Indian Journal of Science and Technology, Vol 9S(1), DOI: 10.17485/ijst/2016/v9iS1/105682, December 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Optical Cryptosystem of Color Images based on Fractional-, Wavelet Transform Domains using Random Phase Masks

Hukum Singh*

Department of Applied Sciences, The NorthCap University, Sector 23-A, Gurgaon - 122017, Haryana, India;
hukumsingh@ncuindia.edu

Abstract

Objectives: A technique based on optical color cryptosystem is carried out in the Fractional Wavelet Transform (FWT) plane. Purpose of this paper is to increase the key space there by the scheme become more secured. **Methods/Statistical Analyis**: The original images are segregated into three: R (red), G (green) and B (blue) color components. After that the each part is encoding independently using 4-f system of DRPE in FWT. The input images to be encrypted are multiplied by RPMs in spatial and frequency planes then subjected to FrFT and inverse FrFT, after that it subjected to Discrete Wavelet Transform. Coefficients from the Discrete Wavelet Transform are further multiplied each one by additional masks of different pixel from RPM. They are further inverse Discrete Wavelet Transform applied to get the encrypted images. Images are recovered by using the all correct parameters of FWT. **Findings**: Proposed algorithm is enough secured because combination of FrFT and DWT. The effectiveness of present technique is tested by computing MSE, Signal to Noise Ratio (SNR) between retrieved and input images. Role of encryption keys, occlusion and noise attacks have been verified in proposed scheme. **Applications/Improvements**: Security of any scheme is based on the keys used. Even a very strong or well-designed scheme can be attack easily if the keys are used in encryption is poorly selected. In this scheme keys are used in both the transforms so the key size is increased. Key space can be further modified for more security.

Keywords: Encryption, Entropy, Fractional Fourier Transform, Mean Squared Error, Noise Attacks, Occlusion

1. Introduction

With the rapid development of communication technologies, image sharing and exchanging across the internet, optical security play a crucial role. Optical systems are of growing interest for image encryption of their distinct advantages of processing two-dimensional complex data in parallel and high speed. Image encryption technology based on optical is an effective measure to ensure the information security. Many methods are initiated in optical and digital of image encodings[1–8]. Optical encryption based methods on optoelectronics systems are much secured as compared digital techniques. The widely-known DRPE for optical image encryption was first proposed by[1]. It is a well-known optically symmetric-key technique that is based on the 4-f system, which encrypts by two RPMs:in input and in Fourier planes. The scheme can be demonstrated digitally and optically and has much potential uses in many streams for example security verification, information concealing and many more image encryptions.

Aim was to strengthen security, so DRPE again extended in several other transforms for examples in Fractional Fourier Transform (FrFT)[9,10], Fresnel Transform (FrT)[11–15], Gyrator Transform (GT)[16–18] and Fractional Mellin Transform (FrMT)[19,20] and Wavelet Transform (WT)[21–31]. In all these techniques, a monochromatic light is used to illuminate a real color image; color information of reconstructed image is lost. However, the color image sends out more information than the gray scale image. In[32] have presented a scheme for color image concealing in Fourier Transform (FT) by transforming the colored images into

*Author for correspondence

indexed image prior to encryption. In decryption, the color images are retrieved by converting the decrypted indexed images back into their color formats. In another study, color image encryption technique was implemented wavelength multiplexing in FrT[33]. In this scheme, the image is segregated into RGB channels and then encryption process is carried out. Propagation distances, wavelength of FrT and RPMs are keys used for image encoding and decoding process. After that Joshi et al. proposed color image encryption and decryption in the FrFT domain[34]. Their method is more secure because more fractional orders are used. Some more number of algorithms has been proposed for color image encryption[35–38]. In[23] also proposed a scheme in FWT for better encryption because of combination of two transform i.e. FrFT and WT. Optical realization of WT for two-dimensional objects was proposed by[21] in 1993 and FWT was first defined by[22] in 1997.

In the present communication, a scheme for colored images encryption in FWT domain is proposed. The use of FWT possesses an advantage over Fourier domain by providing extra parameters such as fractional orders and RPMs used in encoding and decoding process. Fractional order keys are used for enlarging the key space and system is more secured. RGB of color components images i.e. $f_r(x_i, y_i)$, $f_g(x_i, y_i)$ and $f_b(x_i, y_i)$ are encoding independently using DRPE. Collectively in this scheme requires ten different RPMs and twelve fractional orders for the RGB channels. In all, there are twenty three independent parameters and they are used as encryption keys.

2. Principle

2.1 Wavelet Transform (WT)

A two-dimensional Wavelet Transform $W_{x,y}(a_1, a_2, b_1, b_2)$ can be expressed as[21].

$$W_{x,y}(a_1, a_2, b_1, b_2) = \frac{1}{\sqrt{a_1 a_2}} \oint_{-\infty}^{\infty} f_r(x_i, y_i) \boldsymbol{h}^* \left(\frac{x - b_1}{a_1}, \frac{x - b_2}{a_2} \right) dx_i dy_i \quad (1)$$

Where $f_r(x_i, y_i)$ is input signal for red channel.

2.2 Fractional Wavelet Transform (FWT)

Two dimensional FWT of an input image f(x, y) can be written as[22,23].

$$W^{(\alpha)}(a, b) = \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} C_{\alpha_1,\alpha_2}(x, y; x', y') f(x, y) \boldsymbol{h}^*_{a_{mn}\bar{b}}(x', y') dx dy dx' dy' \quad (2)$$

Where the $C_{\alpha_1,\alpha_2}(x, y; x', y')$ operator denotes fractional kernel and is given by:

$$C_{\alpha_1,\alpha_2}(x, y; x', y') = C_{\alpha_1}(x, x') C_{\alpha_2}(y, y') \quad (3)$$

and

$$C_{\alpha_1}(x, x') = \frac{\exp\left\{-i\left[\pi sgn(\sin \varnothing_1)/4 - \varnothing_1/2\right]\right\}}{\left|\lambda f_{s1} \sin \varnothing_1\right|^{1/2}} \times \exp\left(i\pi \frac{x^2 + x'^2}{\lambda f_{s1} \tan \varnothing_1} - 2i\pi \frac{xx'}{\lambda f_{s1} \sin \varnothing_1} \right)$$

$$C_{\alpha_2}(y, y') = \frac{\exp\left\{-i\left[\pi sgn(\sin \varnothing_2)/4 - \varnothing_2/2\right]\right\}}{\left|\lambda f_{s2} \sin \varnothing_2\right|^{1/2}} \times \exp\left(i\pi \frac{y^2 + y'^2}{\lambda f_{s2} \tan \varnothing_2} - 2i\pi \frac{yy'}{\lambda f_{s2} \sin \varnothing_2} \right)$$

Where α_1 and α_2 are the Fractional Fourier orders of (FrFT), $\boldsymbol{\varnothing_1} = \frac{\pi \alpha_1}{2}$, $\boldsymbol{\varnothing_2} = \pi \frac{\alpha_2}{2}$, λ is the wavelength of incident light f_{s1} and f_{s2} are standard focal lengths in x and y directions, respectively and $\boldsymbol{h}_{a_{mn}\bar{b}}(x', y')$ is the scaled and shifted wavelet function of mother wavelet function and is given by:

$$\boldsymbol{h}_{a_{mn}\bar{b}}(x', y') = (a_m a_n)^{-\frac{1}{2}} \boldsymbol{h}\left(\frac{x' - b_{x'}}{a_m}, \frac{y' - b_{y'}}{a_n} \right). \quad (4)$$

2.3 Discrete Wavelet Transform (DWT)

A one dimensional DWT is performed column wise on intermediate result to form the final DWT coefficients such as LL_1, HL_1, LH_1, HH_1. Where L, H are low and high frequencies sub bands. LL_1, HH_1 are called low-low and high- high frequencies respectively and other two are the diagonal matrices. Further, it can be is decomposed into next level, again LL_1 can be decomposed into four matrices LL_2, HL_2, LH_2, HH_2. And in the third level, LL_2 is further decomposed and so on. This process can be continuing to the required number of levels, it is known as multiple level decomposition. But the matrices with high frequency and diagonal parts will not be decomposed into higher sub-bands. Figure 1 represents four level wavelet decomposition sketches and fourth level decomposition of the color image Lena is shown in Figure 2.

2.4 Algorithm for Encryption Scheme

In the proposed method the FrFT and DWT is used with different RPMs multiplied in each sub-band in FWT domain. The original images to be encrypted are decomposed in RGB parts each color matrices are bonded by phase masks (RPM_1, RPM_2, RPM_3) in the spatial domain. The RPM_1, RPM_2, RPM_3 are defined as $exp\{i2\pi n_1(x, y)\}$, $exp\{i2\pi n_2(x, y)\}$, $exp\{i2\pi n_3(x, y)\}$ where $n_1(x, y)$, $n_2(x, y)$, $n_3(x, y)$, are uniformly distributed between 0 and 1. The

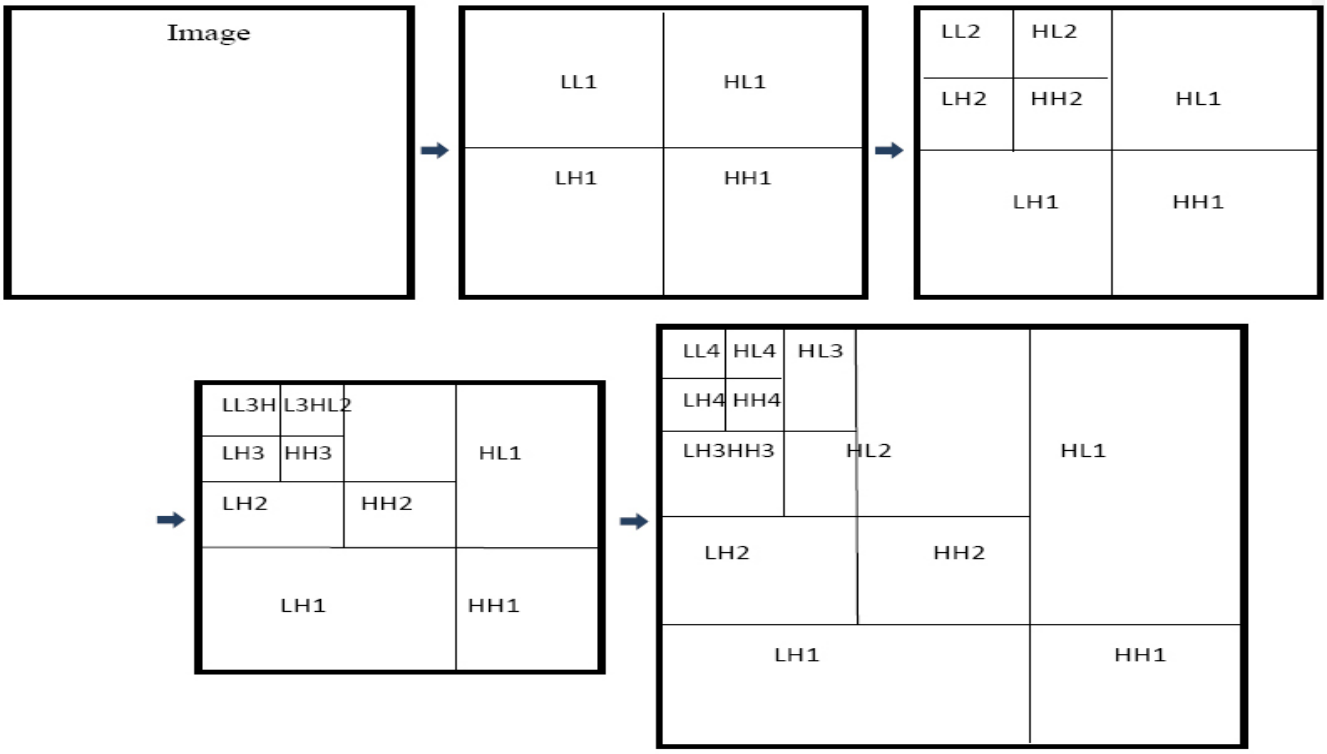

Figure 1. shows the four levels wavelet decomposition sketch.

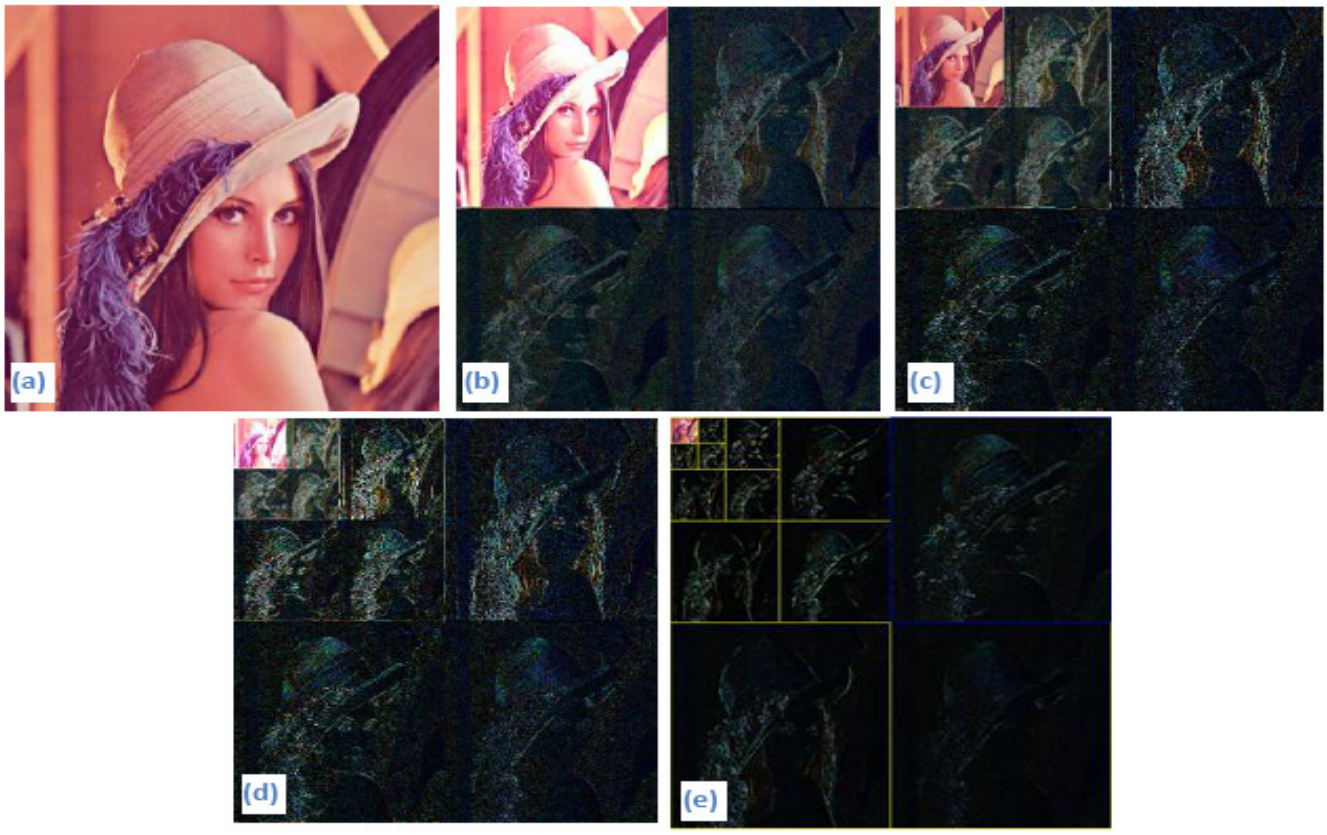

Figure 2. The fourth level decomposition of the given digital image Lena.

RPMs used above are statistically independent of each other. First FrFT is performed for three R, G and B components i.e. fractional orders (α_1, α_1) for R, (β_1, β_1) for G and (γ_1, γ_1) for B colors respectively as displays in Figure 3. The FrFT transformed primary color images are then bonded with another 03 phase masks (RPM_4, RPM_5, RPM_6) in the fractional domain and are defined as: $exp\{i2\pi n_4(u, v)\}$, $exp\{i2\pi n_5(u, v)\}$, $exp\{i2\pi n_6(u, v)\}$. Another FrFT is performed i.e. ($-\alpha_1$, $-\alpha_1$) for R, ($-\beta_1$, $-\beta_1$) for G and ($-\gamma_1$, $-\gamma_1$) for blue, in order to get ciphered images for 03 RGB color components. After a single-level DWT, the given image is segregated into four matrices $\{LL_1, HL_1, LH_1, HH_1\}$, which are bonded by four additional RPMs for encryption. RPMs are independently chosen; therefore researcher can keep them in several desired places, and of course, it strengthens the encryption security. The process of FrFT is quite important in encryption, because we cannot only add the encoding keys with fractional orders to protect the information. But it also disturbs the information of the original image before DWT that makes the energy not be mostly included in the LL_1 sub-band. Then each of images is performed by IDWT. Finally, these three encrypted images are combined to get the coloured encrypted image. In the given technique involves 23 input security parameters in all, including 12 different fractional orders, wavelet family and 10 independent RPMs which can be considered as keys for decryption. Improper selection of any of these parameters during decryption comes negative results. Presence of many of encryption keys helps in making the system more secure against unauthorized attacker.

$$\{LL_1, HL_1, LH_1, HH_1\} = \left[DWT\ \left[\left[FrFT\right]^{-p_i,-q_i}\{FrFT\right]^{p_i q_i}\left\{I(x,y) \times RPM_i\right\} \times RPM_i\right\}, family\Big]$$

$LLM_1 = LL_1$ x $Mask1$; $HLM_1 = HL_1$ x $Mask2$;
$LHM_1 = LH_1$ x $Mask3$; $HHM_1 = HH_1$ x $Mask4$;

$I_{E(RGB)} = IDWT\{LLM_1, LHM_1, HLM_1, HHM_1, family\}$ and
$Mask_n = \exp[2\Pi ir_n]$ n=1, 2, 3, 4

$I_{E(RGB)}$ are the encrypted images of red, green and blue components of color images, LL_1, HL_1, LH_1 and HH_1 are low-low, high-low, low-high and high-high coefficients. LLM_1, LHM_1, HLM_1 and HHM_1 are the matrices of LL_1, LH_1, HL_1 and HH_1 when multiply by RPM_s. $FrFT^{pi, qi}$ & $FrFT^{-pi, -qi}$ are fractional Fourier transform in two dimensions with fractional orders p_i, q_i = (α_1, α_1), (β_1, β_1) and (γ_1, γ_1).

2.5 Algorithm for Decryption Scheme

Flow chart for decryption method is shown in Figure 4. Then each decomposed encrypted component is subjected with Discrete Wavelet Transform and then sub-bands components are bonded by conjugates of $mask_s$ after then apply inverse wavelet transform. The FrFT orders (α_1, α_1), (β_1, β_1) and (γ_1, γ_1) are chosen for the RGB parts, respectively and are subsequently multiplied with random phase masks (RPM_4*, RPM_5*, RPM_6*) in the spatial domain of FrFT. Further, the FrFT orders ($-\alpha_1$, $-\alpha_1$) for R, ($-\beta_1$, $-\beta_1$) for G, and ($-\gamma_1$, $-\gamma_1$) for B images are applied in the final steps they are combined together to get input images.

Mathematical expression for decryption is given by:

$$\left[\{LLM\right]_2, LHM_2, HLM_2, HHM_2\} = DWT\ \left\{I_{E(RGB)}, family\right\}$$

$$LH_1' = LLM_2 \times conj(Mask1);$$
$$HL_1' = LHM_2 \times conj(Mask2);$$
$$HL_1' = HLM_2 \times conj(Mask3);$$
$$HH_1' = HHM_2 \times conj(Mask4);$$

$$I(x,y) = \left[FrFT^{-p_i,-q_i}\left[FrFT\right]^{p_i q_i}\left\{IDWT\ \{LH_1', HL_1', LH_1', HH_1', family\}\right\} \times conj(RPM_i)\right]$$

If the DWT and FrFT parameters are same then decrypted image is image that was input image.

3. Computational Results

In this scheme three color images of pixels 256×256 as input is considered. The color image of Lena is shown in Figure 5a using encryption scheme, its red, green and blue encrypted component are shown in Figures 5 (b-d). When the decryption process is done with correct keys (fractional orders, wavelet family and RPMs) the original image is recovered and is shown in Figure 5e. The fractional orders of FrFT used for the present scheme in combination form were 0.3, 0.4, 0.5, 0.6 and 0.7. These fractional orders are chosen arbitrarily for simplicity. Having seen for color image Lena, the simulation results were performed for two more color images. Figure 5f is input color image of baby girl and Figures 5(g-i) are encrypted images of red, green and blue components of baby girl. Using correct decryption scheme, the input image is retrieved and shown in Figure 5j. Similar process has been applied for third color image baboon shown in

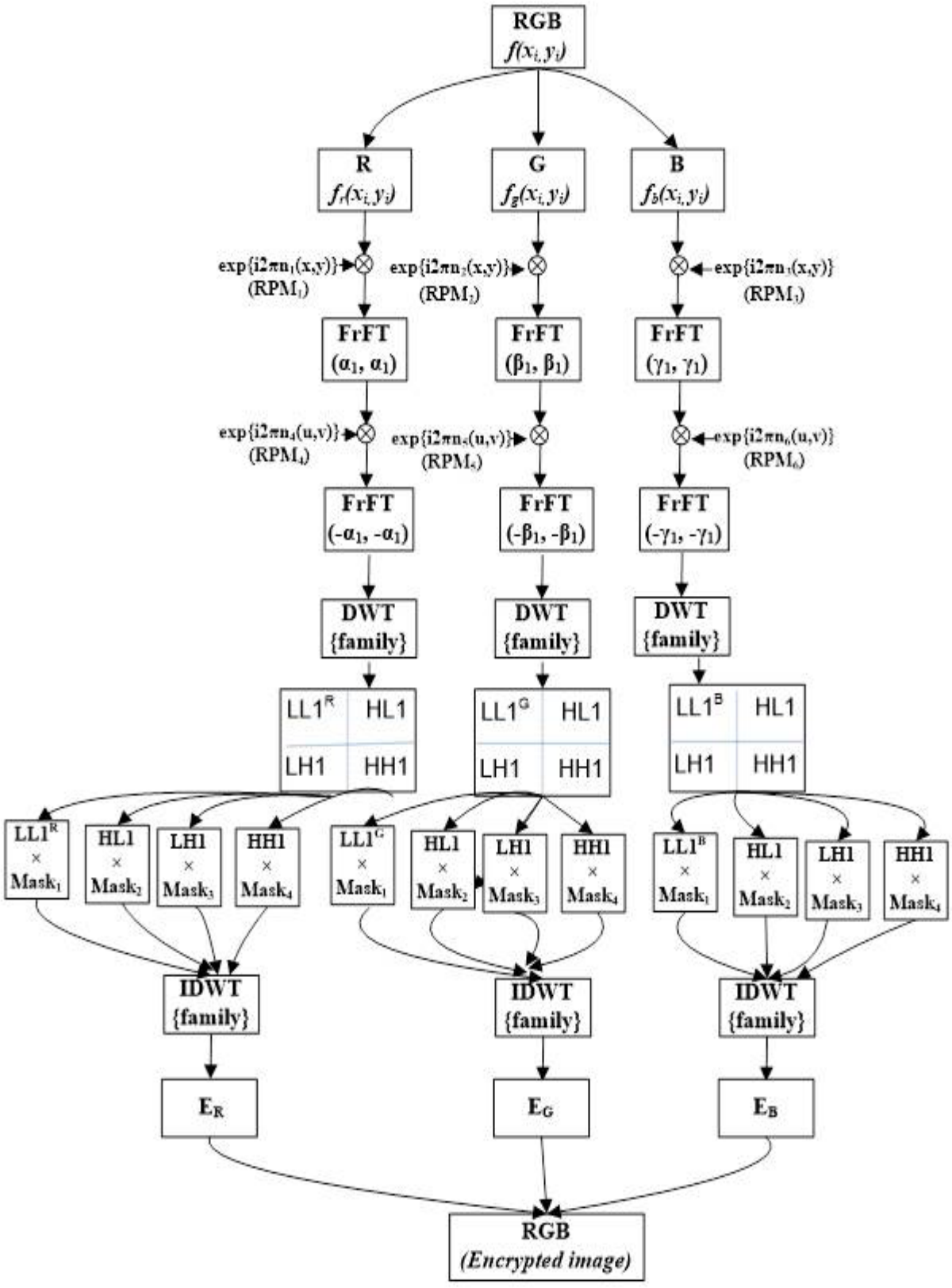

Figure 3. Flow chart of the proposed scheme for encryption process.

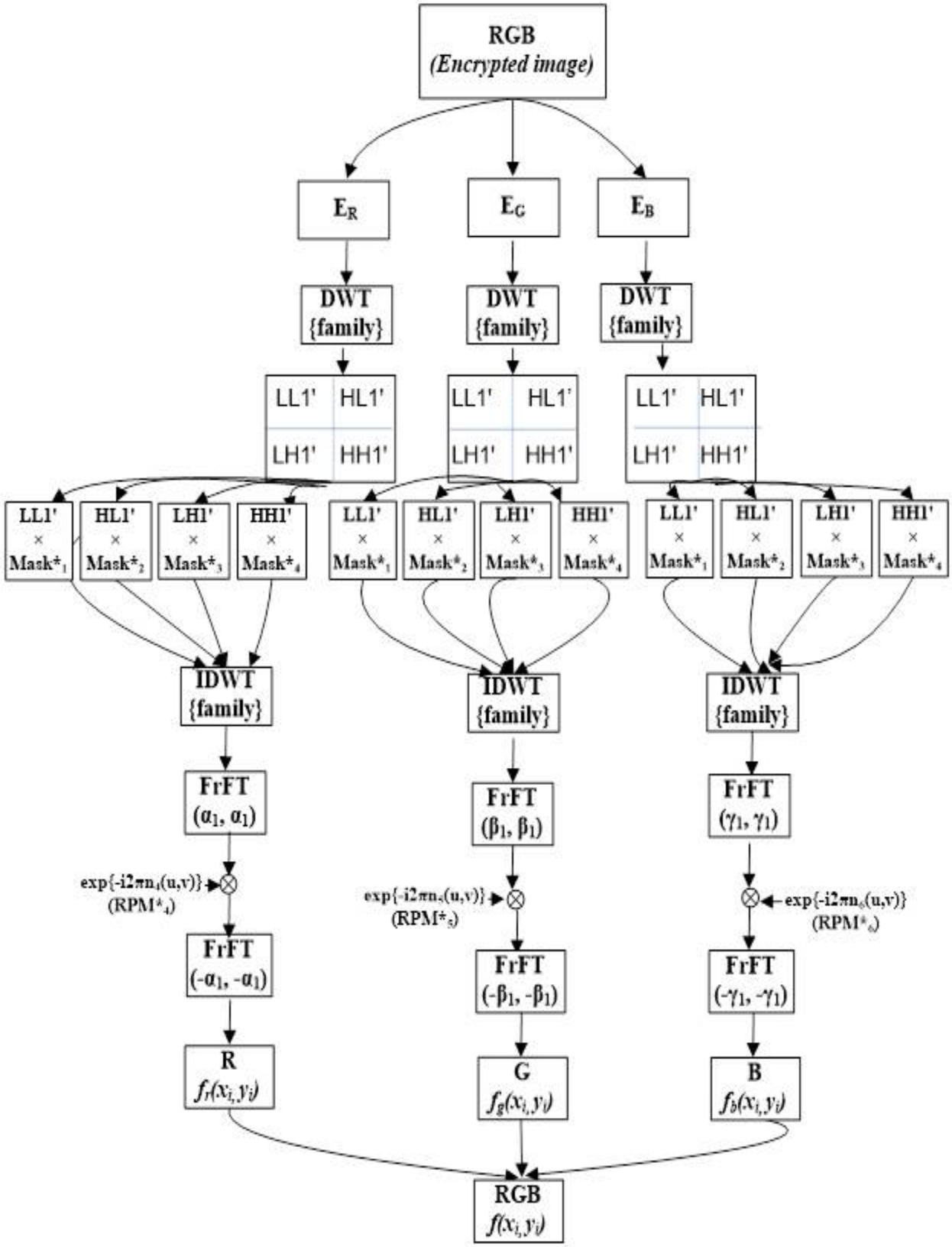

Figure 4. Flow chart of the proposed scheme for decryption process.

Figure 5k. Its red, green and blue encrypted components are shown in Figures 5(l-n). The Figure 5(o) is recovered image of baboon. To express the quality of decrypted image and to verify the reliability of the encryption algorithm, it is to introduce the common Mean Square Error (MSE) between the decrypted image and the original image as:

$$MSE = \sum_{x=0}^{255}\sum_{y=0}^{255}\frac{|\mathbf{I_{in}}(\mathbf{x},\ \mathbf{y}) - \mathbf{I_{out}}(\mathbf{x},\mathbf{y})|^2}{\mathbf{256 \times 256}} \quad (5)$$

If $I_{in}(x, y)$ and $I_{out}(x, y)$ represents respectively 256×256 pixel value of the input image and output images. The computed error for R, G and B component of color image Lena are 5.4382×10^{-20}, 5.5617×10^{-20} and 1.5388×10^{-19} respectively. In the same way for two other color images Baby and baboon and MSE of its red, green and blue components are 4.8648×10^{-20}, 4.7625×10^{-20}, 4.8648×10^{-20} and 7.1496×10^{-20}, 8.1835×10^{-20}, 9.758548×10^{-20} respectively. Similarly SNR is another term calculated between original and decrypted image by the following mathematical formula:

$$SNR = \frac{\sum_{x=0}^{255}\sum_{y=0}^{255}|\mathbf{I_0}(\mathbf{x},\ \mathbf{y})|^2}{\sum_{x=0}^{255}\sum_{y=0}^{255}|\mathbf{I_{in}}(\mathbf{x},\ \mathbf{y}) - \mathbf{I_{out}}(\mathbf{x},\mathbf{y})|^2} \quad (6)$$

Calculated SNR between the input and the recovered images of red, green and blue component for the color image Lena, baby and baboon is almost same as 537 dB.

3.1 Correlation Analysis

It is well known that the less Correlation Coefficient (CC) of two adjacent pixels the stronger ability of resisting statistical attack. So in order to test and verify the correlation of original image and encrypted image, use the formula below to calculate the related coefficient of neighbourhood pixels which are horizontal adjacent pixels pairs,

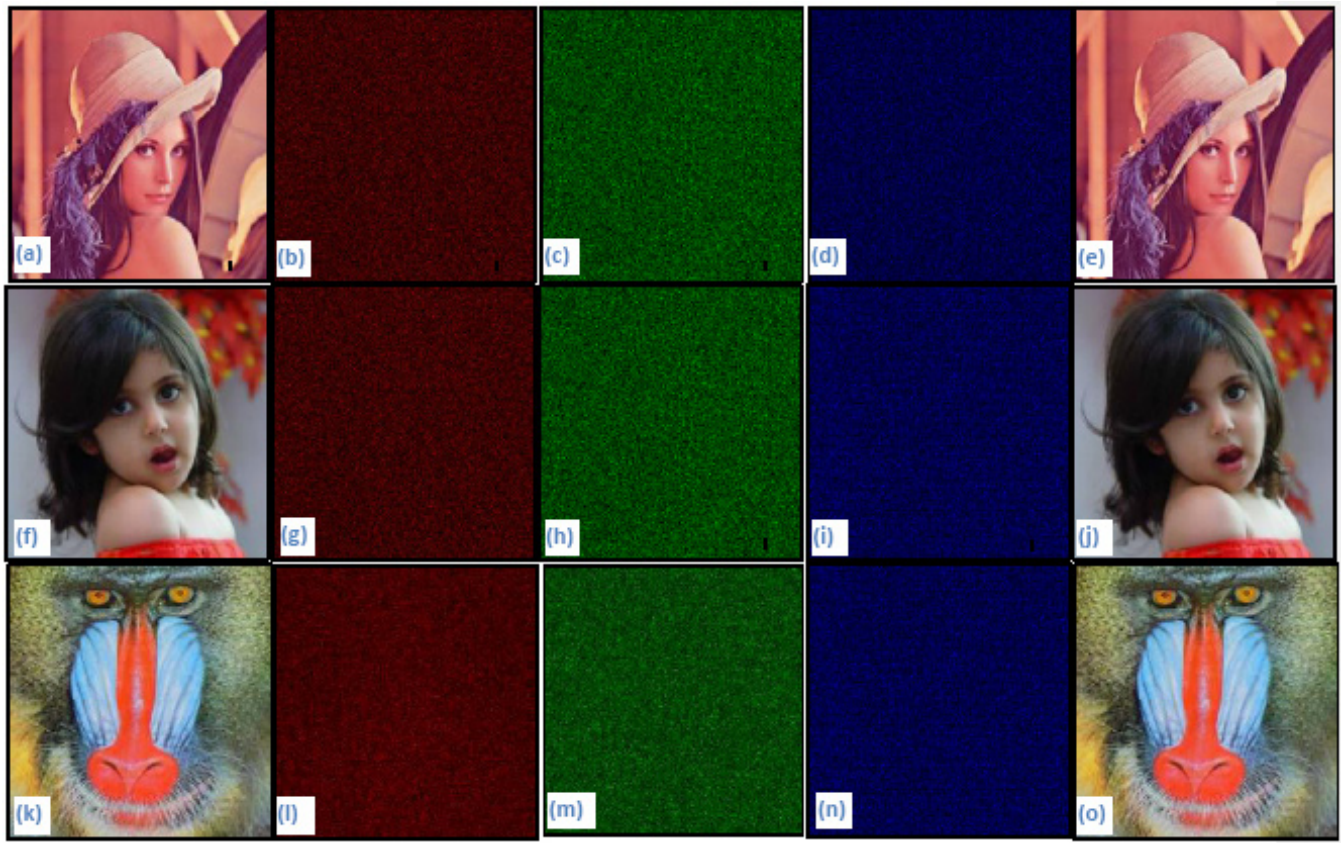

Figure 5. Results of validation of the proposed scheme for three color images: (a) input color image Lena of size 256×256 pixels; (b-d) are encrypted images of R, G and B components (e) decrypted image of Lena (f) input color image of baby girl , (g-i) are encrypted images of its color components, (j) decrypted image of baby girl. (k) is another color image of baboon, (l-n) are the encrypted images of its color components, (o) is decrypted of baboon.

verticals adjacent pixels pairs and some diagonal pixels pairs randomly selected from images. CC is another method used in the many papers[39–41] to see similarity of two images quantitatively. In given scheme randomly chosen 10,000 pairs of adjacent pixels (horizontal, vertical or diagonal) for computation of CC of the input and the encrypted images. Then, the CC of each pair is calculated by the following relations expressed as:

$$CC = \frac{\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{(\sum_{i=1}^{N}(x_i - \bar{x})^2)(\sum_{i=1}^{N}(y_i - \bar{y})^2)}} \quad (7)$$

Where $\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i$ and $\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$, the mean values of x_i and y_i

Calculated correlation coefficients of horizontal, vertical and diagonal of input and their encrypted images are given in Table 1. It is obvious from input images; correlation coefficients values are large as it is seen from cipher images. It demonstrates that nearby pixels in input images are strongly matched. However, for the encrypted images, correlation coefficient are low and approximate zero, this means that nearby pixels in the horizontal, vertical or diagonal directions are weakly matched.

3.2 Statistical Analysis

3.2.1 Histograms

Image histograms are other criteria in image analysis. Figure 6(a) represents the color image Lena and Figures 6(b-d) are histograms of R, G and B parts of Lena. It looks that they are much differ in each other. On the other hand, it is observed that the histograms of their ciphered images are nearly matched after a many simulations done, it can be concluded that the cipher-text of original images have similar histograms. So, it is difficult to an attacker to obtain meaningful info as the statistical point of view.

3.2.2 Entropy

Statistical measurement of randomness of pixels can be used to characterize the texture of the input and retrieved images in terms of entropy. Image entropy tells the distribution of pixel value color image. If image pixels are more, then its entropy is more.

The entropy $E(n)$ of image can be computed by following relation[42,43] as:

$$E(n) = -\sum_{i=0}^{L} P(n_i)log_2 p(n_i) \quad (8)$$

Where n_i is the ith color value for L level color image, $P(n_i)$ displays the probability symbol n_i. The known entropy for cipher-text image is 8. Entropy of cipher-image Lena, Baby girl and baboon images is calculated by scheme and shown in Table 2. It is clear form Table 2 that the entropy is near to slandered entropy, so proposed algorithm is very effective by entropy point of view.

3.3 Robustness

Supposed that intruder knows the cryptosystem and encryption process. As the Kerckhoff's principle state that, only security of the used keys is required. Even a very strong or well-designed scheme can be attacked easily if the keys are used in encryption is poorly selected. It is also examined the scheme's sensitivity of encryption parameters by taken wrong parameters. The retrieved color images for incorrect values are displays in Figure 7. The correct discrete wavelet family used in the algorithm is *sym4* and the incorrect family discrete wavelet

Table 1. CC value of horizontal, vertical and diagonal three images of RGB components

Image (color)	RGB parts	CC of Input image H V D			CC of Encrypted image H V D		
Lena	Red	0.9553	.9836	.9439	.0138	.0123	.0129
	Green	.9499	.9808	.9489	.0070	.0094	.0063
	Blue	.9333	.9733	.9553	.0133	.0252	.0113
Baby	Red	.9845	.9911	.9876	.0018	.0377	.0067
	Green	.9845	.9874	.9822	.0189	.0576	.0110
	Blue	.9862	.9890	.9842	.0327	.0388	.0044
Baboon	Red	.9422	.8034	.7594	.0248	.0192	.0049
	Green	.9124	.8041	.7581	.0070	.0179	.0106
	Blue	.9512	.8640	.8350	.0156	.0303	.0050

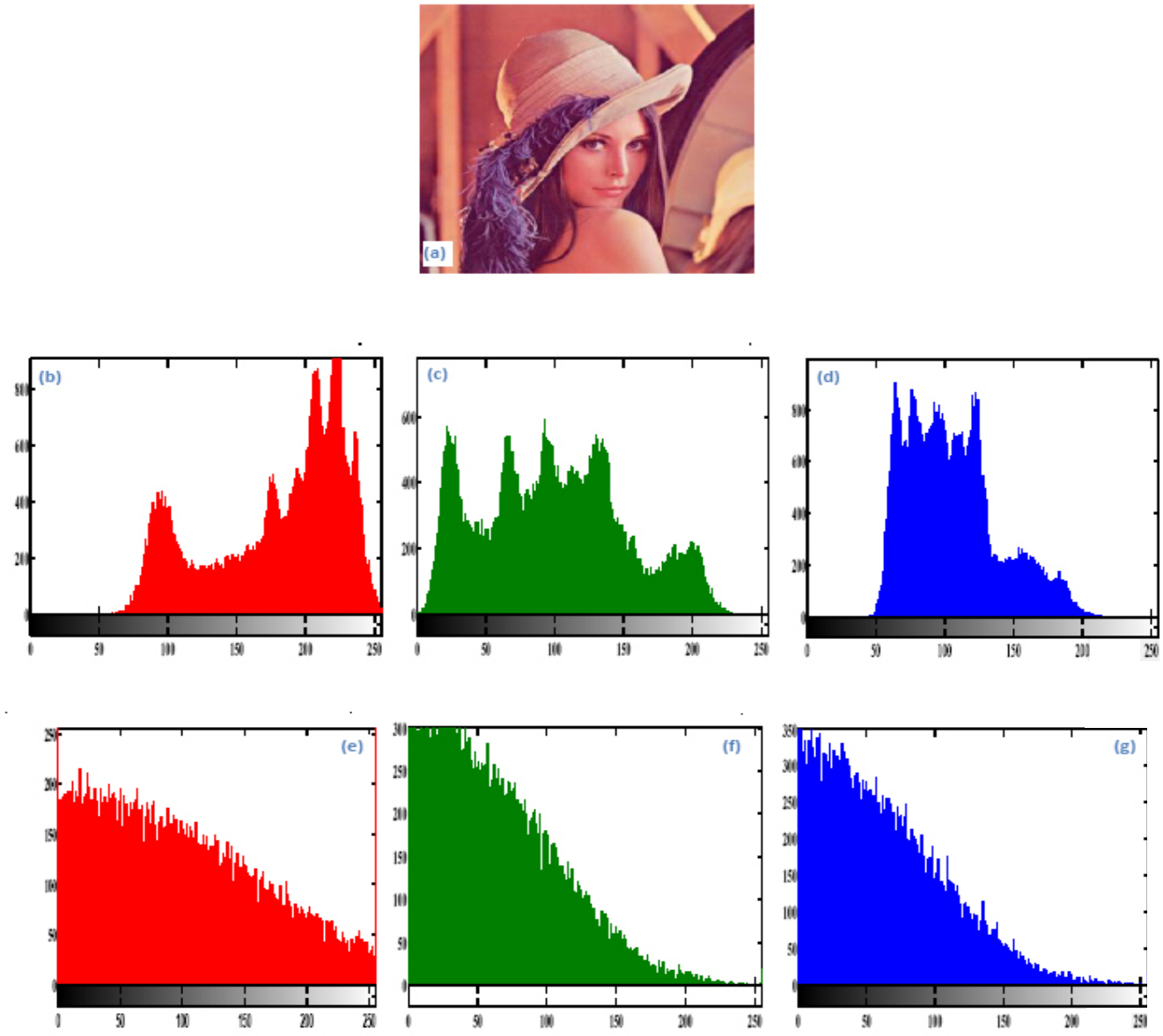

Figure 6. **(a)** is input image Lena, **(b-d)** are the histograms of input image R, G and B components of Lena and **(e-g)** are its encrypted R, G and B components of image Lena.

Table 2. Represents the entropy value of three image of RGB components

Image (color)	RGB parts	Type/size	Entropy of input image	Entropy of encrypted image	Entropy of decrypted image
Lena	Red	PNG/256×256	7.0748	8.1412	7.0506
	Green	PNG/256×256	6.5261	7.5462	3.8229
	Blue	PNG/256×256	5.8815	7.5107	3.1944
Baby	Red	JPEG/256×256	2.9335	7.7440	4.6342
	Green	PNG/256×256	2.4247	7.4607	4.0317
	Blue	JPEG/256×256	2.1808	7.3575	3.5174
baboon	Red	JPEG/256×256	7.1140	7.9263	7.1140
	Green	JPEG/256×256	6.9944	7.8662	6.9944
	Blue	JPEG/256×256	6.6833	7.6701	6.6833

are *dmey, sym3, db4* and correct fractional Fourier order used in the present scheme is in combination of (α_1, α_1), (β_1, β_1), (γ_1, γ_1), = 0.4, (α_1, α_1), (β_1, β_1), (γ_1, γ_1) = 0.4, 0.5, 0.6 and (α_1, α_1), (β_1, β_1), (γ_1, γ_1) = 0.3, 0.5, 0.7 respectively. Figure 7(a) represents input color Lena, Figure 7(b) is decrypted image of Lena with first wrong RPM used in DWT domain. Figure 7(c) is corresponded to another recovered image with first 02 wrong RPM used in DWT domain, Figures 7 (d-e) are recovered images with 03 and first 04 wrong RPM used in scheme. Similarly, it has been tested the incorrect family of DWT. Figures 7(f-i) are the recovered images with wrong discrete wavelet value (*sym3, haar, db4*). Figures 7(j), 7(k) are decrypted images with incorrect FrFT orders. It clearly explains scheme is highly sensitive.

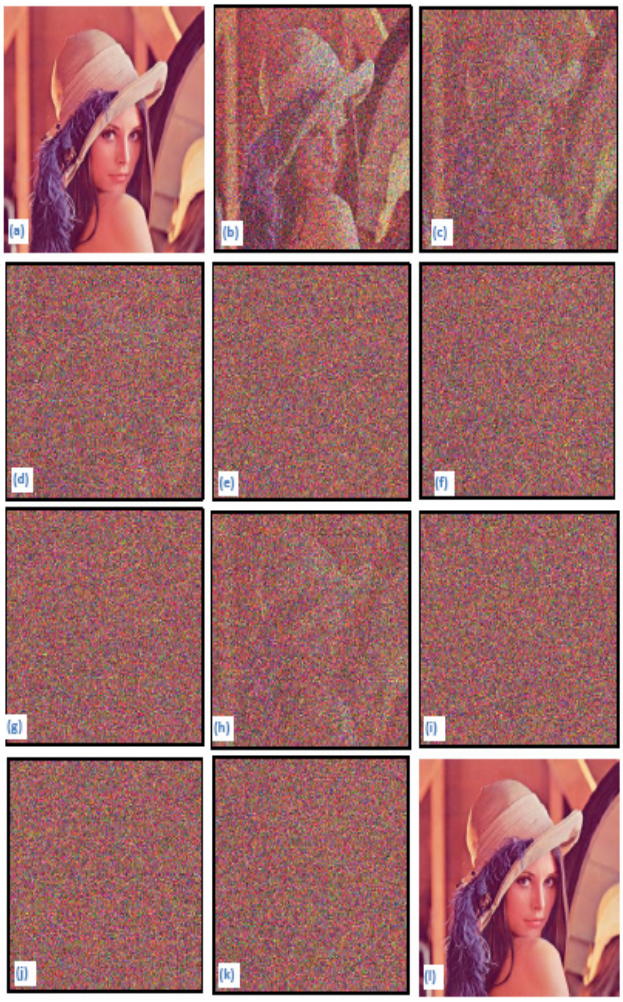

Figure 7. Results with incorrect parameters of FWT: **(a)** is input image Lena; **(b-e)** are decrypted images with incorrectmasks of used in the wavelet domain; **(f-i)** decrypted images with incorrect parameters of DWT family, **(j-k)** decrypted images with incorrect parameter of FrFT; **(l)** is recovered image with all correct parameters of DWT.

It is shown that the MSE and SNR graphs of FrFT orders in Figure 8. Figures 8(a,b) are MSE and SNR plots of color image Lena with fractional Fourier is 0.4. Figures 8(c,d) are also MSE and SNR plots of second image baby with change fractional Fourier orders (0.4, 0.5 and 0.6). Figures 8(e-f) are also MSE and SNR plots of third color image baboon with change fractional Fourier orders (0.3, 0.5 and 0.7). It is clearly seen from the graphs that the proposed algorithm is highly sensitive to the FrFT.

3.4 Occlusion and Noise Attacks

The robustness against the occlusion attacks on the encrypted image is examined. The occluded images are shown in Figures 9(a-d) for 6.25%, 25%, 50% and 75% occlusion in encrypted image of Lena. Figures 9(e-h) show the corresponding decrypted images which are recovered fairly well even for occlusion up to 75%. Additionally, we have plotted MSE and Correlation Coefficient (CC) against varying degrees of occlusion of the encrypted images Figures 10(a,b). The variation of MSE and CC curves clearly indicates the scheme's robustness to occlusion attack.

It is inevitable that the noise impacts directly the quality of the decrypted image. It is also tested the strength of the present algorithm scheme against noise attack[44–49] by taking multiplicative Gaussian noise in the encrypted images. The noise interferes with the ciphered images by relation[44].

$$A' = A(1 + kG) \tag{9}$$

Where A and A' are the ciphered and the noise-affected ciphered images, k is noise strength, and G is a Gaussian noise with 0 and 1 standard deviation. Figures 11(a-i) are indicates the retrieved images when k is set to 0, 0.5, 1.5, 2, 2.5, 3, 3.5 and 4. From the retrieved images, it has been observed that the scheme is secure and robust to noise attack. The drop in quality of the retrieved images is indicating the effect of noise about the robustness of scheme. Figures 12 shows plots of MSE curves against noise factor (k) for the component of color image Lena. It is seen that there is a certain increase in MSE curves of red, green and blue components due to noise factor. It clearly established the fact about present scheme is robustness on noise attack and occlusion attacks.

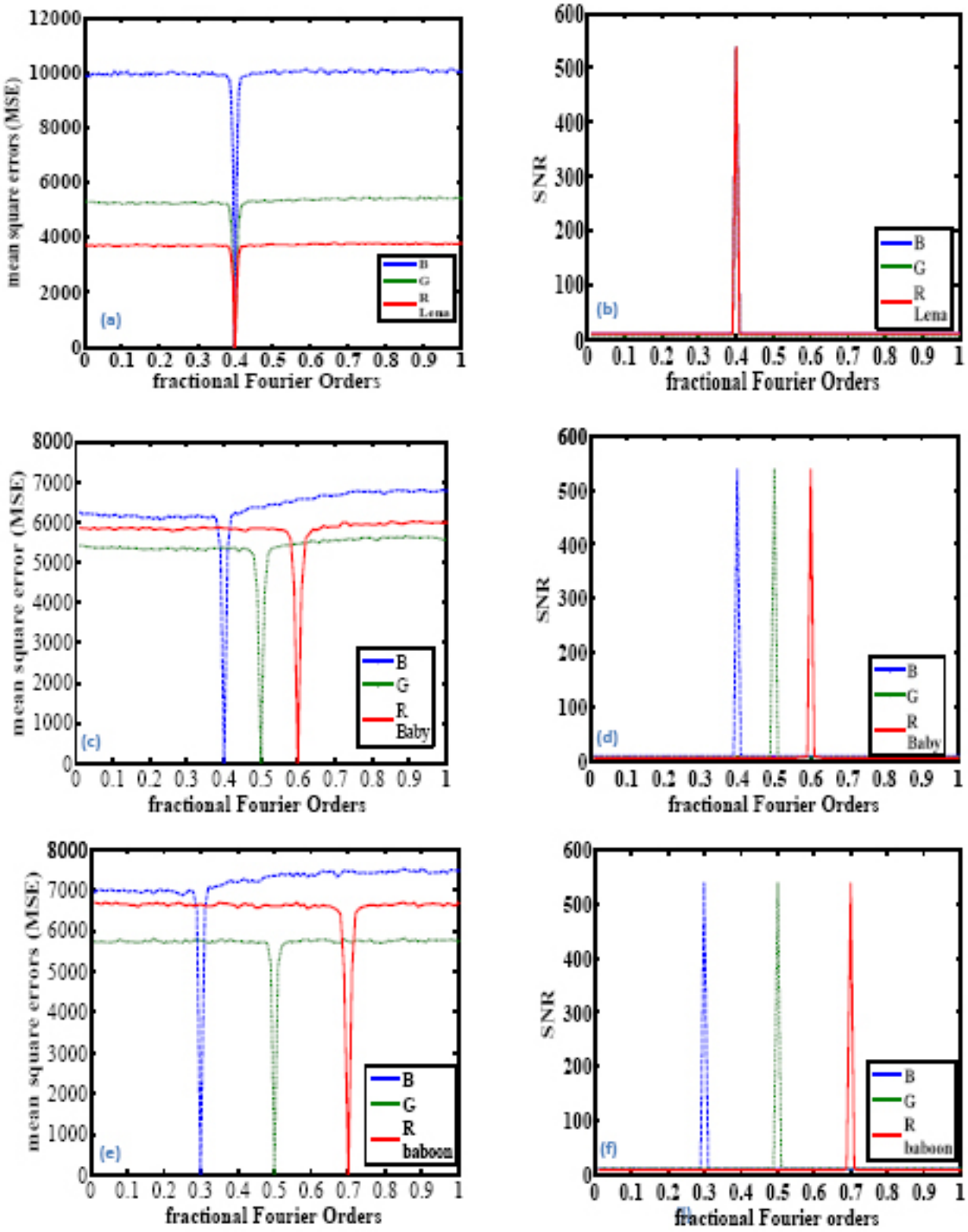

Figure 8. Sensitivity plots of MSE & SNR as a function of deviation from the correct value of various parameters of FrFT and DWT: **(a)** is MSE plot with (α_1, α_1), (β_1, β_1), (γ_1, γ_1) = 0.4, **(b)** is SNR with (α_1, α_1), (β_1, β_1), (γ_1, γ_1) =0.4, **(c)** is MSE plot with (α_1, α_1), (β_1, β_1), (γ_1, γ_1) = 0.3, 0.5, 0.6 **(d)** is SNR plot with (α_1, α_1), (β_1, β_1), (γ_1, γ_1) = 0.3, 0.5, 0.6, **(e)** is MSE plot with (α_1, α_1), (β_1, β_1), (γ_1, γ_1) = 0.3, 0.5, 0.7, **(f)** is SNR plot with (α_1, α_1), (β_1, β_1), (γ_1, γ_1) = 0.3, 0.5, 0.7.

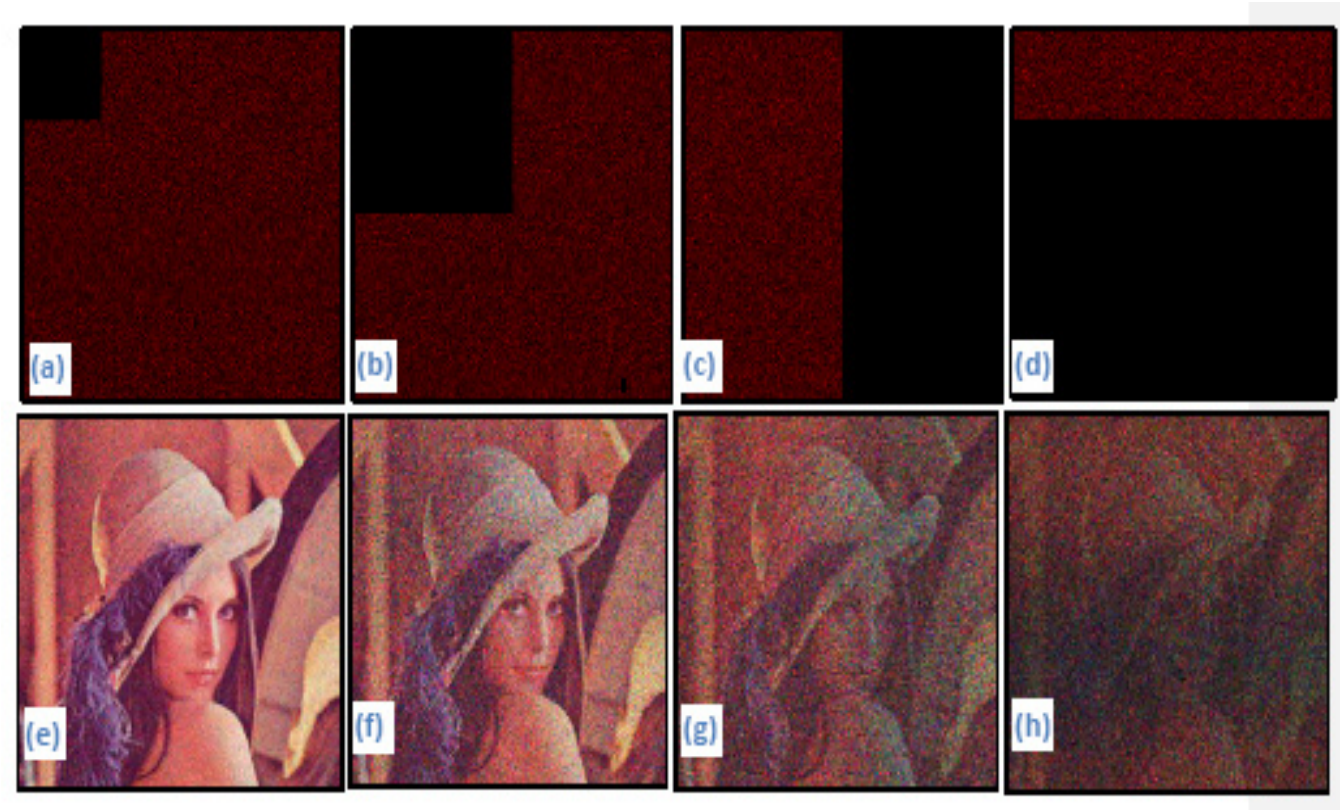

Figure 9. Occlusion results for the grayscale and the binary image for varying degrees of occlusion: Figs. 9(a-d) for $(1/16)^{th}$, $(1/4)^{th}$ $(1/2)^{th}$ and $(3/4)^{th}$ occlusion of the encrypted image of Lena. Figs. 9(e-h) show the corresponding decrypted images.

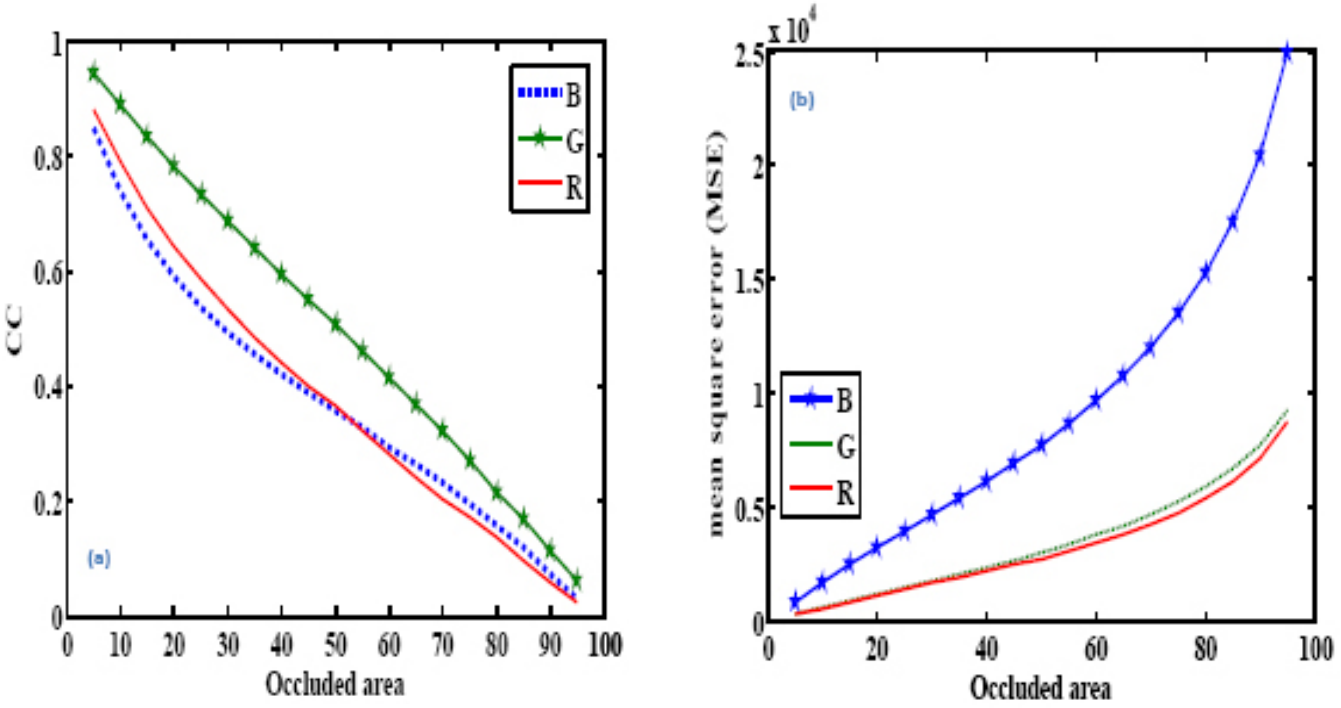

Figure 10. Plots of **(a)** Correlation coefficient with varying occluded area, and **(b)** MSE for color image Lena with varying occluded area

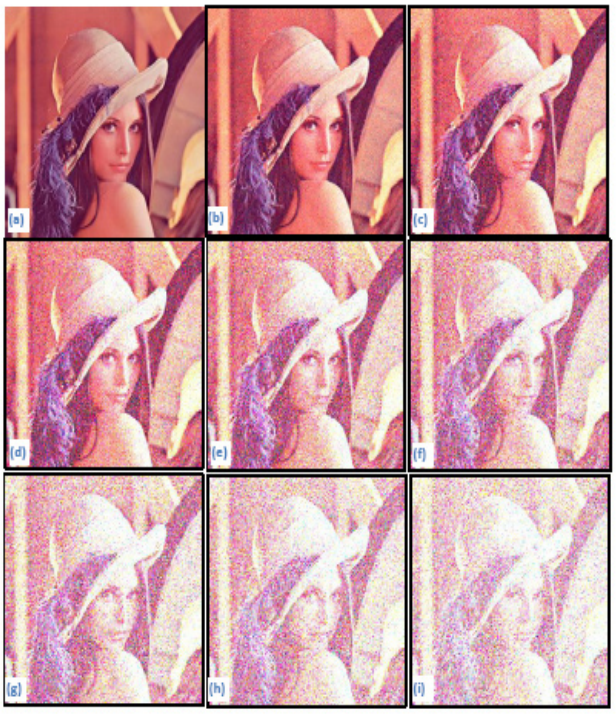

Figure 11. **(a)** Input image Lena; **(b-i)** recovered images corresponding to Gaussian noise factor k = 0.5, 1, 1.5, 2, 2.5, 3, 3.5 and 4 respectively.

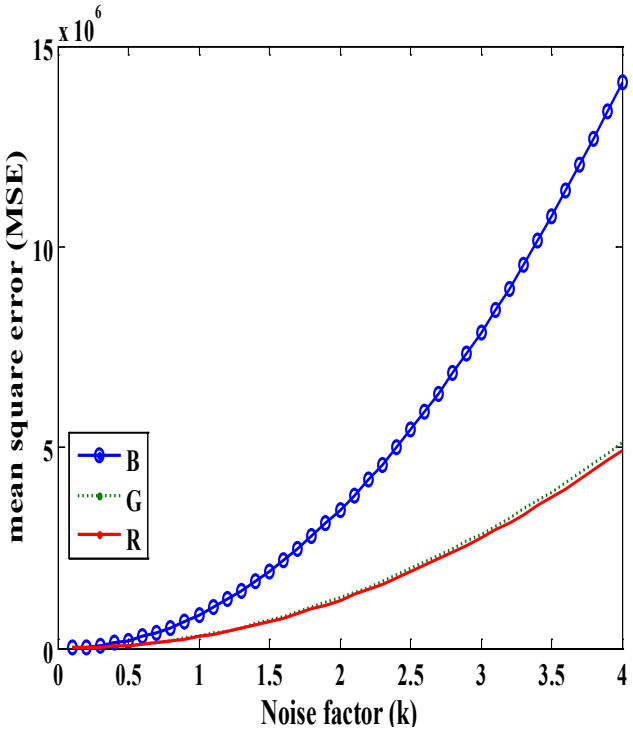

Figure 12. MSE plot of R, G & B components for color image Lena with varying noise factor k.

4. Conclusions

A study for color images has been proposed by using RPMin FWT planes. The RPMs are also used in the wavelet region that creates additional encryption keys and also enlarges keys. Present approach not only solves the difficulty of key management and makes the proposed algorithm is most secured. The entropy values and histograms show the validity of proposed scheme. Numerical results are presented to demonstrate the feasibility and security of the proposed system. The effectiveness of the proposed algorithm is seen from the calculated values of MSE and SNR. The sensitivity plots have also been studied for many parameters of FrFT and DWT. Results also demonstrates robustness of scheme against noise and occlusion attacks.

5. References

1. Refregier P, Javidi B. Optical image encryption based on input plane and Fourier plane random encoding. Opt Lett. 1995; 20:767–9.
2. Matoba O, Nomura T, Perez-Cabre E, Millan MS, Javidi B. Optical techniques for information security. Proc IEEE. 2009; 97:1128–48.
3. Alfalou A, Brosseau C. Optical image compression and encryption methods. Adv Opt Photon. 2009; 1:589–636.
4. Millan MS, Perez-Cabre E. Optical data encryption. Optical and Digital Image Processing: Fundamentals and Applications. G. Cristobal P. Schelkens and H. Thienpont, editors. Wiley; 2011. P. 739–67.
5. Kumar P, Joseph J, Singh K. Double random phase encoding based optical encryption systems using some linear canonical transforms: Weaknesses and countermeasures. John J. Healy, M. A. Kutay, H. M. Ozaktas, J. T. Sheridan, editors. Springer series in Optical Sciences. 2016; 198:367–96.
6. Markman A, Javidi B, Tehranipoor M. Photon-counting security tagging and verification using optically encoded QR codes. IEEE Photon J. 2014; 6:6800609.
7. Yadav AK, Vashisth S, Singh H, Singh K. Optical cryptography and watermarking using some fractional canonical transforms and structured masks. Advances in Optical and Engg. Proc IEM Optronix 2014; Springer. 2015. p. 25–36.
8. Singh H. Devil's vortex Fresnel lens phase masks on an asymmetric cryptosystem based on phase-truncated in gyrator wavelet transform. Opt and Lasers Eng. 2016; 81:125–39.
9. Unnikrishnan G, Joseph J, Singh K. Optical encryption by double-random phase encoding in the fractional Fourier domain. Opt Lett. 2000; 25:887–9.

10. Hennelly BM, Sheridan JT. Image encryption and the fractional Fourier Transform. Optik. 2003; 114:251–65.
11. Matoba O, Javidi B. Encrypted optical memory system using three-dimensional keys in the Fresnel domain. Opt Lett. 1999; 24:762–4.
12. Situ G, Zhang J. Double random-phase encoding in the Fresnel domain. Opt Lett. 2004; 29:1584–6.
13. Hennelly BM, Sheridan JT. Random phase and jigsaw encryption in the Fresnel domain. Opt Eng. 2004; 43:2239–49.
14. Rajput SK, Nishchal NK. Fresnel domain non-linear optical encryption scheme based on Gerchberg- Saxton phase retrieval algorithm. Appl Opt. 2014; 53:418–25.
15. Singh H, Yadav AK, Vashisth S, Singh K. Optical image encryption using devil's vortex toroidal lens in the Fresnel transform domain. International J of Opt. 2015**;** 2015: 926135. 13 pages.
16. Rodrigo JA, Alieva T, Calvo ML. Gyrator transform: Properties and applications. Opt Express. 2007;15: 2190–203.
17. Singh H, Yadav AK, Vashisth S, Singh K. Fully-phase image encryption using double random-structured phase masks in gyrator domain. Appl Opt. 2014; 53:6472–81.
18. Singh H, Yadav AK, Vashisth S, Singh K. Double phase-image encryption using gyrator transforms and structured phase mask in the frequency plane. Opt Lasers Eng. 2015; 67: 145–56.
19. Zhou NR, Wang Y, Gong L. Novel optical image encryption scheme based on fractional Mellin transform. Opt Commun. 2011; 284:3234–42.
20. Vashisth S, Singh H, Yadav AK, Singh K. Devil's vortex phase structure as frequency plane mask for image encryption using the fractional Mellin transform. Int J Opt. 2014; 728056:1–9.
21. Mendlovic D, Konforti N. Optical realization of the Wavelet Transform for two-dimensional objects. Appl Opt. 1993; 32:6542–6.
22. Mendlovic D, Zalevsky Z, Mas D, Gercia J, Ferreira C. Fractional Wavelet Transform. Appl Opt.1997; 36:4801–6.
23. Chen L, Zhao D. Optical image encryption based on fractional wavelet transform. Opt Commun. 2005; 254:361–7.
24. Chen L, Zhao D. Image encryption with fractional wavelet packet method. Optik. 2008; 119:286–91.
25. Chen L, Zhao D. Color image encoding in dual fractional Fourier wavelet domain with random phases. Opt Commun. 2009; 282:3433–8.
26. Vilardy JM, Useche J, Torres CO, Mattos L. Image encryption using the fractional Wavelet Transform. J Phys conf seri. (IOP). 2011; 274: 012047.
27. Prasad A, Kumar M, Choudhury DR. Color image encoding using fractional transformation associated with wavelet transform. Opt Commun. 2012; 285:1005–9.
28. Bao L, Zhou Y, Philip Chen CL. Image encryption in the wavelet domain. Proc SPIE. 2013; 8755:875502–1/12.
29. Kumar M, Mishra DC, Sharma RK. A first approach on an RGB image encryption. Opt Lasers Eng. 2014; 52:27–34.
30. Kong D, Shen X. Multiple-image encryption based on optical Wavelet Transform and multichannel fractional Fourier transform. Opt Lasers Eng. 2014; 57:343–9.
31. Mehra I, Nishchal NK. Wavelet-based image fusion for multiple images through asymmetric keys. Opt Commun. 2015; 335:153–60.
32. Zhang SQ, Karim MA. Color image encryption using double random phase encoding. Microw Opt Technol Lett. 1999; 21:318–23.
33. Chen LF, Zhao D. Optical color image encryption by wavelength multiplexing and lensless Fresnel transform holograms. Opt Express. 2006; 14:8552–60.
34. Joshi M, Shakher C, Singh K. Color image encryption using fractional Fourier transform. Opt Commun. 2007; 279:35–42.
35. Dahiya M, Sukhija S, Singh H. Image encryption using quad masks in fractional fourier domain and case study. IEEE International Advance Computing Conference (IACC); 2014 1048–53.
36. Abuturab MR. Color image security system using double random-structured phase encoding in gyrator domain. Appl Opt. 2012; 51:3006–16.
37. Abuturab MR. An asymmetric color image cryptosystem based on Schur decomposition in gyrator domain. Opt Lasers Eng. 2014; 58:39–47.
38. Singh H. Optical cryptosystem of color images using random phase masks in the Fractional Wavelet Transform domain. AIP Conf Proc. 2016; 1728**:**020063–1/4.
39. Tong X, Liu Y, Zhang M, Xu H, Wang Z. An image encryption scheme based on hyperchaotic rabinovich and exponential chaos maps entropy. 2015; 17:181–96.
40. Liang Y, Liu G, Zhou NR, Wu J. Image encryption combining multiple generating sequences controlled fractional DCT with dependent scrambling and diffusion. J Mod Opt. 2015; 62:251–64.
41. Zhang Q, Wei XP. A novel couple images encryption algorithm based on DNA subsequence and chaotic system. Optik. 2013; 124:6276–81.
42. Yadav AK, Vashisth S, Singh H, Singh K. A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask. Opt Commun. 2015; 344:172–80.
43. Meng XF, Cai LZ, Yang XL, Xu XF, Dong GY, Shen XX, Zhang H, Wang YR. Digital color image watermarking based on phase-shifting interferometry and neighboring pixel value subtraction algorithm in the discrete-cosine-transform domain. Appl Opt. 2007; 46: 4694–701.
44. Joshi M, Shakher C, Singh K. Image encryption using radial Hilbert transform filter bank as an additional key in

the modified double random fractional Fourier encoding architecture. Opt Laser Eng. 2010; 48:605–15.
45. Joshi M, Shakher C, Singh K. Fractional fourier plane image encryption technique using radial Hilbert- and Jigsaw transform. Opt Laser Eng. 2010; 48:754–9.
46. Sui L, Xin M, Tian A, Jin H. Single-channel color image encryption using phase retrieval algorithm in fractional Fourier domain. Opt Laser Eng. 2013; 51:1297–309.
47. Vashisth S, Yadav AK, Singh H, Singh K. Watermarking in gyrator domain using an asymmetric cryptosystem. Proc of SPIE. 2015; 9654:96542E–1/8.
48. Singh H. Crytosystem for securing image encryption using structured phase masks in Fresnel Wavelet Transform domain. 3D Res. 2016; 7:34.
49. Vashisth S, Singh H, Yadav AK, Singh K. Image encryption using fractional Mellin transform, structured phase filters and phase retrieval. Optik. 2014; 125:5309–15.