A

Project Report on

IMAGE ENCRYPTION AND DECRYPTION USING RANDOM IMAGE KEY

Submitted in partial fulfillment of the Requirement for the award of degree of

BACHELOR OF TECHNOLOGY

IN

ELECTRONICS AND COMMUNICATION ENGINEERING

Submitted By

M.BHUVANESWARI DEVI	**16551A04A0**
B.PAVAN SAI	**16551A0410**
CH.PAVAN KUMAR	**16551A0417**
G.GOPI VENKATA RAJA REDDY	**16551A0430**

Under the esteemed guidance of

Mr.A.V.BHARADWAJA , M. Tech,(Ph.D)

Assistant Professor

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

GODAVARI INSTITUTE OF ENGINEERING AND TECHNOLOGY
(AN AUTONOMOUS INSTITUTION)
(NAAC 'A' Grade, Accredited by NBA, Approved by AICTE, Affiliated to JNTUK, Kakinada)
NH-16, Chaitanya Knowledge City, Rajahmundry-533 294.

GODAVARI INSTITUTE OF ENGINEERING & TECHNOLOGY

(Autonomous)

CHAITANYA KNOWLEDGE CITY, NH-16, RAJAMAHENDRAVARAM-533296, AP

BONAFIDE CERTIFICATE

Certified that this project report **"AUTOMATED MICROANEURYSMS DETECTION IN FUNDUS IMAGES USING IMAGE SEGMENTATION"** is the bonafide work of **"M.BHUVANESWARI DEVI(16551A04AO),B.PAVAN SAI(16551A0410),CH.PAVANKUMAR(16551A0478), G.GOPI VENKATA RAJA REDDY(16551A0447)"**, who carried out the project work under my supervision during the year 2019 to 2020, towards partial fulfilment of the requirements of the Degree of Bachelor of Technology in Electronics and Communication Engineering as administered under the Regulations of Godavari Institute of Engineering & Technology (A), Rajamahendravaram, AP, India and award of the Degree from Jawaharlal Nehru Technological University, Kakinada. The results embodied in this report have not been submitted to any other University for the award of any degree.

Signature of the Head of the Department
Prof. P.Venkata Rao
HEAD OF THE DEPARTMENT
Department of ECE

Signature of the Supervisor
Mr. BHARADWAJA
SUPERVISOR
Assistant Professor
Department of ECE

Date:

External Viva voce conducted on_____

Internal Examiner **External Examiner**

ACKNOWLEDGEMENT

My profound sense of gratitude runs beyond puny limits of vocabulary when we are to acknowledge the contribution of my esteemed training guide **Mr. BHARADWAJA,** He is instrumental in instilling us intense motivation and tremendous confidence through the conception and execution of the project. This project work could be completed in time due to his expertise and consistent supervision.

I would like to thank **Prof. P.Venkata Rao, Head of the Department of Electronics and Communication Engineering, GIET (A)** for his constant guidance, support and co-operation during the project work.

Special thanks are due to **Dr. T V Prasad, Principal, GIET (A)** for their constant guidance, continuous interactions and technical support along with their encouragement, co-operation and enthusiasm towards the project work.

I express my special thanks to **Mr. BHARADWAJA**, Assistant professor of ECE. Dept. **GIET(A)** for his constant support and timely evaluation of my project work during the duration of the course.

M.BUVANESWARI DEVI (16551A04A0)

B.PAVAN SAI (16551A0410)

CH.PAVAN KUMAR (16551A0417)

G.GOPI VENKATA RAJA REDDY(16551A0430)

ABSTRACT

In the past decade, image encryption is given much attention in research of information security and a lot of image encryption algorithms have been introduced and Internet plays an important role in circulating a huge amount of multimedia. An example of this multimedia is the image. To send an image over the network secretly, the sender tries to find encryption algorithm to hide image information.

This paper 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 make more diffusion of the encrypted image to maintain a higher level of security upon. transference. than it is with the original image.

CONTENTS

NAME OF THE TITLE PAGENO

ABSTRACT

LIST OF FIGURES

LIST OF TABLES

CHAPTER -1 :INTRODUCTION 1-11

1.1Images and pictures 1

1.2 What is image processing 1

1.3 Images and digital images 2

1.4 Aspects of image processing 3

1.5 An image processing task 4

1.6 Types of digital images 5

1.7 Segmentation 7

1.8 IMAGE SEGMENTATION 8

1.8.1 Edge detection techniques 8

CHAPTER -2 :WAVELETS 12-17

2.1Wavelet 12

2.2 The Continuous Wavelet Transform and the Wavelet Series 13

2.3 The Discrete Wavelet Transform 14

2.4Classification of wavelets 14

2.5 Wavelet Families 15

2.5.1 Haar wavelets 16

CHAPTER -3 :LITERATURE SURVEY 18 -19

CHAPTER -4 :IMAGE ENCRYPTION 20-23

4.1 introduction 20

4.2 Theory Background 21

4.2.1 *Image encryption* *22*

4.2.2 *Image Transformation* *22*

CHAPTER -5 :EXISTING SYSTEM 24-25

5.1 Data Encryption Standard (DES) 24

5.2 Advanced Encryption Standard (AES) 24

5.3 Rivest-Shamir-Adleman (RSA) 24

5.4 Elliptical Curve Cryptography (ECC) : 25

5.5 LIMITATIONS 26

CHAPTER -6 :PROPOSING SYSTEM 26-29

CHAPTER -7 : SIMULATION RESULTS 30-36

CONCLUSION AND FUTURE SCOPE 37

APPENDIX-A (MATLAB SOFTWARE DESCRIPTION) 38-46

APPENDIX-B MATLAB 47-49

REFERENCES 50-51

LIST OF FIGURES

FIGURE NO	NAME OF FIGURE	PAGE NO.
1.1	Image sharpening	2
1.2	Binary image	5
1.3	Gray scale image	6
1.4	color image	6
2.1	Wavelet families	15
4.1	Sample Encryption and Decryption Process	20
4.2	represents discreet wavelet transform decomposition for 1 level	23
4.3	represents discreet inverse wavelet transform Decomposition for 1 level	23
6.1	Proposed encryption algorithm	27
6.	Proposed dencryption algorithm	28
7.1	Selected Input image30	
7.2	R, G and B Channel extraction of input image	31
7.3	Red component of an image with its Histogram	31
7.4	Green component of an image with its Histogram	32
7.5	Blue component of an image with its Histogram	32
7.6	Wavelet based decomposed image	33
7.7	Inverse Discrete Wavelet transform of Scrambled image	33
7.8	Final encrypted image for transmitting over the channel	34
7.9	Histogram for the red channel of encrypted image	34
7.10	Histogram for the green channel of encrypted image	35
7.11	Histogram for the blue channel of encrypted image	35
7.12	Final Decrypted image using proposed algorithm	36

LIST OF TABLES

TABLE NO NO	TABLE	PAGE
4.1	Different Encryption algorithms comparison	21
1	Elementary matrices	39
2	disp and fprint commands	40
3	Relational and logical operators	41

CHAPTER 1
INTRODUCTION

1.1 Images and pictures:

As we mentioned in the preface, human beings are predominantly visual creatures: we rely heavily on our vision to make sense of the world around us. We not only look at things to identify and classify them, but we can scan for differences, and obtain an overall rough "feeling" for a scene with a quick glance. Humans have evolved very precise visual skills: we can identify a face in an instant; we can differentiate colors; we can process a large amount of visual information very quickly. However, the world is in constant motion: stare at something for long enough and it will change in some way. Even a large solid structure, like a building or a mountain, will change its appearance depending on the time of day (day or night); amount of sunlight (clear or cloudy), or various shadows falling upon it. We are concerned with single images: snapshots, if you like, of a visual scene. Although image processing can deal with changing scenes, we shall not discuss it in any detail in this text. For our purposes, an image is a single picture which represents something. It may be a picture of a person, of people or animals, or of an outdoor scene, or a microphotograph of an electronic component, or the result of medical imaging. Even if the picture is not immediately recognizable, it will not be just a random blur.

1.2 What is image processing?

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.

We shall be concerned with digital image processing, which involves using a computer to change the nature of a digital image (see below). It is necessary to realize that these two aspects represent two separates but equally important aspects of image processing. A procedure which satisfies condition (1)—a procedure which makes an image "look better"—may be the very worst procedure for satisfying condition (2). Humans like their images to be sharp, clear and detailed; machines prefer their images to be simple and uncluttered. Examples of (1) may include:

Enhancing the edges of an image to make it appear sharper; an example is shown in figure 1.1. Note how the second image appears “cleaner”; it is a more pleasant image. Sharpening edges is a vital component of printing: in order for an image to appear “at its best” on the printed page; some sharpening is usually performed.

(a) The original image (b) Result after “sharperning”

Figure 1.1: Image sharperning

1.3 Images and digital images:

Suppose we take an image, a photo, say. For the moment, let’s make things easy and suppose the photo is black and white (that is, lots of shades of grey), so no color. We may consider this image as being a two-dimensional function, where the function values give the brightness of the image at any given point. We may assume that in such an image brightness values can be any real numbers in the range **0**(black) to **1** (white). The ranges of x and y will clearly depend on the image, but they can take all real values between their minima and maxima. A digital image differs from a photo in that the x, y, and f(x, y) values are all discrete. Usually they take on only integer values, so the image will have 0 and 1 ranging from 1 to 256 each, and the brightness values also ranging from 0 (black) to 255 (white). A digital image can be considered as a large array of discrete dots, each of which has a brightness associated with it. These dots are called picture elements, or more simply pixels.

➢ Some applications:

Image processing has an enormous range of applications; almost every area of science and technology can make use of image processing methods. Here is a short list just to give some indication of the range of image processing applications.

1. Medicine Inspection and interpretation of images obtained from X-rays, MRI or CAT scans, analysis of cell images, of chromosome karyotypes.

2. Agriculture Satellite/aerial views of land, for example to determine how much land is being used for different purposes, or to investigate the suitability of different regions for different crops, inspection of fruit and vegetables—distinguishing good and fresh produce from old.

3. Industry Automatic inspection of items on a production line, inspection of paper samples.
4. Law enforcement Fingerprint analysis, sharpening or de-blurring of speed-camera images.

1.4 Aspects of image processing:

It is convenient to subdivide different image processing algorithms into broad subclasses. There are different algorithms for different tasks and problems, and often we would like to distinguish the nature of the task at hand.

- ***Image enhancement:***

This refers to processing an image so that the result is more suitable for a particular application. Example includes:

- sharpening or de-blurring an out of focus image,
- highlighting edges,
- improving image contrast, or brightening an image,
- Removing noise.

- ***Image restoration:***

This may be considered as reversing the damage done to an image by a known cause, for example: removing of blur caused by linear motion, removal of optical distortions, removing periodic interference.

- ***Image segmentation:***

This involves subdividing an image into constituent parts, or isolating certain aspects of an image: finding lines, circles, or particular shapes in an image, in an aerial photograph, identifying cars, trees, buildings, or roads. These classes are not disjoint; a given algorithm may be used for both image enhancement or for image restoration. However, we should be

able to decide what it is that we are trying to do with our image: simply make it look better (enhancement), or removing damage (restoration).

1.5 An image processing task

We will look in some detail at a particular real-world task, and see how the above classes may be used to describe the various stages in performing this task. The job is to obtain, by an automatic process, the postcodes from envelopes. Here is how this may be accomplished:

- ***Acquiring the image:***

First, we need to produce a digital image from a paper envelope. This can be done using either a CCD camera, or a scanner.

- ***Preprocessing***

This is the step taken before the "major" image processing task. The problem here is to perform some basic tasks in order to render the resulting image more suitable for the job to follow. In this case it may involve enhancing the contrast, removing noise, or identifying regions likely to contain the postcode.

- ***Segmentation:***

Here is where we actually "get" the postcode; in other words we extract from the image that part of it which contains just the postcode.

- ***Representation and description:***

These terms refer to extracting the particular features which allow us to differentiate between objects. Here we will be looking for curves, holes and corners which allow us to distinguish the different digits which constitute a postcode.

- ***Recognition and interpretation***

This means assigning labels to objects based on their descriptors (from the previous step), and assigning meanings to those labels. So, we identify particular digits, and we interpret a string of four digits at the end of the address as the postcode.

1.6Types of digital images

We shall consider four basic types of images:

- ***Binary:***

Each pixel is just black or white. Since there are only two possible values for each pixel, we only need one bit per pixel. Such images can therefore be very efficient in terms of storage. Images for which a binary representation may be suitable include text (printed or handwriting), fingerprints, or architectural plans. In the below image we have only the two colors: white for the edges, and black for the background. See figure 1.2 below.

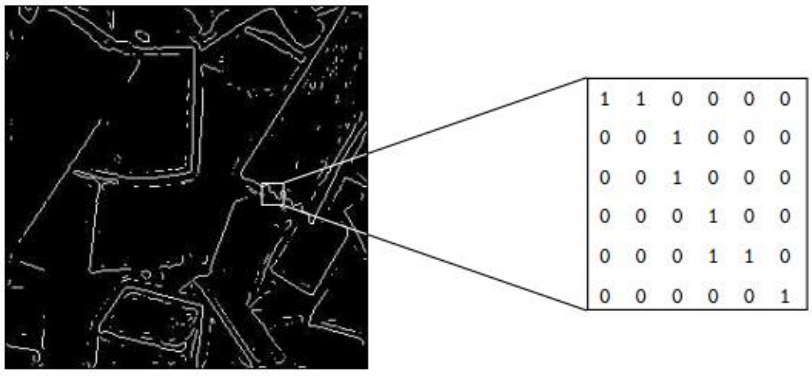

Figure 1.2: Binary Image

- ***Greyscale***:

Each pixel is a shade of grey, normally from 0(black) to255 (white). This range means that each pixel can be represented by eight bits, or exactly one byte. This is a very natural range for image file handling. Other greyscale ranges are used, but generally they are a power of 2. Such images arise in medicine (X-rays), images of printed works, and indeed 256 different grey levels are sufficient for the recognition of most natural objects.

Figure 1.3: Gray scale image

- ***True colour or RGB:***

Here each pixel has a particular colour; that colour being described by the amount of red, green and blue in it. If each of these components has a range – 0 to 255, this gives a total of 16,777,216 different possible colors in the image. This is enough colors for any image. Since the total number of bits required for each pixel is 24, such images are also called 24 -bit colour images. Such an image may be considered as consisting of a "stack" of three matrices; representing the red, green and blue values for each pixel. This means that for every pixel there correspond three values.

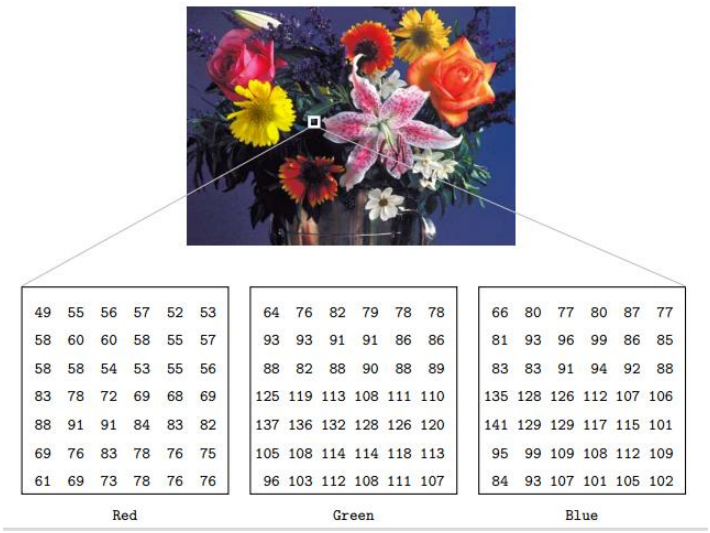

Figure 1.4: COLOR IMAGE

1.7Segmentation:

Image segmentation is an essential step in image analysis. Segmentation separates an image into its component parts or objects. The level to which the separation is carried depends on the problem being solved. When the objects of interest in an application have been inaccessible the segmentation must stop. Segmentation algorithms for images generally based on the discontinuity and similarity of image intensity values. Discontinuity approach is to partition an image based on abrupt changes in intensity and similarity is based on partitioning an image into regions that are similar according to a set of predefined criteria. Thus the choice of image segmentation technique is depends on the problem being considered. Edge detection is a part of image segmentation. The effectiveness of many image processing also computer vision tasks depends on the perfection of detecting meaningful edges. It is one of the techniques for detecting intensity discontinuities in a digital image. The process of classifying and placing sharp discontinuities in an image is called the edge detection. The discontinuities are immediate changes in pixel concentration which distinguish boundaries of objects in a scene. Classical methods of edge detection engage convolving the image through an operator, which is constructed to be perceptive to large gradients in the image although returning values of zero in uniform regions. There is a very large amount of edge detection techniques available, each technique designed to be perceptive to certain types of edges. Variables concerned in the selection of an edge detection operator consist of Edge orientation, Edge structure and Noise environment. The geometry of the operator establishes acharacteristic direction in which it is most perceptive to edges. Operators can be optimized to look for vertical, horizontal, or diagonal edges. Edge detection is a difficult task in noisy images, since both the edges and noise hold high- frequency content. Efforts to reduce the noise result in unclear and distorted edges. Techniques used on noisy images are typically larger in scope; therefore, they can common enough data to discount localized noisy pixels. This results in less perfect localization of the detected edges. Not all edges involve a step change in intensity. Things such as refraction or reduced focus can result in objects through boundaries defined by a regular change in intensity. The method wants to be chosen to be receptive to such a regular change in those cases. So, there are some problems of fake edge detection, edge localization, missing true edges, problems due to noise and high computational time etc. Hence, the objective is to do the comparison of a variety of edge detections and analyze the performance of the different techniques in various conditions.

1.8 IMAGE SEGMENTATION

Image Segmentation is the process of partitioning a digital image into multiple regions or sets of pixels. Essentially, in image partitions are different objects which have the same texture or color. The image segmentation results are a set of regions that cover the entire image together and a set of contours extracted from the image. All of the pixels in a region are similar with respect to some characteristics such as color, intensity, or texture. Adjacent regions are considerably different with respect to the same individuality. The different approaches are (i) by finding boundaries between regions based on discontinuities in intensity levels, (ii) thresholds based on the distribution of pixel properties, such as intensity values, and (iii) based on finding the regions directly. Thus the choice of image segmentation technique is depends on the problem being considered. Region based methods are based on continuity. These techniques divide the entire image into sub regions depending on some rules like all the pixels in one region must have the same gray level. Region-based techniques rely on common patterns in intensity values within a cluster of neighboring pixels. The cluster is referred to as the region in addition to group the regions according to their anatomical or functional roles are the goal of the image segmentation. Threshold is the simplest way of segmentation. Using thresholding technique regions can be classified on the basis range values, which is applied to the intensity values of the image pixels. Thresholding is the transformation of an input image to an output that is segmented binary image. Segmentation Methods based on finding the regions directly find for abrupt changes in the intensity value. These methods are called as Edge or Boundary based methods. Edge detection is the problem of fundamental importance in image analysis. Edge detection techniques are generally used for finding discontinuities in gray level images. To detect consequential discontinuities in the gray level image is the important common approach in edge detection. Image segmentation methods for detecting discontinuities are boundary-based methods.

1.8.1 EDGE DETECTION TECHNIQUES:

The edge representation of an image significantly reduces the quantity of data to be processed, yet it retains essential information regarding the shapes of objects in the scene. This explanation of an image is easy to incorporate into a large amount of object recognition algorithms used in computer vision along with other image processing applications. The major property of the edge detection technique is its ability to extract the exact edge line with good orientation as well as more literature about edge detection has been available in the past

three decades. On the other hand, there is not yet any common performance directory to judge the performance of the edge detection techniques. The performance of an edge detection techniques are always judged personally and separately dependent to its application. Edge detection is a fundamental tool for image segmentation. Edge detection methods transform original images into edge images benefits from the changes of grey tones in the image. In image processing especially in computer vision, the edge detection treats the localization of important variations of a gray level image and the detection of the physical and geometrical properties of objects of the scene. It is a fundamental process detects and outlines of an object and boundaries among objects and the background in the image. Edge detection is the most familiar approach for detecting significant discontinuities in intensity values. Edges are local changes in the image intensity. Edges typically occur on the boundary between two regions. The main features can be extracted from the edges of an image. Edge detection has major feature for image analysis. These features are used by advanced computer vision algorithms. Edge detection is used for object detection which serves various applications like medical image processing, biometrics etc. Edge detection is an active area of research as it facilitates higher level image analysis. There are three different types of discontinuities in the grey level like point, line and edges. Spatial masks can be used to detect all the three types of discontinuities in an image. There are many edge detection techniques in the literature for image segmentation. The most commonly used discontinuity based edge detection techniques are reviewed in this section. Those techniques are Roberts edge detection, Sobel Edge Detection, Prewitt edge detection and Canny Edge Detection.

Roberts Edge Detection:

The Roberts edge detection is introduced by Lawrence Roberts (1965). It performs a simple, quick to compute, 2-D spatial gradient measurement on an image. This method emphasizes regions of high spatial frequency which often correspond to edges. The input to the operator is a grayscale image the same as to the output is the most common usage for this technique. Pixel values in every point in the output represent the estimated complete magnitude of the spatial gradient of the input image at that point.

-1	0
0	+1

G_x

0	-1
+1	0

G_y

Sobel Edge Detection:

The Sobel edge detection method is introduced by Sobel in 1970 (Rafael C.Gonzalez (2004)). The Sobel method of edge detection for image segmentation finds edges using the Sobel approximation to the derivative. It precedes the edges at those points where the gradient is highest. The Sobel technique performs a 2-D spatial gradient quantity on an image and so highlights regions of high spatial frequency that correspond to edges. In general it is used to find the estimated absolute gradient magnitude at each point in n input grayscale image. In conjecture at least the operator consists of a pair of 3x3 complication kernels as given away in under table. One kernel is simply the other rotated by 90o . This is very alike to the Roberts Cross operator.

-1	-2	-1
0	0	0
+1	+2	+1

G_x

-1	0	-1
-2	0	+2
-1	0	+1

G_y

Prewitt Edge Detection:

The Prewitt edge detection is proposed by Prewitt in 1970 (Rafael C.Gonzalez [1]. To estimate the magnitude and orientation of an edge Prewitt is a correct way. Even though different gradient edge detection wants a quite time consuming calculation to estimate the direction from the magnitudes in the x and y-directions, the compass edge detection obtains the direction directly from the kernel with the highest response. It is limited to 8 possible directions; however knowledge shows that most direct direction estimates are not much more perfect. This gradient based edge detector is estimated in the 3x3 neighborhood for eight directions. All the eight convolution masks are calculated. One complication mask is then selected, namely with the purpose of the largest module.

-1	-1	-1
0	0	0
+1	+1	+1

G_x

-1	0	+1
-1	0	+1
-1	0	+1

G_y

Prewitt detection is slightly simpler to implement computationally than the Sobel detection, but it tends to produce somewhat noisier results.

Canny Edge Detection:

In industry, the Canny edge detection technique is one of the standard edge detection techniques. It was first created by John Canny for his Master's thesis at MIT in 1983, and still outperforms many of the newer algorithms that have been developed. To find edges by

separating noise from the image before find edges of image the Canny is a very important method. Canny method is a better method without disturbing the features of the edges in the image afterwards it applying the tendency to find the edges and the serious value for threshold. The algorithmic steps are as follows:

• Convolve image f(r, c) with a Gaussian function to get smooth image f^(r, c). f^(r, c)=f(r,c)*G(r,c,6)

• Apply first difference gradient operator to compute edge strength then edge magnitude and direction are obtain as before.

• Apply non-maximal or critical suppression to the gradient magnitude.

• Apply threshold to the non-maximal suppression image. Unlike Roberts and Sobel, the Canny operation is not very susceptible to noise. If the Canny detector worked well it would be superior.

Original

Roberts

Sobel

Prewitt

Canny

CHAPTER 2
WAVELETS

2.1 Wavelet

A wavelet is a wave-like oscillation with amplitude that starts out at zero, increases, and then decreases back to zero. It can typically be visualized as a "brief oscillation" like one might see recorded by a seismograph or heart monitor. Generally, wavelets are purposefully crafted to have specific properties that make them useful for signal processing. Wavelets can be combined, using a "revert, shift, multiply and sum" technique called convolution, with portions of an unknown signal to extract information from the unknown signal.As a mathematical tool, wavelets can be used to extract information from many different kinds of data, including - but certainly not limited to - audio signals and images. Sets of wavelets are generally needed to analyze data fully. A set of "complementary" wavelets will deconstruct data without gaps or overlap so that the deconstruction process is mathematically reversible. Thus, sets of complementary wavelets are useful in wavelet based compression/decompression algorithms where it is desirable to recover the original information with minimal loss.

The transform of a signal is just another form of representing the signal. It does not change the information content present in the signal. The Wavelet Transform provides a time-frequency representation of the signal. It was developed to overcome the short coming of the Short Time Fourier Transform (STFT), which can also be used to analyze non-stationary signals. While STFT gives a constant resolution at all frequencies, the Wavelet Transform uses multi-resolutions. A wave is an oscillating function of time or space and is periodic. In contrast, wavelets are localized waves. They have their energy concentrated in time or space and are suited to analysis of transient signals. While Fourier Transform and STFT use waves to analyze signals, the Wavelet Transform uses wavelets of finite energy on technique by which different frequencies are analyzed with different resolutions. The wavelet analysis is done similar to the STFT analysis.

The signal to be analyzed is multiplied with a wavelet function just as it is multiplied with a window function in STFT, and then the transform is computed for each segment generated. However, unlike STFT, in Wavelet Transform, the width of the wavelet function changes with each spectral component. The Wavelet Transform, at high frequencies, gives

good time resolution and poor frequency resolution, while at low frequencies; the Wavelet Transform gives good frequency resolution and poor time resolution.

2.2The Continuous Wavelet Transform and the Wavelet Series

The Continuous Wavelet Transform (CWT) is provided by equation 2.1, where x(t) is the signal to be analyzed. ψ(t) is the mother wavelet or the basis function. All the wavelet functions used in the transformation are derived from the mother wavelet through translation (shifting) and scaling (dilation or compression).

$$X_{WT}(\tau,s)=\frac{1}{\sqrt{|s|}}\int x(t)\cdot\psi^{*}\left(\frac{t-\tau}{s}\right)dt \qquad 2.1$$

The mother wavelet used to generate all the basic functions is designed based on some desired characteristics associated with that function. The translation parameter τ relates to the location of the wavelet function as it is shifted through the signal. Thus, it corresponds to the time information in the Wavelet Transform. The scale parameter s is defined as |1/frequency| and corresponds to frequency information. Scaling either dilates (expands) or compresses a signal. Large scales (low frequencies) dilate the signal and provide detailed information hidden in the signal, while small scales (high frequencies) compress the signal and provide global information about the signal. Notice that the Wavelet Transform merely performs the convolution operation of the signal and the basis function. The above analysis becomes very useful as in most practical applications, high frequencies (low scales) do not last for a long duration, but instead, appear as short bursts, while low frequencies (high scales) usually last for entire duration of the signal. The Wavelet Series is obtained by discretizing CWT. This aids in computation of CWT using computers and is obtained by sampling the time-scale plane.

The sampling rate can be changed accordingly with scale change without violating the Nyquist criterion. Nyquist criterion states that, the minimum sampling rate that allows reconstruction of the original signal is 2ω radians, where ω is the highest frequency in the signal. Therefore, as the scale goes higher (lower frequencies), the sampling rate can be decreased thus reducing the number of computations.

2.3 The Discrete Wavelet Transform

The Wavelet Series is just a sampled version of CWT and its computation may consume significant amount of time and resources, depending on the resolution required. The Discrete Wavelet Transform (DWT), which is based on sub-band coding, is found to yield a fast computation of Wavelet Transform. It is easy to implement and reduces the computation time and resources required. The foundations of DWT go back to 1976 when techniques to decompose discrete time signals were devised. Similar work was done in speech signal coding which was named as sub-band coding. In 1983, a technique similar to sub-band coding was developed which was named pyramidal coding. Later many improvements were made to these coding schemes which resulted in efficient multi-resolution analysis schemes.In CWT, the signals are analyzed using a set of basic functions which relate to each other by simple scaling and translation. In the case of DWT, a time-scale representation of the digital signal is obtained using digital filtering techniques. The signal to be analyzed is passed through filters with different cutoff frequencies at different scales.

2.4Classification of wavelets

We can classify wavelets into two classes: (a) orthogonal and (b) biorthogonal. Based on the application, either of them can be used.

(a)Features of orthogonal wavelet filter bank

The coefficients of orthogonal filters are real numbers. The filters are of the same length and are not symmetric. The low pass filter, G_0 and the high pass filter, H_0 are related to each other by

$$H_0(z) = z^{-N} G_0(-z^{-1}) \qquad 2.4$$

The two filters are alternated flip of each other. The alternating flip automatically gives double-shift orthogonality between the low pass and high pass filters, i.e., the scalar product of the filters, for a shift by two is zero. i.e., $\Sigma G[k]\, H[k-2l] = 0$, where $k,l \in Z$. Filters that satisfy equation 2.4 are known as Conjugate Mirror Filters (CMF). Perfect reconstruction is possible with alternating flip.

Also, for perfect reconstruction, the synthesis filters are identical to the analysis filters except for a time reversal. Orthogonal filters offer a high number of vanishing moments. This

property is useful in many signal and image processing applications. They have regular structure which leads to easy implementation and scalable architecture.

(b) Features of biorthogonal wavelet filter banks

In the case of the biorthogonal wavelet filters, the low pass and the high pass filters do not have the same length. The low pass filter is always symmetric, while the high pass filter could be either symmetric or anti-symmetric. The coefficients of the filters are either real numbers or integers.

For perfect reconstruction, biorthogonal filter bank has all odd length or all even length filters. The two analysis filters can be symmetric with odd length or one symmetric and the other anti-symmetric with even length. Also, the two sets of analysis and synthesis filters must be dual. The linear phase biorthogonal filters are the most popular filters for data compression applications.

2.5 Wavelet Families

There are a number of basic functions that can be used as the mother wavelet for Wavelet Transformation. Since the mother wavelet produces all wavelet functions used in the transformation through translation and scaling, it determines the characteristics of the resulting Wavelet Transform. Therefore, the details of the particular application should be taken into account and the appropriate mother wavelet should be chosen in order to use the Wavelet Transform effectively.

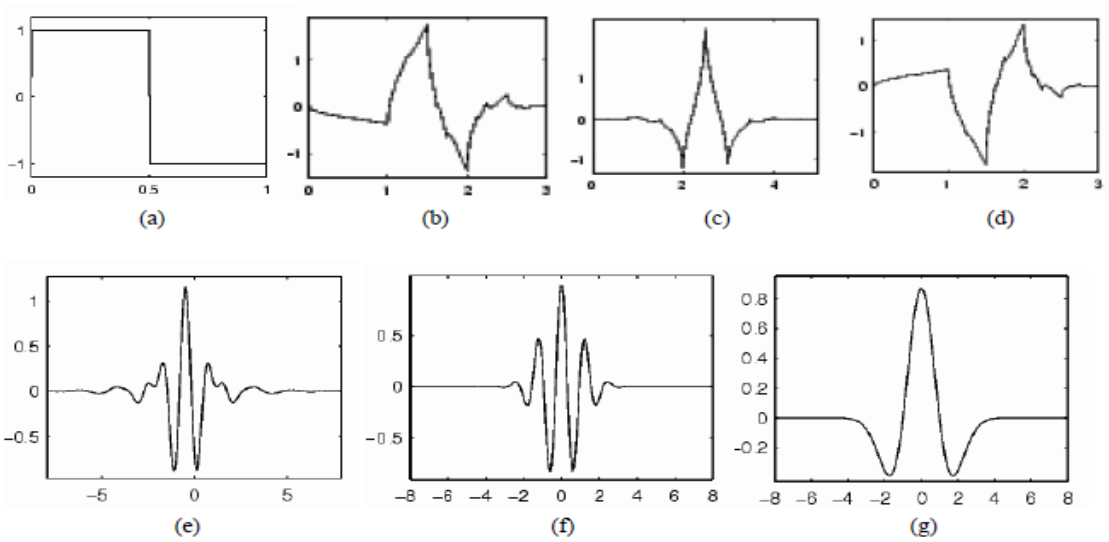

Fig 2.1 Wavelet families (a) Haar (b) Daubechies4 (c) Coiflet1 (d) Symlet2 (e) Meyer (f) Morlet (g) Mexican Hat.

Figure 2.3 illustrates some of the commonly used wavelet functions. Haar wavelet is one of the oldest and simplest wavelet. Therefore, any discussion of wavelets starts with the Haar wavelet. Daubechies wavelets are the most popular wavelets. They represent the foundations of wavelet signal processing and are used in numerous applications. These are also called Maxflat wavelets as their frequency responses have maximum flatness at frequencies 0 and π. This is a very desirable property in some applications. The Haar, Daubechies, Symlets and Coif lets are compactly supported orthogonal wavelets. These wavelets along with Meyer wavelets are capable of perfect reconstruction. The Meyer, Morlet and Mexican Hat wavelets are symmetric in shape. The wavelets are chosen based on their shape and their ability to analyze the signal in a particular application.

2.5.1 Haar wavelets

The first DWT was invented by the Hungarian mathematician Alfred Haar. For an input represented by a list of 2^n numbers, the Haar Wavelet transform may be considered to simply pair up input values, storing the difference and passing the sum. This process is repeated recursively, pairing up the sums to provide the next scale: finally resulting in $2^n - 1$ differences and one final sum. In mathematics, the Haar wavelet is a sequence of rescaled "square-shaped" functions which together form a wavelet family or basis. Wavelet analysis is similar to Fourier analysis in that it allows a target function over an interval to be represented in terms of an orthonormalfunction basis. The Haar sequence is now recognized as the first known waveletbasis and extensively used as a teaching example. The Haar wavelet is also the simplest possible wavelet. The technical disadvantage of the Haar wavelet is that it is not continuous, and therefore notdifferentiable. This property can, however, be an advantage for the analysis of signals with sudden transitions, such as monitoring of tool failure in machines.

The Haar wavelet's mother wavelet function $\psi(t)$ can be described as

$$\psi(t) = \begin{cases} 1 & 0 \le t < 1/2, \\ -1 & 1/2 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Its scaling function $\phi(t)$ can be described as

$$\phi(t) = \begin{cases} 1 & 0 \le t < 1, \\ 0 & \text{otherwise.} \end{cases}$$

Haar Wavelet Properties

Haar wavelet has several notable properties:

1. Any continuous real function can be approximated by linear combinations of $\phi(t), \phi(2t), \phi(4t), \ldots, \phi(2^k t), \cdots$ and their shifted functions. This extends to those function spaces where any function therein can be approximated by continuous functions.
2. Any continuous real function can be approximated by linear combinations of the constant function, $\psi(t), \psi(2t), \psi(4t), \ldots, \psi(2^k t), \cdots$ and their shifted functions.
3. Orthoganalityin the form

$$\int_{-\infty}^{\infty} 2^m \psi(2^m t - n)\psi(2^{m_1} t - n_1)\, dt = \delta_{m,m_1}\delta_{n,n_1}.$$

   Here $\delta_{i,j}$ represents the Kronecker delta. The dual function of $\psi(t)$is $\psi(t)$itself.
4. Wavelet/scaling functions with different scale m have a functional relationship:

$$\phi(t) = \phi(2t) + \phi(2t-1)$$
$$\psi(t) = \phi(2t) - \phi(2t-1)$$

5. Coefficients of scale m can be calculated by coefficients of scale m+1:

   If $\chi_w(n,m) = 2^{m/2} \int_{-\infty}^{\infty} x(t)\phi(2^m t - n)\, dt$

   And $\mathrm{X}_w(n,m) = 2^{m/2} \int_{-\infty}^{\infty} x(t)\psi(2^m t - n)\, dt$

   Then

$$\mathrm{X}_w(n,m) = \sqrt{\frac{1}{2}}(\chi_w(2n, m+1) - \chi_w(2n+1, m+1)).$$
$$\chi_w(n,m) = \sqrt{\frac{1}{2}}(\chi_w(2n, m+1) + \chi_w(2n+1, m+1))$$

CHAPTER 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. [3] 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. [4] proposed an image encryption algorithm using bit sequence random generator based on Chaotic Logistic and Tent maps. Mirzaei et al. [5] 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. [6] 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 [7] 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 [8] present a new effective approach for image encryption which employs the main Discrete Fourier Transform (DFT) followed by Differential Evolution (DE) approach.

On the other hand, Wang et al. [9] suggested a new image encryption algorithm based on chaotic maps. It changes the values of the image pixels jointly with the pseudorandom which is -512 by taking half data of image for encryption of the other half to increase the speed of processing. Min and Lu [11] proposed an algorithm to generate a relation between the plain image and the generated pseudo numbers which are used to shuffle process and pixel value. Pall et al. [12] suggested three encryption algorithms in order to develop the security image. Codebook, Index table and Codebook Index Table were applied by using Vector Quantization to compress data of image and XOR operation followed by random methods.

Pang [13] introduced an encryption algorithm depending on Daubechies wavelet transform to encrypt image data using binary sequences which were generated by chaos theory. Acharya et al. [14] suggested an efficient approach using Hill Cipher and random key for every block for encryption of image depending on the properties of the matrix. Al-

Khassaweneh et al. [15] proposed an approach based on random vectors to encrypt the image by stratifying the least square approximation techniques.

CHAPTER-4

IMAGE ENCRYPTION

4.1 Introduction

There is no doubt that information technology plays a significant role to support the computer applications to many users and establishments in the world like information security, information hiding and information retrieval. As a matter of fact, all users, who use multimedia such as image, audio, video and text, may need to protect information from attacks during sending or receiving them through channel. There are two challenges for multimedia encryption; the first one is the size of data and the second is the cost of encryptions [1]. 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. Sample encryption and decryption process are as shown in the following figure 3.1.

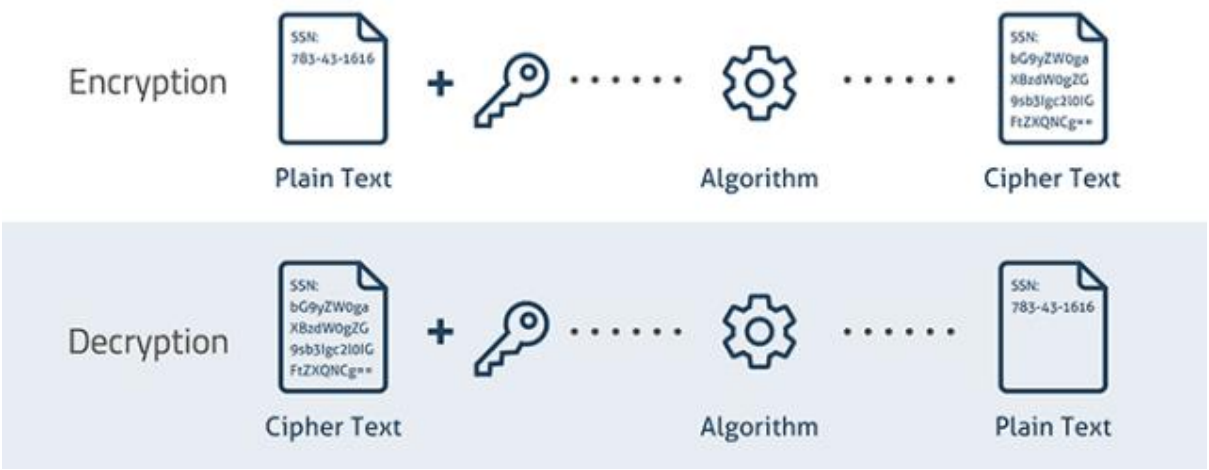

Figure 4.1: Sample Encryption and Decryption Process

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.

The comparison among some of the existing techniques for encryption are tabulated below.

Table 4.1: Different Encryption algorithms comparison

Technique	Pros	Cons	Use case
No encryption	No effort	Dangerously insecure	Not suitable for any app handling personal data
DB-level encryption	Offered by most DB or cloud providers	Any hack of the application or server reveals all the data	Suitable for apps handling personal data (not special data)
Record-level or Application-level encryption	Highest security for applications which need access to the data	Implementation is complex and searching data is hard	Ideal for apps handling sensitive and special data (e.g. health data)
E2E or End-to-End encryprion	Highest security as only end-hosts have keys and can see the data	Not feasible if the data needs any form of processing	Ideal for securing sensitive messages (e.g. Doctor to patient chats)

4.2 Theory Background

This section introduces the main theoretical background of image encryption and image transformation. There are many types of encryption algorithms developed through the previous time. Most of these methods dealt with text such as Rivest, Shamir and Adelman (RSA), Data Encryption Standard (DES) and Advanced Encryption Standard (AES) to generate stream cipher from original text called plain text. Usually, there are three categories of image encryption approaches. First category depends on transposition, second category depend on substitution, the third category is hybrid between first and second [16].

4.2.1 Image encryption

In multimedia encryption field, a big data can be obtained from an image. Therefore one of two strategies can applied, the first one is stream cipher, while the second is block cipher. Encryption algorithms require secret key. Secret key can beeither symmetric cipher or asymmetric cipher. Secret key in symmetric encryption means that both the sender and the receiver agree on a single key for their communication; it is used to encrypt and to decrypt the data. While public key in asymmetric encryption through which everyone can encrypt data, but cannot decrypt it; only the person holding the secret key can decrypt this, such as RSA and ElGamal [17]. In block image cipher encrypt one block of input to process a block of output have the same size based on the same key then proceed to the next block. Stream ciphers are different to block ciphers; they do not transform blocks of data to another block of data instead based on a key [18].

4.2.2 Image Transformation

One of important spatial domain is wavelet transform. Haar wavelet transform gives us approximation coefficients in four components for color image. Assume we have an image, wavelet decomposition will filter this image into two component depend on rows these are Low pass filter (L) and High pass filter (H) each one will decompose with the same way to extract four components: LL,HL,LH and HH based on columns; the last three components represent the horizontal, vertical and diagonal respectively. Two-dimension inverse wavelet transform reconstructs the four components to recover the original image; figure 3.2 and 3.3 illustrates the discrete wavelet transform and inverse discrete wavelet transforms [19].

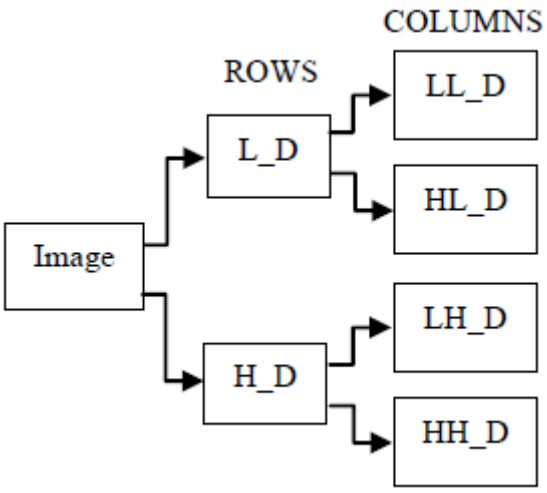

Figure 4.2: represents discreet wavelet transform decomposition for 1 level

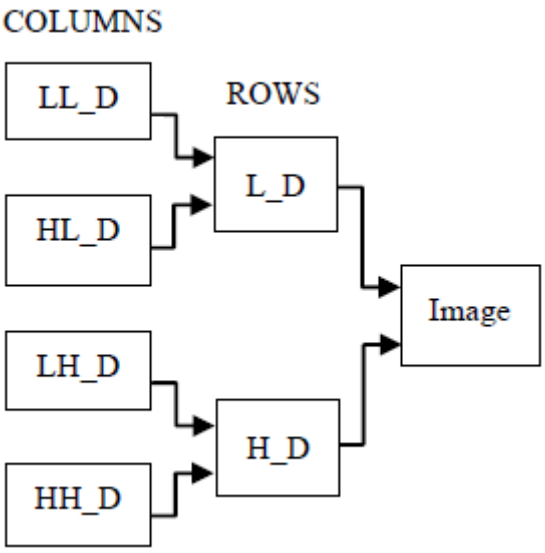

Figure 4.3: represents discreet inverse wavelet transform decomposition for 1 level

Where, D:Decomposition, R:Reconstruct, L: Low pass filter and H:High pass filter.

CHAPTER 5

EXISTING SYSTEM

Last few decades have seen lots of schemes being proposed for image encryption using keys. Image Encryption Process using key is shown in a good encryption algorithm uses a strong key (the key that is almost impossible to be cracked by any intruder) to convert the plaintext image into encrypted image and the vice versa (i.e. decryption). The data is seen as random string of bits in encrypted format when an attacker intercepts it, hence the technique is secure. Key Management and Distribution is difficult and challenging task. some of the prominent ones have been here

5.1 Data Encryption Standard (DES)

It is a algorithm is based on symmetric key block cipher. DES operates on block size of 64 bits a time, length of the key used is 64 bits (56 bits key and 8 bits are parity check bits) . Initially input is split into 64 bits blocks. If input bits are unevenly divided with 64 then the last block is padded. Same key is used for both encryption and decryption. The encryption process holds two permutations (initial permutation and final permutation) and 16 rounds. The 64 bits block is subjected to initial permutation and then the block is split into two halves (right half and left half) each 32 bits long. Then there are 16 rounds of identical operations in which data is combined with the key in 4 steps in each 16 rounds.

5.2 Advanced Encryption Standard (AES)

It is a symmetric key encryption algorithm introduced to replace DES Algorithm. AES operates on block sizes of 128, 168, 192, 224, and 256 bits; key length of 128, 192, and 256 bits . The standard encryption uses AES-128 where both the block and key size are 128 bits. The size of block and key decides the number of rounds in the process. If both the block length and key length are 128 bits, AES will perform 9 processing rounds. If the block and key are of 192 bits, AES performs 11 processing rounds. If the block and key are of length 256 bits then it performs 13 processing rounds .

5.3 Rivest-Shamir-Adleman (RSA):

Algorithm is proposed by Ron Rivest, Adi Shamir, and Leonard Adleman in 1978 . The idea behind RSA is motivated by Diffie and Hellman's method of exponential key exchange. RSA

is an asymmetric cryptographic algorithm and it is operates on 1024,2048,3072,7680 bits key length. It is developed by using two distinct prime number.

5.4Elliptical Curve Cryptography (ECC) :

It is an asymmetric key encryption which is introduced by Miller and Koblitz in 1985. . ECC poses same level of security that is provided by RSA, Diffie Hellman but with much shorter keys. it operates on 160,224,256,384 bits key length. The general form of ECC is:
y 2 = x3 +ax+b(modp), over a finite field Fp where p is a prime or a prime power, x, y are coordinates and a, b are coefficients (real numbers). The private key d is randomly chosen from d ∈ n {1,2,3,…n-1} where n is the integer, whereas the public key Q is calculated by dP, where P and Q are the points on elliptical curve. The key pair (d, Q) is used in cryptosystems.

5.5LIMITATIONS:

- Long computational time
- Not suitable for practical image encryption and for online communications
- Loss of quality of image by random shares.

CHAPTER-6

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 by 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 images are cut and scrambled randomly then using XOR logic to generate image 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. Generate primary key from step 3 using XOR logic.
5. Analysis primary key to three channels (R, G and B).
6. Flip R to three directions (left to right, up to down and right to left)
7. Rotate R and flip it to three directions (left to right, up to down and right to left)
8. For all matrixes generated in steps 6 and 7 use XOR to get new R.
9. Repeat steps from 6-8 to get new G and New B.
10. Reconstruct R, G and B to new image.
11. Use XOR between origin image in step1 and new image in step 9.
12. Analysis image in step 11 to three channels (R, G and B).
13. Apply XOR for R, G and B to generate image key.
14. End.

After introducing color image, the system will generate the symmetric random image key to use in image encryption. As shown in figure 4.1 each channel of origin image will extract features by applying Haar wavelet transform to give us four components Low Low, High Low, Low High and High Low. In scrambling stage, the complements of last three components take to multiply by (-1) to reverse sign of elements then use shifting to satisfy

more confusion and diffusion. To get the scrambled image, Inverse Wavelet Transform is used here. Image encryption will be completed by using XOR logic between the image key generate and scrambling image. Finally, reconstruct image from three channels to get the cipher image.

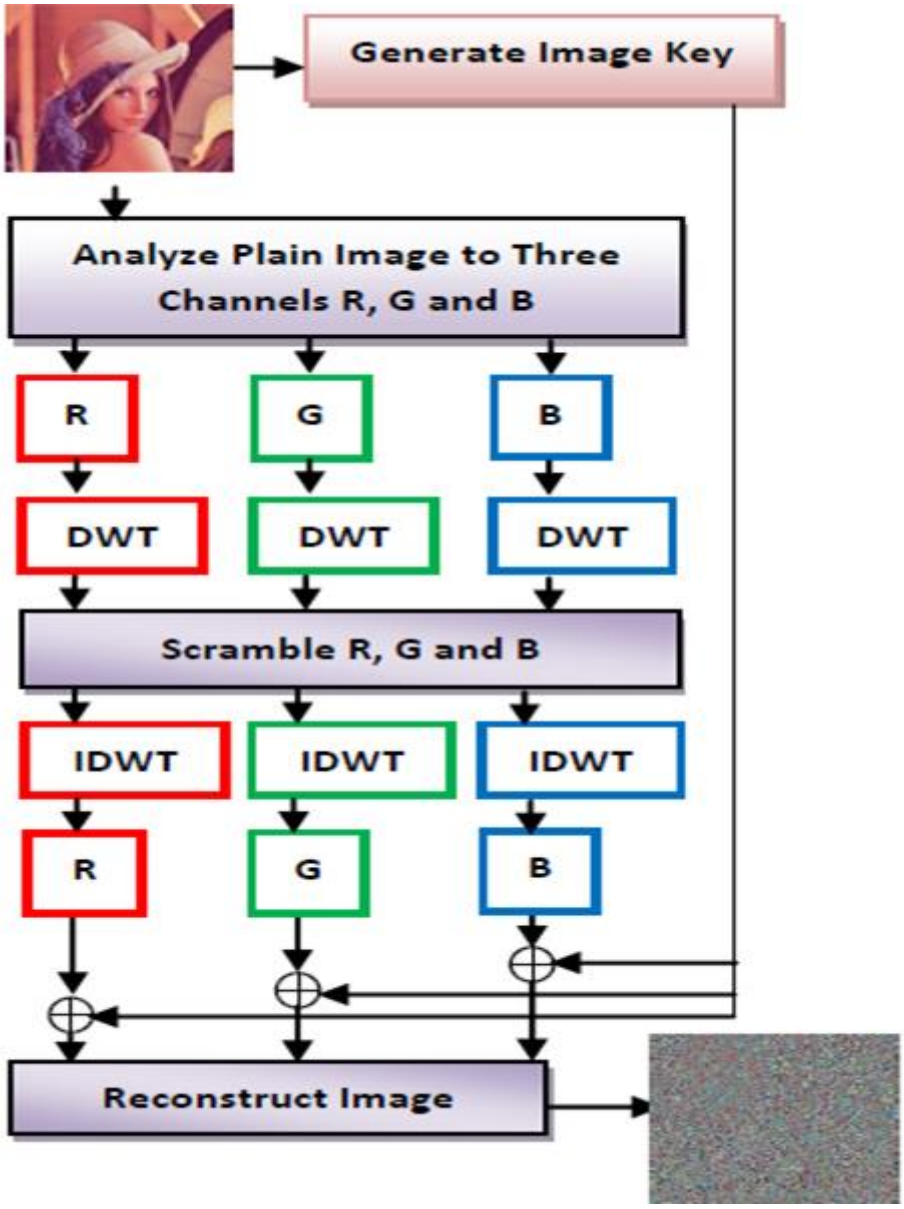

Figure 6.1: Proposed encryption algorithm

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

1. Input plain color image
2. Generate secret key from the plain color image.
3. Get R, G, and B components for color 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 image.
7. Encrypt every channel by secret key using XOR.
8. Combine R, G, and B channels to create the cipher color 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.

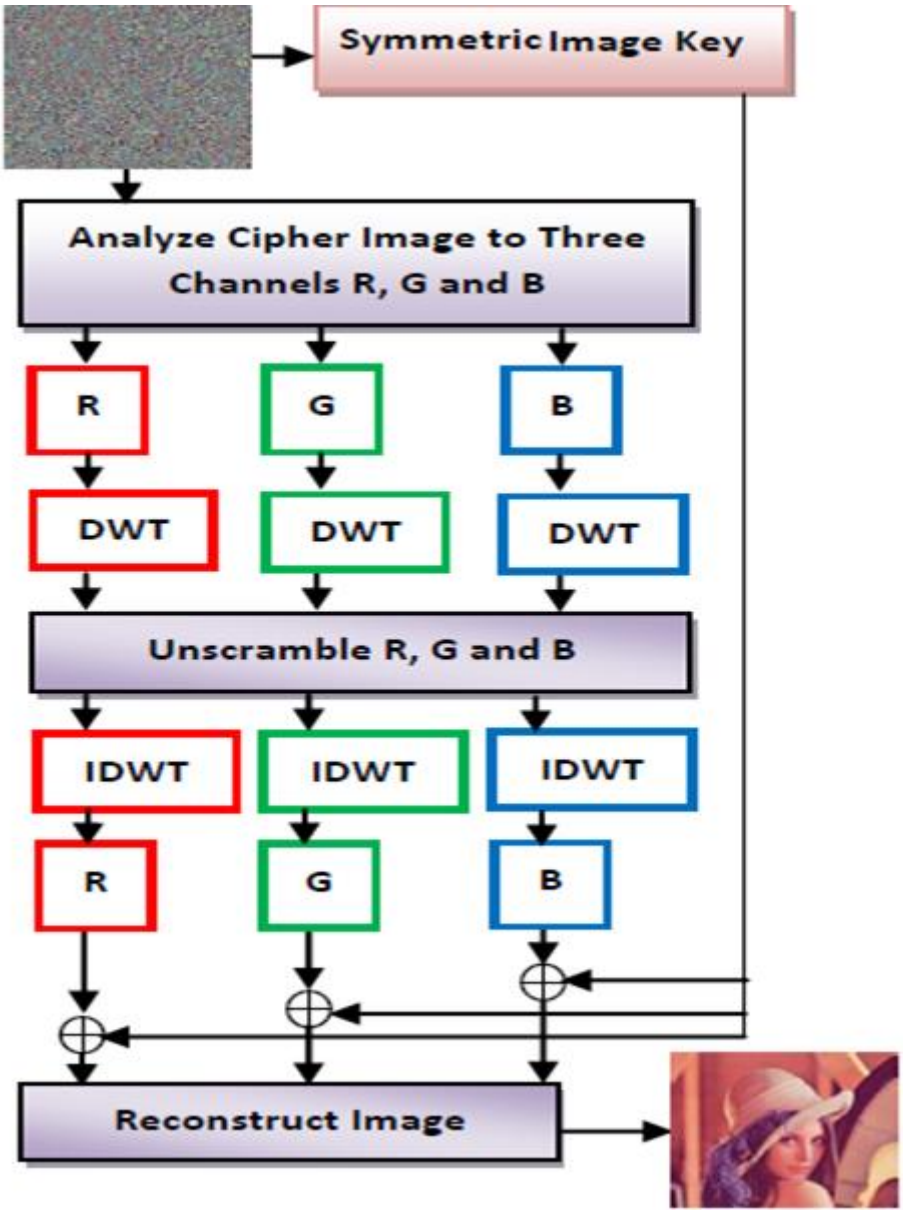

Figure 6.2: Proposed Decryption Algorithm

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

1. Input plain color image.
2. Get R, G, and B components for color 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 obtain new image.
6. Decrypt every channel by secret key using XOR.
7. Combine R, G, and B channels to recover the plain color image.
8. Display origin image.
9. End.

CHAPTER-7

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, blue and green channels of origin image are decomposed here for the same image.

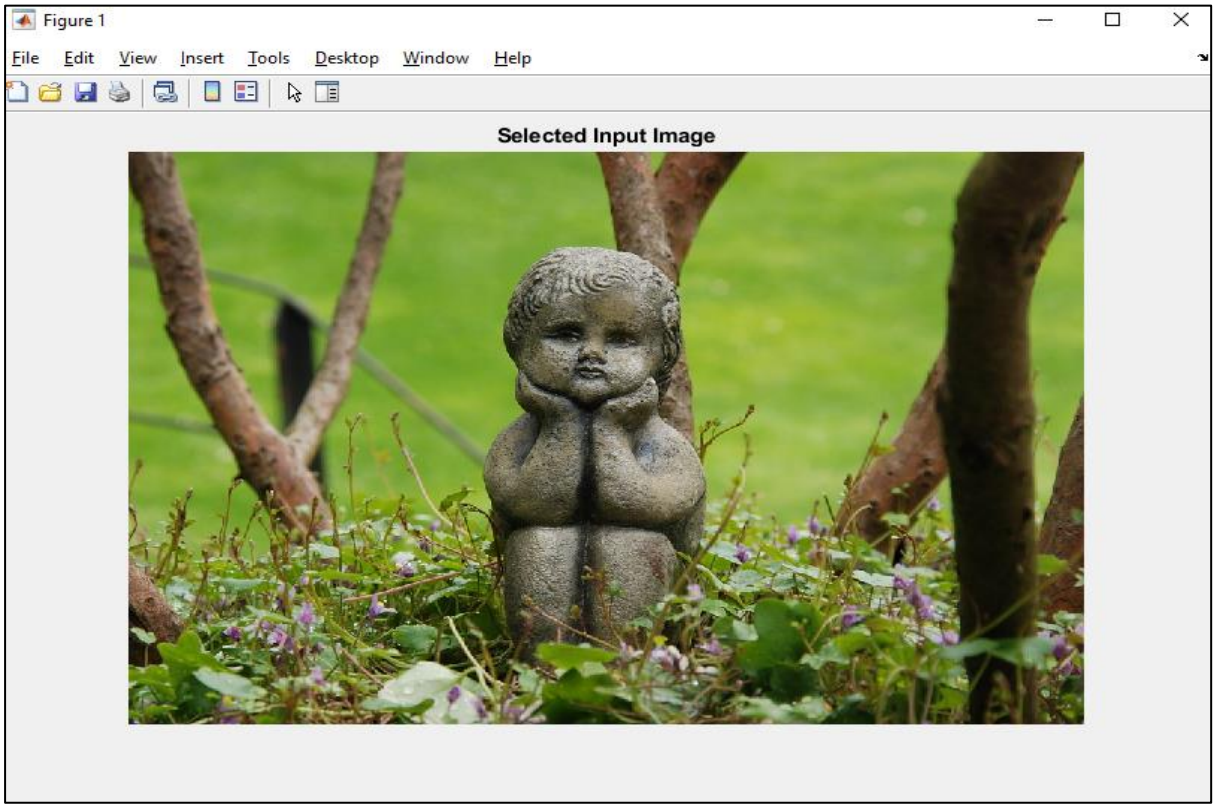

Figure 7.1: Selected Input image

Figure 7.2: R, G and B Channel extraction of input image

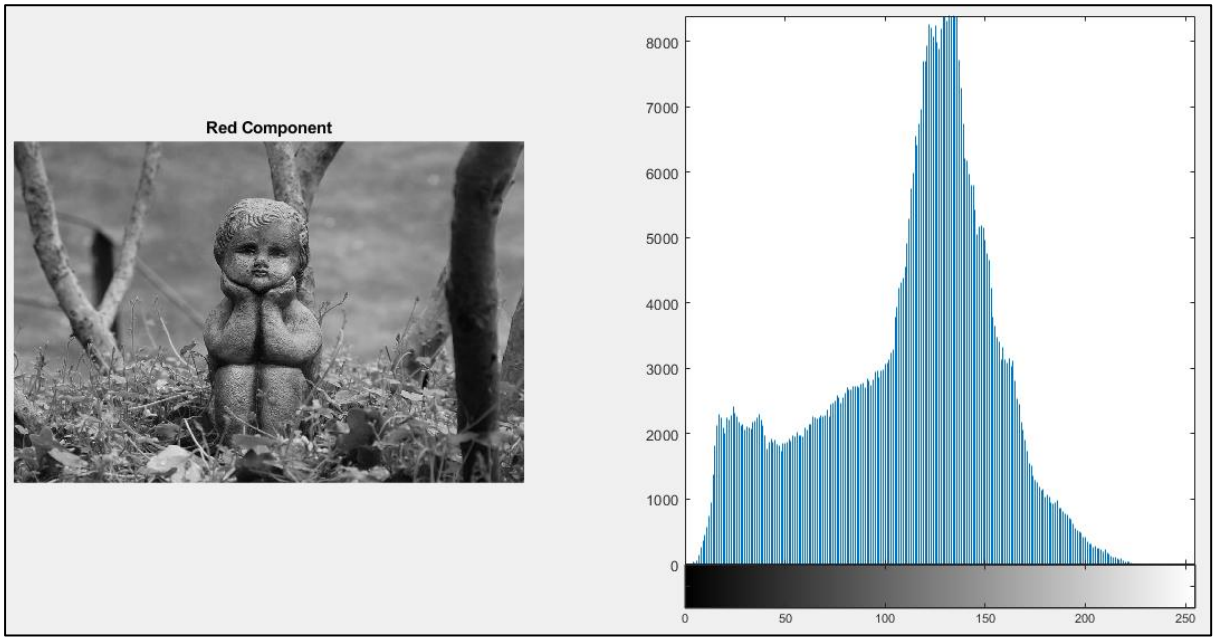

Figure 7.3: Red component of an image with its Histogram

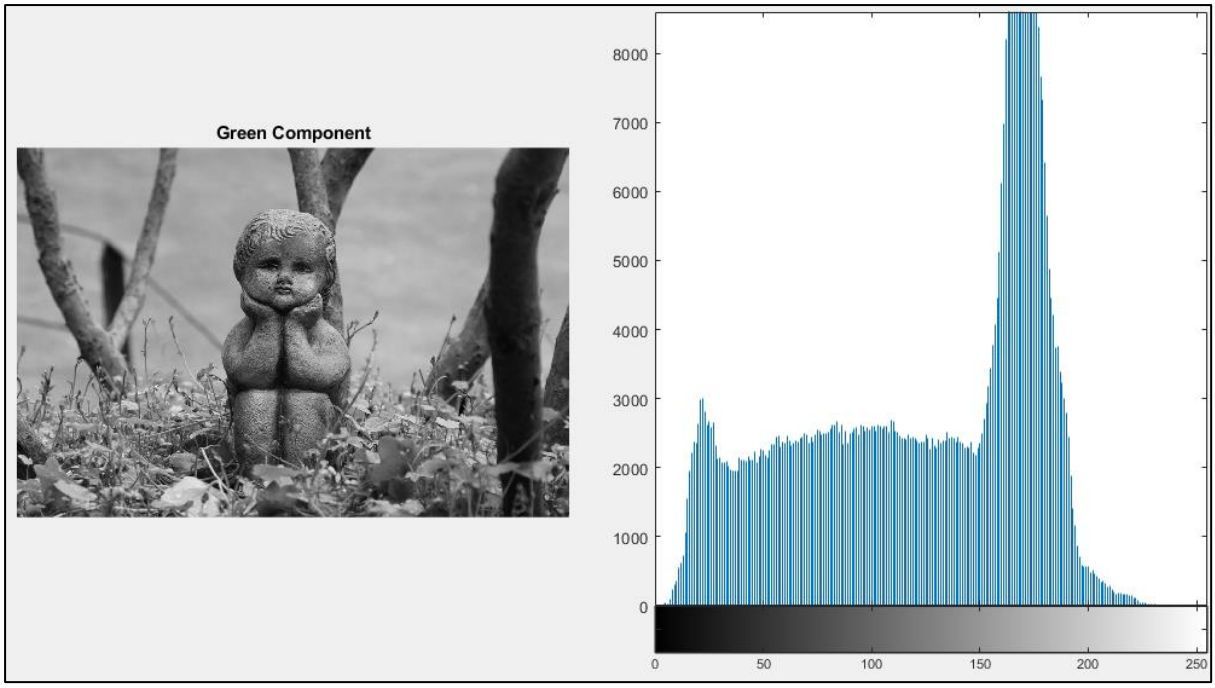

Figure 7.4: Green component of an image with its Histogram

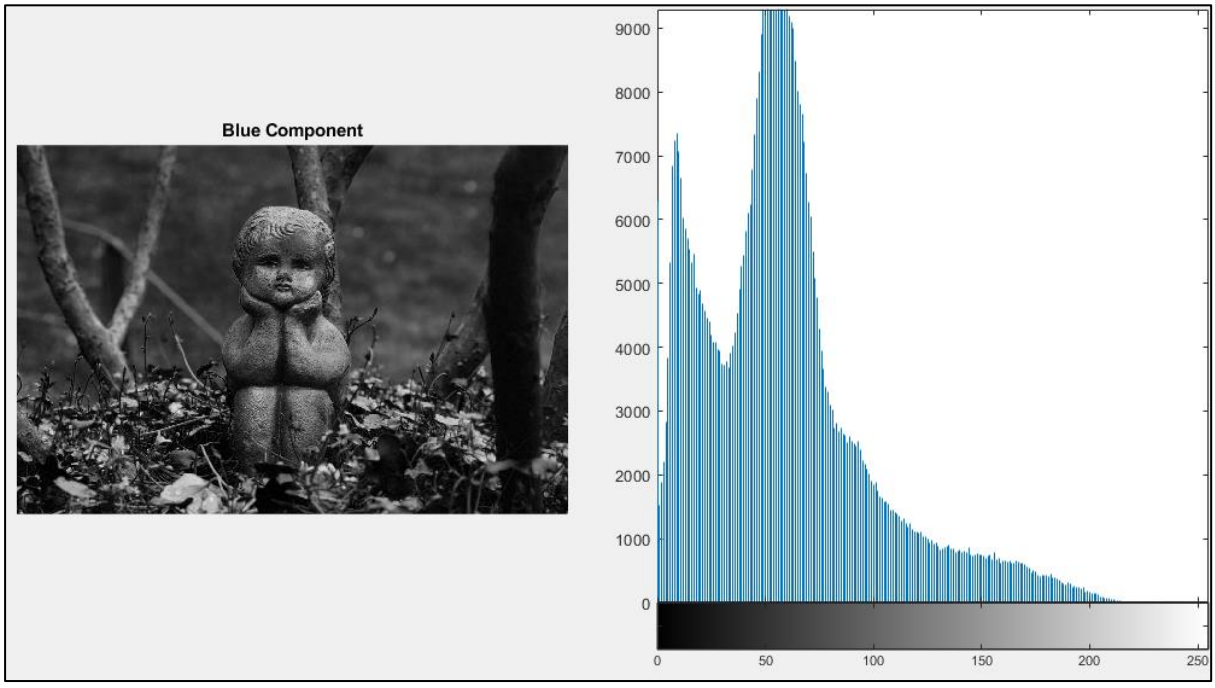

Figure 7.5: Blue component of an image with its Histogram

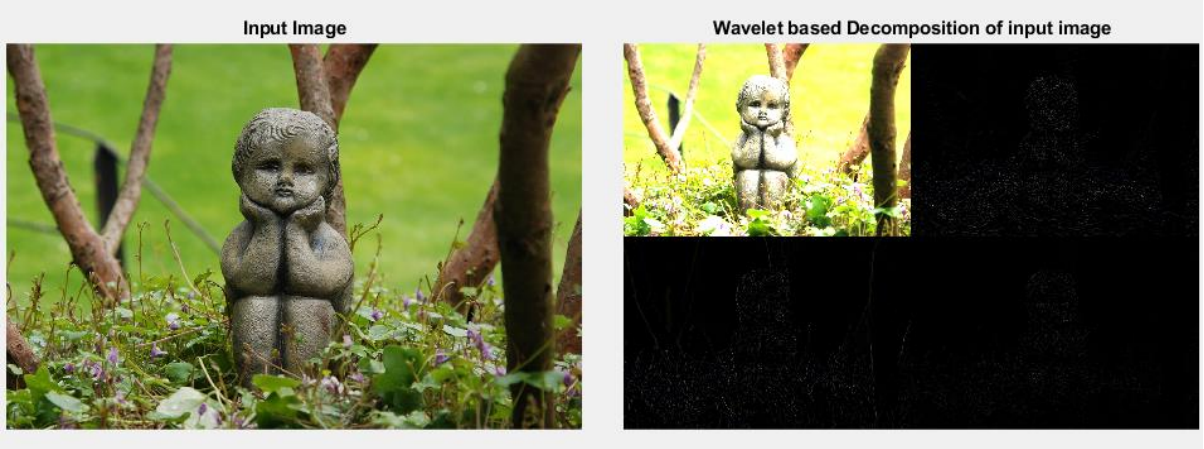

Figure 7.6: Wavelet based decomposed image

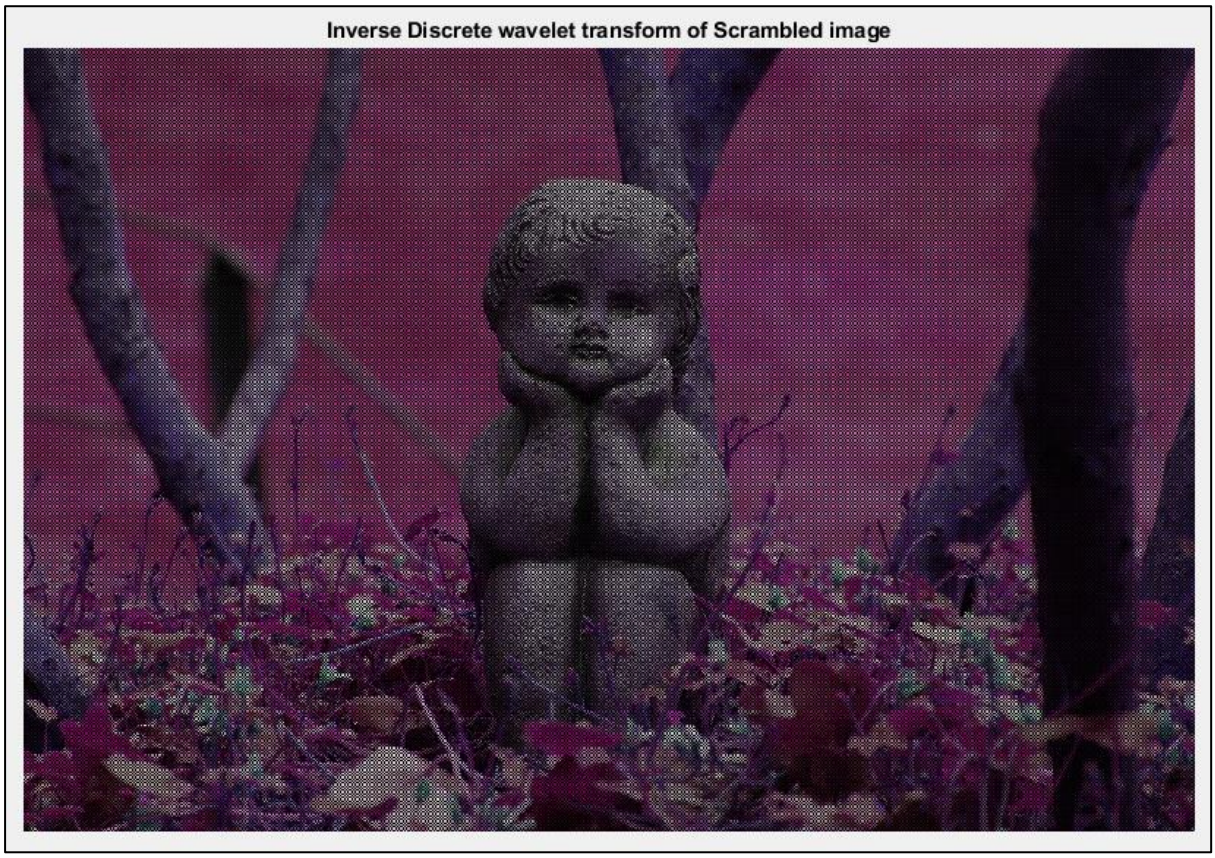

Figure 7.7: Inverse Discrete Wavelet transform of Scrambled image

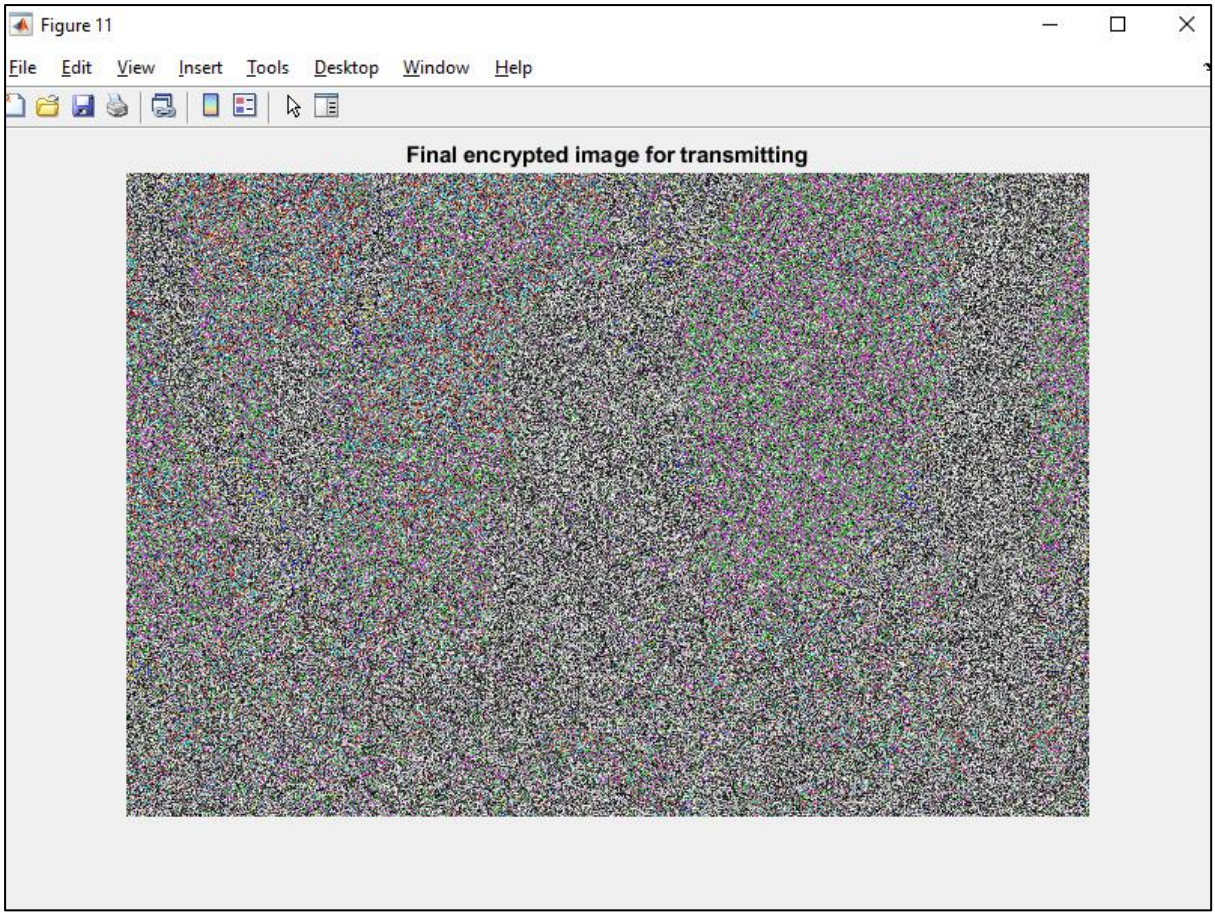

Figure 7.8: Final encrypted image for transmitting over the channel

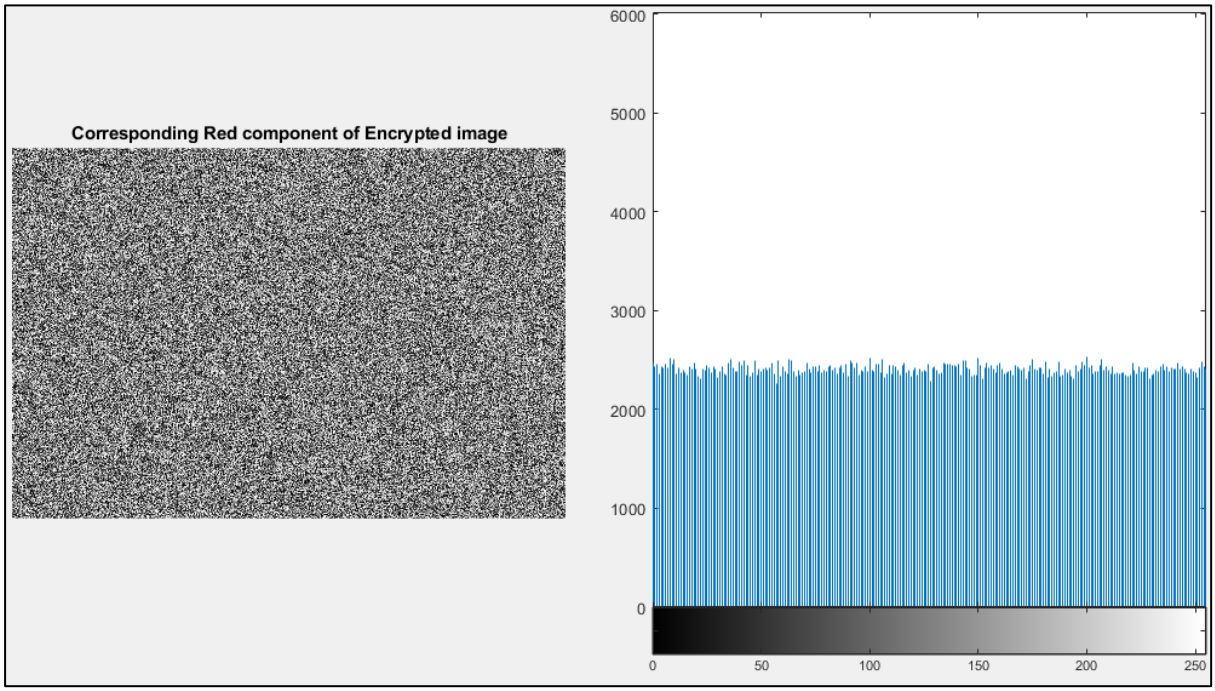

Figure 7.9: Histogram for the red channel of encrypted image

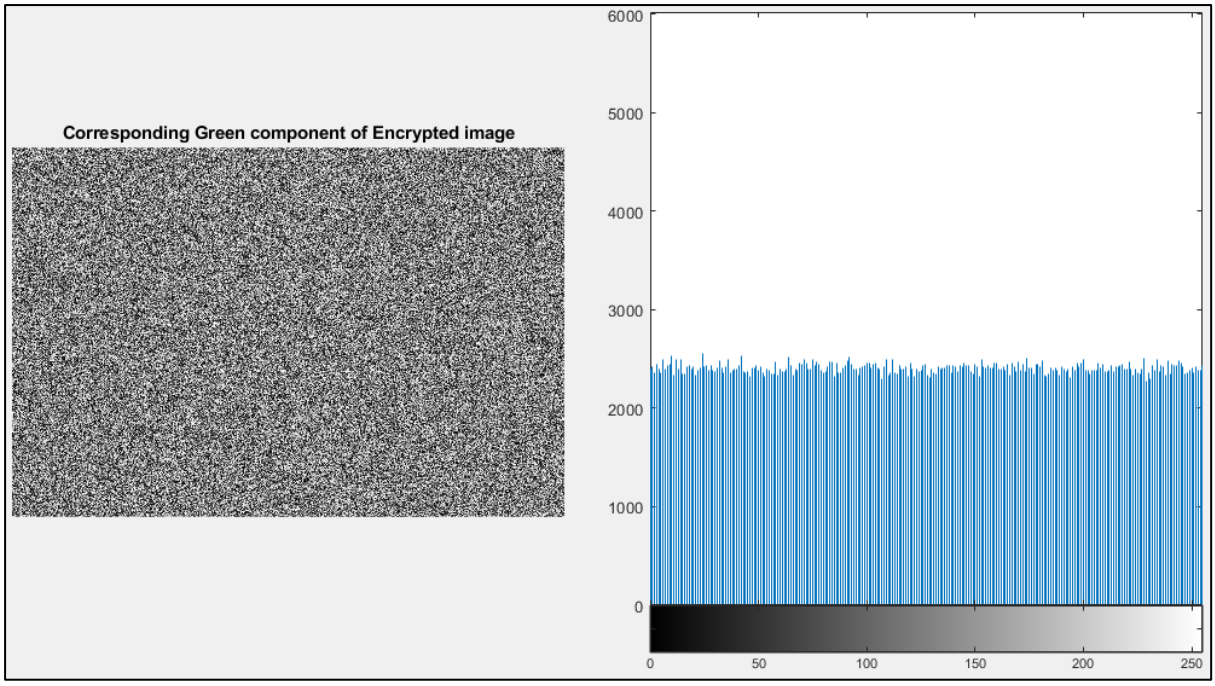

Figure 7.10: Histogram for the green channel of encrypted image

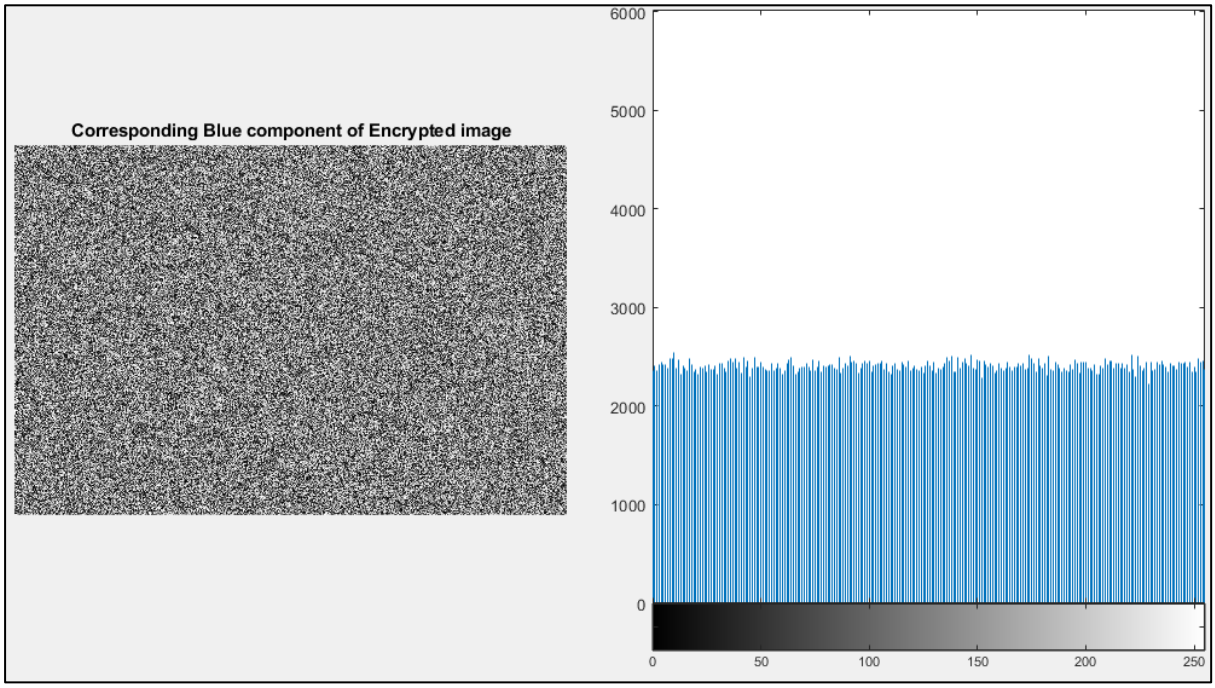

Figure 7.11: Histogram for the blue channel of encrypted image

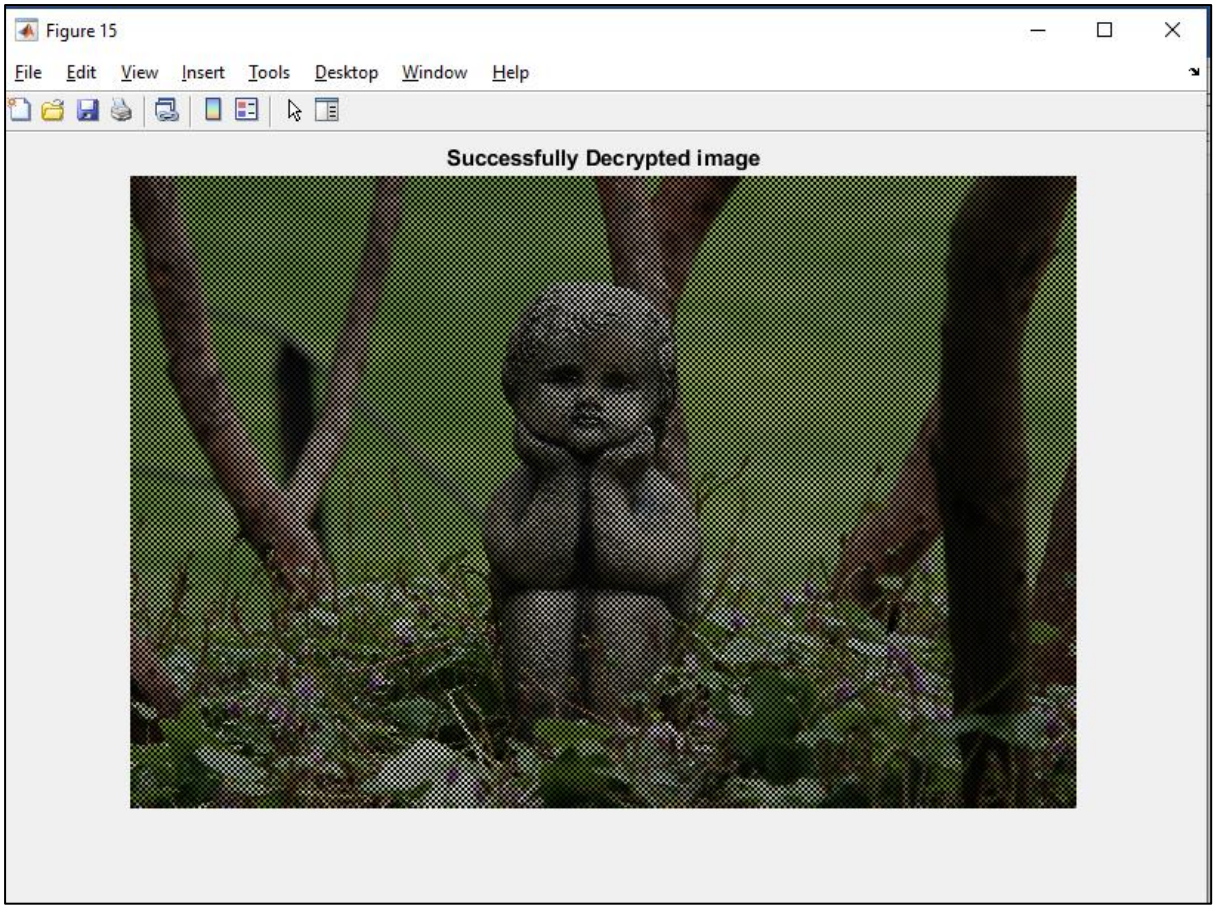

Figure 7.12: Final Decrypted image using proposed algorithm

CHPATER-8

CONCLUSION & FUTURE WORK

Now-a-days information security is becoming more important in data storage and transmission. Images are generally used in different processes. Therefore, the security of image data from unauthorized uses is important. 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 generate from the same image or any image must the same size of origin color image. The sender and receiver shared the same image key which has the same properties of hash function therefore, the attacker cannot discover the plain image from the image key notably, if one pixel value is changed, different key will generated. Proposed algorithm give a good results through applied some statistical tests as well the proposed algorithm achieved 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.

APPENDIX-A

MATLAB SOFTWARE DESCRIPTION

MATLAB Introduction:

The name MATLAB stands for Matrix Laboratory. MATLAB was written originally. To provide easy access to matrix software developed by the LINPACK (linear system package) and EISPACK (Eigen system package) projects. MATLAB is a high-performance language for technical computing. It integrates computation, visualization, and programming environment. Furthermore, MATLAB is a modern programming language environment: it has sophisticated data structures, contains built-in editing and debugging tools, and supports object-oriented programming. These factors make MATLAB an excellent tool for teaching and research. MATLAB has many advantages compared to conventional computer languages (e.g., FORTRAN) for solving technical problems. MATLAB is an interactive system whose basic data element is an arraythat does not require dimensioning. The software package has been commercially available since 1984 and is now considered as a standard tool at most universities and industries worldwide. It has powerful built-inroutines that enable a very wide variety of computations. It also has easy to use graphics commands that make the visualization of results immediately available. Special applications are collected in packages referred to *as toolbox*. There are toolboxes for signal processing, symbolic computation, control theory, simulation, optimization, and several other fields of applied science and engineering.

Mathematical functions:

MATLAB offers many predefined mathematical functions for technical computing which

Contains a large set of mathematical functions. Typing help elfin and help spec fun calls up full lists of *elementary* and *special* functions respectively. There is a long list of mathematical functions that are *built* into MATLAB. These functions are called *built-ins*. Many standard mathematical functions, such as sin(x), cos(x), tan(x), ex, $ln(x)$, are evaluated by the functions sin, cos, tan, exp, and log respectively in MATLAB.

Basic plotting

MATLAB has an excellent set of graphic tools. Plotting a given data set or the resultsof computation is possible with very few commands. We are highly encouraged to plotMathematical functions and results of analysis as often as possible. Trying to understand mathematical equations with graphics is an enjoyable and very efficient way of learning mathematics.

Matrix generation

Matrices are the basic elements of the MATLAB environment. A matrix is a two-dimensionalArray consisting of mrows and ncolumns. Special cases are column vectors (n= 1) and rowVectors(m= 1). MATLAB supports two types of operations, known as matrix operationsand array operations

MATLAB provides functions that generate elementary matrices. The matrix of zeros, theMatrix of ones, and the identity matrix are returned by the functions zeros, ones, and eye,Respectively.

`eye(m,n)`	Returns an m-by-n matrix with 1 on the main diagonal
`eye(n)`	Returns an n-by-n square identity matrix
`zeros(m,n)`	Returns an m-by-n matrix of zeros
`ones(m,n)`	Returns an m-by-n matrix of ones
`diag(A)`	Extracts the diagonal of matrix A
`rand(m,n)`	Returns an m-by-n matrix of random numbers

Table 1:Elementary matrices

Programming in Matlab

M-File scripts

A script fileis an external file that contains a sequence of MATLAB statements. Script Files have a filename extension .m and are often called M-files. M-files can be scripts that simply execute a series of MATLAB statements, or they can be functionsthat can accept arguments and can produce one or more outputs.

Script side-effects

All variables created in a script file are added to the workspace. This may have undesirable effects, because:

- Variables already existing in the workspace may be overwritten.
- The execution of the script can be affected by the state variables in the workspace.

As a result, because scripts have some undesirable side-effects, it is better to code any Complicated applications using rather function M-file.

Input to script Files

When a script file is executed, he variables that are used in the calculations within the file must have assigned values. The assignment of a value to a variable can be done in three ways.

1. The variable is defined in the script file.
2. The variable is defined in the command prompt.
3. The variable is entered when the script is executed.

Output Commands

MATLAB automatically generates a displaywhen commands are executed. In addition to this automatic display, MATLAB has several commands that can be used to generate displays or outputs. Two commands that are frequently used to generate output are: disp and fprintf.

`disp`	. Simple to use. . Provide limited control over the appearance of output
`fprintf`	. Slightly more complicated than `disp`. . Provide total control over the appearance of output

Table 2:disp and fprint commands

Control Flow

MATLAB has four control flow structures:

1. The if statement
2. The for loop
3. The while loop

4. The switch statement

The ``if...end'' structure

MATLAB supports the variants of “if" construct.

- if ... end
- if ... else ... end
- if ... elseif ... else ... end

The simplest form of the if statement is

If expression

Statements

end

It should be noted that:

- elseif has no space between else and if (one word)
- no semicolon (;) is needed at the end of lines containing if, else, end
- indentation of if block is not required, but facilitate the reading.
- the end statement is required

Relational and logical operators

A relational operator compares two numbers by determining whether a comparison is *true* or *false*. Note that the “equal to" relational operator consists of two equal signs (==) (with no space between them), since = is reserved for the *assignment* operator

Operator	Description
>	Greater than
<	Less than
>=	Greater than or equal to
<=	Less than or equal to
==	Equal to
~=	Not equal to
&	AND operator
|	OR operator
~	NOT operator

Table 3: Relational and logical operators

The “for...end" loop

In the for ... end loop, the execution of a command is repeated at a fixed and predetermined number of times. The syntax is

for variable = expression

Statements

end

It is a good idea to indent the loops for readability, especially when they are nested. Note that MATLAB editor does it automatically. Multiple for loops can be nested, in which case *indentation* helps to improve the readability. The following statements form the 5-by-5 symmetric matrix A with (*i; j*) element *i=j* for *j > i*:

The ``while...end'' loop

This loop is used when the number of *passes* is not specified. The looping continues until a stated condition is satisfied. The while loop has the form:

while expression

statements

end

Other flow structures

- The break statement. A while loop can be terminated with the break statement,which passes control to the first statement after the corresponding end. The breakstatement can also be used to exit a for loop.
- The continue statement can also be used to exit a for loop to pass immediately tothe next iteration of the loop, skipping the remaining statements in the loop.
- Other control statements include return, continue, switch, etc.

Bitwise operators

1) bitand - Bit-wise AND.
2) bitcmp - Complement bits.
3) bitor - Bit-wise OR.
4) bitmax - Maximum floating point integer.
5) bitxor - Bit-wise XOR.
6) bitset - Set bit.
7) bitget - Get bit.
8) bitshift - Bit-wise shift.

Above are the bitwise operators that are used in Matlab.

Other Commands

- Imread command is used to read an image
- Imshow command is used to display an image
- Waveread command is used to read a audio signal
- Wavplay command is used to play the audio file.
- Imresize command is used to resize the image for given value.
- Reshape command is used to convert into one dimension.

Saving output to a File

In addition to displaying output on the screen, the command fprintf can be used forWriting the output to a file. The saved data can subsequently be used by MATLAB or other software's.To save the results of some computation to a file in a text format requires the following

Steps:

1. Open a file using fopen
2. Write the output using fprintf
3. Close the file using fclose

Debugging M-Files

Introduction

This section introduces general techniques for finding errors in M-files. Debugging is the Process by which you isolate and fix errors in your program or code.

Debugging helps to correct two kinds of errors:

- Syntax errors - For example omitting a parenthesis or misspelling a function name.
- Run-time errors - Run-time errors are usually apparent and difficult to track down. They produce unexpected results.

Debugging process

We can debug the M-files using the Editor/Debugger as well as using debugging functions from the Command Window. The debugging process consists of Preparing for debugging:

- Setting breakpoints
- Running an M-file with breakpoints

- Stepping through an M-file
- Examining values
- Correcting problems
- Ending debugging

Preparing for debugging

Here we use the Editor/Debugger for debugging. Do the following to prepare for debugging:

- Open the file
- Save changes
- Be sure the file you run and any files it calls are in the directories that are on the search path.

Setting breakpoints

Set breakpoints *to pause* execution of the function, so we can examine where the problem might be. There are three basic types of breakpoints:

- A standard breakpoint, which stops at a specified line.
- A conditional breakpoint, which stops at a specified line and under specified conditions.
- An error breakpoint that stops when it produces the specifed type of warning, error,NaN, or infinite value.

Running with breakpoints

After setting breakpoints, run the M-file from the Editor/Debugger or from the Command Window. Running the M-file results in the following:

- The prompt in the Command Window changes to

  K>>

  Indicating that MATLAB is in debug mode.
- The program pauses at the ¯*rst*breakpoint. This means that line will be executedwhen you continue. The pause is indicated by the green arrow.
- In breakpoint, we can examine variable, step through programs, and run other calling functions.

Examining values

While the program is paused, we can view the value of any variable currently in the workspace. Examine values when we want to see whether a line of code has produced the expected result or not. If the result is as expected, step to the next line, and continue running. If the result is not as expected, then that line, or the previous line, contains an*error*. When we

run a program, the current workspace is shown in the Stack field. Use who or whos to list the variables in the current workspace.

Viewing values as datatips

First, we position the cursor to the left of a variable on that line. Its current value appears.This is called a datatip, which is like a tooltipfor data. If you have trouble getting thedatatip to appear, click in the line and then move the cursor next to the variable.

Correcting and ending debugging

While debugging, we can change the value of a variable to see if the *new* value produces expected results. While the program is paused, assign a new value to the variable in the Command Window, Workspace browser, or Array Editor. Then continue running and stepping through the program.

Ending debugging

After identifying a problem, end the debugging session. It is best to quit debug modebefore editing an M-file. Otherwise, you can get unexpected results when you run the file. To enddebugging, select Exit Debug Mode from the Debug menu.

Correcting an M-file

To correct errors in an M-file,

- Quit debugging
- Do not make changes to an M-file while MATLAB is in debug mode
- Make changes to the M-file
- Save the M-file
- Clear breakpoints

Strengths

MATLAB may behave as a calculatoror as a programming langua*ge*

- MATLAB combine nicely calculation and graphic plotting.
- MATLAB is relatively easy to learn
- MATLAB is interpreted (not compiled), errors are easy to fix
- MATLAB is optimized to be relatively fast when performing matrix operations
- MATLAB does have some object-oriented elements

Weaknesses

- MATLAB is not a general purpose programming language such as C, C++, or FORTRAN.
- MATLAB is designed for scientific computing, and is not well suitable for other applications.
- MATLAB is an interpreted language, slower than a compiled language such as C++
- MATLAB commands are specific for MATLAB usage. Most of them do not have a direct equivalent with other programming language commands

APPENDIX-B
MATLAB Code

```
clc;
close all;
clear all;

%% Reading an input image
[f,p] = uigetfile('.jpg');
x = strcat(p,f);
im = imread(x);

figure, imshow(im); title('Selected Input Image');

%% Extracting the individual planes from the original image
R = im(:,:,1);
G = im(:,:,2);
B = im(:,:,3);

figure, subplot(2,2,1); imshow(im); title('Original RGB Image');
subplot(2,2,2); imshow(R); title('Red Component Image');
subplot(2,2,3); imshow(G); title('Green Component Image');
subplot(2,2,4); imshow(B); title('Blue Component Image');

figure, subplot(1,2,1); imshow(R);title('Red Component');
subplot(1,2,2); imhist(R);
figure, subplot(1,2,1); imshow(G);title('Green Component');
subplot(1,2,2); imhist(G);
figure, subplot(1,2,1); imshow(B);title('Blue Component');
subplot(1,2,2); imhist(B);
```

```
%% Generating Image Key
key_1D = keyGeneration(im);

size_key = size(key_1D)

%% ENCRYPTION PROCESS STARTS NOW
%%% Applying Discrete Wavelet Transform for the individual plane of Input image
[iLLr1,iLHr1,iHLr1,iHHr1]=dwt2(R,'haar');
[iLLg1,iLHg1,iHLg1,iHHg1]=dwt2(G,'haar');
[iLLb1,iLHb1,iHLb1,iHHb1]=dwt2(B,'haar');
First_Level_Decompositioni(:,:,1)=[iLLr1,iLHr1;iHLr1,iHHr1];
First_Level_Decompositioni(:,:,2)=[iLLg1,iLHg1;iHLg1,iHHg1];
First_Level_Decompositioni(:,:,3)=[iLLb1,iLHb1;iHLb1,iHHb1];
First_Level_Decompositioni=uint8(First_Level_Decompositioni);

%Display Image
figure, subplot(1,2,1);imshow(im);title('Input Image');
subplot(1,2,2);imshow(First_Level_Decompositioni,[]);title('Wavelet based Decomposition
of input image');

idwt_image(:,:,1) = uint8(idwt2(iLLr1,iLHr1,iHLr1,iHHr1,'haar'));
idwt_image(:,:,2) = uint8(idwt2(iLLg1,iLHg1,iHLg1,iHHg1,'haar'));
idwt_image(:,:,3) = uint8(idwt2(iLLb1,iLHb1,iHLb1,iHHb1,'haar'));
figure, imshow(idwt_image); title('original idwt image');

Scrambled_Image(:,:,1) = uint8(idwt2(iLHg1,iHLg1,iHHg1,iLLg1,'haar'));
Scrambled_Image(:,:,2) = uint8(idwt2(iLHb1,iHLb1,iHHb1,iLLb1,'haar'));
Scrambled_Image(:,:,3) = uint8(idwt2(iLHr1,iHLr1,iHHr1,iLLr1,'haar'));

figure, imshow(Scrambled_Image); title('Inverse Discrete wavelet transform of Scrambled
image');

encrypted_image = imageProcess(Scrambled_Image,uint8(key_1D));
```

```
figure,imshow(encrypted_image); title('Final encrypted image for transmitting');

%% DECRYPTION PROCEDURE
R1 = encrypted_image(:,:,1);
G1 = encrypted_image(:,:,2);
B1 = encrypted_image(:,:,3);

figure, subplot(1,2,1); imshow(R1);title('Corresponding Red component of Encrypted
image');
subplot(1,2,2); imhist(R1);
figure, subplot(1,2,1); imshow(G1);title('Corresponding Green component of Encrypted
image');
subplot(1,2,2); imhist(G1);
figure, subplot(1,2,1); imshow(B1);title('Corresponding Blue component of Encrypted
image');
subplot(1,2,2); imhist(B1);

%%% Applying Discret Wavelet Transform for the individual plane of Input image
[iLLr2,iLHr2,iHLr2,iHHr2]=dwt2(R1,'haar');
[iLLg2,iLHg2,iHLg2,iHHg2]=dwt2(G1,'haar');
[iLLb2,iLHb2,iHLb2,iHHb2]=dwt2(B1,'haar');
First_Level_Decompositionj(:,:,1)=[iLLb2,iLHb2;iHLb2,iHHb2];
First_Level_Decompositionj(:,:,2)=[iLLr2,iLHr2;iHLr2,iHHr2];
First_Level_Decompositionj(:,:,3)=[iLLg2,iLHg2;iHLg2,iHHg2];
First_Level_Decompositionj=uint8(First_Level_Decompositionj);

UnScrambled_Image(:,:,1) = uint8(idwt2(iLLb2,iLHb2,iHLb2,iHHb2,'haar'));
UnScrambled_Image(:,:,2) = uint8(idwt2(iLLr2,iLHr2,iHLr2,iHHr2,'haar'));
UnScrambled_Image(:,:,3) = uint8(idwt2(iLLg2,iLHg2,iHLg2,iHHg2,'haar'));

Decrypted_image = imageProcess(UnScrambled_Image,uint8(key_1D));

figure,imshow(Decrypted_image); title('Successfully Decrypted image');
```

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.

[12] Pall A. K., Biswas G. P. and Mukhopadhyay S. 2010 "Designing of High-Speed Image Cryptosystem Using VQ Generated Codebook and Index Table", International Conference on Recent Trends in Information, Telecommunication and Computing IEEE, pp39-43.

[13] Pang C. 2009 "An Image Encryption Algorithm Based on Discrete Wavelet Transform and Two Dimension Cat Mapping", Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing IEEE, Vol. 2, pp711-714.

[14] Acharya B., Patra S. K., and Panda G. 2008 "Image Encryption by Novel Cryptosystem Using Matrix Transformation", 1st International Conference on Emerging Trends in Engineering and Technology IEEE, pp77-81.

[15] Al-Khassaweneh M. and Aviyent S. 2008 "Image Encryption Scheme Based on Using Least Square Approximation Techniques", International Conference Electro Information Technology IEEE, pp108-111.

[16] Gupta M. et al. 2012 "A New Approach for Information Security using Asymmetric Encryption and Watermarking Technique" International Journal of Computer Applications (IJCA) Vol.57 No.14.

[17] Francia A., Yang M. and Trifas M. 2009 "Applied image processing to multimedia information security", Int. Conf. Image Analysis and Signal Processing IEEE, pp286 - 291

[18] Mursi M. et al. 2014 "Combination of Hybrid Chaotic Encryption and LDPC for Secure Transmission of Images over Wireless Networks", International Journal of Image, Graphics and Signal Processing, pp8-16.

[19] Toufik, B. and Mokhtar N. 2012 "The Wavelet Transform for Image Processing Applications. In: Advances in Wavelet Theory and Their Applications in Engineering, Physics and Technology", Chapter 17, InTech, USA, pp395-422.

[20] Sivakumar T. and Venkatesan R. 2014 "A Novel Approach for Image Encryption Using Dynamic Scan Pattern" International Journal of Computer Science IAENG, Vol. 41, No. 2, pp91-101.

[21] Thakur N, Devi S. 2011 "A new method for color image quality assessment" International Journal Computer Application. Vol. 15, No.2, pp10–17.

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.

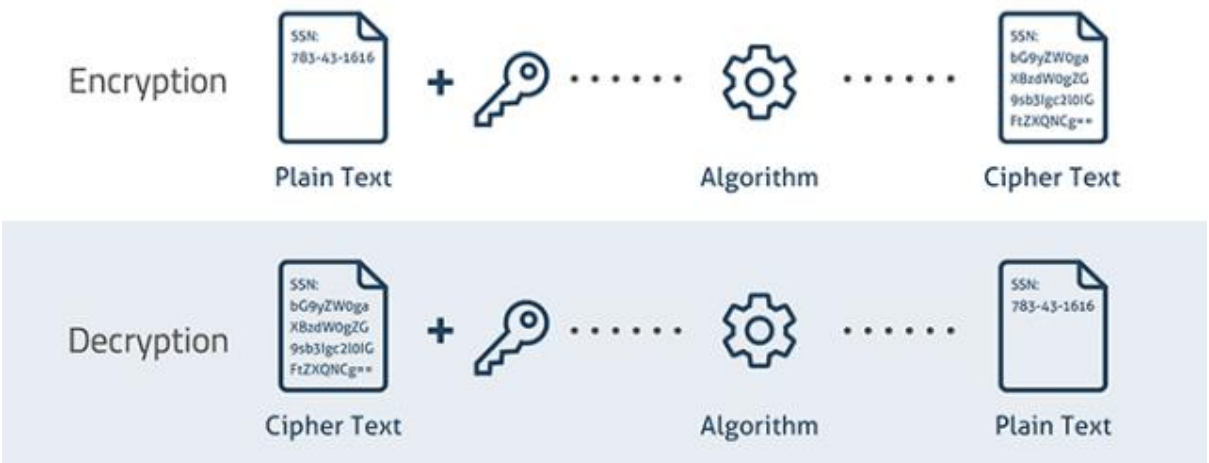

Figure 2.1: Sample Encryption and Decryption Process

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:

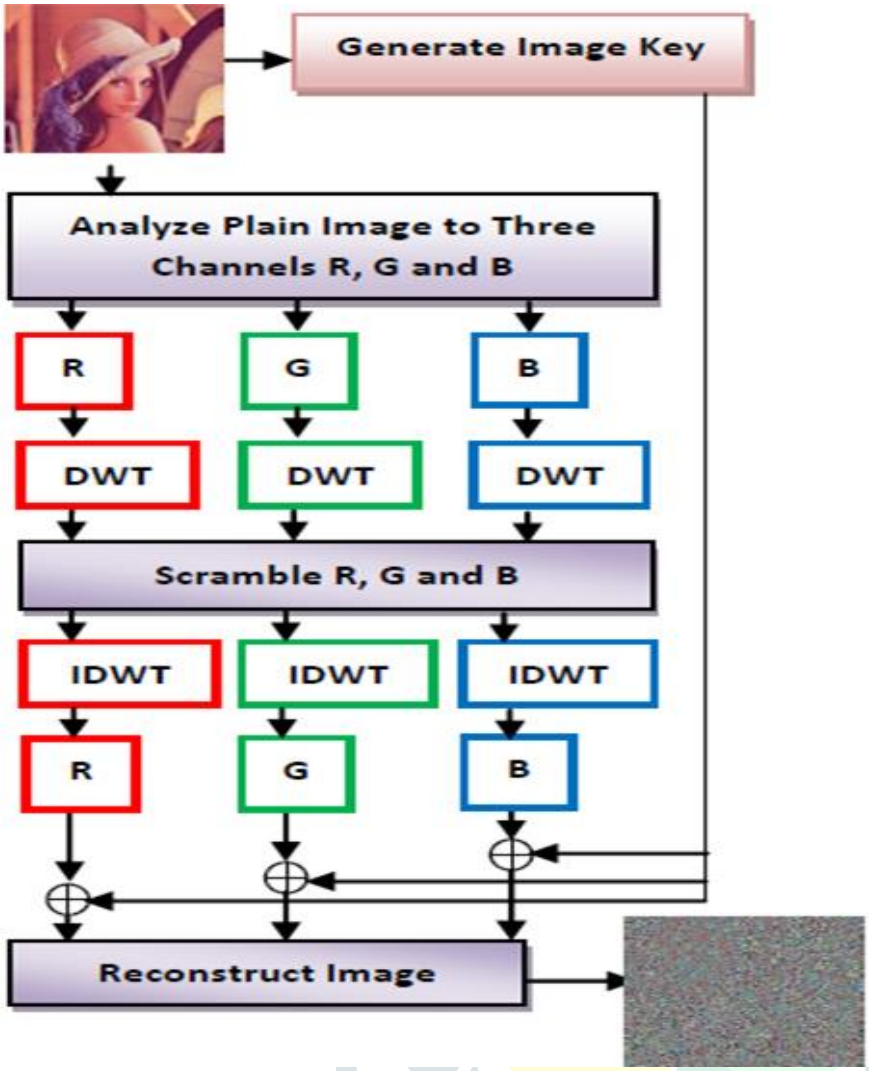

Figure 5.1: Proposed Decryption Algorithm

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.

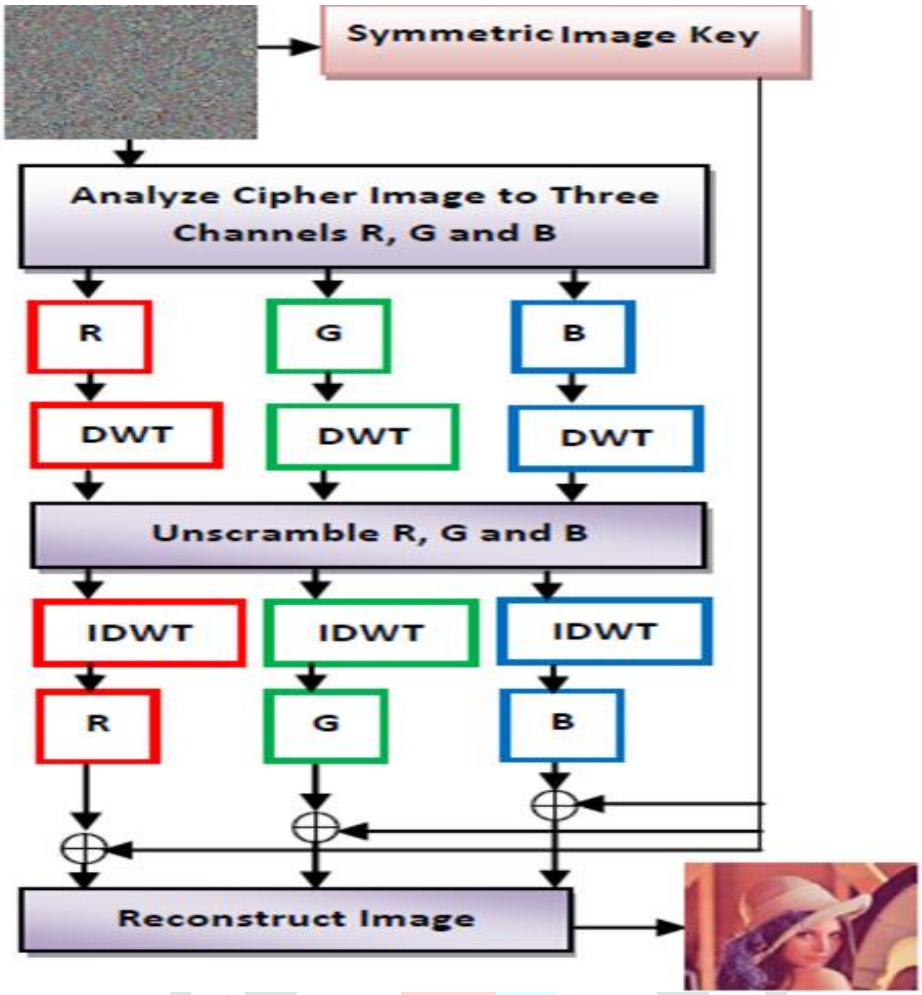

Figure 5.2: Proposed Decryption Algorithm

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.

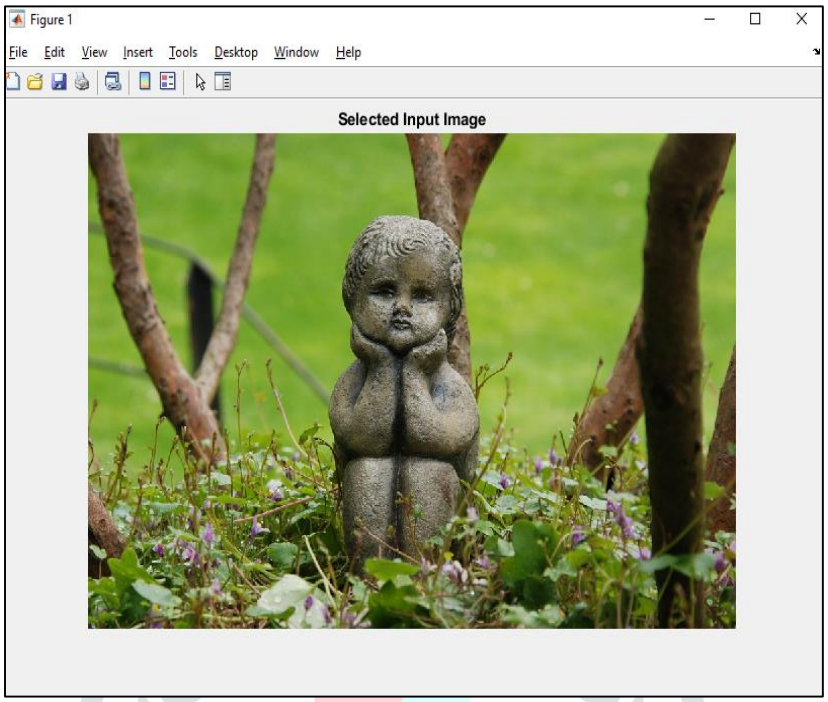

Figure 6.1: Selected Input image

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

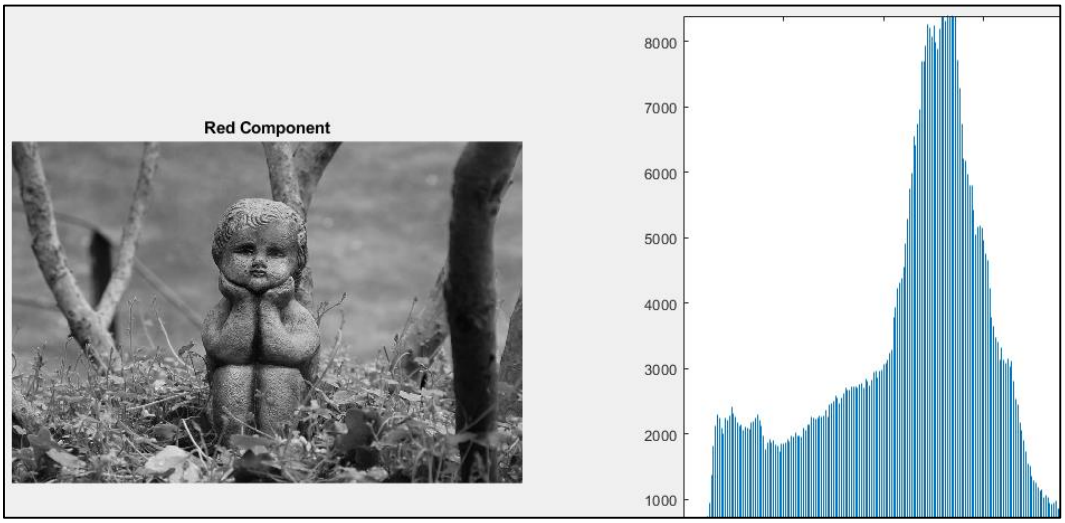

Figure 6.3: Red component of an image with its Histogram

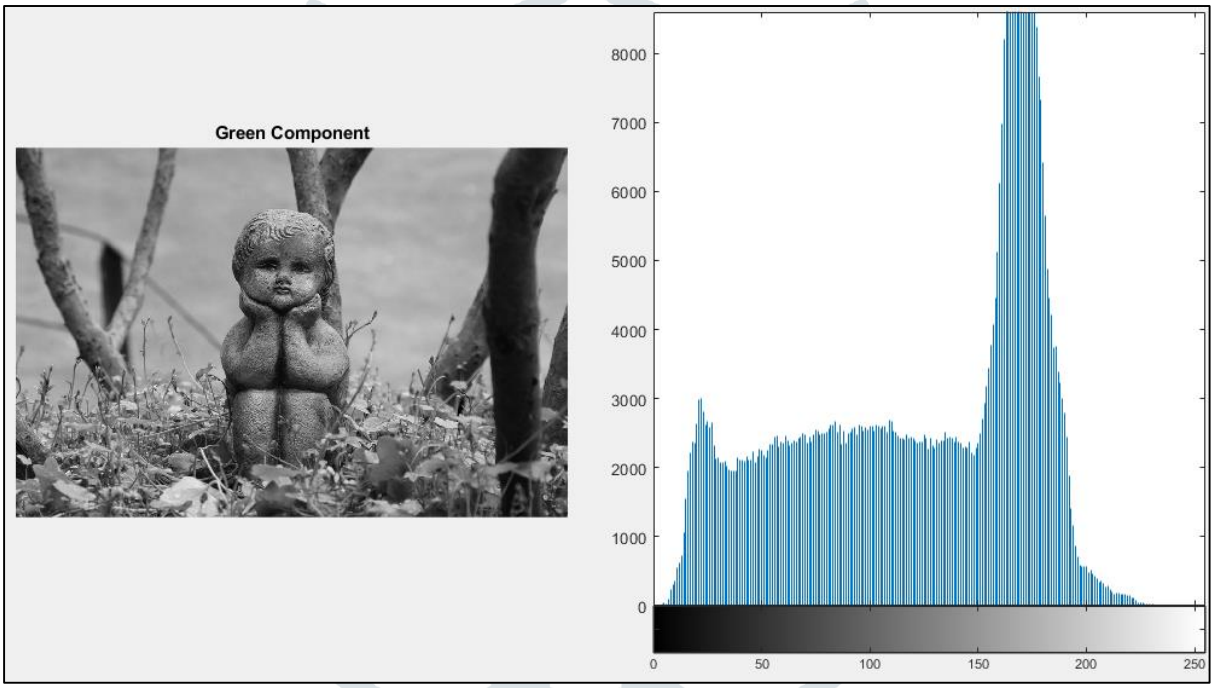

Figure 6.4: Green component of an image with its Histogram

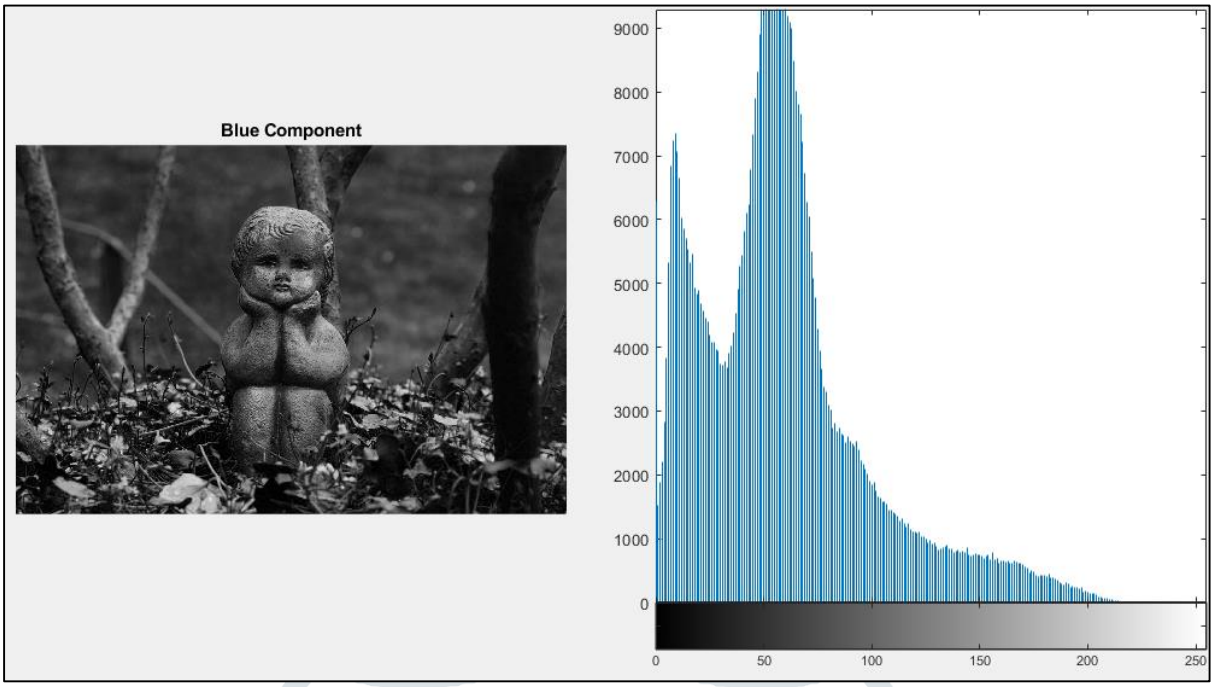

Figure 6.5: Blue component of an image with its Histogram

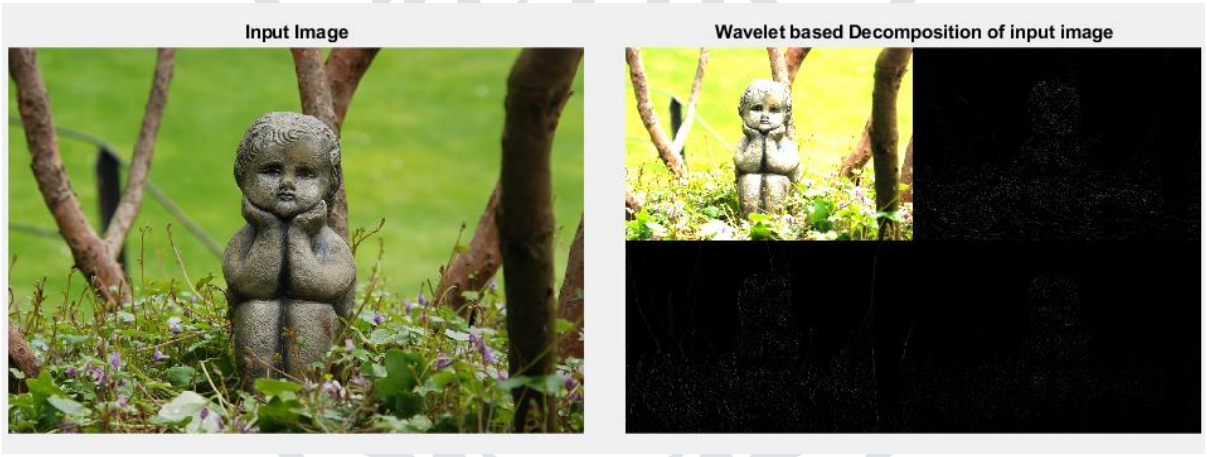

Figure 6.6: Wavelet based decomposed image

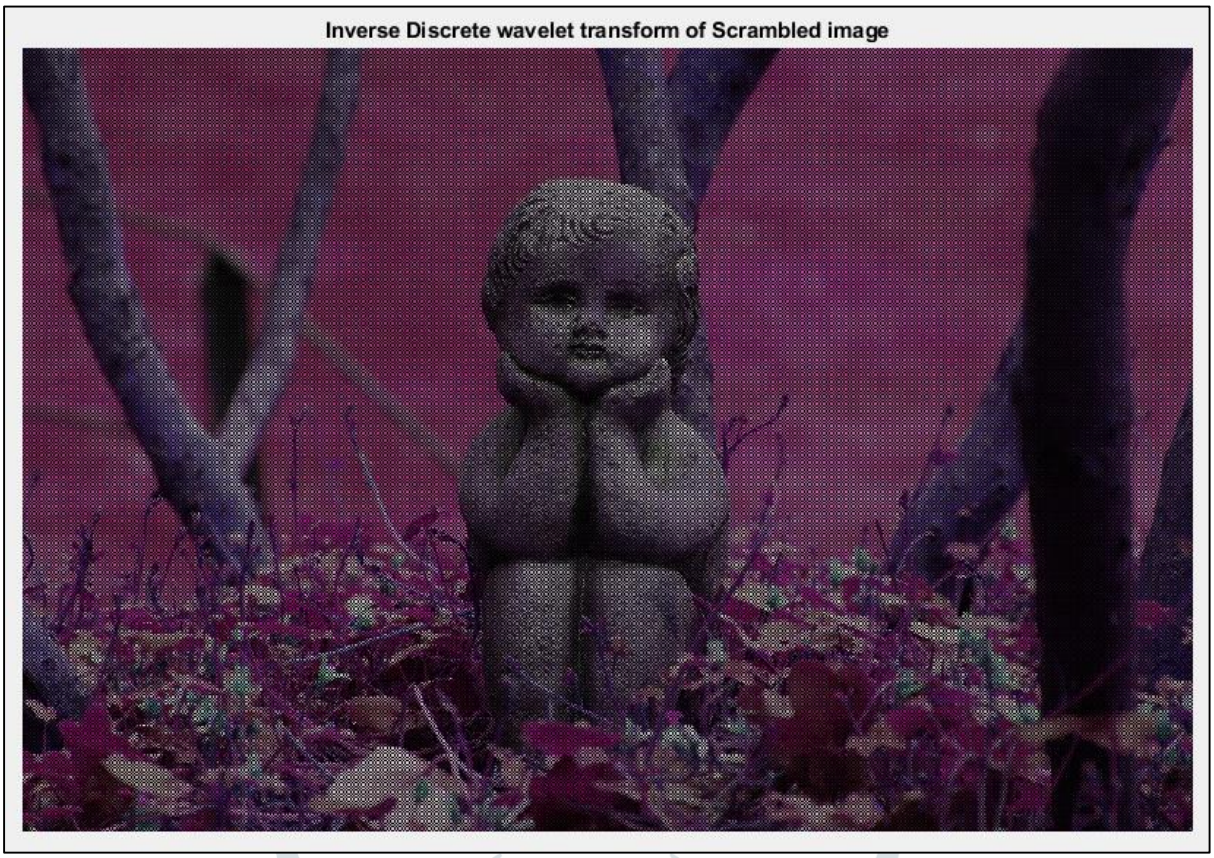

Figure 6.7: Inverse Discrete Wavelet transform of Scrambled image

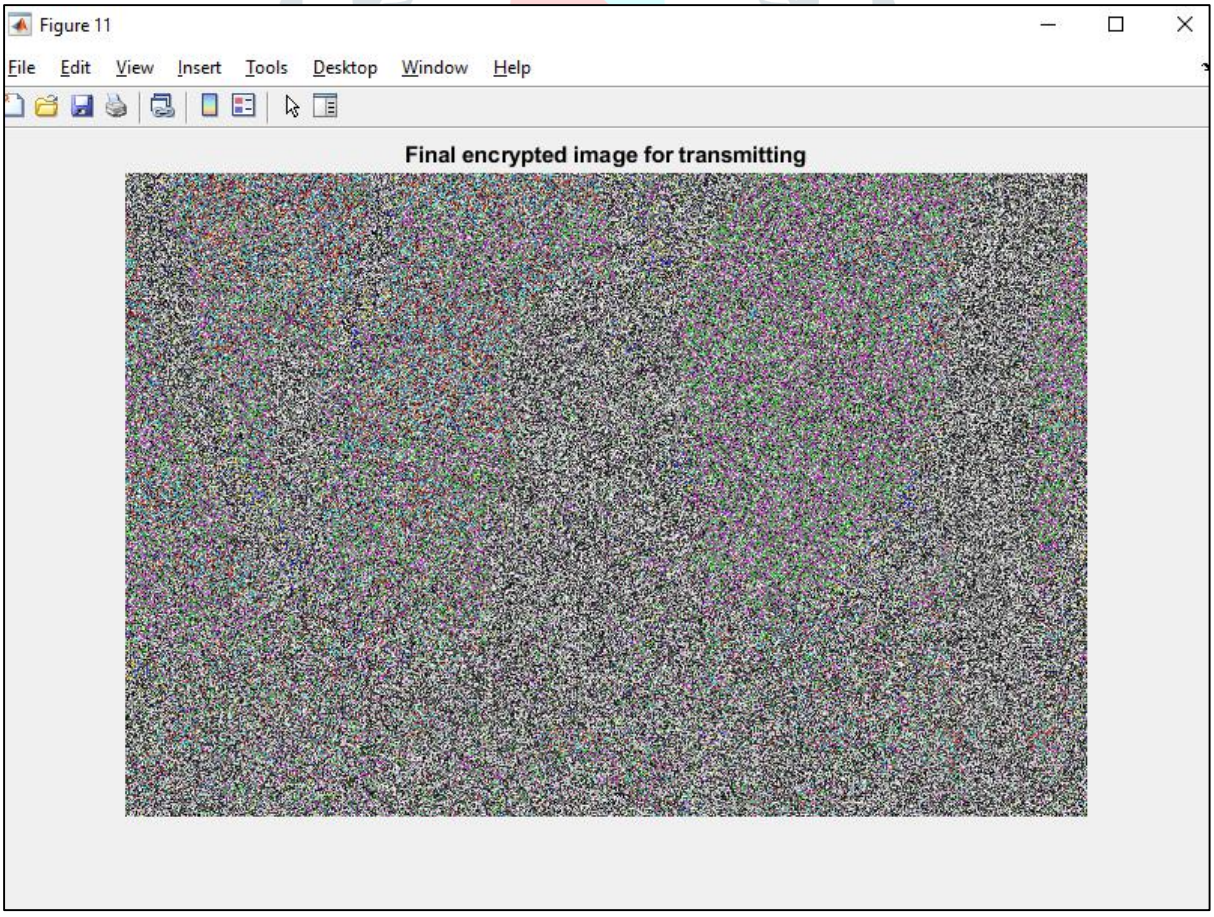

Figure 6.8: Final encrypted image for transmitting over the channel

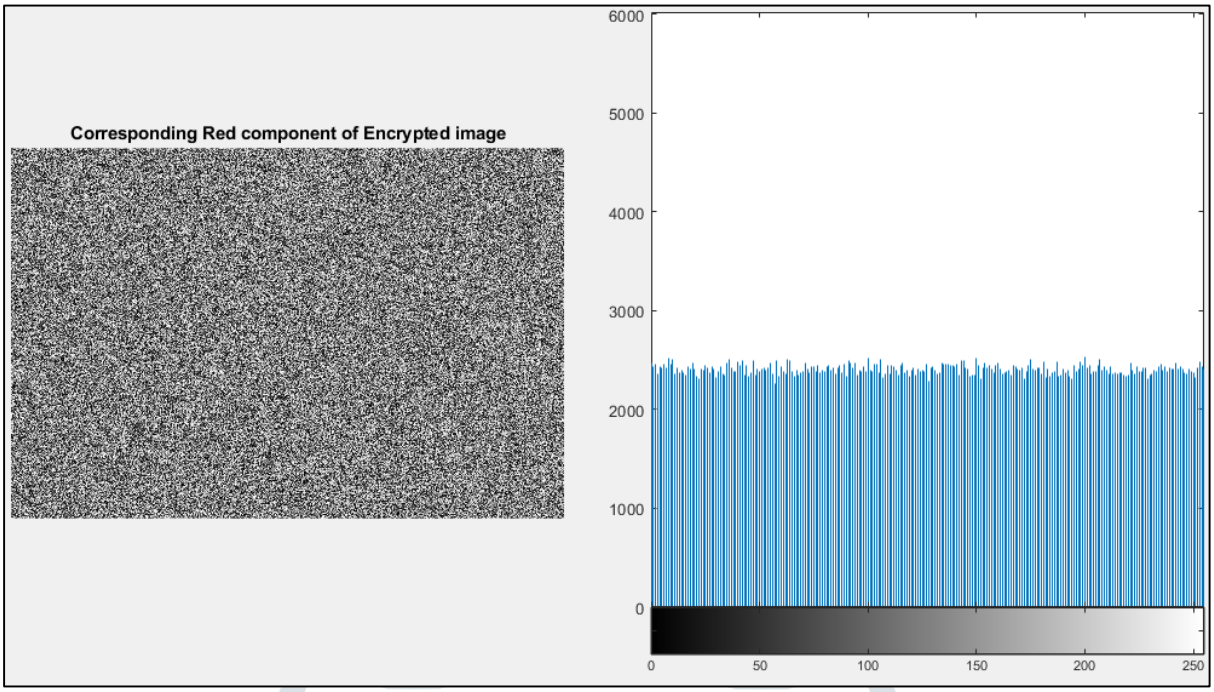

Figure 6.9: Histogram for the red channel of encrypted image

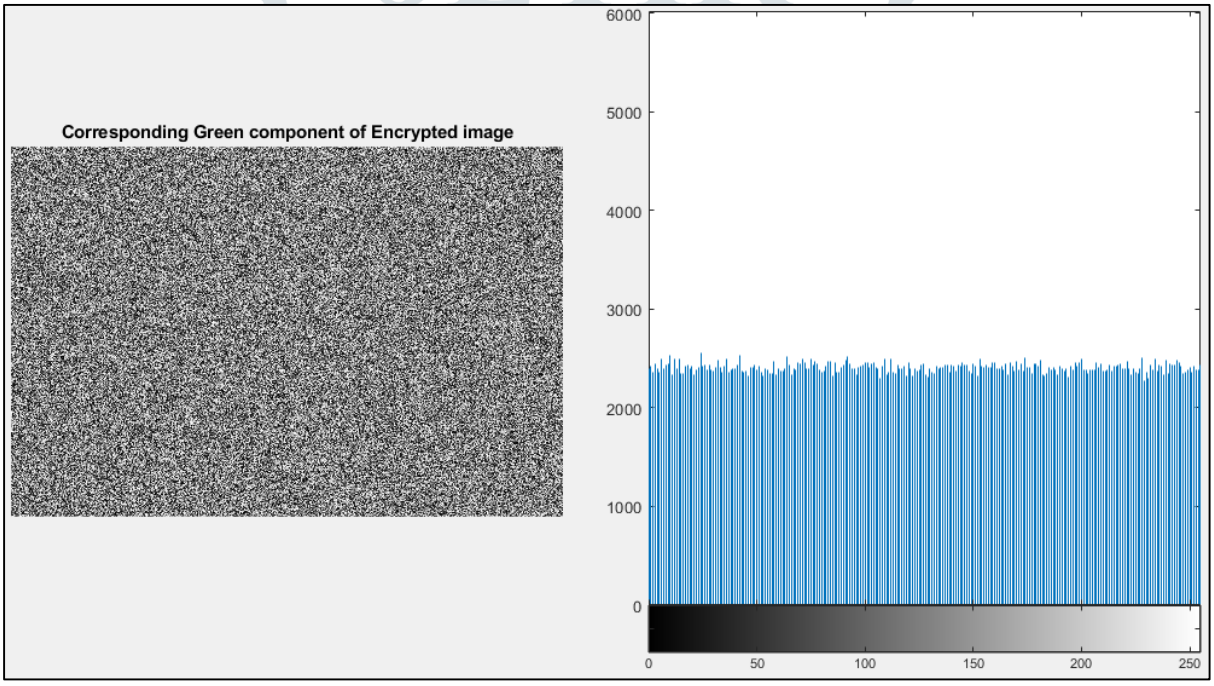

Figure 6.10: Histogram for the green channel of encrypted image

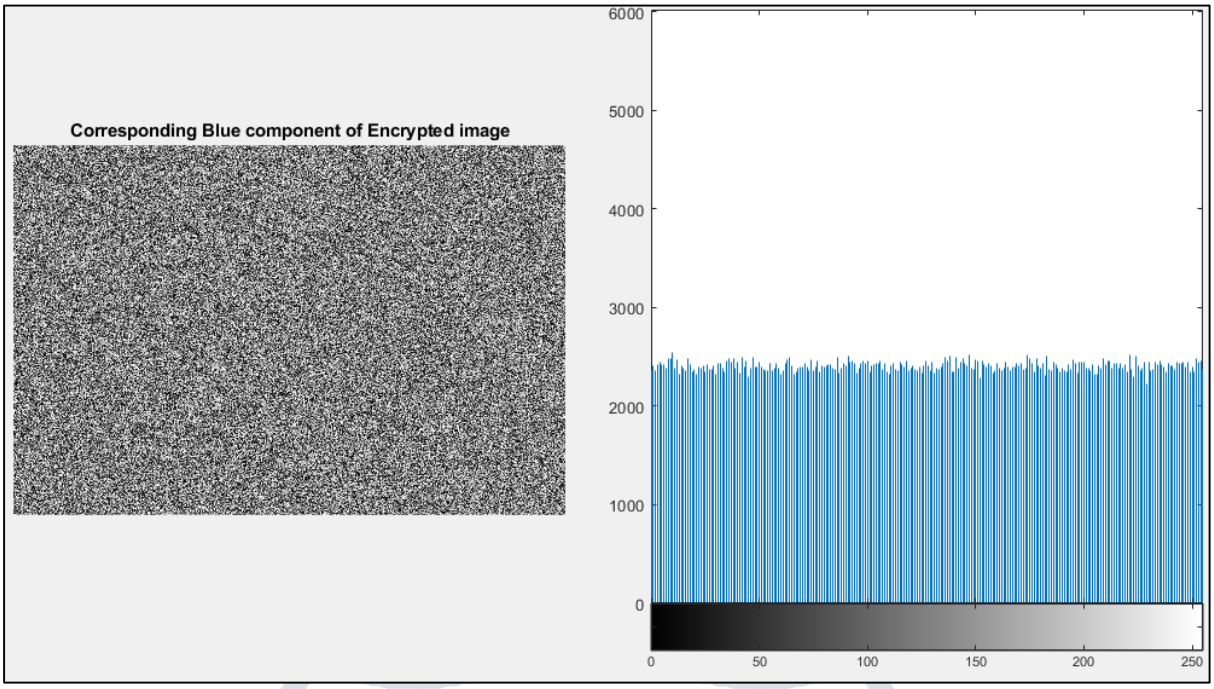

Figure 6.11: Histogram for the blue channel of encrypted image

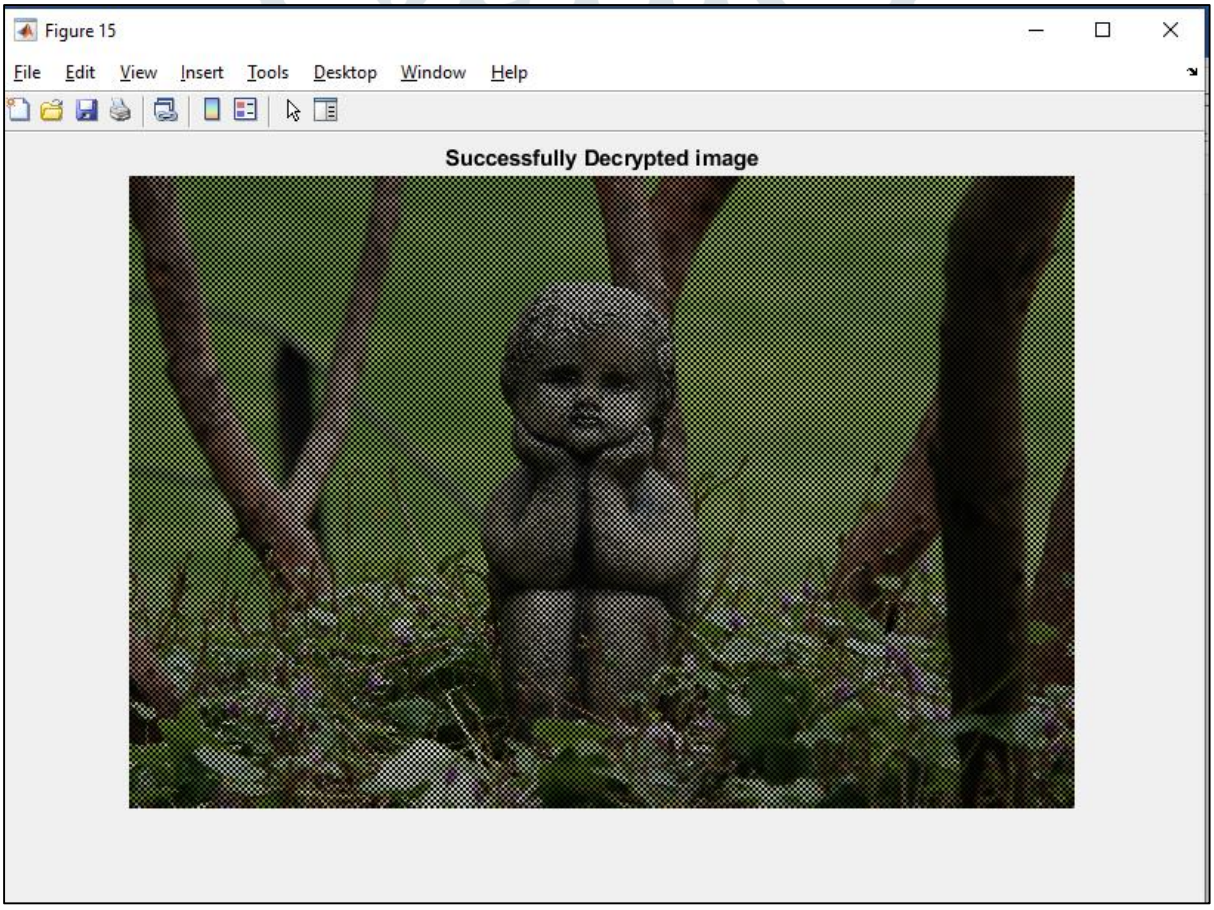

Figure 6.12: Final Decrypted image using proposed algorithm

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.

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal
www.jetir.org | editor@jetir.org

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

CH.Pavan Kumar

In recognition of the publication of the paper entitled

IMAGE ENCRYCPTION AND DECRYPTION USING RANDOM IMAGE KEY

Published In JETIR (www.JETIR.org) ISSN UGC Approved (Journal No: 63975) & 5.87 Impact Factor

Published in Volume 7 Issue 4 , April-2020 | Date of Publication: 2020-04-29

EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2004451 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2004451 Registration ID : 231125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal
www.jetir.org | editor@jetir.org

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

M. Bhuvaeswari Devi

In recognition of the publication of the paper entitled

IMAGE ENCRYCPTION AND DECRYPTION USING RANDOM IMAGE KEY

Published In JETIR (www.JETIR.org) ISSN UGC Approved (Journal No: 63975) & 5.87 Impact Factor

Published in Volume 7 Issue 4 , April-2020 | Date of Publication: 2020-04-29

Parin P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2004451 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2004451 Registration ID : 231125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal
www.jetir.org | editor@jetir.org

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

B.pavan sai

In recognition of the publication of the paper entitled

IMAGE ENCRYCPTION AND DECRYPTION USING RANDOM IMAGE KEY

Published In JETIR (www.JETIR.org) ISSN UGC Approved (Journal No: 63975) & 5.87 Impact Factor

Published in Volume 7 Issue 4 , April-2020 | Date of Publication: 2020-04-29

EDITOR

EDITOR IN CHIEF

JETIR2004451 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2004451 Registration ID : 231125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal
www.jetir.org | editor@jetir.org

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

G.Gopi Venkata Raja Reddy

In recognition of the publication of the paper entitled

IMAGE ENCRYCPTION AND DECRYPTION USING RANDOM IMAGE KEY

Published In JETIR (www.JETIR.org) ISSN UGC Approved (Journal No: 63975) & 5.87 Impact Factor

Published in Volume 7 Issue 4 , April-2020 | Date of Publication: 2020-04-29

Parisa P
EDITOR

EDITOR IN CHIEF

ISSN 2349-5162

JETIR2004451 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2004451 Registration ID : 231125

Journal of Emerging Technologies and Innovative Research
An International Open Access Journal
www.jetir.org | editor@jetir.org

Certificate of Publication

The Board of

Journal of Emerging Technologies and Innovative Research (ISSN : 2349-5162)

Is hereby awarding this certificate to

A. Vyasa Bharadwaja

In recognition of the publication of the paper entitled

IMAGE ENCRYCPTION AND DECRYPTION USING RANDOM IMAGE KEY

Published In JETIR (www.JETIR.org) ISSN UGC Approved (Journal No: 63975) & 5.87 Impact Factor

Published in Volume 7 Issue 4 , April-2020 | Date of Publication: 2020-04-29

EDITOR

EDITOR IN CHIEF

JETIR2004451 Research Paper Weblink http://www.jetir.org/view?paper=JETIR2004451 Registration ID : 231125