Utilization of Double Random Phase Encoding for Securing Color Images

Mohammed A. AlZain
College of Computers and Information Technology
Taif University, P.O. Box 888
Al-Hawiya-Taif, 21974, KSA

ABSTRACT
This paper investigates the Double Random Phase Encoding (DRPE) implementation in encrypting color digital images. The color optical image cipher works through splitting color plainimage into red (R), green (G) and blue (B) channels. The color plainimage RGB components are multiplied with the random phase mask (RPM) and transformed with Fourier Transform (FT). The modulated RGB components are again multiplied using the second RPM and subjected again to inverse FT. A set of experimental tests using different color images has been employed to study the security of DRPE for encrypting digital color images. Experimental results demonstrated the efficiency of DRPE for encrypting digital color images and its immunity regarding the most potential attacks.

General Terms
Security, Image Encryption.

Keywords
DRPE, Fourier Transform (FT), Color image encryption

1. INTRODUCTION
The optical cryptography methods have significant impact on the optical information processing field. Efficient and dependable security methods in transmitting and storing digital images are required for several applications such as video conferencing, pay TVs, medical images storing and transmission, military usage, police identification, online banking, and governmental systems.

The Opto-security schemes have gained a lot of advances because of their features of parallel processing and fast processing. The Optics offers several freedom degrees in optical beams can be modulated, like as the phase, amplitude, wavelength, and polarization. So, many optical encryption schemes have been introduced [1-4].

The DRPE presented in [5], may be considered the most commonly utilized optical encryption method. The Fractional Fourier transform (FrFT) was introduced as generalization for traditional encryption [6-7]. The Fourier Transform (FT) is commonly utilized in optical image encryption [8-10].

The optical DRPE color image encryption begins with splitting color plainimage into RGB components that modulated by the first RPM and FT transformed. The achieved RGB channels are secondly modulated using another RPM and again FT transformed.

The paper remainder is appeared as follows. Sec. 2 gives the main fundamentals regarding DRPE. Sect. 3 presents encryption/decryption stages. Sect. 4 gives the security study of the optical DRPE encryption. And conclusions are given in Sect. 5.

2. DRPE FUNDAMENTALS
The DRPE depends on modifying the image spectral allocation regardless information of spectral alternation or received image in receiving side. The basic is based on putting two RPM (encoding secret keys) in setup named 4f. The DRPE encryption can be defined as [5]:

$$Y(a,b) = FT\{FT[X(a,b)\exp(j2\pi\theta(a,b))]\exp(j2\pi\omega(u,v))\} \qquad 1$$

The DRPE decryption can be defined as [5]:

$$X(a,b) = \{FT^{-1}[FT^{-1}(Y(a,b))\exp(-j2\pi\omega(u,v))\}\exp(-j2\pi\theta(a,b)) \qquad 2$$

The $\exp(j2\pi\theta(x,y))$ and $\exp(-j2\pi\omega(u,v))$ represent two RPM secret keys which will be transmitted with the encrypted color image. FT/FT−1 represents the Fourier and inverse Fourier transformations.

3. THE OPTICAL DRPE FOR COLOR IMAGE ENCRYPTION
The encryption/decryption stages using DRPE encryption are listed below in the next two subsections, respectively.

3.1 Encryption Stage
The color plainimage $I(x_i, y_j)$ is split into R, G, and B component as $I_R(x_i, y_j)$, $I_G(x_i, y_j)$ and $I_G(x_i, y_j)$, respectively. Each of RGB components is multiplied using the first $RPM_{r1}(x_i, y_j)$, $RPM_{g1}(x_i, y_j)$, and $RPM_{b1}(x_i, y_j)$, and perform FT. The transformed R, G, and B components are multiplied with the second $RPM_{r2}(u_i, v_j)$, $RPM_{g2}(u_i, v_j)$ and $RPM_{b2}(u_i, v_j)$, and then employed second FT. The three encrypted R, G, and B components $E_{r2}(x_i, y_j)$, $E_{g2}(x_i, y_j)$ and $E_{b2}(x_i, y_j)$ are multiplexed to obtain the encrypted color image $E(x_i, y_j)$.

3.2 Decryption Stage
The encrypted color image $E(x_i, y_j)$ is split into R/G/B components $E_r(x_i, y_j)$, $E_g(x_i, y_j)$ and $E_b(x_i, y_j)$, respectively. The FT^{-1} is applied to color R/G/B components, and modulated using $RPM^*_{r2}(u_i, v_j)$, $RPM^*_{g2}(u_i, v_j)$, and $RPM^*_{b2}(u_i, v_j)$. Another FT^{-1} is applied to modulated R/G/B components and modulated with $RPM^*_{r1}(x_i, y_j)$, $RPM^*_{g1}(x_i, y_j)$ and $RPM^*_{b1}(x_i, y_j)$. The decrypted R/G/B components $B_{r2}(x_i, y_j)$, $B_{g2}(x_i, y_j)$ and $B_{b2}(x_i, y_j)$ are assembled to get the final decrypted color image $D(x_i, y_j)$.

4. SIMULATION EXPERIMENT
Several tests are carried out for studying the efficiency of the optical DRPE for color image encryption. The performance of optical DRPE for color image encryption is performed using

several encryption performance metrics such as visually inspection, entropy estimation, statistical evaluation, differential measures, quality estimation, and noise immunity. Tests were performed using three 256×256 color Lena, House, and House images. The original test plainimages are illustrated in Fig. 1.

a) Lena b) House c) Sailboat

Fig. 1: Color plainimages – Lena, House, and House

4.1 Visual Quality Inspection

The efficiency of DRPE is investigated in encrypting color Lena, House and Sailboat images. The encryption results of optical DRPE are depicted in Fig. 2 for color Lena, House and Sailboat images. The obtained test consequences for encrypted color Lena, House and Sailboat images ensure the superiority of optical DRPE in hiding all features of their corresponding color plainimages.

Color Image Channels | Image name: Lena, House, House

Rows: Red, Green, Blue, encrypted color image

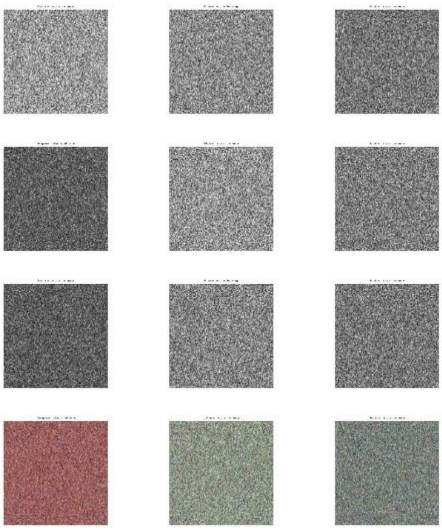


Fig. 2: Encrypted color Lena, House and Sailboat color image components using optical DRPE

4.2 Histogram Test

The histogram test for is a graph which show the pixels number for each intensity value. The histogram should be uniform for an efficient encryption. Also, the histograms of encrypted color RGB components should be different from their corresponding original color RGB components. Experimental histogram tests of the original/encrypted RGB components of colored Lena, House and Sailboat images using optical DRPE are shown in Fig. 3-5. The obtained results show that the histograms of encrypted RGB components for Lena, House and Sailboat images were completely different from corresponding histograms of their original color RGB components. The encrypted RGB components histogram for color Lena, House and Sailboat images using optical DRPE are quite uniform. So, the optical DRPE has the ability to resist any histogram based attack.

Color Image Channels | Color plainimage | Color Plainimage | Decrypted cipherimage

Rows: Red, Green, Blue

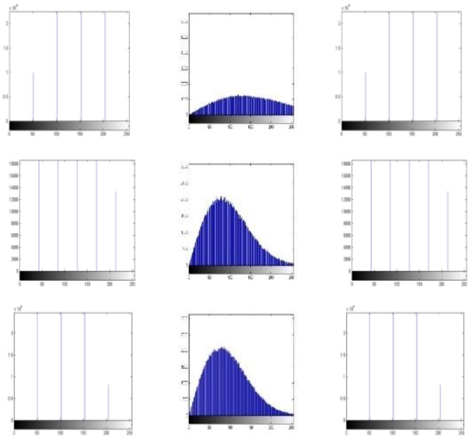


Fig. 3: RGB components Histogram of encrypted/decrypted color Lena image using optical DRPE

Color Image Channels | Color plainimage | Color Plainimage | Decrypted cipherimage

Rows: Red, Green, Blue

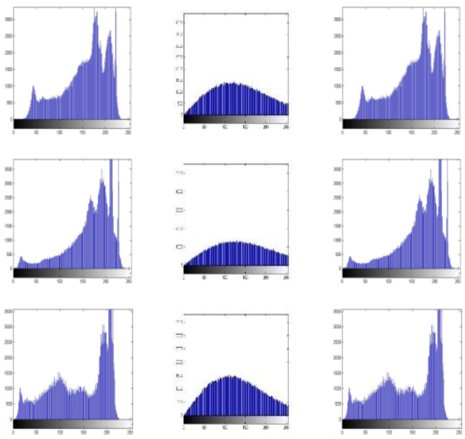
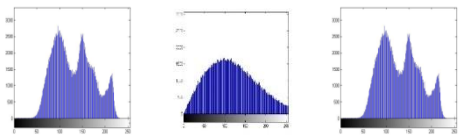


Fig. 4: RGB components Histogram of encrypted/decrypted color House image using optical DRPE

Color Image Channels | Color plainimage | Color plainimage | Decrypted cipherimage

Red



Green

Blue

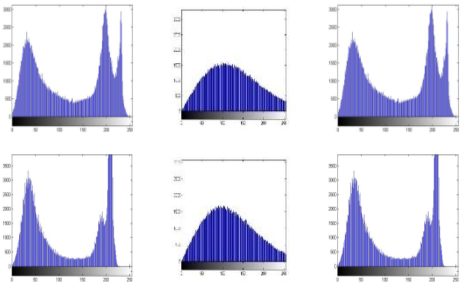


Fig. 5: RGB components Histogram of encrypted/decrypted color Sailboat image using optical DRPE

4.3 Encryption Quality Tests

The encryption quality can be estimated using several estimations like correlation coefficient, histogram deviation and irregular deviation.

The correlation coefficients r is estimated among original image $OI(x_i, y_j)$ and encrypted image $EI(x_i, y_j)$ RGB components as [11-12]:

$$r(OI, EI) = \frac{E\{(EI - E(EI)) \cdot (OI - E(OI))\}}{\sqrt{E\{[EI - E(EI)]^2\}}\sqrt{E\{[OI - E(OI)]^2\}}}, \quad (3)$$

where $E\{\}$ is expectation operator. Small r indicates high difference between the original image $OI(x_i, y_j)$ and encrypted image $EI(x_i, y_j)$ RGB components.

The ID measure estimates the encryption efficiency in terms of how much irregular is the difference caused by encryption. The ID can be estimated as [13-15]:

$$ID(I,E) = \frac{\left|\sum_{i=0}^{255} h_d(i)\right|}{MxN}, \quad (4)$$

$$h_d(i) = |h(i) - M_h|, \quad (5)$$

where h(i) is cipherimage histogram and M_h is average uniform histogram for encrypted image. Small ID values indicate good encryption quality.

The HD measure estimates the encryption quality by how it enlarges the difference among the original image $OI(x_i, y_j)$ and encrypted image $EI(x_i, y_j)$ RGB components. The HD can be calculated as [13-15]:

$$HD(I,E) = \frac{\left|\sum_{i=0}^{255} d(i)\right|}{MxN}, \quad (6)$$

where $d(i)$ is absolute difference among the original image $OI(x_i, y_j)$ and encrypted image $EI(x_i, y_j)$ RGB components. The variables M and N represent image dimensions. High HD values ensure large difference between the original image $OI(x_i, y_j)$ and encrypted image $EI(a_i, b_j)$ RGB components. Table 1 shows the Correlation coefficients, Irregular Deviation, and histogram deviation metrics of encrypted RGB components for color Lena, House and sailboat using Optical DRPE. The resulted correlation coefficients, Irregular and histogram deviations metrics shown in Table 1 ensure good encryption quality of optical DRPE.

Table 1: Correlation coefficients, Irregular deviation, and histogram deviation metrics for encrypted RGB components for colored Lena, House and sailboat using Optical DRPE

Color Image	Security Metrics	Optical DRPE		
		Red	Green	Blue
Lena	r_{xy}	-0.0034	7.830e-004	-0.002
	D_H	1.7053	1.07053	1.9605
	D_I	0.7120	0.7094	0.9852
House	r_{xy}	0.0029	0.0015	1.997e-004
	D_H	0.6495	0.8097	0.5952
	D_I	0.7230	0.7109	0.6583
Sailboat	r_{xy}	-0.0019	0.0028	-0.0024
	D_H	0.4942	0.8075	0.9772
	D_I	0.8334	0.5504	0.5685

4.4 Information Entropy Measure

The information entropy test is utilized for estimating encrypted R, G, and B components information amount. The information entropy measure may be estimated as [16]:

$$E(S) = \sum_{i=1}^{2^N - 1} P(S_i) \log_2 \frac{1}{P(S_i)}, \quad (7)$$

where $E(S)$, and $P(S_i)$ are the entropy and the occurrence must be 8 bits.

The objective of information entropy measure is to estimate information amount of encrypted RGB components for colored Lena, House and sailboat using Optical DRPE. Table 2 gives the information entropy estimates of encrypted RGB components for colored Lena, House and sailboat using Optical DRPE. The obtained results demonstrated that the information entropy values of encrypted RGB components for colored Lena, House and sailboat are near the optimal information entropy estimate of 8 bits.

Table 2: Information entropy metric of original/encrypted RGB components for colored Lena, House and sailboat using Optical DRPE

Image	Colored Plainimage			Encrypted Colored Cipherimage with DRPE Optical Encryption		
	Red	Green	Blue	Red	Green	Blue
Lena	1.973	1.973	1.628	7.3099	7.3109	7.5895
House	7.416	7.229	7.435	7.5970	7.4505	7.6727
Sailboat	7.312	7.643	7.214	7.7504	7.7320	7.7520

4.5 Differential Measure

Differential measure is carried out to study the impact of one pixel changing in two plainimages on their respected cipherimages with optical DRPE. The differential test is evaluated using the number of pixels changing rate (NPCR) and the unified averaging changing intensity (UACI) [40].

The $NPCR_{R,G,B}$ may be computed as [17-20]:

$$NPCR_{R,G,B}(C^1, C^2) = \frac{\sum_{i,j} D_{R,G,B}(a_i, b_j)}{N} \times 100\%, \quad (8)$$

where N is image pixels number and $D_{R,G,B}(a_i, b_j)$ is as:

$$D_{R,G,B}(C^1, C^2) = \begin{cases} 0, & C^1_{R,G,B}(a_i, b_j) = C^2_{R,G,B}(a_i, b_j) \\ 1, & C^1_{R,G,B}(a_i, b_j) \neq C^2_{R,G,B}(a_i, b_j) \end{cases} \quad (9)$$

where $C^1_{R,G,B}(a_i, b_j)$ and $C^2_{R,G,B}(a_i, b_j)$ are the corresponding color RGB components in the two color cipherimages $C^1(a_i, b_j)$ and $C^2(a_i, b_j)$, respectively.

The $UACI_{R,G,B}$ can be defined as [17-20]:

$$UACI_{R,G,B}(C^1, C^2) = \frac{1}{N}\left[\sum_{i,j} \frac{\left|C^1_{R,G,B}(a_i, b_j) - C^2_{R,G,B}(a_i, b_j)\right|}{255}\right] \times 100\%, \quad (10)$$

The NPCR/UACI experimental tests are illustrated in Table 3. The experimental tests ensure the sensitivity of optical DRPE regarding small modification in color plainimages RGB components.

Table 3: NPCR/UACI of encrypted RGB components for color Lena, House and sailboat using Optical DRPE

Image	Metric	Encrypted color images with Optical DRPE		
		Red	Green	Blue
Lena	NPCR	97.7814	97.7921	99.3645
	UACI	0	0	0
House	NPCR	99.5644	99.6082	99.6151
	UACI	0	0	0
Sailboat	NPCR	99.5125	99.6452	99.6742
	UACI	0	0	0

4.6 Noise Resistance Test

The optical DRPE resistance regarding noise attacks is tested in the decryption phase using peak signal to noise ratio (PSNR), SSIM and FSIM. The employed noises are salt and pepper, additive white Gaussian noise (AWGN), and speckle noises, respectively. The PSNR is employed to test the quality of decrypted RGB components.

The PSNR may be estimated as [21-22]:

$$PSNR(OI, EI) = 10\log_{10} \frac{(255)^2}{MSE(OI, EI)} \quad (11)$$

The SSIM is utilized to test quality of decrypted image. The SSIM is computed as [23-26]:

$$SSIM(x, y|w) = \frac{(2\overline{w}_x\overline{w}_y + C_1)(2\sigma_{w_x w_y} + C_2)}{(\overline{w}_x^2 + \overline{w}_y^2 + C_1)(\sigma^2_{w_x} + \sigma^2_{w_y} + C_2)} \quad (12)$$

where, C1, C2 are minor constants, $\overline{w}_x$ and $\overline{w}_y$ are average of w_x and w_y regions, respectively. $\Sigma^2_{w_x}$ is the region w_x variance and $\sigma_{w_x w_y}$ is two regions covariance among w_x and w_y. High SSIM values mean perfect resistance against noise.

The FSIM is utilized to test the decrypted image quality. The FSIM is computed as [23-26]:

$$FSIM = \frac{\sum_{x\in\Omega} S_L(x).PC_m(x)}{\sum_{x\in\Omega} PC_m(x)} \quad (13)$$

where Ω is image spatial domain, $S_L(x)$ is overall similarity among two images and $PC_m(x)$ is phase congruency. High FSIM values mean perfect resistance against noise. The noise immunity results of decrypted RGB components for color Lena, House and sailboat using Optical DRPE with AWGN with variance = 0.01, 0.05 and 0.1, speckle noise with variance = 0.01, 0.05 and 0.1, and salt & pepper with density = 0.01, 0.05 and 0.1 are shown in Tables 4-6 and Figs. 6-8. The noise resistance results using PSNR, SSIM and FSIM demonstrated the efficiency of the optical DRPE with respect to all the three different types of noise like AWGN with variance = 0.01, 0.05 and 0.1, speckle noise with variance = 0.01, 0.05 and 0.1, and salt & pepper with variance = 0.01, 0.05 and 0.1.

Table 4: PSNR of deciphered RGB components for colored Lena, House and sailboat using Optical DRPE in the presence of AWGN, Salt & peppers, and Speckle noises

Image	Components	PSNR								
		AWGN variance			Salt &peppers density			Speckle density		
		0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1
Lena	Red	2.8390	2.8390	2.8391	2.8392	2.8392	2.8392	2.8387	2.8381	3.8375
	Green	7.3240	7.3239	7.3238	7.3238	7.3237	7.3238	7.3235	7.3231	7.3228
	Blue	7.4922	7.4919	7.4919	7.4918	7.4919	7.4923	7.4916	7.4914	7.4913
House	Red	3.8936	3.8936	3.8937	3.8938	3.8938	3.8938	3.8932	3.8926	3.8922
	Green	3.8937	3.2914	3.2915	3.2916	3.2916	3.2915	3.3911	3.290	3.2901
	Blue	4.3604	4.3605	4.3606	4.3607	4.3606	4.3604	4.3600	4.3593	4.3589
Sailboat	Red	5.3763	5.3762	5.3762	5.3763	5.3762	5.3763	5.3758	5.3752	5.3749

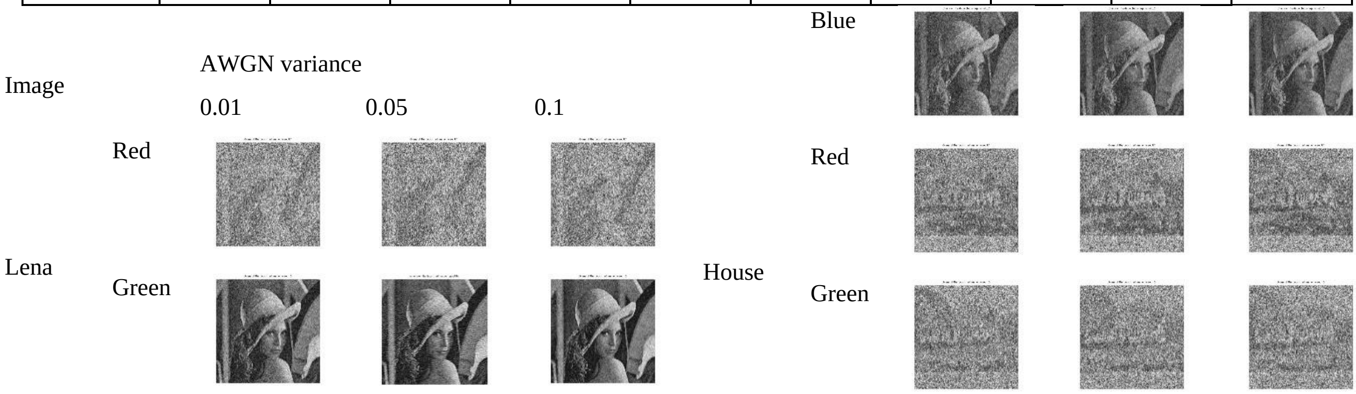
	Green	4.8409	4.8410	4.8411	4.8412	4.8409	4.8405	4.8395	4.8395	4.8385
	Blue	5.3506	5.3506	5.3507	5.3508	5.3502	5.3502	5.3502	5.3492	5.3485

Table 5: SSIM of deciphered RGB components for colored Lena, House and sailboat using Optical DRPE in the presence of AWGN, Salt & peppers, and Speckle noises

Image		Feature Similarity Index (FSIM)								
		AWGN variance			Salt &peppers density			Speckle density		
		0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1
Lena	Red	0.0027	0.0027	0.0027	0.0027	0.0027	0.0027	0.0026	0.0026	0.0026
	Green	0.0043	0.0041	0.0041	0.0041	0.0045	0.0048	0.0041	0.0043	0.0045
	Blue	0.0035	0.0034	0.0034	0.0034	0.0035	0.0036	0.0034	0.0034	0.0035
House	Red	0.0029	0.0029	0.0029	0.0029	0.0030	0.0030	0.0029	0.0029	0.0028
	Green	0.0029	0.0029	0.0029	0.0029	0.0029	0.0029	0.0028	0.0028	0.0028
	Blue	0.0036	0.0035	0.0035	0.0036	0.0036	0.0036	0.0035	0.0035	0.0035
Sailboat	Red	0.0035	0.0035	0.0035	0.0035	0.0035	0.0036	0.0035	0.0034	0.0035
	Green	0.0043	0.0042	0.0042	0.0042	0.0043	0.0045	0.0042	0.0044	0.0045
	Blue	0.0056	0.0055	0.0054	0.0054	0.0057	0.0060	0.0055	0.0057	0.0059

Table 6: FSIM of deciphered RGB components for colored Lena, House and sailboat using Optical DRPE in the presence of AWGN, Salt & peppers, and Speckle noises

Image		Feature Similarity Index (FSIM)								
		AWGN variance			Salt &peppers density			Speckle density		
		0.01	0.05	0.1	0.01	0.05	0.1	0.01	0.05	0.1
Lena	Red	0.4048	0.4051	0.4066	0.4055	0.4057	0.4050	0.4046	0.4037	0.4033
	Green	0.4258	0.4301	0.4312	0.4297	0.4198	0.4090	0.4294	0.4217	0.4144
	Blue	0.4624	0.4692	0.4719	0.4683	0.4526	0.4406	0.4684	0.4570	0.4486
House	Red	0.3127	0.3122	0.3129	0.3129	0.3127	0.3131	0.3127	0.3115	0.3121
	Green	0.3148	0.3189	0.3179	0.3179	0.3161	0.3163	0.3175	0.3178	0.3168
	Blue	0.3370	0.3392	0.3397	0.3397	0.3367	0.3337	0.3369	0.3326	0.3303
Sailboat	Red	0.4294	0.4329	0.4333	0.4333	0.4279	0.4237	0.4299	0.4241	0.4221
	Green	0.3411	0.3427	0.3439	0.3439	0.3410	0.3372	0.3416	0.3316	0.3315
	Blue	0.4006	0.4016	0.4027	0.4027	0.3979	0.3950	0.4001	0.3949	0.3916



Blue

Sailboat: Red, Green, Blue

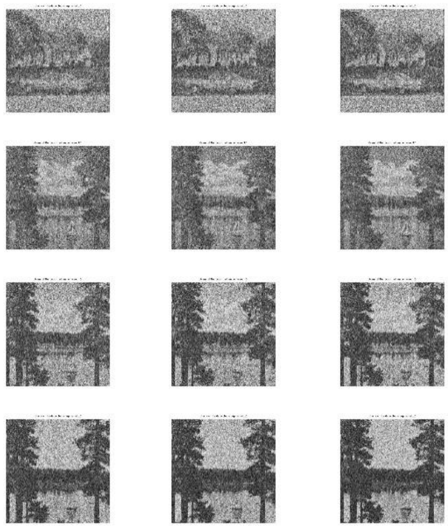


Fig. 6: Deciphered RGB components for color Lena, House and Sailboat images using Optical DRPE in the presence of AWGN noise

Image — Salt & peppers density: 0.01, 0.05, 0.1

Lena: Red, Green, Blue

House: Red, Green, Blue

Sailboat: Red, Green, Blue

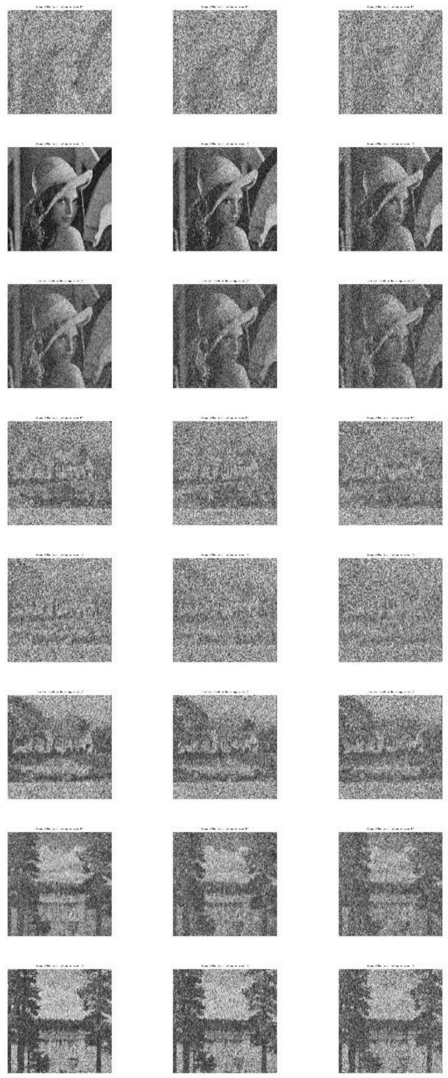


Fig. 7: Deciphered RGB components for color Lena, House and Sailboat images using Optical DRPE in the presence of Salt & peppers noise

Image — Speckle density: 0.01, 0.05, 0.1

Lena: Red, Green, Blue

House: Red, Green, Blue

Sailboat: Red, Green, Blue

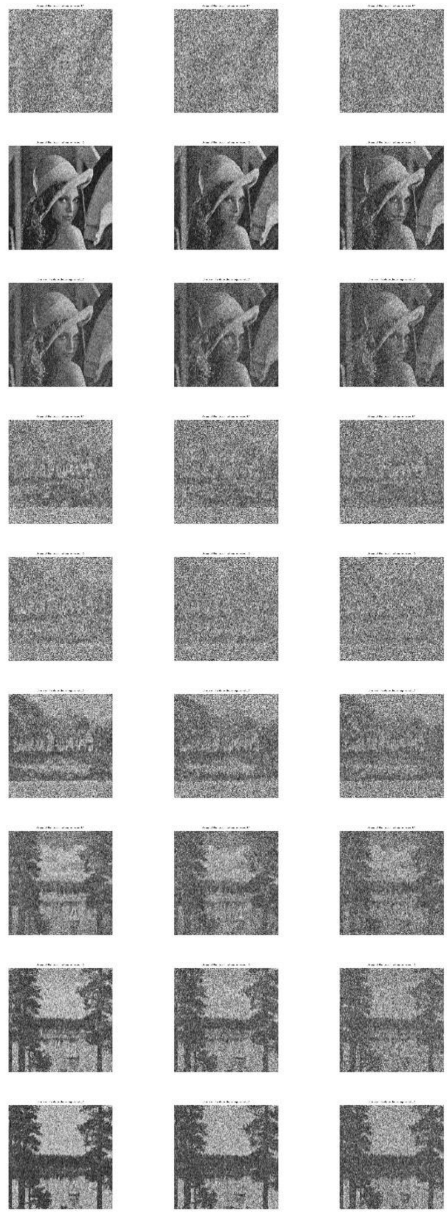


Fig. 8: Deciphered RGB components for color Lena, House and Sailboat images using Optical DRPE in the presence of Speckle noise

5. CONCLUSION

The paper proposed an efficient implementation of optical DRPE for encrypting digital color images. The optical DRPE color image encryption firstly divides colored image into RGB components that are multiplied with first RPM and FT transformed. The transformed RGB components are secondly multiplied by another RPM and secondly inverse FT transformed. The optical DRPE color image decryption divides the encrypted colored image into RGB components that are FT transformed and multiplied with the second RPM conjugate. The transformed RGB components are gain multiplied by the first RPM conjugate and secondly inverse FT transformed. A set of tests are examined for studying the optical DRPE color image encryption. Test demonstrated efficiency of the optical DRPE encryption applied to color images.

6. REFERENCES

[1] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding"applied optics, 41, 5462-5470, 2002.

[2] Z. Liu Z, S. Li, W. Liu, Y. Wang, S. Liu, "Image encryption algorithm by using fractional Fourier transform and pixel scrambling operation based on double random phase encoding," Opt. Lasers Eng., vol. 51, pp. 8-14, 2013.

[3] M. R. Abuturab, "Color image security system based on discrete Hartley transform in gyrator transform domain, " Opt. Lasers Eng., vol. 51, pp. 317-324, 2013.

[4] Liu Z, Dai J, Sun X, Liu S., "Color image encryption by using the rotation of color vector in Hartley transform domains," Opt. Laser Eng., vol. 48, pp. 800–805, 2010.

[5] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding" Opt. Lett., vol. 20, pp. 767-769, 1995.

[6] R. Tao, J. Lang, Y. Wang, "Optical image encryption based on the multipleparameter fractional Fourier transform," Opt. Lett. 33, pp. 581–583, 2008.

[7] Z. Liu, S. Liu, "Double image encryption based on iterative fractional Fourier transform," Opt. Commun. vol. 275, pp. 324–329, 2007.

[8] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, "Security analysis of optical encryption," Proc SPIE, vol. 5986, pp. 25–34, 2005.

[9] Y. Frauel, A. Castro, T. J. Naughton, B. Javidi, "Resistance of the double random phase encryption against various attacks," Opt. Express, vol. 15, pp. 10253-10265, 2007.

[10] X. Peng, P. Zhang, H. Wei, B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," Opt. Lett., vol. 31, pp. 1044-1046, 2006.

[11] Ensherah A. Naeem, Mustafa M. Abd Elnaby, Naglaa F. Soliman, Alaa M. Abbas, Osama S. Faragallah, Noura Semary, Mohiy M. Hadhoud, Saleh A. Alshibeili, and Fathi E. Abd El-Samie, "Efficient Implementation of Chaotic Image Encryption in Transform Domains," Journal of Systems and Software, vol. 97, pp. 118-127, 2014.

[12] Z. Liu, Y. Zhang, W. Liu, F. Meng, Q. Wu, S. Liu, Optical color image hiding scheme based on chaotic mapping and Hartley transform, Optics and Lasers in Engineering, 51, pp. 967-972, 2013.

[13] Ensherah A. Naeem, Mustafa M. AbdElnaby, Hala S. El-sayed, Fathi E. Abd El-Samie, and Osama S. Faragallah, "Wavelet Fusion for Encrypting Images with a Few Details," Computers and Electrical Engineering, vol. 54, pp. 450-470, 2016.

[14] Heba M. Elhoseny, Hossam E. H. Ahmed, Alaa M. Abbas, Hassan B. Kazemian, Osama S. Faragallah, Sayed M. El-Rabaie, Fathi E. Abd El-Samie, "Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation," Signal, Image and Video Processing Journal "Springer-Verlag" ISSN 1863-1703, 2013, DOI 10.1007/s11760-013-0490-x

[15] Elsayed M. Elshamy, Sayed El-Rabaie, Osama S. Faragallah, Osama Elshakankiry, Fathi. E. Abd El-Samie, Hala S. El-sayed, and S. F. El-Zoghdy, "Efficient Audio Cryptosystem based on Chaotic Maps and Double Random Phase Encoding," International Journal of Speech Technology, vol. 18(4), pp. 619-631, 2015, Springer.

[16] Osama S. Faragallah, "An Enhanced Chaotic Key-Based RC5 Block Cipher Adapted to Image Encryption," International Journal of Electronics, vol. 99(7), pp. 925-943, Taylor & Francis, 2012.

[17] Joshi M, Shakher C, Singh K., "Logarithms-based RGB image encryption in the fractional Fourier domain: a non-linear approach," Opt. Lasers Eng., vol. 47, pp. 721-727, 2009.

[18] Liu Z, Xu L, Liu T, Chen H, Li P, Lin C, et al., "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," Opt. Commun. vol. 284, pp. 123-128, 2011.

[19] Chen W, Chen X, Sheppard CJR. "Optical color-image encryption and synthesis using coherent diffractive imaging in the Fresnel domain," Opt. Express, vol. 20, pp. 3853-3865, 2012.

[20] Q. Guo, Z. Liu, S. Liu, Color image encryption by using Arnold and discrete fractional random transforms in IHS space, Optics and Lasers in Engineering, 48, 1174-1181, 2010.

[21] Hu Y J, Lee H K, Chen K Y.D. "Difference expansion based reversible data hiding using two embedding direction, " IEEE Trans on Multimedia, vol. 10(8), pp. 1500-1512, 2008.

[22] T. Narasimmalou, R. Allen Joseph, "Discrete Wavelet Transform Based Steganography for Transmitting Images," Science And Management (lCAESM), pp. 370-375, IEEE, Villupuram, India, March 30-31, 2012.

[23] Z. Liu, Y. Zhang, S. Li, W. Liu, W. Liu, Y. Wang, S. Liu, Double image encryption scheme by using random phase encoding and pixel exchanging in the gyrator transform domains, Optics and Laser Technology, vol. 47, pp. 152-158, 2012.

[24] L. Zhang,D. X. Mou, FSIM: A Feature Similarity Index for Image Quality Assessment, Image Processing, IEEE Transactions on, 20 (8), 2378-2386, 2011.

[25] G. N. Raut, P. L. Paikrao, D. S. Chaudhari, A Study of Quality Assessment Techniques For Fused Images, IJITEE, 2 (4) , 2013.

[26] Osama S. Faragallah, "Optical Double Color Image Encryption Scheme in the Fresnel-based Hartley Domain Using Arnold Transform and Chaotic Logistic Adjusted Sine Phase Masks," Optical and Quantum Electronics, vol. 50(3):118, pp. 1-27, 2018.