Journal of Theoretical and Applied Information Technology
30th September 2019. Vol.97. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

OPTICAL COLOR IMAGE CRYPTOSYSTEM BASED ON DISCRETE COSINE TRANSFORM AND DOUBLE RANDOM PHASE ENCODING

ASHRAF AFIFI[1,2]
[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Kingdom of Saudi Arabia
[2]Department of Electrical Engineering and Computers, Higher Technological Institute, 10th of Ramadan, Egypt
E-mail: ashrafifi@yahoo.com

ABSTRACT

This paper introduces an efficient optical color image cryptosystem using the discrete cosine transform (DCT) and the Double Random Phase Encoding (DRPE). The proposed method employs the DCT on input red, green and blue color plain image components. The resulting color image components are then decomposed by the Fourier Transform (FT). A number of test experiments are performed in order to evaluate the proposed method performance mainly the security and the quality of the encryption. The achieved results demonstrated the superiority of the proposed approach with respect to encryption quality, statistical, information entropy, maximum deviation, and irregular deviation, differential, and noise immunity tests.
Keywords: *Discrete cosine transform, Double Random Phase Encoding, Color Image Cryptosystem.*

1. INTRODUCTION

Nowadays, internet and multimedia networks have increasingly captured attention in information security researches like in optical information processing manners for high computation speed, parameters selection, and parallel processing capability [1-4]. Optical designs are largely used in disguising data, encoding, recognition, correlation, determination, verification, as well as in multimedia watermarking [5-10]. The primary work of Javidi and Refregier in optical image cryptosystem area brought about suggesting DRPE technique as an optical symmetric key encryption technique. For each of the Fourier and spatial domains, the DRPE technique uses 2 phase code keys called random phase masks (RPMs) to code the plain image data. A composite conjugate of the Fourier-plane phase code key are applied to descramble the encrypted image data [11].

Different schemes using multiplexing [12], digital holography [13], FrFt domain [14] Fresnel domain [15], diffractive imaging [16], and polarized light [17] have been proposed. Also, several DRPE based cryptosystems are proposed to obtain efficient security [18-20]. The quantitative techniques for compression encryption of images are also developed [21-23].

The authors of [24], applied DRPE to single-channel color image ciphering by the Fourier Transform, then it was further extended to the FrFt [25], Arnold and discrete cosine transforms [26], Fresnel transform [27].

This paper is mainly focusing on the optical communications applications with high security levels using DCT based DRPE optical color security scheme. This scheme is worked by splitting the color plain image into red, green, and blue component images. Then, the color component plain images will be independently discrete cosine transformed then multiplied by the first random phase masks and finally Fourier transformed. The complex distribution of three transformed color component images are again multiplied discrete cosine transformed, and Fourier transformed. The three ciphered color component images are generated in output plane and gathered to construct the ciphered color image.

The remaining of the paper is organized as follows. Section 2 covers literature review on DRPE and DCT. Section 3 is devoted to detail the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ciphered and deciphered phases of the proposed DCT optical DRPE color image cryptosystem. Section 4 explores the detailed security study of the introduced DCT optical DRPE color image cryptosystem. Ending, section 5 gives the employing remarks.

2. BASIC KNOWLEDGE

This section introduces a literature survey on the DRPE and the discrete cosine transform which were used with the suggested method for color image encryption.

2.1 DRPE

The DRPE includes employing of two 2D random phase masks [11]. Assume that Im(α, β) stands for the digital plain image to be encrypted and F(α, β) denotes the cipher image which is a complex image. θ(α, β) and ω(x, y) stand for the key functions in both frequency and spatial domains and their values range uniformly within [0-1].

The encryption procedure of DRPE can be represented as:

$$F(\alpha,\beta) = FT\{FT[\mathrm{Im}(\alpha,\beta)\exp(j2\pi\theta(\alpha,\beta))]\exp(j2\pi\omega(x,y))\} \quad (1)$$

The decryption steps of DRPE can be represented as:

$$\mathrm{Im}(\alpha,\beta) = \{FT^{-1}[FT^{-1}(F(\alpha,\beta))\exp(-j2\pi\omega(x,y))]\}\exp(-j2\pi\theta(\alpha,\beta)) \quad (2)$$

Here both the keys $\exp(j2\pi\theta(\alpha,\beta))$, $\exp(-j2\pi\omega(x,y))$, and the encrypted image are conveyed jointly. FT and FT^{-1} are the Fourier transform and its inverse respectively.

2.2 Discrete Cosine Transform (DCT)

The 2-D DCT and the IDCT of N × N image are defined as [27]:

$$C(u,v) = \frac{2}{N}\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (3)$$

$$f(x,y) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1}\alpha(u)\alpha(v)C(u,v)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (4)$$

Where f (x, y) is the pixel intensity at the image location (x, y), and C (u, v) is the DCT coefficient at the transform location (u, v) [28].

$$\alpha(u) = \alpha(v) = \begin{cases} 1/\sqrt{2} & u = v = 0 \\ 1 & \text{otherwise} \end{cases} \quad (5)$$

3. THE PROPOSED ALGORITHM

In this section, the suggested DCT optical DRPE color image cryptosystem will be defined in terms of two basic processes namely encryption and decryption.

3.1 Encryption Process

This process can be described in the following steps:

1. The color plain image is separated into red, green, and blue color image components.
2. Each image component is independently shuffled using the discrete cosine transform.
3. The scrambled components are multiplied with the first random phase masks and then submitted to the first FT .
4. The scrambled transformed components are multiplied with the second random phase masks in the FT plane, and then submitted to the second FT .
5. The three encrypted components are achieved in output plane and multiplexed to obtain the color encrypted image as illustrated in figure (1.a).

3.2 Decryption Process

This process can be described in the following steps:

1. The color cipher image is firstly decomposed into image components.
2. The inverse Fourier transform FT^{-1} is applied to the encrypted color image components, and then multiplied by the 2nd random phase mask conjugate in the FT^{-1} plane.
3. The transformed complex components are individually shuffled secondly using the inverse of discrete cosine transform.
4. Another inverse Fourier transform FT^{-1} is applied to DCT transformed scrambled complex color components, and then multiplied with the conjugate of the first random phase mask in the FT^{-1} plane.
5. The transformed red, green, and blue components are individually shuffled by applying the inverse discrete cosine transform.
6. The three deciphered image components are obtained in output plane and multiplexed to get the find decrypted color image $\mathrm{Im}(\alpha_i, \beta_j)$ as illustrated in figure (1.b).
7.

Journal of Theoretical and Applied Information Technology
30th September 2019. Vol.97. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

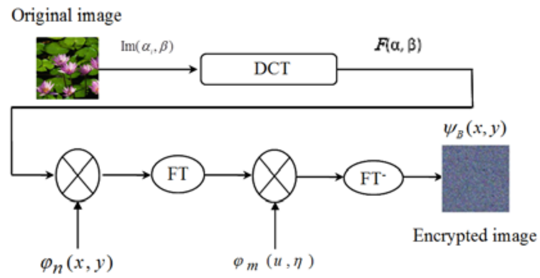


Figure (1a). Block diagram of encryption process for the proposal system

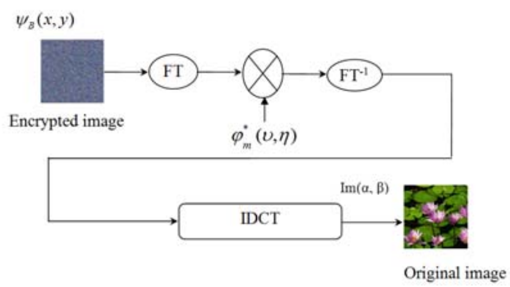


Figure (1b).Block diagram of proposed decryption process

4. EXPERIMENTS SIMULATION

Measuring experiments are carried out to investigate the proposed DCT optical DRPE color image cryptosystem. Also, its performance is compared with the standard double random phase encoding. Tests are performed using 256x256-sized color Water Lillies, Lichtenstein and Bata images as illustrated in Figure (2).

a) Water Lillies b) Lichtenstein c) Bata

Fig. 2: Color Test Images - Water Lillies, Lichtenstein and Bata Images

4.1 Visual Measuring

The ciphering outcomes of color plain images employing the proposed DCT optical DRPE color image cryptosystem and conventional DRPE are illustrated in Figures. 3-5 for color images Water Lillies, Lichtenstein and Bata, respectively. It is abvious that ciphering with the proposed DCT optical DRPE color image cryptosystem achieved in concealment of all images in color details.

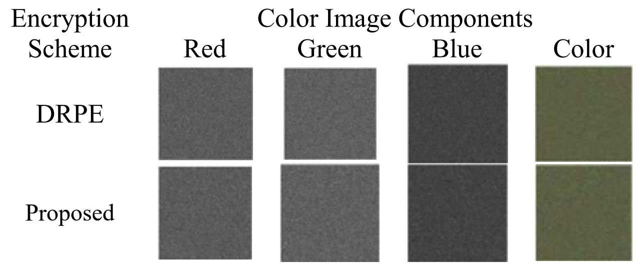


Fig. 3: Ciphered results of color Water lilies component images employing DRPE and the proposed DCT optical DRPE color image cryptosystem

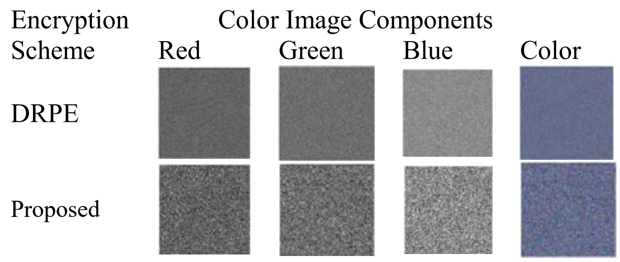


Fig. 4: Encryption results of color Lichtenstein component images using DRPE and the proposed DCT based-DRPE optical color image cryptosystem

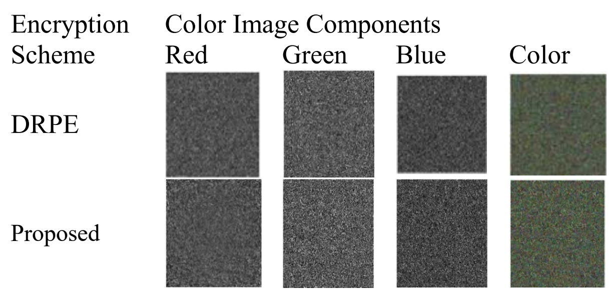


Fig. 5: Ciphered results of color Bata component images employing DRPE and the proposed DCT optical DRPE color image cryptosystem

4.2 Measure of Entropy

The Entropy measure is conducted for investigating the ciphered image components. It calculates the information included in the ciphered image components. The entropy is defined as [30-32]:

$$Entropy(E) = -\sum_{i=1}^{n} P(E_i)\log P(E_i) \quad (6)$$

where E_i of the i^{th} point is its intensity value, and P is its probability. It is clear that the image is good if it has a high $Entropy$ value. The values of entropy for the ciphered components of images using the the proposed DCT optical DRPE color image cryptosystem and DRPE are shown in Table

Journal of Theoretical and Applied Information Technology
30th September 2019. Vol.97. No 18

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

1. The results of entropy verified the effectivity of the proposed DCT optical DRPE color image cryptosystem in term of its outcomes entropy results for image channels correspond with its comparing entropy outcomes achieved by DRPE. Finally, the entropy outcomes of ciphered image channels of color images resulted by the proposed DCT optical DRPE color image cryptosystem is greaer than their comparing values in color plain images.

4.3 Measure of Histogram

Measure of histogram of encrypted image components is performed to measure and ensure the proposed DCT optical DRPE color image cryptosystem. For good ciphering, the encryption imagecomponents histograms must be completely distinguished from the image components histograms of plain images. Figures. 6-8 show the histograms of encrypted Water Lillies, Lichtenstein and Bata image components and the histogram of their deciphered versions. The histograms of encrypted Water Lillies, Lichtenstein and Bata image components employed DRPE and the proposed DCT optical DRPE color image cryptosystem are completely different from the histograms of red, green and blue Water Lillies, Lichtenstein and Bata component plain images.

Table 1: Entropy outcomes of ciphered Water Lillies, Lichtenstein and Bata image components employing DRPE and the proposed DCT optical DRPE color image cryptosystem

Image	Plain image			Encrypted image in Optical Encryption Techniques					
				DRPE			Proposed		
	R	G	B	R	G	B	R	G	B
Water lilies	7.3916	7.3642	5.7566	7.538	7.5990	7.7134	7.5404	7.5986	7.6117
Lichtenstein	7.3520	7.4734	7.4925	7.464	7.7250	7.7641	7.4585	7.7139	7.8240
Bata	7.3222	7.4494	6.5965	7.366	7.4851	7.5630	7.3666	7.4924	7.5803

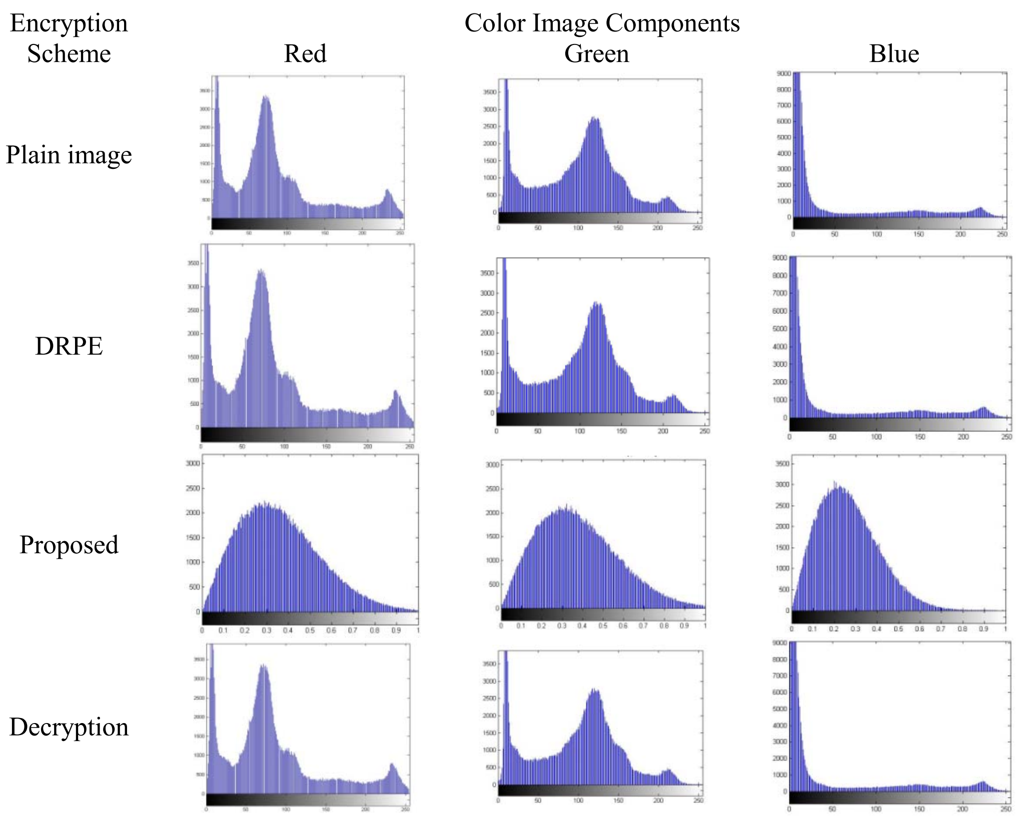


Fig. 6: Histogram results of ciphered and decrypted color Water Lillies component images using DRPE and the proposed DCT optical DRPE color image cryptosystem

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

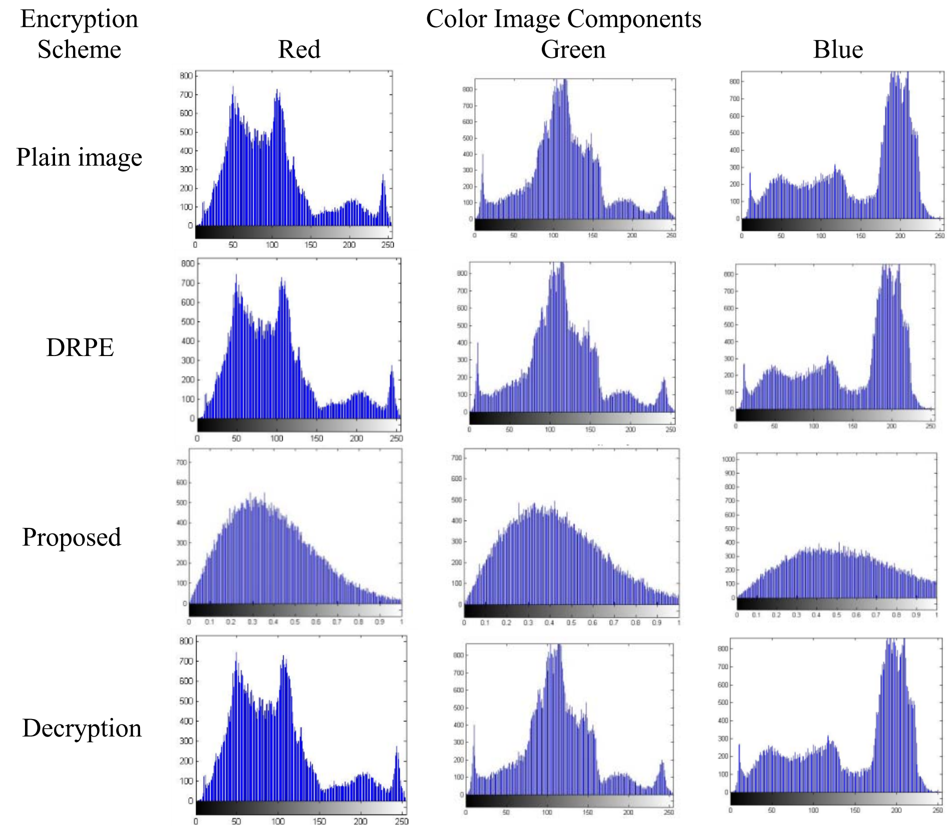
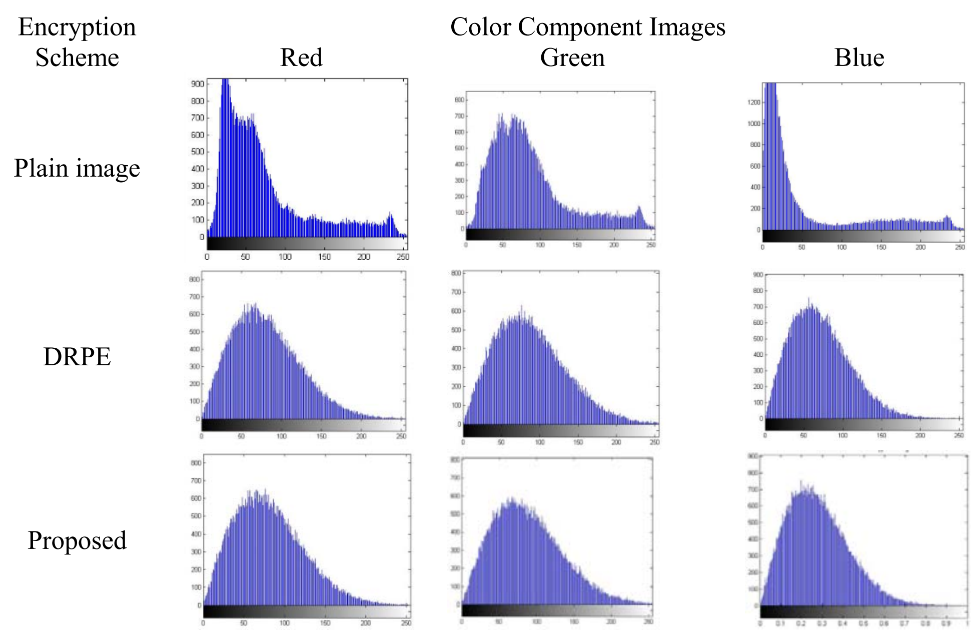


Fig. 7: Histogram outcomes of encrypted color Lichtenstein component images using DRPE and the proposed DCT optical DRPE color image cryptosystem



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Decryption

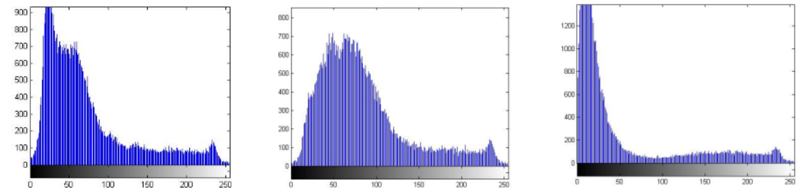


Fig. 8: Histogram results of ciphered color Bata component images using DRPE and the proposed DCT based-DRPE optical color image cryptosystem

4.4 Measures of Encryption Quality

The ciphered quality measures like correlation coefficient r_{xy}, irregular deviation D_I and histogram deviation D_H, are conducted for comparing the ciphered quality of different ciphered schemes. The correlation coefficient $r(\mathrm{Im}, E)$ is estimated between the original and ciphered image components that arranged like 1-D sequences as [29-31]:

$$r(\mathrm{Im},E) = \frac{\mathrm{cov}(\mathrm{Im},E)}{\sqrt{D(I)}\sqrt{D(E)}}, \tag{7}$$

$$\mathrm{cov}(\mathrm{Im},E) = \frac{1}{L}\sum_{i=l}^{L}(\mathrm{Im}(l) - Mean(\mathrm{Im}))\ \ (E(lm) - Mean(E)), \tag{8}$$

$$D(\mathrm{Im}) = \frac{1}{L}\sum_{i=l}^{L}(\mathrm{Im}(l) - Mean(\mathrm{Im}))^2, \tag{9}$$

$$D(E) = \frac{1}{L}\sum_{i=l}^{L}(E(lm) - Mean(E))^2, \tag{10}$$

where L is the number of pixels within the image. The objective is to get tiny correlation values between the original $\mathrm{Im}(x_i, y_j)$ and encrypted $E(x_i, y_j)$ image components. Table 2 shows the correlation coefficient calculations among the original and encrypted image components using DRPE and the proposed DCT optical DRPE color image cryptosystem. The outcomes domenstrated that the porposed DCT optical DRPE color image cryptosystem verify correlation coefficient values that are close to tiny value than DRPE in all Water Lillies, Lichtenstein and Bata image components. This verifies the superiority of the proposed DCT optical DRPE color image cryptosystem with respect to correlation coefficient test. The histogram deviation estimates the ciphering quality with respect to how it increases the difffence between the plain and the encrypted image components. The histogram deviation H_d can be estimated as [29-31]:

$$H_d(\mathrm{Im},E) = \frac{\left|\sum_{i=0}^{255} d(i)\right|}{MxN}, \tag{11}$$

where $d(i)$ points the absolute difference between the histograms of original and the encrypted image components at pixel level i. The M and N denote dimensions of image. The main objective is to verify higher H_d value to ensure that the ciphered image components are deviated from their corresponding image components. Table 3 shows the H_d test calculations for the original and encrypted image components using DRPE and the proposed DCT optical DRPE 1 color image cryptosystem. The outcomes of the proposed DCT optical DRPE color image cryptosystem give larger H_d values compared with DRPE.

The irregular deviation estimates the encryption quality in terms of how much the deviation resulted by encryption is irregular [30-32]. The irregular deviation can be computed as [30-32]:

$$\mathrm{Im}_d(I, E) = \frac{\left|\sum_{i=0}^{255} h_d(i)\right|}{MxN}, \tag{12}$$

$$h_d(i) = \left|h(i) - M_h\right|, \tag{13}$$

where $h(i)$ is the ciphered image histogram with intensity level i, and M_h is the average value for an ideal uniform ciphered image histogram. The main aim is to achieve lower Im_d values that indicate a better encryption quality. Table 3 illustrates Im_d values for DRPE and the proposed DCT based-DRPE optical color image cryptosystem. The porposed DCT optical DRPE color image cryptosystem have low Im_d values against DRPE which ensures their achieved ciphered quality.

Table 2: Deviation metrics and Correlation coefficient values for the encrypted Water Lillies, Lichtenstein and Bata images using DRPE and the proposed DCT optical DRPE color image cryptosystem

Image	Metrics	Ciphered image in Optical Encryption Techniques					
		DRPE			Proposed		
		R	G	B	R	G	B
Water lilies	r_{xy}	-9.9*10-4	-0.0019	-0.0012	0.0036	0.0011	-8.3*10-4
	D_H	0.6108	0.5699	1.4303	0.6083	0.5714	1.4313
	D_I	0.7829	0.8648	0.8198	0.7850	0.8552	0.8222
Lichtenstein	r_{xy}	-0.0027	-0.0037	0.0013	2.7*10-4	0.0029	0.0010
	D_H	0.3119	0.5035	0.7012	0.0808	0.1206	0.1748
	D_I	0.8413	0.8564	0.6231	0.2129	0.2174	0.1575
Bata	r_{xy}	2.6*10-4	-0.0025	0.0069	-8.6*10-4	0.0026	-0.0030
	D_H	0.1397	0.0799	0.3091	0.1412	0.0785	0.3099
	D_I	0.2231	0.2270	0.2055	0.2232	0.2276	0.2053

Table 3: NPCR and UACI using DRPE and the proposed DCT optical DRPE color image cryptosystem.

Image		Ciphered image in Optical Encryption Techniques					
		DRPE			Proposed		
		R	G	B	R	G	B
Water lilies	NPCR	99.5113	99.5171	99.7547	99.4930	99.5316	99.7604
	UACI	0	0	0	0	0	0
Lichtenstein	NPCR	99.4438	99.4762	99.6353	99.4598	99.4888	99.6231
	UACI	0	0	0	0	0	0
Bata	NPCR	99.3561	99.3912	99.6155	99.3698	99.3652	99.5911
	UACI	0	0	0	0	0	0

4.5 Differential Measure

The differential measure is emploed to measure the effect of one-pixel modification on the whole encrypted image with baker mapping, DRPE and the proposed DCT optical DRPE color image cryptosystem. Two common tests are employed; number-of pixels changing rate (NPCR) and unified average changing Intensity (UACI). Assume two ciphered images E_1 and E_2 whose corresponding plain images have only one-pixel difference. The values of pixels at index (x_i, y_j) in E_1 and E_2 are $E_1(x_i, y_j)$ and $E_2(x_i, y_j)$, respectively. If a pipolar array $D(x_i, y_j)$ with the same ciphered images size . The $D(x_i, y_j)$ is computed with $E_1(x_i, y_j)$ and $E_2(x_i, y_j)$. If $E_1(x_i, y_j) = E_2(x_i, y_j)$, then $D(x_i, y_j) = 1$; otherwise, $D(x_i, y_j) = 0$. The NPCR can be estimated as [29-31]:

$$NPCR(E_1, E_2) = \frac{\sum i, j\, D(x_i, y_j)}{M \times N} \times 100\%, \quad (14)$$

where the width M and hight N of E_1 and E_2. The NPCR is the percentage of different pixels number to the total pixels number among the two ciphered images. The UACI can be computed as [30-32]:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

$$UACI(E_1,E_2)=\frac{1}{M\times N}\left[\sum_{x_i y_j}\frac{E_1(x_i,y_j)-E_1(x_i,y_j)}{255}\right]\times 100\%, \quad (15)$$

The UACI calculates the average intensity of difference among the two encrypted color images. The results of number-of pixels changing rate and unified average changing Intensity measures are shown in table 3. The results encures that the proposed DCT optical DRPE color image cryptosystem is very sensitive to small modifications in image components, but the DRPE encryption is sensitive to small modifications in image components.

4.6 Measure of Noise Immunity

The robustness of DRPE and the proposed DCT optical DRPE color image cryptosystem in existence of Additive White Gaussian Noise (AWGN), Salt&peppers and Speckle existence are examined in the decryption process.

4.6.1 The peak signal to noise ratio (PSNR)

The Peak Signal to Noise Ratio (PSNR) is conducted to estimate the deciphered image components.
The Peak Signal to Noise Ratio can be defined as [32-33]:

$$PSNR(\mathrm{Im},D)=10\log\frac{(255)^2}{\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}[\mathrm{Im}(x_i,y_j)-D(x_i,y_j)]^2} \quad (16)$$

where $\mathrm{Im}(x_i,y_j)$ is the pixel value of color plain image location (x_i,y_j), and $D(x_i,y_j)$ is the decrypted of pixel value color image at location (x_i,y_j). High PSNR values indicate good immunity against noise. The noise immunity results are given in Tables 4,5,6,7,8 and 9. The results demonstrate that the proposed DCT optical DRPE color image cryptosystem has better immunity against noise than DRPE which verifies it a best choice for ideal optical telecommunication applications which can cancelling the noise effects.

4.6.2 The Structural Similarity (SSIM)

The SSIM is computed to estimate the decrypted red, green and blue components.

The SSIM can be computed as [33]:

$$SSIM(x,y|w)=\frac{(2\bar{w}_x\bar{w}_y+C_1)(2\sigma_{w_xw_y}+C_2)}{(\bar{w}_x^2+\bar{w}_y^2+C_1)(\sigma_{w_x}^2+\sigma_{w_y}^2+C_2)} \quad (17)$$

where, C_1, C_2 are minor constants, $\bar{w}_x$ and $\bar{w}_y$ are the average of w_x and w_y regions, respectively. $\Sigma_{w_x}^2$ is the variance of w_x region and $\sigma_{w_xw_y}$ is covariance among two regions w_x and w_y. The SSIM test results are given in Tables 10,11 and 12. The results demonstrate that the proposed DCT based-DRPE optical color image cryptosystem has good resistance against noise.

4.6.3 The Feature Similarity Index (FSIM)

The FSIM estimates the decrypted red, green and blue components.

The SSIM can be computed as [33]:

$$FSIM=\frac{\sum_{x\in\Omega}S_L(x).PC_m(x)}{\sum_{x\in\Omega}PC_m(x)} \quad (18)$$

where Ω is spatial domain of mage, $S_L(x)$ is overall similarity between two images and $PC_m(x)$ is the value of phase congruency. large FSIM values means the noise immunity is good.

The FSIM measure results are given in Tables 13,14 and 15. The results show that the proposed DCT optical DRPE color image cryptosystem is immune against noise than DRPE.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 4: Peak Signal to Noise Ratio (PSNR) values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of AWGN noise with different variances (var) on the encrypted images.

Image		PSNR				
		AWGN				
		var = 0.01	var = 0.05	var = 0.1	var= 0.15	var =0.2
Water lilies	R	14.6064	11.8063	10.1885	9.1293	8.4097
	G	14.2552	11.7532	10.3585	9.4343	8.7664
	B	14.0415	10.8038	9.0007	7.8425	7.0153
Lichtenstein	R	14.4901	12.0559	10.6245	9.7062	9.0010
	G	13.3891	11.6358	10.5730	9.8548	9.3025
	B	9.8104	9.1715	8.7834	8.4596	8.2084
Bata	R	15.6171	12.3209	10.5778	9.3952	8.5785
	G	15.4682	12.5313	10.8348	9.7710	9.0262
	B	14.6890	11.2465	9.4431	8.2239	7.4330

Table 5: Peak Signal to Noise Ratio (PSNR) values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of Salt&peppers noise with different variances (var) on the encrypted images

Image		PSNR				
		Salt&peppers				
		var = 0.01	var = 0.05	var = 0.1	var= 0.15	var =0.2
Water lilies	R	22.3027	17.0963	14.5444	12.9861	11.8078
	G	21.1566	16.7094	14.3526	12.9235	11.8410
	B	23.8650	16.7729	13.5545	11.7115	10.4636
Lichtenstein	R	20.1842	16.7091	14.5869	13.2449	12.2969
	G	17.2028	15.2261	13.7265	12.7022	11.9365
	B	10.8939	10.4978	10.0706	9.7401	9.4364
Bata	R	24.8585	18.3254	15.1928	13.4860	12.2926
	G	23.3574	17.8493	15.3634	13.7585	12.5552
	B	25.2418	17.3425	14.2191	12.2869	10.9702

Table 6: Peak Signal to Noise Ratio (PSNR)values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of Speckle noise with different variances (var) on the encrypted images

Image		PSNR				
		Speckle				
		var =0.01	var = 0.05	var = 0.1	var= 0.15	var =0.2
Water lilies	R	22.8564	18.8908	16.6980	15.4729	14.4877
	G	21.1890	17.7256	15.8119	14.6641	13.8811
	B	31.9634	24.7476	21.5646	19.35424	17.9088
Lichtenstein	R	19.7610	17.0235	15.5422	14.5421	13.7974
	G	16.5384	14.8396	13.7313	13.1105	12.6271
	B	10.5300	9.9767	9.6577	9.4716	9.3337
Bata	R	28.0192	22.5749	20.0008	18.0856	17.0251
	G	24.6064	20.4146	18.2009	16.7122	15.7371
	B	32.6287	24.8078	21.4833	19.5123	18.0014

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 7: Peak Signal to Noise Ratio (PSNR) values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the exitance of AWGN noise with different variances (var) on the encrypted images

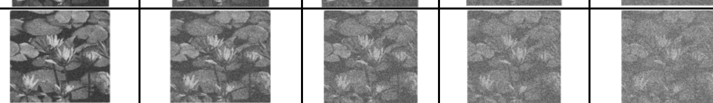
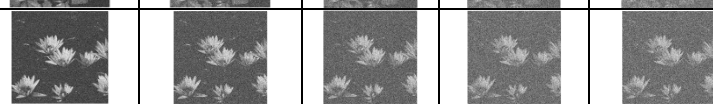
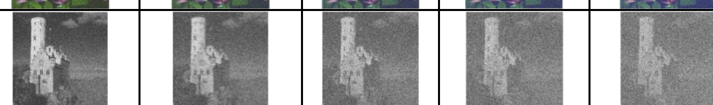
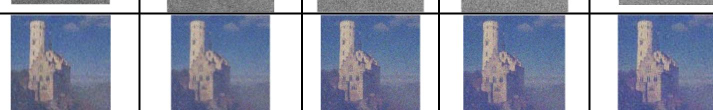
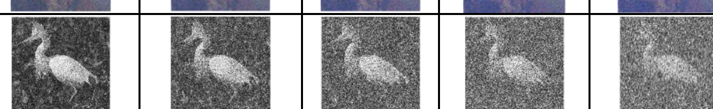
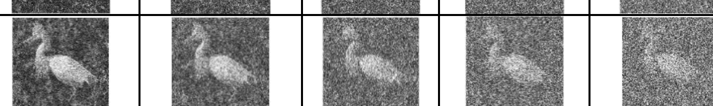
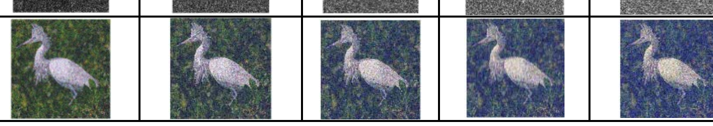
Image		Peak Signal to Noise Ratio (PSNR)				
		AWGN				
		var = 0.01	var = 0.05	var = 0.1	var= 0.15	var =0.2
Water lilies	R					
	G					
	B					
	RGB					
Lichtenstein	R					
	G					
	B					
	RGB					
Bata	R					
	G					
	B					
	RGB					

Table 8: Peak Signal to Noise Ratio (PSNR)values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of Salt&peppers noise with different variances (var) on the encrypted image components

Image	Peak Signal to Noise Ratio (PSNR)
	Salt&peppers

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

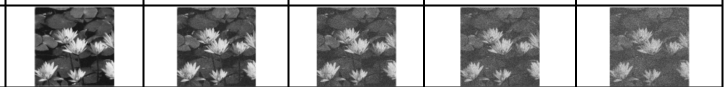
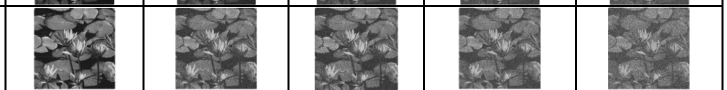
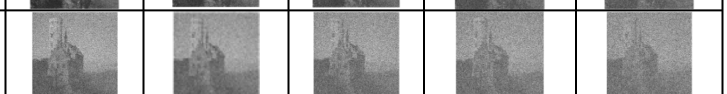
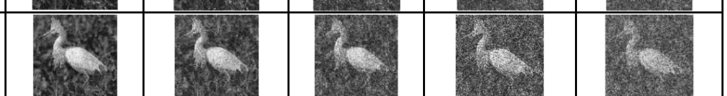
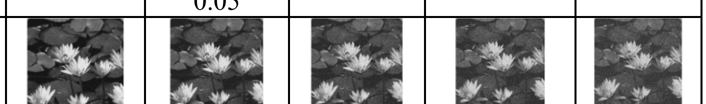
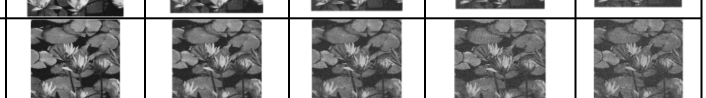
		var = 0.01	var = 0.05	var = 0.1	var= 0.15	var =0.2
Water lilies	R					
	G					
	B					
	RGB					
Lichtenstein	R					
	G					
	B					
	RGB					
Bata	R					
	G					
	B					
	RGB					

Table 9: Peak Signal to Noise Ratio (PSNR)values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of Speckle noise with different variances (var) on the encrypted image components

Image		PSNR				
		Speckle				
		var = 0.01	var = 0.05	var = 0.1	var= 0.15	var =0.2
Water lilies	R					
	G					
	B					

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

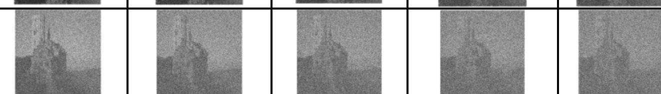
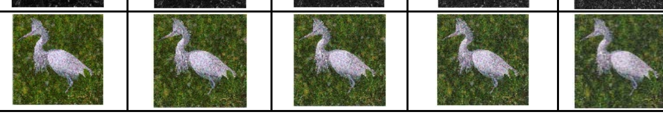
	RGB	
Lichtenstein	R	
	G	
	B	
	RGB	
	R	
	G	
	B	
	RGB	

Table 10: SSIM values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of AWGN noise with zero mean and different variances (var)on the ciphered red, green and blue component images

Image		Structural Similarity index (SSIM)				
		AWGN				
		var = 0.05	var = 0.1	var= 0.15	var = 0.20	var =0.25
Water lilies	R	0.3979	0.2762	0.2080	0.1661	0.1333
	G	0.4183	0.2912	0.2157	0.1721	0.1326
	B	0.2815	0.2025	0.1553	0.1271	0.1045
Lichtenstein	R	0.3110	0.2149	0.1645	0.1330	0.1070
	G	0.2456	0.1739	0.1373	0.1140	0.0962
	B	0.1025	0.0846	0.0645	0.0561	0.0523
Bata	R	0.2671	0.1544	0.1036	0.0744	0.0567
	G	0.2545	0.1464	0.0996	0.0729	0.0560
	B	0.1939	0.1113	0.0780	0.0563	0.0448

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 11: SSIM values of the decrypted red, green and blue Water Lillies, Lichtenstein and Bata images using the proposed DCT based-DRPE optical color image cryptosystem in the excitance of Salt&peppers noise different variances (var) on the encrypted image components

Image		Structural Similarity index (SSIM)				
		Salt&peppers				
		var=0.01	var=0.05	var=0.1	var=0.15	var=0.20
Water lilies	R	0.7221	0.5028	0.3815	0.3113	0.2526
	G	0.7191	0.5312	0.4133	0.3323	0.2658
	B	0.5822	0.3486	0.2604	0.2090	0.1735
Lichtenstein	R	0.5598	0.4061	0.3084	0.2520	0.2099
	G	0.4086	0.3196	0.2558	0.2115	0.1757
	B	0.1457	0.1296	0.1129	0.1029	0.0884
Bata	R	0.6632	0.3652	0.2332	0.1688	0.1298
	G	0.5987	0.3443	0.2356	0.1725	0.1308
	B	0.5849	0.2679	0.1734	0.1245	0.0900

Table 12: SSIM values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of Speckle noise with different variances (var) on the encrypted image components .

Image		Structural Similarity index (SSIM)				
		Speckle				
		var=0.01	var=0.05	var=0.1	var=0.15	var=0.20
Water lilies	R	0.7420	0.5814	0.4798	0.4231	0.3742
	G	0.7206	0.5794	0.4823	0.4182	0.3739
	B	0.8433	0.6137	0.5020	0.4286	0.3820
Lichtenstein	R	0.5409	0.4209	0.3498	0.3031	0.2674
	G	0.3772	0.3009	0.2491	0.2213	0.1964
	B	0.1302	0.1075	0.0937	0.0851	0.0793
Bata	R	0.7822	0.5630	0.4449	0.3540	0.3065
	G	0.6534	0.4629	0.3577	0.2856	0.2442
	B	0.8535	0.5661	0.4250	0.3466	0.2890

Table 13: FSIM values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of AWGN noise with zero mean and different variances (var)on the encrypted image components.

Image		Feature Similarity index (FSIM)				
		AWGN				
		var = 0.05	var = 0.1	var = 0.15	var = 0.20	var =0.25
Water lilies	R	0.7295	0.6499	0.6010	0.5675	0.5440
	G	0.7242	0.6433	0.5903	0.5619	0.5429
	B	0.7830	0.6913	0.6246	0.5854	0.5516
Lichtenstein	R	0.6711	0.5982	0.5557	0.5275	0.5082
	G	0.6165	0.5583	0.5262	0.5063	0.4885
	B	0.4721	0.4546	0.4401	0.4326	0.4277
Bata	R	0.6377	0.5499	0.5081	0.4802	0.4629
	G	0.6069	0.5291	0.4891	0.4633	0.4485
	B	0.6398	0.5441	0.4954	0.4612	0.4400

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 14: FSIM values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE color image cryptosystem in the excitance of Salt&peppers noise with different variances (var) on the encrypted image components .

Image		Feature Similarity index (FSIM)				
		Salt&peppers				
		var=0.01	var=0.05	var=0.1	var=0.15	var=0.20
Water lilies	R	0.9008	0.7930	0.7187	0.6721	0.6336
	G	0.8901	0.7919	0.7232	0.6687	0.6264
	B	0.9407	0.8395	0.7558	0.7011	0.6547
Lichtenstein	R	0.8290	0.7375	0.6270	0.6293	0.6001
	G	0.7393	0.6769	0.6243	0.5881	0.5604
	B	0.5115	0.4996	0.4816	0.4730	0.4618
Bata	R	0.8574	0.7077	0.6271	0.5764	0.5461
	G	0.8200	0.6698	0.6001	0.5562	0.5254
	B	0.8709	0.7052	0.6214	0.5676	0.5278

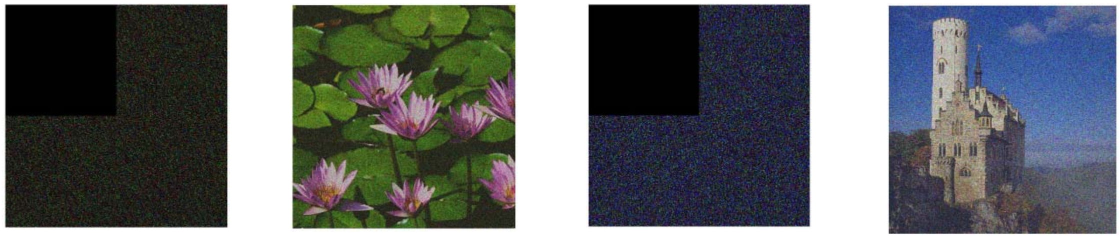
Table 15: FSIM values of the deciphered Water Lillies, Lichtenstein and Bata images using the proposed DCT optical DRPE optical color image cryptosystem in the excitanse of Speckle noise with different variances (var) on the encrypted image components.

Image		Feature Similarity index (FSIM)				
		Speckle				
		var=0.01	var=0.05	var=0.1	var=0.15	var=0.20
Water lilies	R	0.9098	0.8341	0.7768	0.7436	0.7142
	G	0.8881	0.8192	0.7655	0.7238	0.6973
	B	0.9808	0.9481	0.9172	0.8860	0.8613
Lichtenstein	R	0.8164	0.7443	0.7022	0.6665	0.6925
	G	0.7156	0.6627	0.6209	0.5992	0.5815
	B	0.4996	0.4814	0.4710	0.4676	0.4609
Bata	R	0.9073	0.8104	0.7511	0.6977	0.6693
	G	0.8455	0.7446	0.6830	0.6374	0.6097
	B	0.9574	0.8651	0.8012	0.7561	0.7190

4.7 Occlusion measure

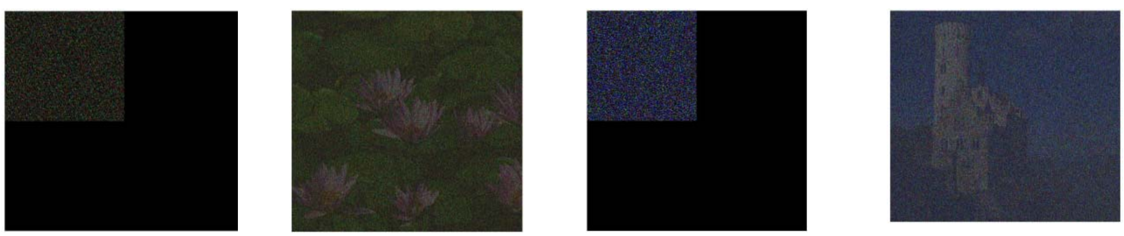
The cipher image may be attached during transmission and strong So, its resistance to occlusion test must be considered. The decryption phase is performed on the occluded ciphered Water Lillies and Lichtenstein. The occluded encrypted Water Lillies and Lichtenstein images with (25,50 and 75) % occlusion are shown in Fig. 9(a), (c), (e), (g), (i) and (k). The deciphered images are shown in Fig 9(b), (d), (f) , (h), (j) and (l). The outcomes show the basic plain images can be reconstructed.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



a) Encrypted image Water Lilies with occlusion 25% *b) Decrypted image Water Lilies with occlusion 25%* *c) Encrypted image Lichtenstein with occlusion 25%* *d) Decrypted image Lichtenstein with occlusion 25%*

e) Encrypted image Water Lilies with occlusion 50% *f) Decrypted image Water Lilies with occlusion 50%* *g) Encrypted Lichtenstein image with occlusion 50%* *h) Decrypted Lichtenstein image with occlusion 50%*



i) Encrypted image Water Lilies with occlusion 75% *j) Decrypted image Water Lilies with occlusion 75%* *k) Encrypted image Lichtenstein with occlusion 75%* *l) Decrypted image Lichtenstein with occlusion 75%*

Fig. 9: Immunity of the proposed encryption syatem to occlusion measure for the encrypted images Water Lilies and Lichtenstein with occlusion (25, 50, and 75%).

5. CONCLUSION

An efficient DCT- optical color image encryption using DCT and DRPE, is the main finding of this paper. In the proposed technique, the image components are discrete cosine transformed and modulated the first random diffuser, then Fourier transformed. The complex color image components are then by discrete cosine transformed modulated by a second random diffuser and Fourier transformed again. A set of experiments have been performed in order to study the performance of the proposed DCT optical-DRPE color image cryptosystem. The outcomes verifie the effectivity of the proposed DCT optical DRPE color image cryptosystem.

REFRENCES:

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

[2] H.M. Ozaktas, A. Koc, I. Sari, M.A. Kutay, "Efficient computation of quadraticphase integrals in optics," Opt. Lett. 31, pp. 35–37, 2006.

[3] Z. Liu, S. Liu, "Randomization of the Fourier transform," Opt. Lett. 32, pp. 478–480, 2007.

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

[5] Abuturab MR., "Color information verification system based on singular value decomposition

in gyrator transform domains," Opt. Lasers Eng., vol. 57, pp. 9-13, 2014.

[6] Abuturab MR., "An asymmetric color image cryptosystem based on Schur decomposition in gyrator transform domains," Opt. Lasers Eng., vol. 58, pp. 39-47, 2014.

[7] Abuturab MR., "Single-channel color information security system using LU decomposition in gyrator transform domains," Opt. Commun., vol. 323, pp. 100-109, 2013.

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

[9] 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.

[10] Liu Z, Dai J, Sun X, Liu S., "Optical color image hiding scheme based on chaotic mapping and Hartley transform," Opt. Laser Eng., vol. 51, pp. 967-72, 2013.

[11] 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.

[12] Matoba O, Javidi B., "Encrypted optical storage with angular multiplexing," Appl. Opt., vol. 38, pp. 7288–7293, 1999.

[13] Javidi B, Takanori N., "Securing information by use of digital holography," Opt. Lett. vol. 25, pp. 28-30, 2000.

[14] Liu Z, Liu S., "Random fractional Fourier transform," Opt. Lett. vol. 32, pp. 2088-2090, 2007.

[15] Hwang H-E, Chang HT, Lie W-N., "Multiple-image encryption and multiplexing using a modified Gerchberg–Saxton algorithm and phase modulation in Fresnel-transform domain," Opt. Lett., vol. 34, pp. 3917–3919, 2009.

[16] Chen W, Chen X, Sheppard CJR. "Optical image encryption based on diffractive imaging," Opt. Lett., vol. 35, pp. 3817-3819, 2010.

[17] Alfalou A, Brosseau C., "Dual encryption scheme of images using polarized light," Opt. Lett., vol. 35, pp. 2185–2187, 2010.

[18] Chen L, Zhao D., "Optical image encryption with Hartley transforms, " Opt. Lett. vol. 20, pp. 767-769, 2006.

[19] Hwang HE. "An optical image cryptosystem based on Hartley transform in the Fresnel transform domain, " Opt. Commun., vol. 284, pp. 3243–3247, 2011.

[20] Chen J, Zhu Z, Liu Z, Fu C, Zhang L, Yu H., "A novel double-image encryption scheme based on cross-image pixel scrambling in gyrator domains," Opt. Express, vol. 22, pp. 7349–7361, 2014.

[21] Alfalou A, Elbouz M, Mansour A, Keryer G., "New spectral image compression method based on an optimal phase coding and the RMS duration principle," J. Opt., vol. 12, 115403, 2010.

[22] Alfalou A, Brosseau C, Abdallah N, Jridi M., "Simultaneous fusion, compression, and encryption of multiple images," Opt. Express, vol. 19, 24023, pp. 2402-2409, 2013.

[23] Alfalou A, Brosseau C, Abdallah N, Jridi M., "Assessing the performance of a method of simultaneous compression and encryption of multiple images and its resistance against various attacks," Opt. Express, vol. 21, 8025-8043, 2013.

[24] Zhang SQ, Karim MA., "Color image encryption using double random phase encoding," Microw. Opt. Technol. Lett. vol. 21, pp. 318-323, 1999.

[25] 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.

[26] 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.

[27] 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.

[28] G. Strang, "The Discrete Cosine Transform", SIAM Review, Volume 41, Number 1, pp.135-147, 1999.

[29] Andrew B. Watson, "Image Compression Using the Discrete Cosine Transform", Technical Report, NASA Ames Research Center, Mathematica Journal, 4(1), 1994, p. 81-88, 1994.

[30] J. Fridrich, "Symmetric Ciphers Based on Two-dimensional Chaotic Maps," International Journal of Bifurcat Chaos, vol. 8(6), pp. 1259-1284, 1998.

[31] Osama S. Faragallah, "Digital Image Encryption Based on the RC5 Block Cipher Algorithm," Sensing and Imaging: An International Journal, vol. 12(3), pp. 73-94, Springer, 2011.

[32] 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, 2012, Taylor & Francis.

[33] Ensherah A. Naeem, Mustafa M. Abd Elnaby, Hala S. El-sayed, Fathi E. Abd El-Samie, and Osama S. Faragallah, “Wavelet Fusion for Encrypting Images with Few Details”, Computers and Electrical Engineering, vol. 60, pp. 450-470, 2016.