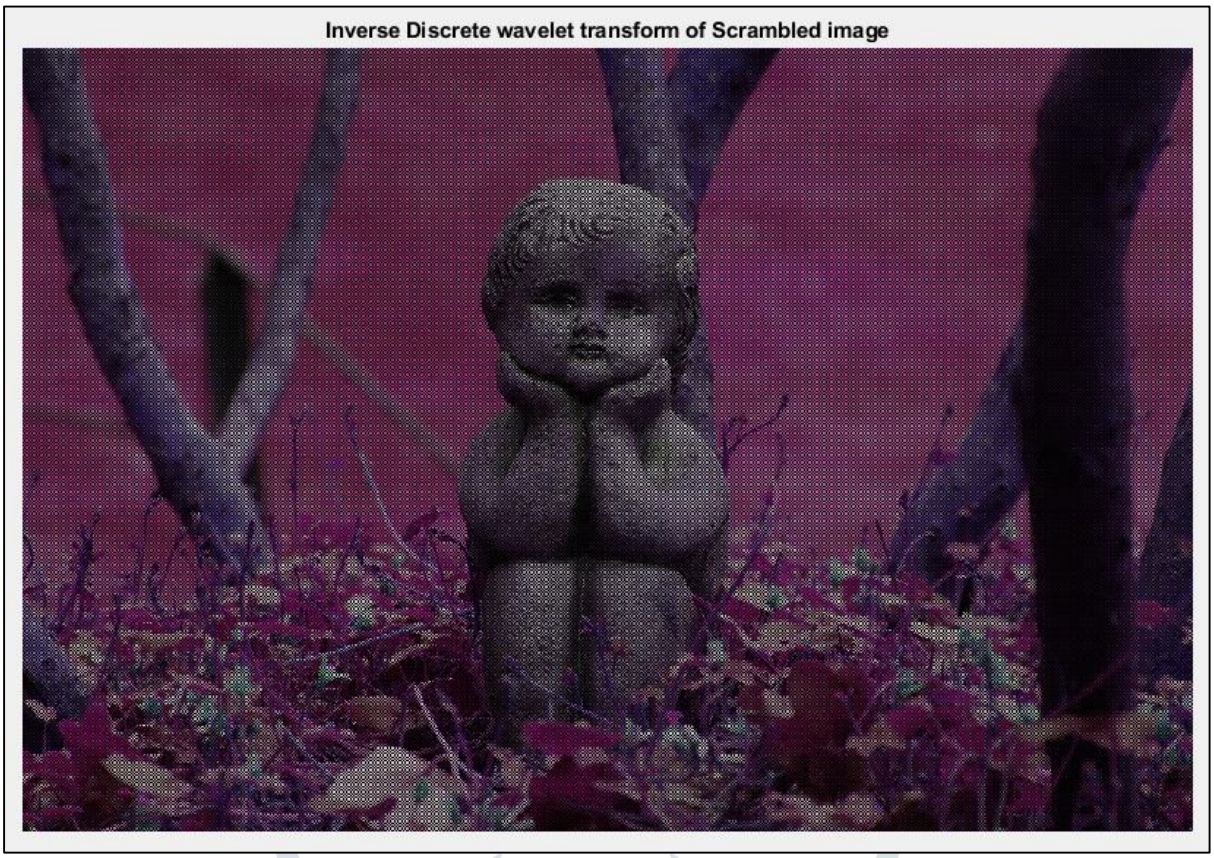

Figure 6.7: Inverse Discrete Wavelet transform of Scrambled image

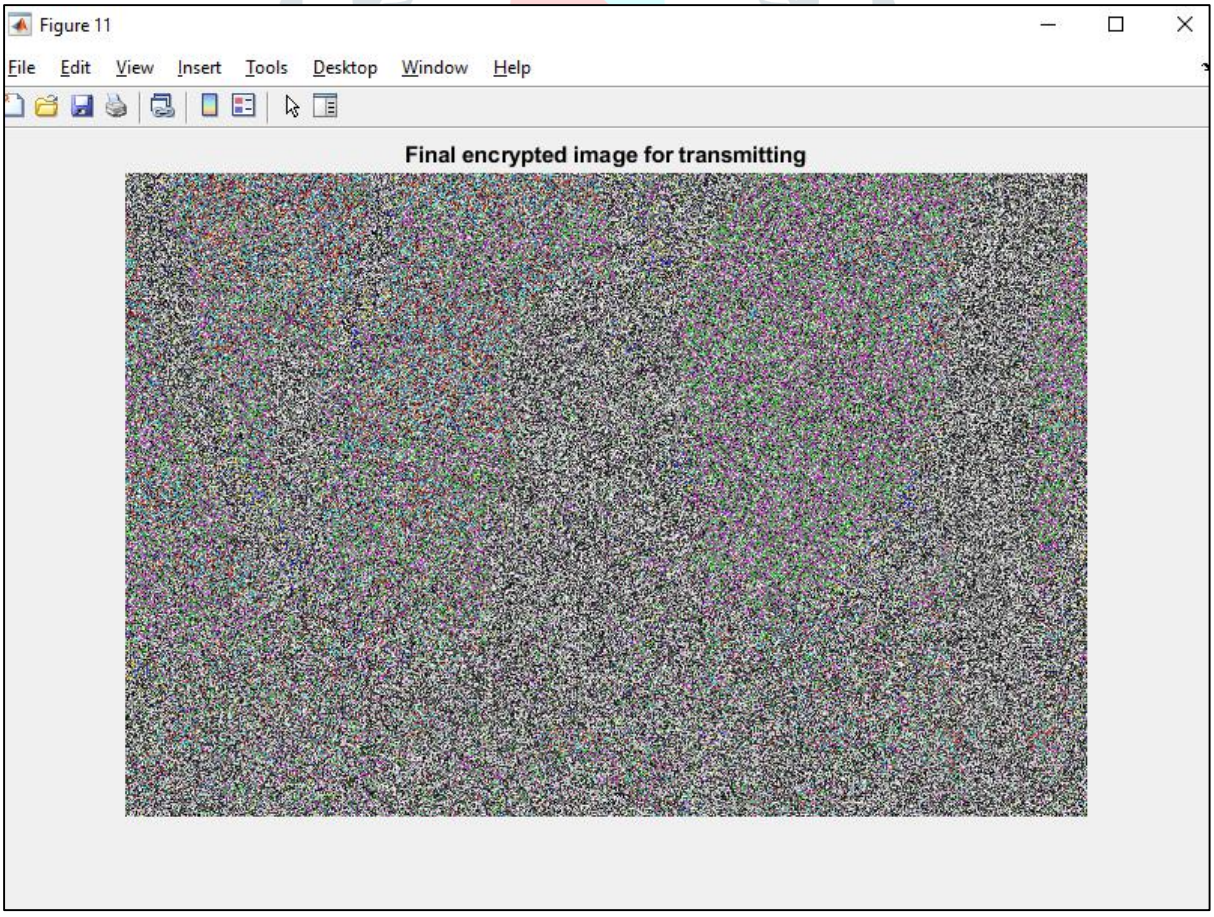

Figure 6.8: Final encrypted image for transmitting over the channel

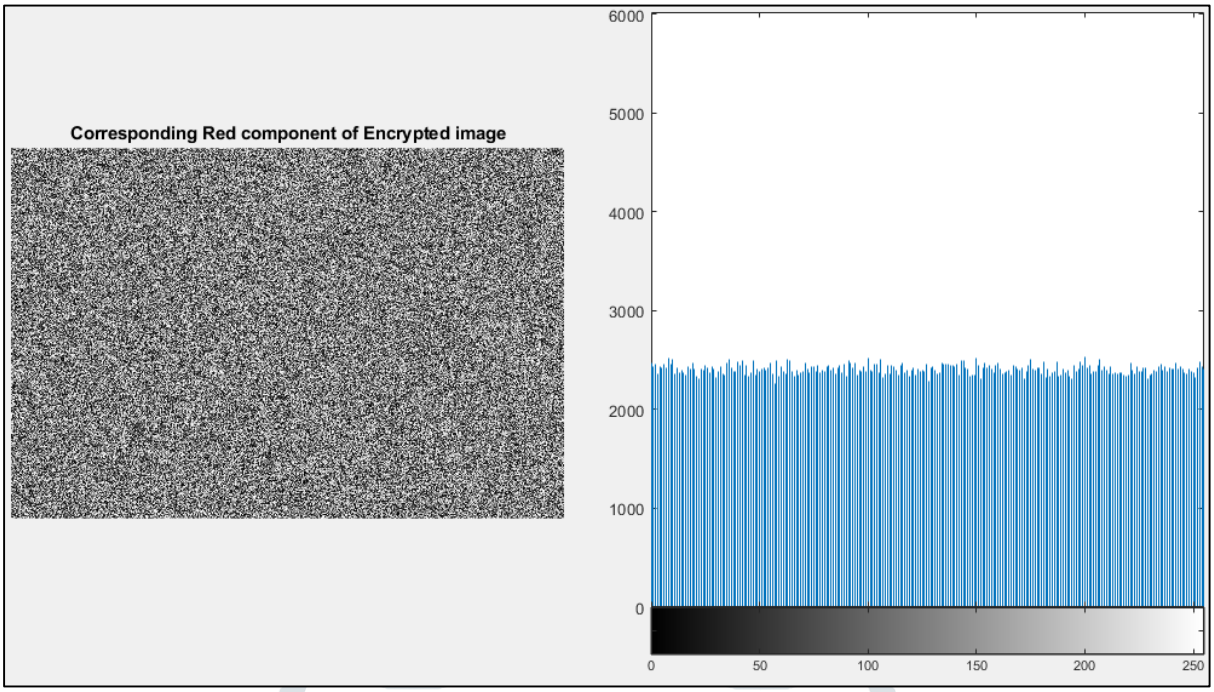

Figure 6.9: Histogram for the red channel of encrypted image

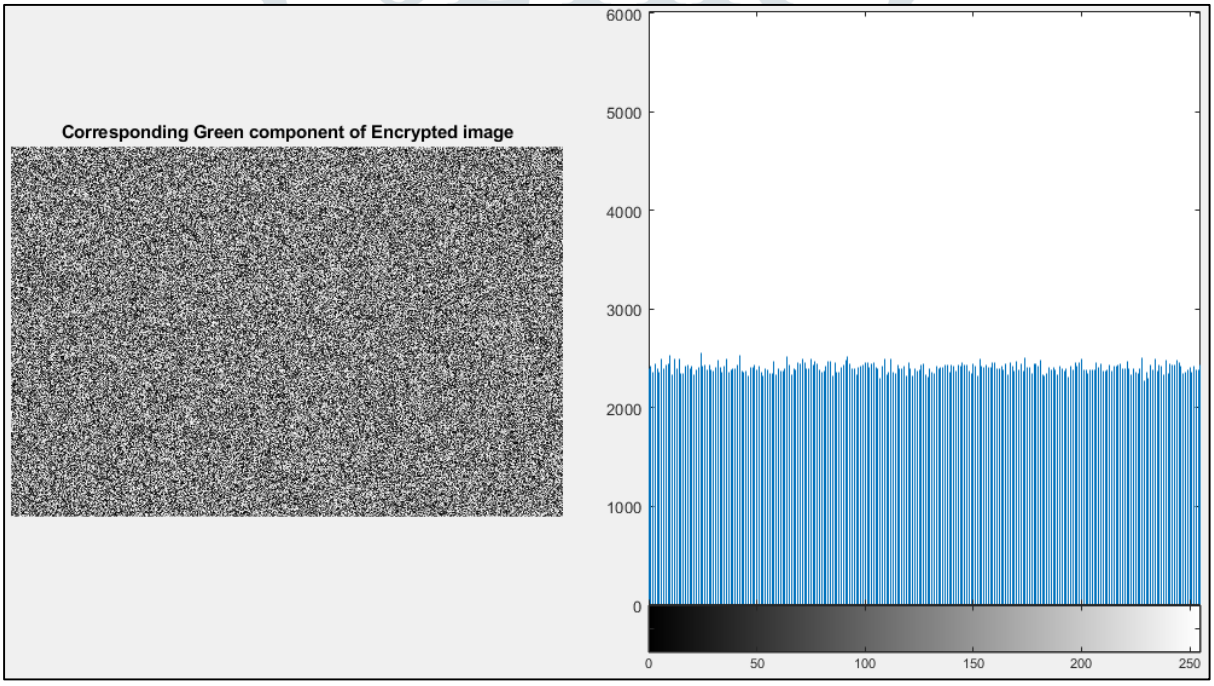

Figure 6.10: Histogram for the green channel of encrypted image

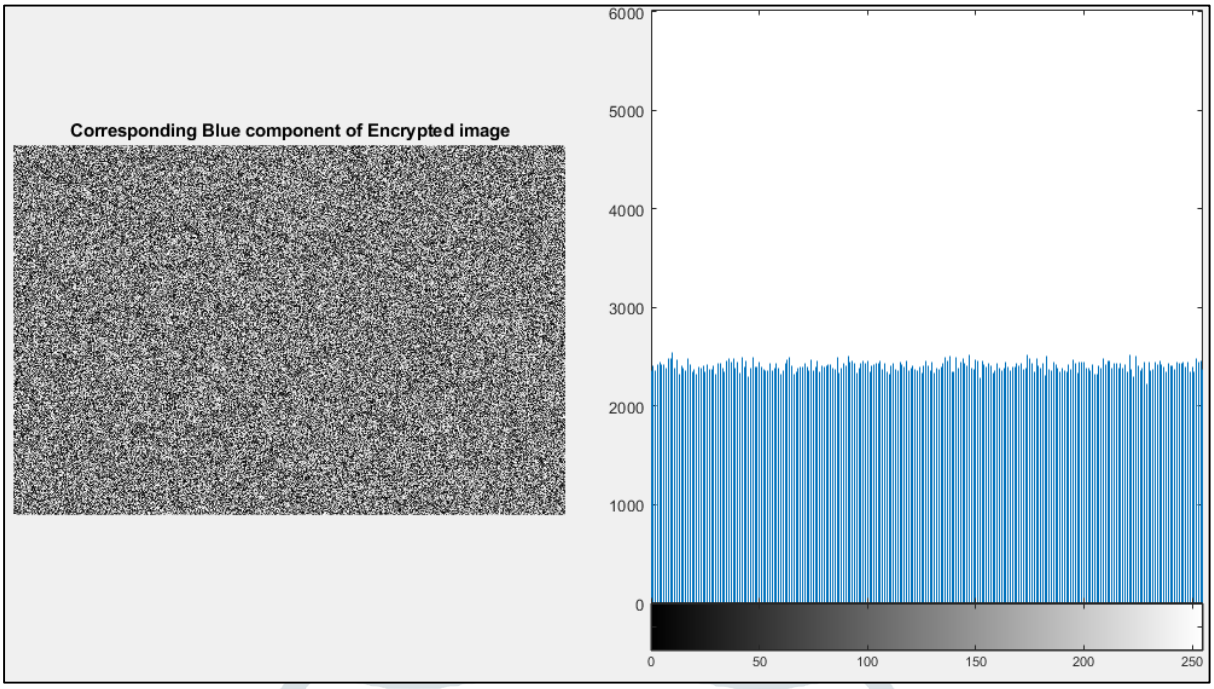

Figure 6.11: Histogram for the blue channel of encrypted image

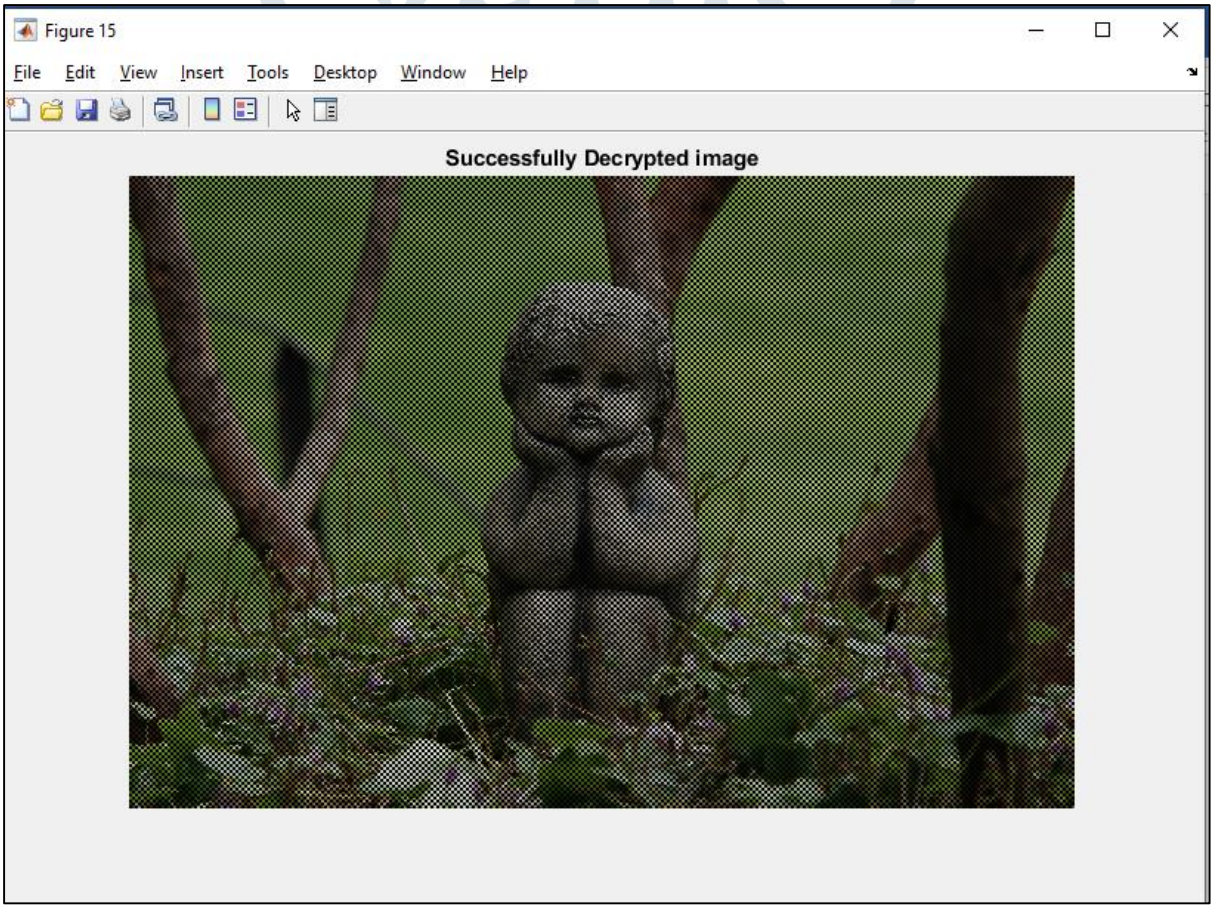

Figure 6.12: Final Decrypted image using proposed algorithm

7.CONCLUSION & FUTURE WORK:

Now-a-days information security is becoming more important in data storage and transmission. Images are generally used in different processes.In this manner, the security of picture information from unapproved utilizes is significant.. Image encryption plays a important role in the field of information hiding or cryptography.

The color image encryption and decryption algorithm is proposed and implemented depend on fast image key. Image key can obtain from the same image or any other image must the same size of original color image. The sender and receiver share's the same image key which has the similar properties of hash function therefore, the attacker cannot discover the plain image from the image key notably, if one pixel value is changed, another key will generated.This proposed algorithm give a good results through applied some statistical tests as well the this proposed algorithm achieve's encryption.

Finally, it is possible to encrypt partial image instead of full image encryption. Also it can be applied as a block cipher instead of stream cipher to get good results. As well as it can be developed by compression of the plain image with image key to reduce the cost of data transition.

8.REFERENCES:

[1] Changgui Shi, Sheng-Yih Wang, Bharat K. Bhargava 1999: "MPEG Video Encryption in Real-time Using Secret Key Cryptography". PDPTA: pp2822-2828.

[2] Wu Y., Noonan J., and Agaian S. 2011: "NPCR and UACI randomness tests for image encryption", Journal of Selected Areas in Telecommunications (JSAT), pp. 31–38.

[3] Pratibha S. Ghode, SEM IV. and Tech M. 2014 "A Keyless approach to Lossless Image Encryption", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, No. 5, pp 1459-1467.

[4] Khanzadi H., Eshghi M. and Borujeni S. E. 2013 "Image Encryption Using Random Bit Sequence Based on Chaotic Maps", Arabian Journal for Science and Engineering AJSE, Vol.39, No. 2, pp1039–1047

[5] Mirzaei O., Yaghoobi M. and Irani H. (2012) "A New Image Encryption Method: Parallel Sub-Image Encryption with Hyper Chaos", Nonlinear Dynamics, Vol. 67, No. 1, pp557-566.

[6] Wei X., Guo L., Zhang Q., Zhang J., and Lian S. 2012 "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system", The Journal of Systems and Software, Vol. 85, No. 2, pp290-299.

[7] Panduranga H. T. and Naveen kumar S. K. 2011 "Hybrid Approach to Transmit a Secrete Image", 2nd National Conference on Emerging Trends and Applications in Computer Science IEEE.

[8] Ibrahim S. I. Abuhaiba and Maaly A. S. Hassan 2011 "Image Encryption Using Differential Evolution Approach In Frequency Domain", Signal & Image Processing An International Journal SIPIJ Vol. 2, No. 1.

[9] Wang X., Zhao J. and Liu H. 2012 "A new image encryption algorithm based on chaos", Elsevier.Vol.285 No.5, pp562–566.

[10] Seyedzade S. M., Atani R. E., and Mirzakuchaki S. 2010 "A Novel Image Encryption Algorithm Based on Hash Function", In 6th Iranian Conference on Machine Vision and Image Processing IEEE.

[11] Min L. and Lu H. 2010 "Design and analysis of a novel chaotic image encryption", 2nd International Conference on Computer Modelling and Simulation, Publication IEEE, pp517-520.