Encoding of color Images in DWT domain using FrFT

Thesis Report

submitted in partial fulfillment of the requirements

for the award of degree of

Master of Engineering

in

Computer Science and Engineering

Submitted By

Kshitij Agrawal

(801432009)

Under the supervision of:

Dr. Shalini Batra

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA – 147004

June 2016

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, ***"Encoding of Color Images in DWT domain using FrFT"***, in partial fulfillment of the requirements forthe award of degree of Master of Engineering in ***Computer Science and Engineering*** submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of ***Dr. Shalini Batra***and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Kshitij Agrawal
801432009
ME(CS)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Dr. Shalini Batra
Assistant Professor
Computer Science and Engineering Department
Thapar University

Countersigned by

Dr. Deepak Garg
Head
Computer Science and Engineering Department
Thapar University
Patiala

Dr. S. S. Bhatia
Dean (Academic Affairs)
Thapar University
Patiala

ABSTRACT

Information security is an important challenge in today's world. As digital information can be transferred through various modes, the security of its content has become an important task to deal with. Various areas like medical imaging, defense and advertising make use of digital information in the form of images. Thus their confidentiality and security needs to be preserved.

This work introduces a novel technique for color image encoding and decoding, which uses Discrete Wavelet Transform (DWT) and Fractional Fourier Transform (FrFT). In proposed work, all three planes of color images are encoded using subbands of DWT and parameters of FrFT. Selection of subband (among the subbands obtained after applying DWT) for applying FrFT and parameters of FrFT are used as security key for the purpose of encoding and decoding of all three color channels. For ensuring that color images are correctly decoded, the knowledge of correct selection of subband of DWT for applying FrFT and exact values of FrFT parameters is required. Correct decoding is not possible without the correct knowledge of DWT subband and FrFT parameters values. The proposed technique is also compared with one of the recent existing scheme and involves the use experimental results to show the performance of the proposed scheme.

CHAPTER 1
INTRODUCTION

1.1 Image Security

With the growing rage of internet and applications of the growing multimedia technology, people make use of digital multimedia information like digital images to communicate easily over the internet. Sometimes, illegal users can access the available digital content and try to modify it, temper it or illegally copy it. Fig.1.1 describes the scenario where a digital image is communicated over an unsecure network and illegal user accesses it and modifies it completely. It may be a major security threat to the digital content easily available over the internet.

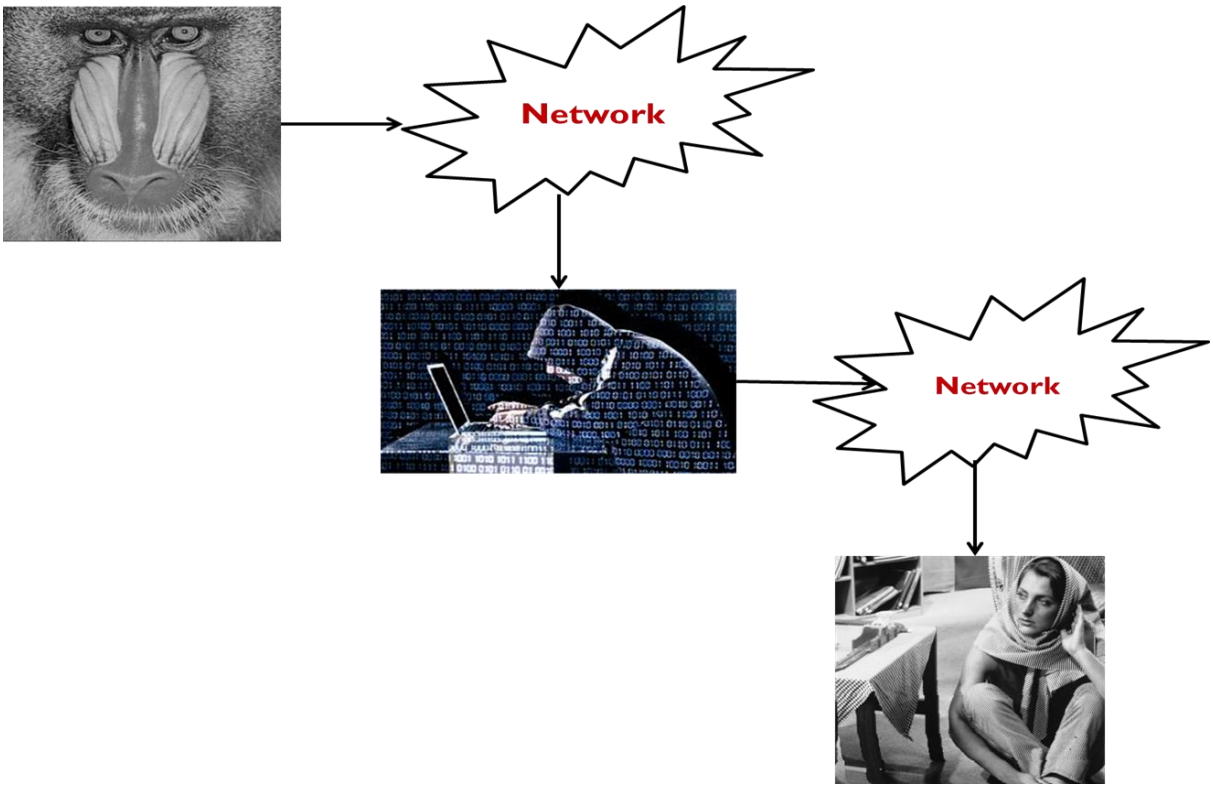


Figure 1.1: Communication over the unsecure channel

Thus, security of digital content is of utmost importance in today's era. In many cases, it is expected that secured digital images over the network will not be accessed by illegal receivers. Thus digital image security has given rise to number of methods of image encryption, which are presented in [1-7][35].

Digital images can be represented in the form of two dimensional matrix because digital image is a two dimensional function. Fig. 1.2 shows the gray scale image's representation.

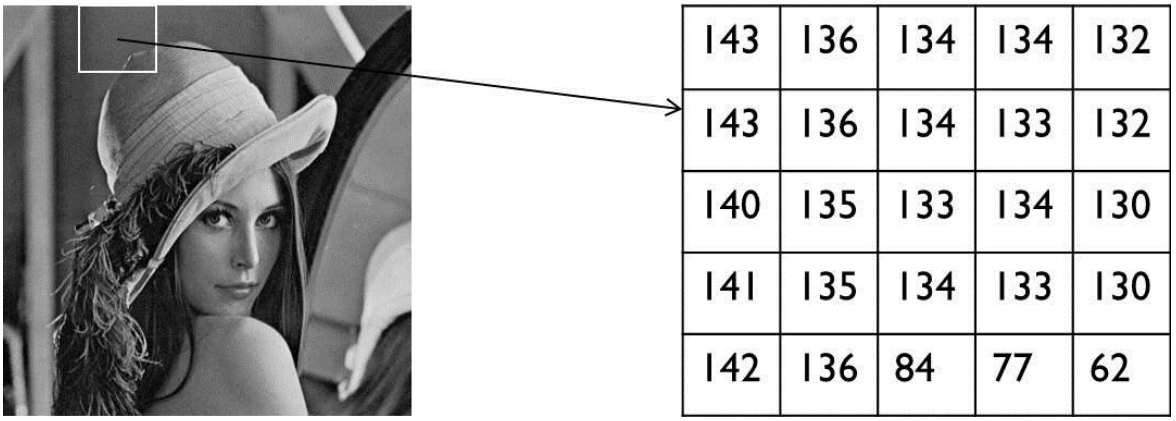


Fig. 1.2: Representation of a digital gray scale image in matrix form

Color images are composed of three color components i.e. Green, Red and Blue. Any processing on color images can be done by decomposing it into three color planes. Fig. 1.3 describes the representation of color image in matrix form.

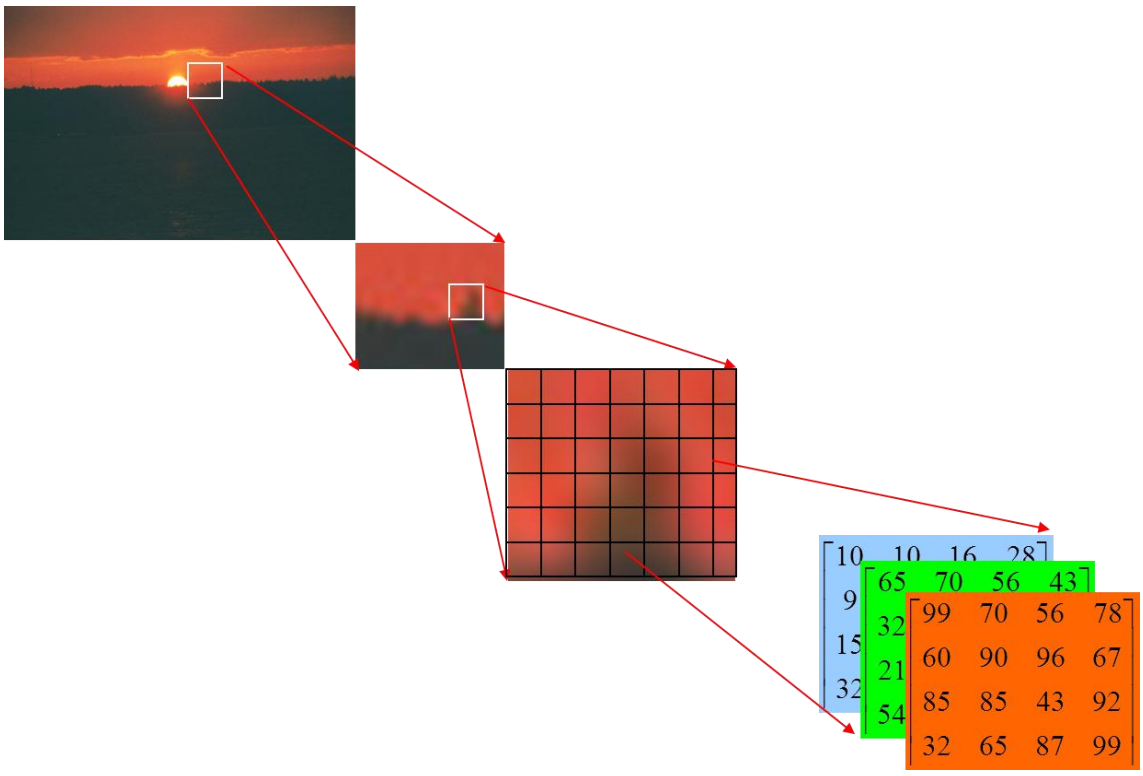


Figure 1.3: Representation of color image in matrix form

Image encryption is tough as compared to text encryption because many intrinsic features like high redundancy, high correlation among pixels and heavy data capacity are involved. Fast (Efficient) image encryption has been an interesting domain for research due to the requirement of real-time image encryption-decryption in many fields such as military image transmission , Cable TV , medical imaging system *etc*.[8].

Various transforms has been used for image encryption .One of them is Fractional Fourier Transform and this work comes up with a new scheme for encoding color images based on DWT and Fractional Fourier Transform. Fourier Transform is of great importance for image security such as image encryption because of the great benefits it offers. The FT is a fascinating tool which converts between two different representations of a signal:

• First one is time-domain representation, or the value of the signal as a function of time.
• Second one is frequency-domain representation, or the phase of the signal as a function of frequency.

Note that phase has the same definition here as it does for waves – it is the angle offset at which we begin drawing a wave. This work has used the properties of Fractional Fourier Transform. If we are given Fractional Fourier Transform (FrFT), we can perform image transformations that cannot be undone unless the correct fractional order is known.

Therefore, one idea that this work is inspired from is by applying Fractional Fourier Transform on an image. For this concept to work properly we must apply few other transformations such as Discrete Wavelet Transform (DWT) before applying the Frft and as a result the fractional orders aren't added.

1.2 Organization of Thesis

The organization of remaining of the thesis as follows: Chapter 2 discusses the previous literature in the field of image encryption in detail. Basic terminology used such as FrFT and DWT are also discussed and elaborated in Chapter 2.

Chapter 3 deals with the representation and elaboration of one of the existing schemes in the field of color image encoding. Existing scheme is discussed in detail and demonstration of existing scheme is also shown.

Proposed scheme is explained in Chapter 4 with diagrams of encoding and decoding procedure. Demonstration of proposed scheme is also shown in Chapter 4.

Chapter 5 includes the experimental results, which are discussed in detail. Comparison with existing scheme is also shown in Chapter 5.

In chapter 6, conclusions and future scope is given.

CHAPTER 2

LITERATURE SURVEY

As of now, a nice amount of work [9-28] has been done on digital content security. Gray scale images are an important component of digital image processing. But color information is also required in some sensitive applications. This information is essential for their visual effects and for security reasons. Encoding is one of the methods used to ensure security of multimedia content over wireless networks and internet. Many image encoding algorithms have been imposed by researchers to ensure the security of digital images. Without using the right keys, it is impossible to retrieve an image if it has been encrypted using a proper method. There are many different algorithms and techniques for image encryption, few of them are as follows:

Hartley transform [14, 24], Gyrator transform [27, 9, 13, 10, 11, 12] and Arnold Transform [17, 23, 21] are used for image encryption. Chen and Zhao [14] used Hartley transform to give a method of image encryption on based on an interferometer. Liu *et al.* [24] put forward a color image encryption technique which uses chaotic mapping and Hartley transform. Baker mapping is used to scramble three color panes. Two selected color planes are used to give the final encrypted results.

Gyrator transform was used by Singh and Sinha [27] to present a novel image encoding technique based on the chaos theory. Abutarab, M.Rafiq [9-13] gave various methods to improve the security of color images. Guo *et al.* [17] gave a method to encrypt color images using Arnold transform. While discrete fractional random transform works on the intensity component, Arnold transform encrypts the hue as well as saturation component. The encryption keys are formed by the Arnold transform and the fractional orders. Liu *et al.* [23] used Discrete Cosine Transform (DCT) and Arnold transform for encryption.

While Arnold transform was used to scramble the color components, random angles and the Arnold transform parameters formed the encryption keys.

Liu *et al.* used Arnold transform to devise double image encryption method [21]. Arnold transform, the pixels are scrambled at a local space of complex function. This transformed function is encrypted with the help of discrete fractional angular transform. This transform, along with the Arnold transform parameters, acts as key to ensure security.

Liu *et al.* has also given an image encoding technique which was based on gyrator transform and Arnold transform [29]. The gyrator transform's results *i.e.* phase and amplitude, are divided into various sub images. The gyrator transform transforms the random spectrum made up of random sub-images. An iterative structure of the scheme helps to improve the security of the scheme used for encryption. The keys used in this encryption are separating scheme and gyrator transform's parameters. An electro optical setup can be used for implementation. Numerical simulations help to prove the overall validity and security of this scheme.

In [30], authors gave a novel method of image encryption to transmit image securely. The encoded version of the actual image is embedded with digital signature. Bose Chaudhuri Hochquenghem (BCH) code, an appropriate error control code can be used for encryption of image. When the receiver decrypts the image, the digital signature authenticates image.

In [31], authors proposed a method of lossless compression and techniques to encrypt binary as well as gray scale images. These work on the SCAN patterns obtained from the SCAN methodology. SCAN is a formal language oriented 2D spatial accessing technology used to give place to scanning paths or space filling curves.

J. Guo and J. Yen [32] proposed an effective mirror like encryption algorithm. Using binary sequences, the image is scrambled as per the algorithm from a chaotic system. Seven steps are followed: Step 1 determines an initial point x(0) along with a 1-D chaotic

system. A variable k is set to 0.Step 2 creates a chaotic sequence from such a system. The main task in Step 3 is to obtain a binary sequence. The pixels of the image are rearranged as per the swap function used in steps 4, 5, 6 and 7.

In [33], authors have given an image encryption scheme that works on the defined chaotic system. This scheme uses chaotic sequence which is unpredictable to generate binary sequence. Next, the image pixels are rearranged. Step 1 includes setting x (0) and determining a chaotic system, a row size M for an image f and its column size N. Other parameters defined are constants and iteration number. In Step 2, the chaotic sequence is obtained while step-3 is used to obtain the binary sequence. Step-4 rearranges the pixels of the image, by using special functions.

Authors in [34] proposed an optical encryption scheme to encrypt color images, which is a new method for color image encryption using optical systems. The images are transformed to indexed range formats. While encoding them, two random phase masks encode image into stationary white noise. Both these masks are in the Fourier plane and input plane. In decryption phase, indexed images are converted to their original RGB formats. The proposed method proves to be robust, compact and better as compared to multi channels techniques.

Visual cryptography is one of the image encryption methods in which images are divided into transparencies. These can be sent to the required person and the receiver decrypts the image using the tool to get original image. The proposed Visual cryptography demonstrates to users how image encryption and decryption could be done. In this technology, the image is identified by the end user, which isn't the right image i.e. while transmitting the image a sender uses the application to encrypt the image. The sender obtains the two or more transparencies of the same image. The application gives an option to the end user of encryption. He can divide the original image into several different ones. These encrypted images are sent in PNG and GIF formats. These transparencies can be saved and sent to another user by other means.

An efficient hybrid model for image security using chaotic function and genetic algorithm introduced by [36]. In the first stage, a secret key and chaotic function are used

to construct a number of encrypted images. In stage 2, images are used as the initial population for genetic algorithm. In the given scheme, an optimum result is obtained from the genetic algorithm and the best cipher image is obtained from correlation coefficient calculation and entropy in the final stage. The efficient cipher image is the one with the lowest correlation coefficient and highest entropy .In this paper, genetic algorithm is used for the first time for image encryption.

Zou *et al.* proposed a method for scrambling a new digital image by using Fibonacci numbers [40]. They discussed the periodicity and standardization of the transformation involved in scrambling. The advantages of this transformation are that it makes encoding and decoding simple and suitable for real time applications. The image data is distributed randomly over the entire image so the effect is sensible. Various attacks like compression, noise and data packet loss can be endured using this method. They presented this technique to examine and analyze video scrambling with respect to embedding algorithms for digital watermarks.

Belkhouche *et al.* gave an appropriate method for encryption of binary images which makes use of the possibility of using various keys ex: initial state, the external parameters and iterations' number [39].

Shin *et al.* [38], an algorithm is proposed which used binary phase OR operation along with image dividing technique in this multilevel form of algorithm. This grey level image is transformed to binary images. The binary pictures are regenerated and binary random phase images are used to encrypt images, by using binary XOR.

Chang *et al.* [37] Made use of vector quantization in order to design better cryptosystem for images. Vector quantization (VQ) was the basis of this technique along with cryptography, and other methods like number theorem. In this technique, images are first converted into vectors and sequential coding is done vector by vector. Finally these cryptosystems are of great importance and use for commercial applications.

Xiao *et al.* [41] proposed a new highly optimized image algorithm which made use of permutation and substitution methods. It was used with the intention of improving the

pseudorandom characteristics of chaotic sequences, thus the method uses an optimized treatment and a cross-sampling disposal.

Gu *et al.* proposed an algorithm making use of two chaotic systems [42]. One chaotic system gave a chaotic sequence, which was transformed into binary stream with the help of a threshold function. A permutation matrix was created from the other system. Pixel values were modified by using binary stream as the key stream. Then permutation matrix was used to encrypt the image.

Zeghid *et al.* studied the Advanced Encryption Standard (AES), and they add a key stream generator in their image encryption technique (W7, A5/1) to AES in order to improve the performance of encryption [43].

Ying *et al.* proposed a block oriented transformation algorithm which uses the combination of image transformation and a popular encryption and decryption algorithm known as Blowfish [44]. A transformation algorithm divides the original image into blocks which is then rearranged. The Blowfish algorithm is used to encrypt these new images. The results prove that correlation value of image elements is greatly reduced. Results also prove that if number of block sizes are increased by making use of small block sizes then correlation would get lower and entropy would become higher.

Younes and Jantan proposed a method in which a new permutation is introduced by merging image permutation with the help of a popular encryption algorithm called RijnDael [45]. The original image is split into 4x4 pixel blocks and then rearrangement into a permuted image is done using a process of permutation. Then encryption is done using RijnDael algorithm. These results prove that correlation between image elements decreases and entropy increases.

Seyedzade *et al.* proposed a novel algorithm based on SHA-512 hash function. It had two sections [46]. The first one does a preprocessing operation that shuffles first half of the image. Then hash function is applied. The random number mask generated is XORed with the image to be encrypted.

Ismail *et al.* proposed chaos-based stream cipher, which composes two chaotic logistic maps and uses an external secret key for image encryption [47]. In this an external secret key of 104 bit along with chaotic logistic maps are used to distinguish between the encrypted image and the plain image. Next the secret key is modified once each pixel of the plain image is encrypted. Thus encrypted image becomes more robust. A feedback mechanism improves the robustness of this system.

Kamali *et al.* proposed a modification to the Advanced Encryption Standard (MAES) to give a high level security as well as better image encryption [48]. The result obtained was better than AES encryption algorithm.

Nag *et al.* proposed a new algorithm using affine transform which involved shuffling the image pixels [49]. It was a two phase algorithm for encryption and decryption. The first task was the use of XOR to encrypt the resulting image and redistribution of pixel values to different locations with the help of affine transformation and 4 bit keys. Firstly the resulting image was encrypted using XOR and then affine transformation was applied using XOR operation they encrypted the resulting image and then using the affine transformation, the pixel values were redistributed to different locations with 4 bit keys. The transformed image then divided into 2 pixels x 2 pixels blocks and each block is encrypted using XOR operation by four 8-bit keys. The result proves that after using affine transformation, correlation is highly reduced for pixel values.

Indrakanti and Avadhani proposed an algorithm based on random pixel permutation with the intent to keep a good the quality of the image [50]. It involves three phases in the process of encryption. In the first stage, there was encryption of image. In stage two, there was key generation and the identification process took place in phase 3. This provided confidentiality to color image, involving less calculations.

Enayatifar and Abdullah proposed a new method which works on a hybrid model, consisting of a genetic algorithm along with a chaotic function for image encryption [51]. In their technique, they used chaotic function to form a number of encrypted images from the original. A chaotic function was used in the first phase. These images form the initial population for carrying out the genetic algorithm operations. Then, the genetic algorithm

is used for the maximum possible optimization of encrypted images. In the end, the final encryption image is the one which resulted to be the best-cipher image.

Shah *et al.* gave a criterion to study prevailing S-boxes and analyze their strengths and drawbacks so as to find how suitable they are for the purpose of image encryption [52]. The proposed criterion makes use of results obtained from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, as well as mean of absolute deviation analysis. These are applied to advanced encryption standard (AES), affine-poweraffine (APA), gray, Lui J, residue prime, S8 AES, SKIPJACK, and Xyi Sboxes.

Abuhaiba and Hassan propose an effective method for encrypting images, which makes use of magnitude along with phase manipulation with the approach of Differential Evolution (DE) [53]. In order to show the security of this new encryption algorithm, they carried out key space analysis, statistical analysis and key sensitivity analysis.

Sun *et al.* proposed a general random scrambling method whose scrambling degree was much stable as compared to the classical method Arnold transform [54]. At first, the gray image was converted to various bit-plane images. Then shuffling was done by using random scrambling by involving another algorithm. Next, the scrambled images were merged with the original levels on bit planes and encrypted images were obtained. As different random sequences were used to scramble bit -plane images, the bits at different points in different planes did not stay on their original positions while each bit-plane is scrambled separately. For each pixel, all gray level bits may come from those pixels located at different positions. Thus there is a change in the reconstructed gray levels of image. Hence this method can simultaneously perform position exchange scrambling and gray level scrambling.

2.1.1 Image Encryption Using FrFt

Using Fractional Fourier Transform (FrFT), many image encoding algorithms have been devised [15, 16, 18, 20, 22, 25, 26, 28]. FrFT gives the advantage of introducing a fractional order, which is known as the parameter of FrFT [55]. It finds usage in various fields like optics, signal processing *etc*. [55, 56]. Due to the presence of additional

parameter, FrFT is comparatively more reliable and flexible. If we vary the order of transform from 0 to 1, FRFT can be developed from the given function to its FT [56, 55]. Thus it is highly useful in the field of encryption of images. The systems thus built are of better security [15, 16, 18, 20, 22, 25, 26, 28].

Liu and Liu gave the concept of random FrFT [22]. This is done by randomizing the traditional FRFT which is highly used in encoding and decoding of images. Henelly and Sheridan developed a technique which used random FrFT [18]. Zhang *et al.* used the FrFT parameters as keys to encode images [28]. Chen and Zhao proposed a new color coding technique with the help of random phases in the wavelet sub bands [16]. The keys used for encryption are wavelet packet filters, random phases and fractional orders of FrFt.

2.2 Basic Terminologies Used

2.2.1 Fourier Transform (FT):

The FT is a kind of tool which divides a waveform (signal or function) into a stand-in representation, is characterized by sine and cosine. The FT explains that we can re- write all the waveforms as the sum of sinusoidal functions.

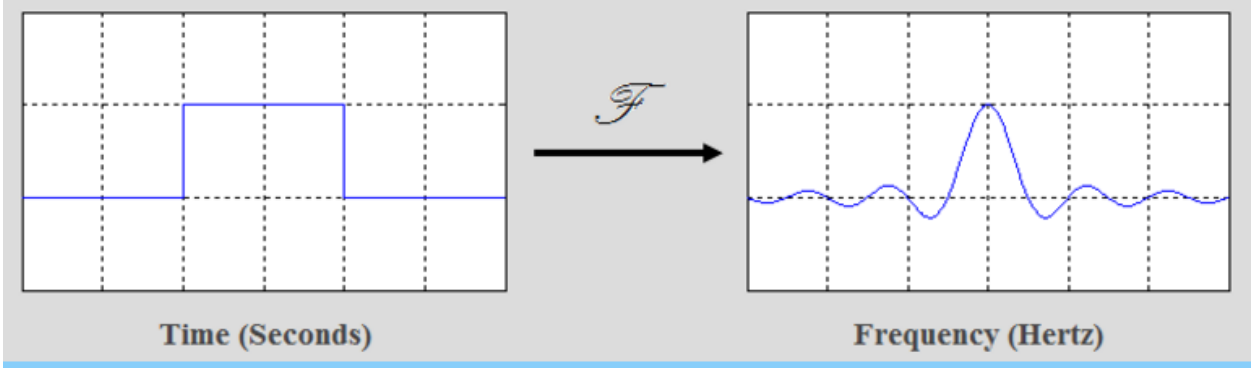


Figure 2.1: Time vs. Frequency

Everything in this world can be virtually explained via a waveform as explained in above Fig. 2.1 a function of space, time or any other variable. For an exemplification, electromagnetic fields, plot of VSWR vs. frequency, sound waves, the amount and price of the stock vs. time *etc*. viewing these waveforms are now easy using FT.

All waveforms are the sum of normal sinusoids of different frequencies despite of what we discover or scribble in the universe.

The FT divides a waveform - normally every real world waveform into sinusoids. That is, FT provides us a different and useful way to present a waveform.

The FT is a fascinating mathematical tool, that divides any function into sinusoidal basic function's sum and each of them is having different frequency and is a complex exponential function. The FT thus provides us an exclusive way of viewing all the functions –as the simple sinusoids.

While the FT is one of the most famous and fascinating tool whose widespread popularity is because of practical applications in almost every field of engineering and science. Sometimes it becomes hard to understand, why FT is so important and useful, but actually it makes the solution of difficult problems much easier (and also gives solution to the problems which were previously unsolved). A part from that, FT provides us a new technique of viewing the world and that is extremely useful for giving better feel for the universe.

FT of a function is given by:

$$\mathcal{F}\{g(t)\} = G(f) = \int_{-\infty}^{\infty} g(t)e^{-2\pi ift}dt \qquad (1)$$

The outcomes received is a function with frequency f .And at the particular frequency f, G (f) provides how much power g (t) has. Often, G (f) is known as spectrum of g. A part from that, inverse FT can be used to obtain g from G.

$$\mathcal{F}^{-1}\{G(f)\} = \int_{-\infty}^{\infty} G(f)e^{2\pi ift}df = g(t) \qquad (2)$$

Eq. 2 denotes that original function g(t) can be obtained via the inverse of FT from the function G(f). And now, G (f) and g(t) together forms a Fourier Pair(FP).

FPs is the unique representation of the similar underlying identity. The equivalence can be written as:

$$g \overset{\mathcal{F}}{\Longleftrightarrow} G \tag{3}$$

The FT of the Box Function:

Box function is also known as the square wave / square pulse.

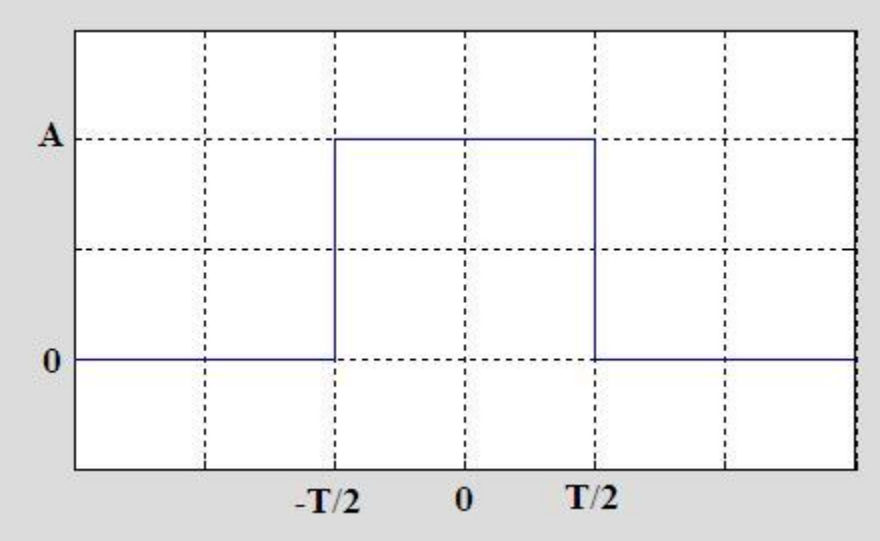


Figure 2.2: Box function.

In Fig. 2.2 function g(t) has amplitude A.

Using the definition of FT and integrating eq. 1.

$$\mathcal{F}\{g(t)\} = G(f) = \int_{-\infty}^{\infty} g(t)e^{-2\pi ift}dt$$

$$= \int_{-T/2}^{T/2} Ae^{-2\pi ift}dt = \frac{A}{-2\pi if}\left[e^{-2\pi ift}\Big|_{-T/2}^{T/2}\right]$$

$$= \frac{A}{-2\pi if}\left[e^{-\pi ifT} - e^{\pi ifT}\right] = \frac{AT}{\pi fT}\left[\frac{e^{\pi ifT} - e^{-\pi ifT}}{2i}\right]$$

$$= \frac{AT}{\pi fT}\sin(\pi fT) = AT\left[\text{sinc}(fT)\right] \tag{4}$$

The result G (f), is normally written as sinc function, that is shown as :

$$\mathrm{sinc}(t) = \frac{\sin(\pi t)}{\pi t} \tag{5}$$

[with the help of L'Hopitals rule , we can show sinc(t)=1]

g(t)'s FT is G(f) , and is plotted in Fig. 2.3 which is the outcome of eq. (2).

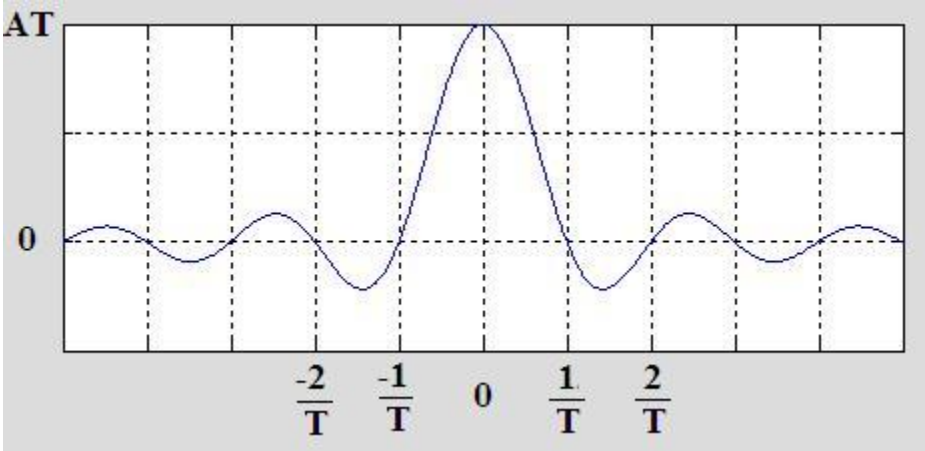


Figure 2.3: FT of the box function is the sinc function.

Let us take the example of square wave explained for T=10 and T=1. For A=1, the FT along with these functions are diagrammatically explained in **Fig 7, Fig 8**.

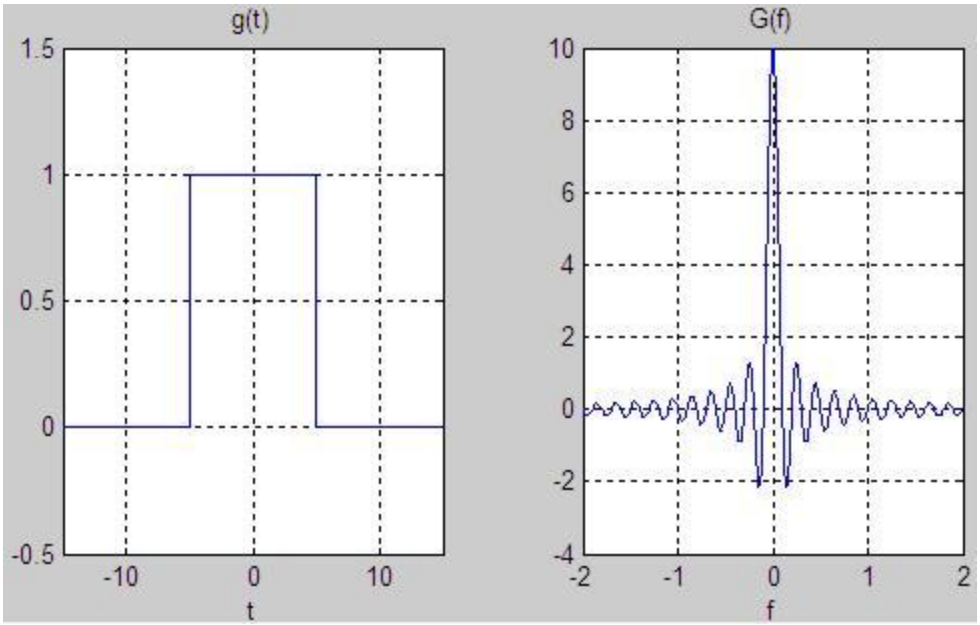


Figure 2.4: The FT and its Box Function with T=10

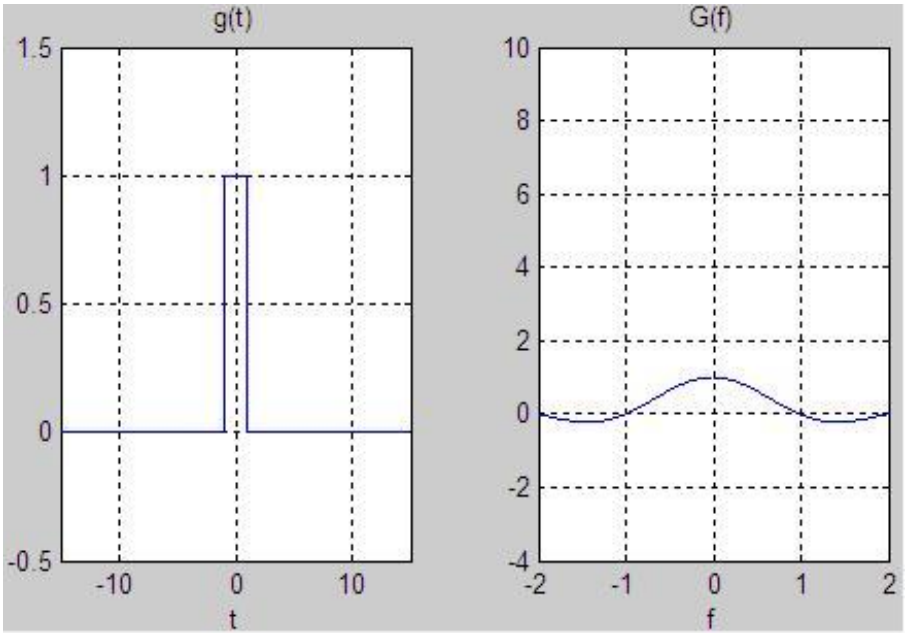


Figure 2.5: The FT and its Box Function with T=1

Fig. 2.4 and Fig. 2.5 give a fundamental lesson. It is seen in Fig. 2.4 that a wider square pulse gives a narrower and more constrained spectrum (the Fourier Transform). From Fig. 2.5**,** it is observed that the square pulse which is thinner gives a wider spectrum in result as compared to that in Fig. 2.4.This fact holds generally : quickly changing functions need higher frequency energy (as in Fig. 2.4).

It is noticed that if the box function is shorter in time as shown in Fig. 2.5, having less energy, there happens to be less energy in the Fourier transform as well.

2.2.1 Fractional Fourier Transform:-

In this era, encoding of data and network security are the key challenges. Fourier Transform (FT) is very important transform and is widely used in all engineering and scientific fields [57]. Namias introduced the concept of FrFT in 1980 [55]. FrFT, a generalization of Fourier Transform with parameter *a*, acts as an improvement [55] and has several applications in various fields such as signal processing, optics *etc*. Its parameter *a*, also called fractional order gives additional advantage over FT [56]. For 2D-FrFT there are two parameters $a1$ and $a2$ for the signal $g(s; t)$ [25]. Inverse of 2D-FrFT can be calculated using negative values of parameters i.e. $-a1$ and $-a2$.

Fractional FT is a subclass with single parameter of the class of linear canonical transforms. There are numbers of different with which we can define fractional FT ways [58]. We can take any of the definitions for the beginning point and then can derive remaining as properties .There is a different physical interpretation for each different definition, which is being used in number of different applications. Below paragraph gives few notations and assumptions in general.

Function f(u)'s ath order fractional FT can be denoted in any of the ways , which depends on the requirement of clarity and context. In general, the fractional FT is denoted by $F^a f(u)$ or $f^a(u)$. The first expression can be presented by two unique and different ways. In the first case, it can be seen as abstract signal f is being acted by operator F^a, whose result is presented in u domain:

$$f_a(u) \equiv F^a f(u) \equiv (F^a f)(u) \equiv F^a[f](u) \equiv (F^a[f])(u). \tag{6}$$

In second case,

$$f_a(u) \equiv F^a f(u) \equiv F^a[f(u)](u) \equiv (F^a[f(u)])(u). \tag{7}$$

2.2.3 Discrete Wavelet Transform:

2D-Discrete Wavelet Transform (DWT) is a very popular when it comes to the field of image processing. It uses the wavelet's concept. Wavelets are localized in time as well as in frequency domain. DWT can be used to examine the images at different resolutions and different frequency parts. For applying 2D –DWT, 1D-DWT are applied first in horizontal direction and then in vertical direction.

2D-DWT divides an image into four divisions LL, HL, LH and HH. LL subband (low frequency subband) defines the approximation part whereas LH, HL and HH (high frequency subbands) defines the detailed part. Low frequency component i.e. approximation part(LL) is again divided into four frequency subbands. Fig. 2.6 shows the first and second level decomposition of DWT.

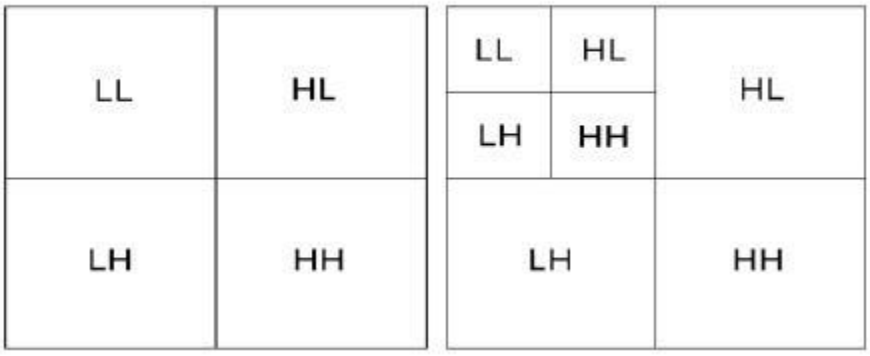


Figure 2.6: First and Second level decomposition of Discrete Wavelet Transform (DWT)

DWT of a given image can be calculated by using following equation defined in eq. (8).

$$W_{\varphi}(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \phi_{j_0, m, n}(x, y)$$

$$W_{\psi}^{i}(j, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \psi_{j, m, n}^{i}(x, y) \quad (8)$$

For eq. (8), Inverse DWT can be calculated by using following eq. (9):

$$f(x,y) = \frac{1}{\sqrt{MN}} \sum_{m} \sum_{n} W_{\varphi}(j_0, m, n)\phi_{j_0,m,n}(x,y) + \frac{1}{\sqrt{MN}} \sum_{i=H,V,D} \sum_{j=j_0}^{\infty} \sum_{m} \sum_{n} W_{\psi}^{i}(j,m,n)\psi_{j,m,n}^{i}(x,y) \quad (9)$$

Fig. 2.7 displays the second level DWT decomposition on Barbara image. As it can be seen in Fig. 2.7 that approximation part is almost similar to original image and thus it shows that approximation part i.e. LL subband holds most of the information of the image. Therefore, this property can be used for image encoding by encoding LL subband as it holds most of the information and if this is encoded, it will be very difficult to decode it without propoer knowledge of proper subband.

(a) **(b)**

Figure 2.7: Implementation of DWT on Barbara Image (a) Barbara Image; (b) First level DWT decomposition of Barbara image

CHAPTER 3
PROBLEM STATEMENT

Information security is an important challenge in today's world. As digital information can be transferred through various modes, the security of its content has become an important task to deal with. Various areas like medical imaging, defense and advertising make use of digital information in the form of images. Thus their confidentiality and security needs to be preserved.

Thus, security of digital content is of utmost importance in today's era. In many cases, it is expected that secured digital images over the network will not be accessed by illegal receivers. Thus digital image security has given rise to number of methods of image encryption.

Many transforms have been used in various ways that ensures the security of an image like gyrator transform, Hartley transform, Arnold transform, Discrete Cosine Transform, Fourier Transform, Fractional Fourier Transform *etc*.

This work refers to the algorithm given by Prasad *et al.* [25]. Properties and characteristics of FrFt and DWT can be exploited to improve the effectiveness and computational time of the existing algorithm, which can be verified on the basis of the results, obtained after comparing existing technique and proposed technique.

In this work, a new technique is proposed for encoding color images, which would not only ensure security but also reduce the cost and transmitting time involved. Overall performance shall be recorded in terms of MSE.

The proposed algorithm is expected to decrease the MSE of existing algorithm and maintain the effectiveness of the existing algorithm.

3.1 Gap Analysis

A lot of research has been done in the area of image security. In this work, a number of image security schemes have been studied to find out the research gap. Most of the existing image security systems are not up to mark for real time applications like medical imaging, military etc. They offer either less security or their image size increases after encoding which increases the time and cost. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea because image size is almost always much greater than that of text. Therefore, the cryptosystems require more time to encrypt the image data directly. Various transforms has been used for image encryption .One of them is Fractional Fourier Transform and this work comes up with a new scheme for encoding color images based on DWT and Fractional Fourier Transform based on FrFt number of algorithms have been given, algorithm given by Prasad *et al.* [25] is one of them and we have encountered some major drawbacks in this scheme, and these drawbacks need to be removed. Fourier Transform is of great importance for image security such as image encryption because of the great benefits it offers. The FT is a fascinating tool which converts between two different representations of a signal. So, we have proposed an effective scheme specially designed for the images. The proposed work is an improvement to Prasad *et al*. [25]. In this research, image security framework has been proposed to overcome the problem stated earlier in existing scheme.

3.2 Objectives

This work is an improvement to the work presented by Prasad *et al.* [25]. The Objectives of the thesis are discussed in the following points:

1. To explore, analyze and study the techniques used for image encryption and security.
2. To improve the image security of an existing algorithm [25].
3. To reduce the MSE involved in the encoding and decoding procedure in existing scheme [25].
4. To make sure that size of the encoded image doesn't increase or doubled for reducing the transmission time and cost ,which is a major drawback of the existing scheme [25] ,

where image size gets doubled after encoding , so it involves more transmission time and cost.

5. None of the part of the original image should be visible in the final decoded image, if it is incorrectly decoded. In the existing algorithm [25], after decoding image incorrectly, still some part of an image is visible which is a major drawback and this drawback need to be removed totally.

CHAPTER 4
EXISTING SCHEME

4.1 Background

In this section, we briefly describe the color image encoding technique given by Prasad *et al.* [21]. In [21], authors have decomposed the original color image into three color components *R*, *G* and *B*. FrFT is applied on all three color channels. After applying FrFT, DWT is applied on the FrFT coefficients. Now, real and imaginary parts of all wavelet subbands (obtained after applying DWT) are separated and rearrangement is done with the use of certain parameters c_i where, $i=1, 2, 3, 4$ and ($0 < c_1 \leq 2$ and $0 < c_1\ c_2 \leq 1$, $0 < c_3\ c_4 \leq 1$) in such a way that with respect to the original image, the resultant encoded image gets doubled in size.

Decoding phase is just reverse of the encoding phase. With the knowledge of correct arrangement, real and imaginary parts are recovered and then these are combined to form the image in complex form. Inverse DWT and FrFT is applied to obtain the correct decoded image. Encoding and decoding procedure of Prasad's scheme [21] is shown in Fig. 4.1.

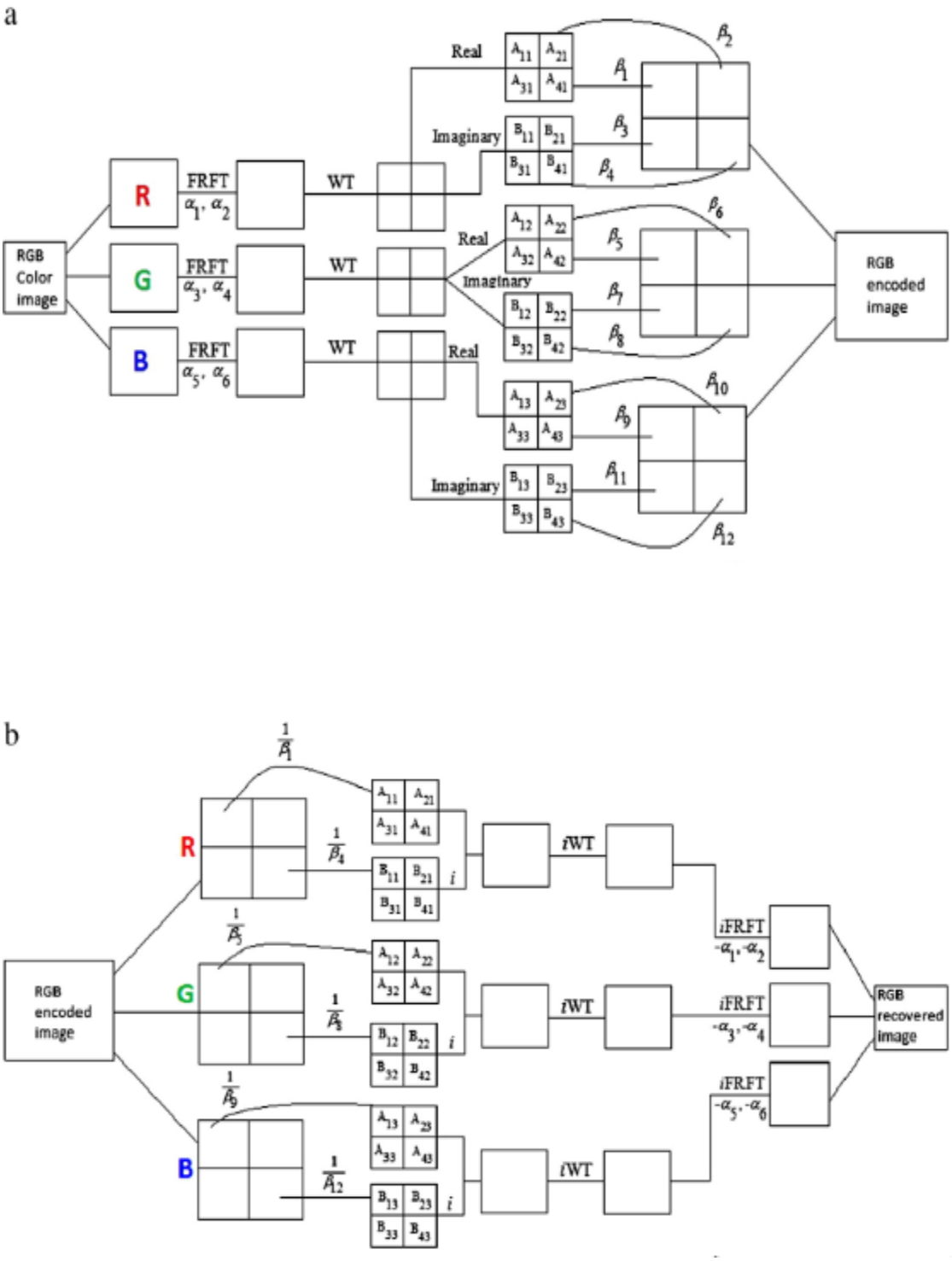
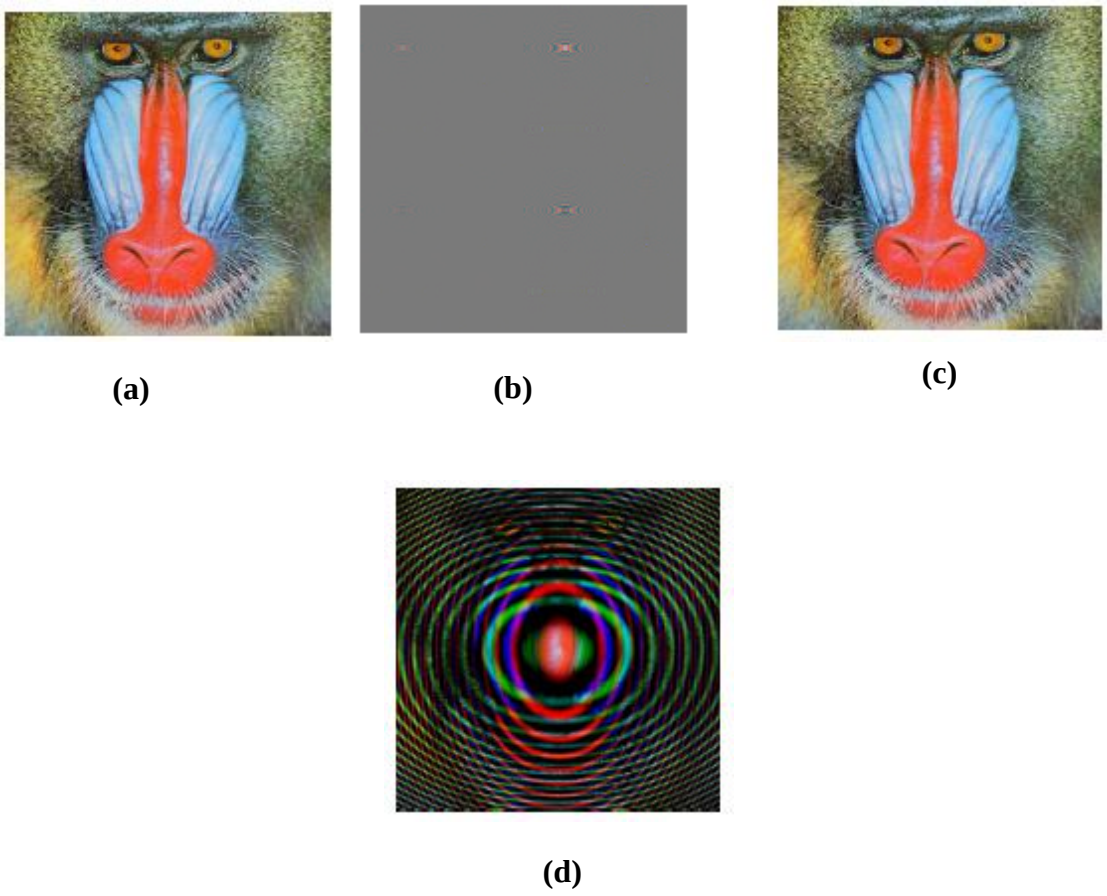


Fig. 4.1: Existing Scheme (a) encoding procedure of [21] (b) decoding procedure of [21]

4.2 Demonstration of Existing Scheme on Baboon Image



(a) **(b)** **(c)**

(d)

Figure 4.2: Implementation of Existing scheme on Baboon Image (a) Primary Baboon image; (b) image after encoding [21] (c) image after correct decoding [21] (d) image after incorrect decoding [21].

Fig. 4.2 displays the result of the existing technique on Baboon image [21]. Prasad *et al*. [21] used FrFT and DWT to encode color images. This has been a major improvement over [16]. The authors used FrFT and DWT to enhance security [21]. The drawback in the existing scheme is that the image is double in size as compared to the original image thus extra time and cost constraints are involved [21]. As it can be seen in Fig. 6.10 (d) that after decoding image incorrectly, still some part of the Baboon image is visible which is also overcome in our proposed work. In proposed work, a novel scheme is proposed to encode color images, which would not only ensure security but also reduce the cost and transmitting time involved.

CHAPTER 5

PROPOSED SCHEME

As stated in Chapter 4, Prasad *et al.* [21] scheme provides the security but it also doubles the encoded image size after the rearrangement step of real and imaginary parts. We have addressed this drawback along with increasing the security.

The proposed procedures of encoding and decoding are described in Fig. 5.1(a) and 5.1(b) respectively. As shown in Fig. 5.1(a), first the primary color image *I* is divided into three color planes red *(R)*, green *(G)* and blue *(B)* and then First level 2D-DWT is applied on every color component separately. As, low frequency component *LL* holds the most of the information of an image, FrFT (with two parameters a_1 and $a_{2)}$ is applied on *LL* subband to enhance the security. Again, inverse DWT is applied using high frequency subbands i.e. *HL*, *LH* and *HH* and modified *LL* subband. Now, all three modified color components are combined to obtain the final encoded color image *E*.

The selection of wavelet subband and values of FrFT parameters are used as security key in encoding process. Without correct knowledge of wavelet subband or values of FrFT parameters, original image cannot be decoded even if one of these is known.

Proposed decoding process is the reverse of the encoding phase and presented in Fig. 5.1(b). Correctly decoded image *D* is obtained at the end of the decoding process. Algorithm of Encoding and decoding processes are as follows:

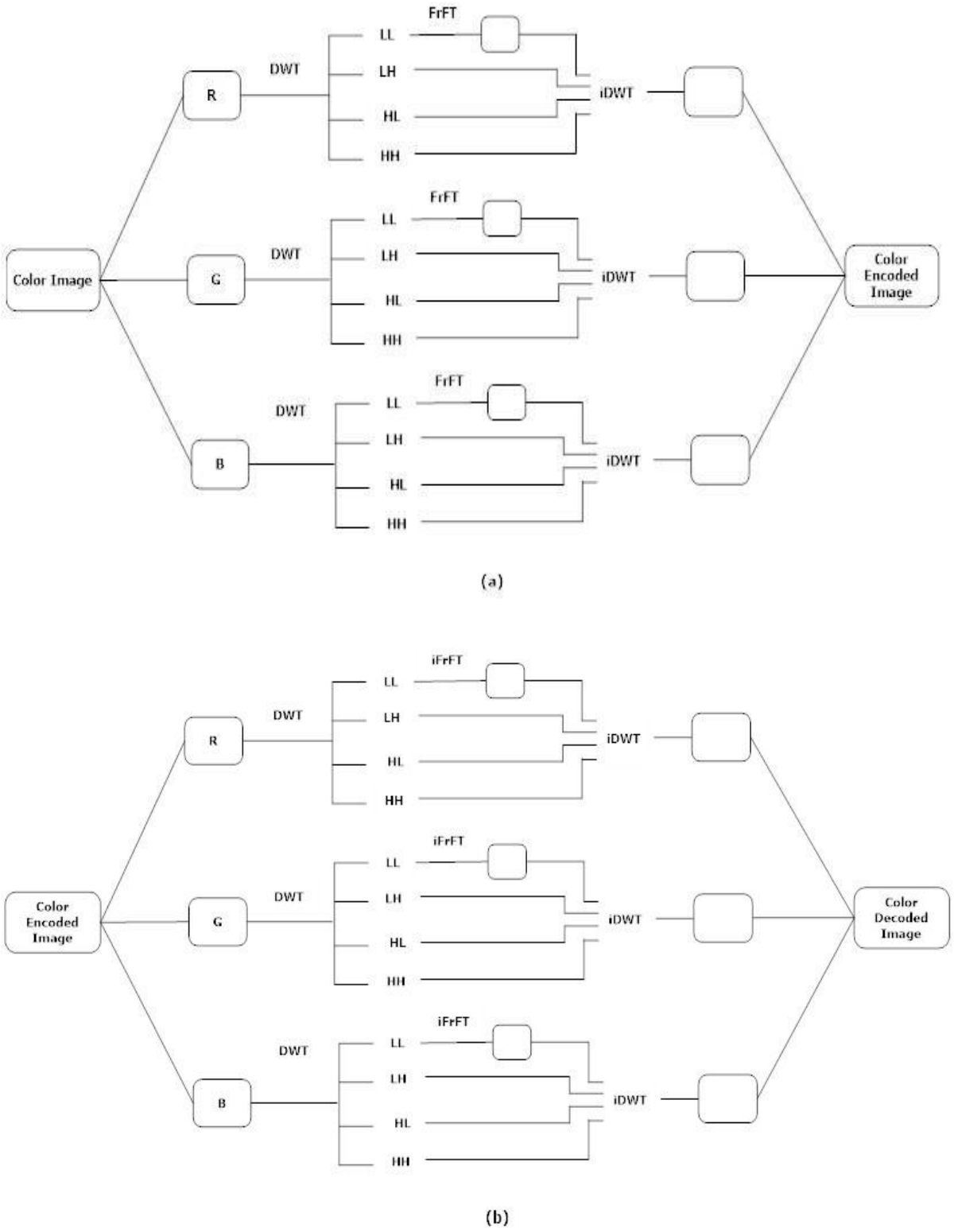


Figure 5.1: Proposed Scheme (a) Encoding Process; (b) Decoding Process.

5.1 Encoding Procedure

1. Decompose primary color image *I* into three color components *R*, *G* and *B*.
2. Apply 2D-DWT on every color component to decompose into four frequency components *HH*, *LH*, *HL* and *LL*.
3. Apply FrFT (using two parameters a_1 and a_2) on *LL* subband and obtain frequency coefficients for *LL* subband.
4. Apply inverse DWT using obtained frequency coefficients of *LL* subband and *HL*, *LH* and *HH* subbands.
5. Combine all three modified color components to obtain final encoded color image *E*.

5.2 Decoding Procedure

1. Decompose primary color image *I* into three color components *R*, *G* and *B*.
2. Apply 2D-DWT on every color component to decompose into four frequency components *HH*, *LH*, *HL* and *LL*.
3. Apply inverse FrFT (parameters a_1 and a_2) on *LL* subband.
4. Apply inverse DWT using modified *LL* subband and *HL*, *LH* and *HH* subbands.
5. Combine all three modified color components to obtain final decoded color image *D*.

5.3 Demonstration of the Proposed Technique

The given technique has been applied on standard color test image Lena of size 512 * 512 shown in Fig. 5.2 (a). Encoded image obtained after applying proposed encoding process is shown in Fig. 5.2 (b). Correctly decoded image obtained after applying proposed decoding procedure is shown in Fig. 5.2 (c). We have demonstrated the encoding procedure on Lena image by taking the same values of FrFT parameters as used in [21].

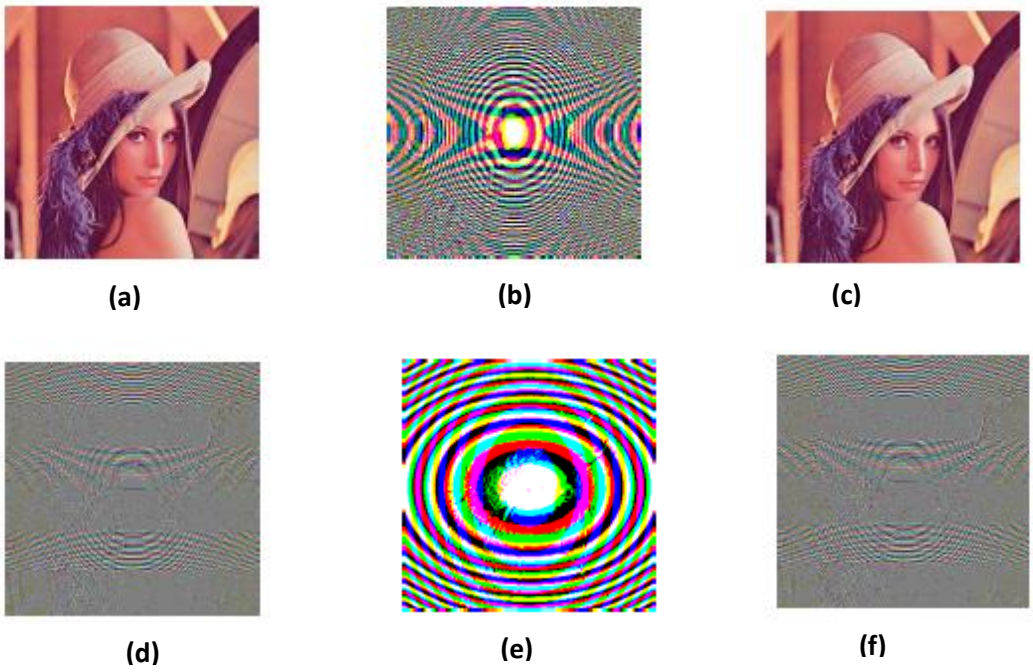


Figure 5.2: Implementation of Proposed scheme on Lena Image (a) Primary Lena image; (b) Image after encoding; (c) Image after decoding; (d) Images after incorrect decoding with wrong selection of DWT subband; (e) Incorrect decoded image using incorrect values of FrFT parameters; and (f) Images after incorrect decoding using wrong selection of DWT subband and incorrect values of FrFT parameters.

Wrongly decoded images obtained after selecting LH band for decoding, wrong values of FrFT parameters and taking both the security keys wrong i.e. wrong subband selection and incorrect values of FrFT parameters are shown in Fig. 5.2 (d), 5.2 (e) and 5.2 (f) respectively. It is clear from Fig. 4.2 (d), 4.2 (e) and 4.2 (f) that it's not possible to recognize original image in any of the wrong cases.

CHAPTER 6

IMPLEMENTATION AND EXPERIMENTAL RESULTS

6.1 Experimental Results and Discussions

6.1.1 Implementation of Proposed technique on Various Standard Test Images

Proposed encoding and decoding processes are applied on various standard color test images of size *512*512* shown in Fig. 6.1

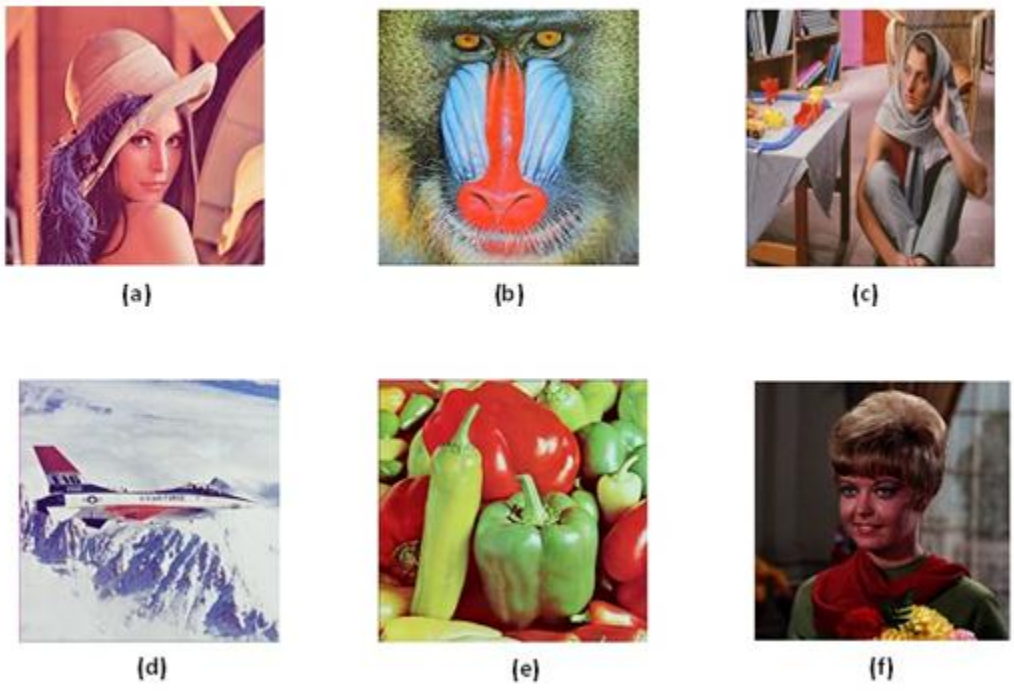


Figure 6.1: Standard Color Images for testing (a) Lena; (b) Baboon; (c) Barbara; (d) Airplane; (e) Peppers; (f) Girl.

Results received after applying proposed technique on Baboon image are shown in Fig. 6.2. Original Baboon image is presented in Fig. 6.2 (a). Encoded image obtained after

applying proposed encoding procedure is presented in Fig. 6.2 (b). Correctly decoded image obtained after applying proposed decoding procedure is presented in Fig. 6.2 (c).

Wrongly decoded images obtained after selecting LH band for decoding, wrong values of FrFT parameters and taking both the security keys wrong i.e. wrong subband selection and incorrect values of FrFT parameters are shown in Fig. 6.2 (d), 6.2 (e) and 6.2 (f) respectively. It is evident from Fig. 6.2 (d), 6.2 (e) and 6.2 (f) that the original image cannot be recognized in any of the wrong cases.

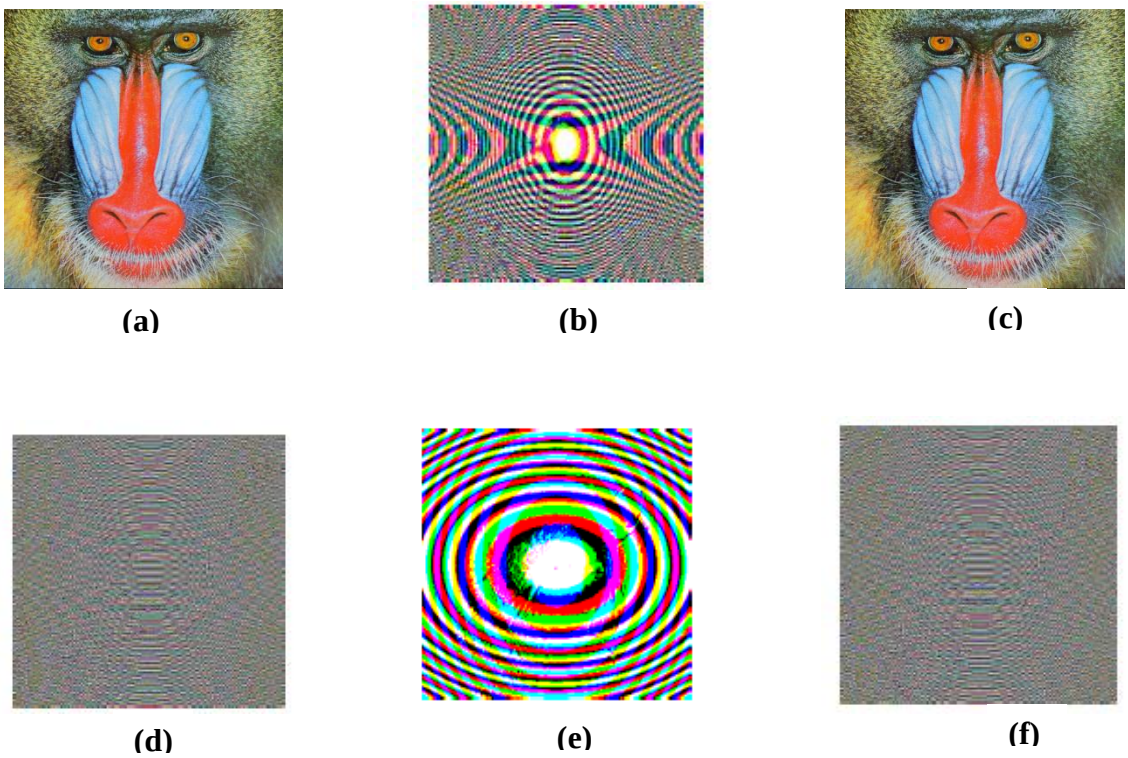


Fig. 6.2: Implementation of Proposed scheme on Baboon Image (a) Primary Baboon image; (b)Image after Encoding; (c) Image after correct decoding; (d) Images are incorrect decoding with wrong selection of DWT subband; (e) incorrect decoded image using incorrect values of FrFT parameters; and (f) incorrectly decoded image using wrong selection of DWT subband and incorrect values of FrFT parameters.

Similarly, results on other test images shown in Fig. 6.1(c), 6.1(d), 6.1(e), 6.1(f), 6.1(g), 6.1(h) and 6.1(i) are shown in Fig. 6.3, 6.4, 6.5, 6.6, 6.7, 6.8 and 6.9 respectively.

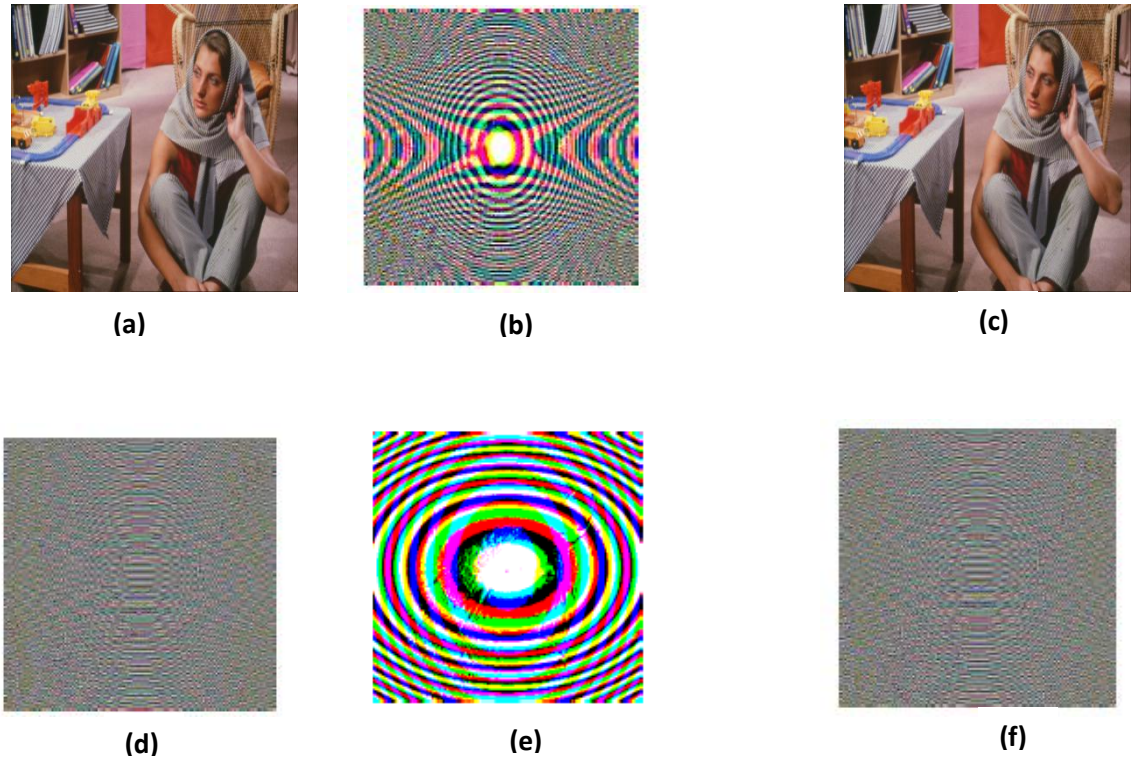


Figure 6.3: Implementation of Proposed scheme on Barbara Image (a) Primary Barbara image; (b) Image after Encoding; (c) Image after correct decoding; (d) Image after incorrect decoding with wrong selection of DWT subband; (e) incorrect decoded image using incorrect values of FrFT parameters; and (f) Image after incorrect decoding using wrong selection of DWT subband and incorrect values of FrFT parameters.

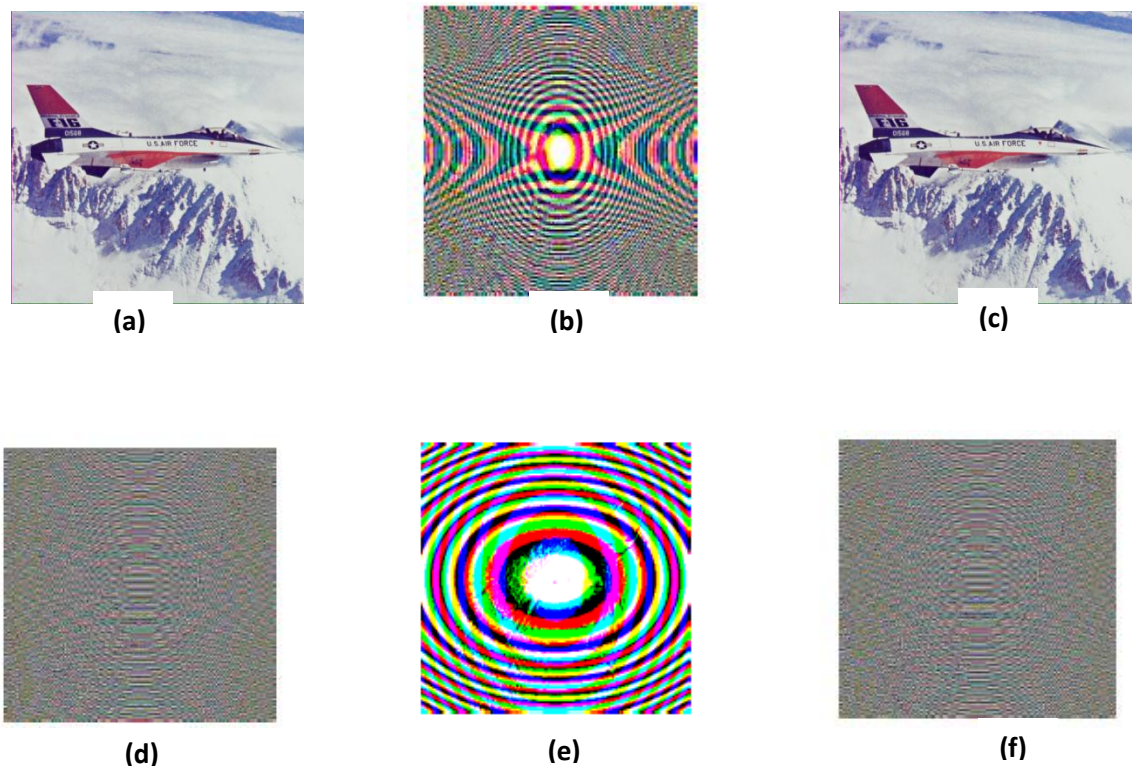


Figure 6.4: Implementation of Proposed scheme on Airplane Image (a) Primary Airplane image; (b) Image after Encoding; (c) Image after correct decoding; (d) Image after incorrect decoding with wrong selection of DWT subband; (e) Image after incorrect decoding using incorrect values of FrFT parameters; and (f) Image after incorrect decoding using wrong selection of DWT subband and incorrect values of FrFT parameters.

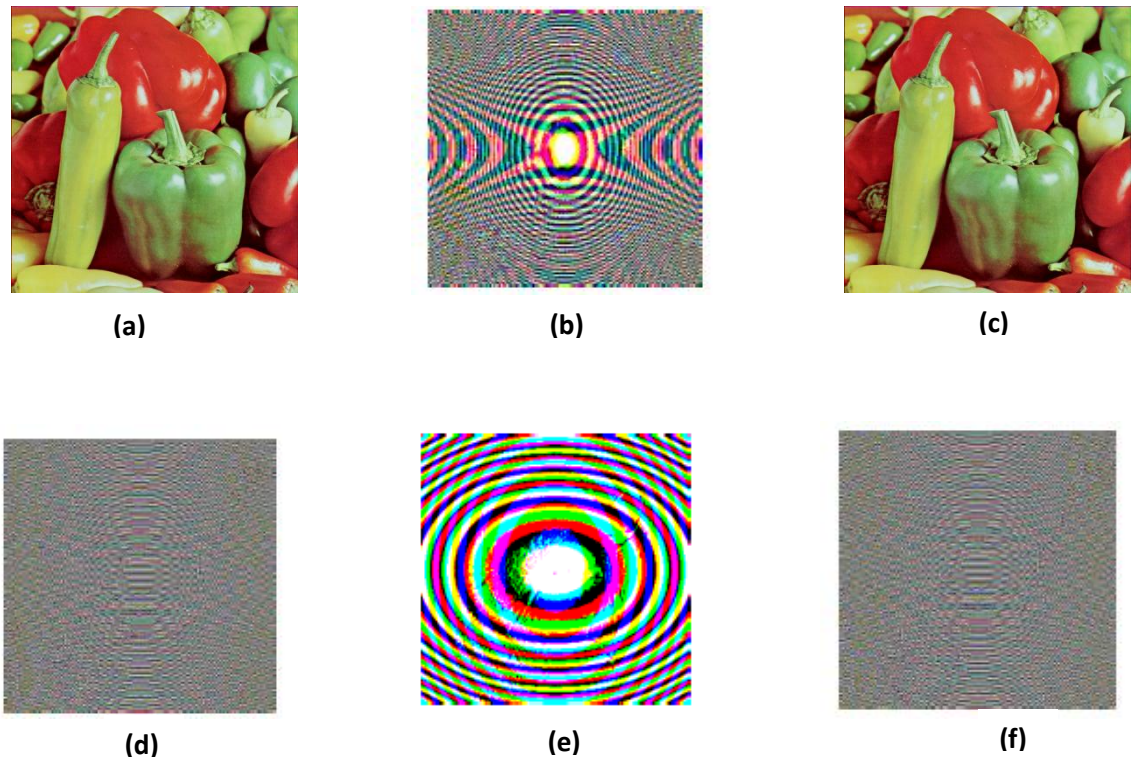


Fig. 6.5: Implementation of Proposed scheme on Pepper Image (a) Primary Pepper image; (b) Image after encoding; (c) Image after correct decoding; (d) Image after incorrect decoding with wrong selection of DWT subband; (e) Image after incorrect decoding using incorrect values of FrFT parameters; and (f) Image after incorrect decoding using wrong selection of DWT subband and incorrect values of FrFT parameters.

6.2 Comparison with Existing Scheme [21]

We have compared the proposed technique with one of the recent existing techniques [21]. The use of FrFT to approximation part i.e. LL subband has enhanced the security aspect as compared to Prasad's scheme [21]. In the scheme, proposed by Prasad *et al.* [21], image size gets doubled as the result of rearrangement step and is not suitable for the communication purpose. Fig. 6.10 displays the result of the existing technique [21] on Lena image. As it can be seen in Fig. 6.10 (d) that after decoding image incorrectly, still some part of the Lena image is visible which is also overcome in our proposed work as no information can be extracted from incorrectly decoded images. The drawback of their scheme of double image size has been overcome by our proposed scheme and security is also increased.

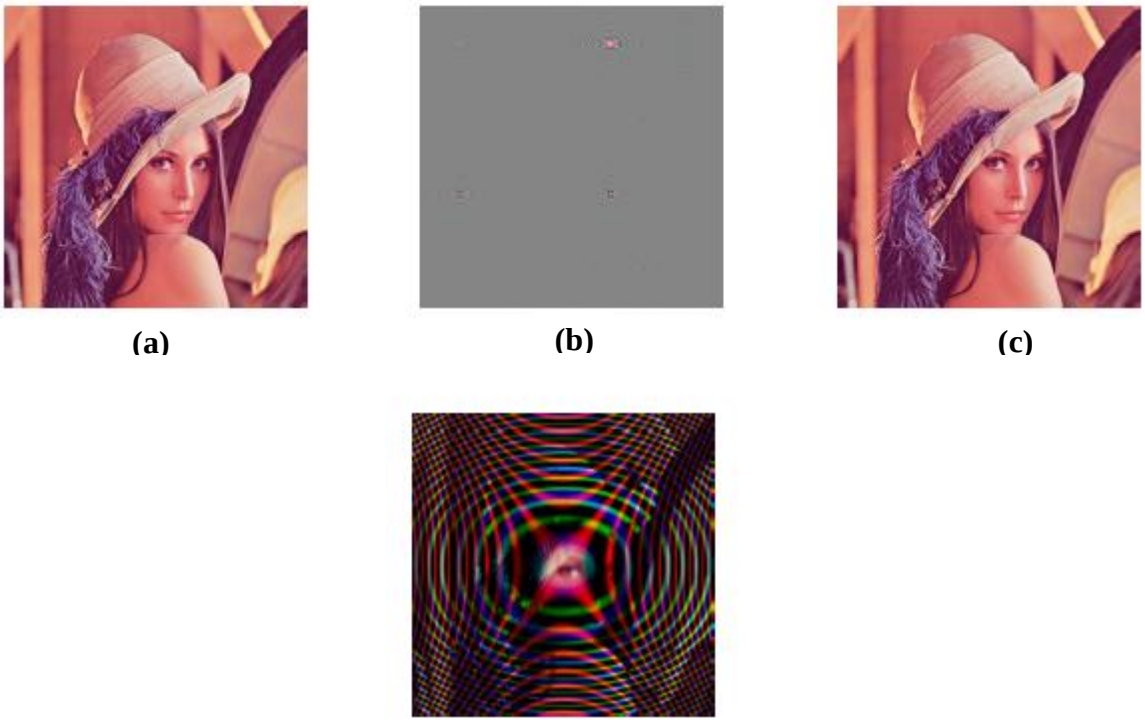


Figure 6.10: Implementation of Existing scheme on Lena Image (a) primary Lena image; (b) image after encoding [21] (c) Image after correct decoding [21] (d) Image after incorrect decoding [21].

6.2.1 Mean Square Error Analysis (MSE)

The Mean Square Error (MSE) values are used for showing the performance of the given technique. MSE is computed between original image and correct decoded image. Through this, the quality of decoded images can be verified. MSE between original image *I* and correct decoded image *D* can be calculated using following formula:

$$MSE = \frac{1}{m*n} \sum_{p=1}^{m} \sum_{q=1}^{n} [K(m\Delta x, n\Delta y) - L(m\Delta x, n\Delta y]^2 \quad (10)$$

where, *K* is the original image and *L* is the correctly decoded image. MSE values for the existing technique [21] and the proposed technique are shown in Table 1 and smaller MSE values for proposed scheme in comparison to [21] indicate towards the reliability and performance of the given technique.

Table 1: MSE values using proposed and existing scheme [21]

S.No.	Standard Test Images	Red, Green and Blue Component	Mean Square Error (MSE-Existing Scheme)	Mean Square Error (MSE-Proposed Scheme)
1.	Lena	Red Green Blue	1.6581×10^{-25} 3.6301×10^{-25} 3.6723×10^{-25}	2.3911×10^{-29} 9.1237×10^{-30} 8.3520×10^{-30}
2.	Baboon	Red Green Blue	5.4772×10^{-25} 2.5581×10^{-25} 6.5808×10^{-25}	1.9147×10^{-29} 1.6974×10^{-29} 1.4618×10^{-29}
3.	Barbara	Red Green Blue	7.5797×10^{-25} 5.7624×10^{-25} 4.9315×10^{-25}	3.6769×10^{-30} 2.2556×10^{-30} 1.9650×10^{-30}
4.	Airplane	Red Green Blue	1.2221×10^{-25} 2.9158×10^{-25} 3.3951×10^{-25}	1.3261×10^{-29} 1.3773×10^{-29} 1.4324×10^{-29}
5.	Peppers	Red Green Blue	1.2662×10^{-24} 2.1286×10^{-24} 8.1254×10^{-24}	6.4280×10^{-30} 5.1586×10^{-30} 1.6727×10^{-30}

CHAPTER 7

CONCLUSION

In today's era of information technology, vast amount of digital data is available on the internet and anyone can access the available data easily. Although it is very convenient for users, it is also a major threat towards the multimedia content security. Image encryption techniques can provide security for digital content such as digital images, videos and digital audios.

This work has proposed a new image encoding technique for color images. All three color planes are encoded separately using DWT and FrFT. Approximation part obtained after applying DWT is used for encoding and FrFT is applied on this. As most of the information is intact in approximation part i.e. LL subband, application of FrFT over it has enhanced the security of the encoded images. Selection of DWT subband and values of FrFT parameters are used as security keys for encoding and decoding purpose without the exact knowledge of these parameters, correct decoded images cannot be obtained.

The proposed scheme is implemented on various standard color test images using MATLAB software. MSE values of correctly decoded images for all three color planes demonstrate that the images can be decoded without any significant loss of information. The proposed scheme has also been compared with one of the recent existing schemes based on color image encoding. Results obtained after applying proposed scheme are better as compared to the existing scheme and thus it proves that the proposed scheme can provide better security for color images.