

Received October 7, 2018, accepted October 21, 2018, date of publication November 9, 2018, date of current version January 11, 2019.

Digital Object Identifier 10.1109/ACCESS.2018.2879857

Block-Based Optical Color Image Encryption Based on Double Random Phase Encoding

OSAMA S. FARAGALLAH^{1,2}, MOHAMMED A. ALZAIN², HALA S. EL-SAYED³,
JEHAD F. AL-AMRI², WALID EL-SHAFAI⁴, ASHRAF AFIFI^{2,5}, ENSHERAH A. NAEEM^{6,7},
AND BEN SOH⁸, (Senior Member, IEEE)

¹Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

²Department of Information Technology, College of Computers and Information Technology, Taif University, Al-Hawiya 21974, Saudi Arabia

³Department of Electrical Engineering, Faculty of Engineering, Menoufia University, Shebin El-Kom 32511, Egypt

⁴Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

⁵Department of Electrical Engineering and Computers, Higher Technological Institute, 10th of Ramadan 228, Egypt

⁶Department of Electronics and Electrical Communications, Higher Institute of Engineering and Technology, Kafr El Sheikh 228, Egypt

⁷Department of Electronics and Electrical Communications, Kafrelsheikh University, Kafr El Sheikh 33511, Egypt

⁸Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, VIC 3086, Australia

Corresponding author: Osama S. Faragallah (osam_sal@yahoo.com)

ABSTRACT This paper investigates and presents a block-based opto-color cipher using double random phase encoding (DRPE) with different block sizes. The color plainimage is divided into equal-sized blocks and then converted to an optical signal by an optical emitter. The obtained optical signal is encrypted by employing the DRPE technique, which applies two types of phase modulation, time, and Fourier domains. Finally, the optical color cipherimage is, upon detection, converted to digital format by a charge-coupled device digital camera. Experiments and security analysis show that the proposed block-based optical color image cipher using DRPE with increased block size is secure, effective, and including a good immunity to channel noise.

INDEX TERMS DRPE, Fourier domain, optical color image, time domain, and image encryption.

I. INTRODUCTION

One of the major problems of digital color image transmission over network is the security issue. Therefore, many image ciphering techniques have been researched on to overcome the security issue.

Optical encryption methods have the power to provide fast processing, parallelism, high degree of freedom, and flexibility for the encoded beam. Different optical ciphers have been suggested in relation to the methodology of data encryption such as full phase ciphering, amplitude-based ciphering, and polarization encoding ciphering [1]–[3]. Researchers have proved that full phase ciphering is more efficient and secure than amplitude-based ciphering because of the existence of nonlinear features of phase function and additive noise.

The DRPE is an optical image encryption technique [4] that is categorized as one of the most utilized and efficient optical ciphering scheme that involves a pair of random phase keys; the first one in time domain and second in Fourier domain. The Fractional Fourier transform (FrFT) is used as polarization for traditional encoding techniques in the time

domain, while the Optical Fourier Transform (OFT) performs a paramount optical image processing function in the Fourier domain for encoding applications [5]. Here, the setup consists of two cascaded lenses that execute the OFT process of the input object in the DRPE scheme [6]–[8].

In the literature, many color image ciphering schemes were proposed depending on the diffusion and confusion [9]–[20]. In [9], a color image cipher utilizing RGB pixel displacements was suggested. Both of the original and key images are split into RGB components. Then, the cipher image is generated by applying XOR operation and scrambling on RGB components. Although the statistical analysis shows a numerous difference, the proposed method was not robust to most common types of attacks and channel noises. Furthermore, the proposed method was not suitable for encrypting color images of different sizes.

In [10], the suggested scheme applied an affine transformation in the gyrator transform (GT). The color image RGB combinations are transformed into real and imaginary portions with affine transformation. The GT is employed twice to improve the cipher security. The affine and GT parameters

are the cipher keys. The work didn't investigate the statistical security analysis to evaluate its efficiency.

In [11], a color ciphering scheme that composing the sine chaotic mapping and DNA encoding to cipher the transmitted images was introduced. The results verify that the presented ciphering scheme can work efficiently and safely in the existence of attacks. In [12], a DRPE scheme for reliable multimedia transmission was proposed. Also, an interleaving process on the streamed data based on chaotic map scheme was introduced. The results confirmed that the presented ciphering scheme can work efficiently for reliable transmission of video data.

In [13], an efficient image ciphering technique using fractional discrete cosine transform was proposed. The test simulations proved the efficiency and validity of the proposed scheme. In [14], a chaotic tent map image cipher was investigated. The suggested technique ciphered the plain image utilizing the key streams of plainimage and secret keys. The statistical security analysis of the suggested technique demonstrated that a lot of problems of the traditional CTM techniques have been solved.

In [15], an image ciphering scheme was introduced that utilized a pixel shuffling operator for hiding and mixing the primary color data. The simulated results showed that the suggested cipher was secure, sensible to keys, feasible and has a good resistance to multimedia attacks. In [16], a double self-adaptive encryption technique for ciphering color images was suggested. The proposed technique compressed and encrypted each color image component with using 2D compressive sensing which are generated through compound chaotic schemes. The suggested ciphering technique results ensured high security.

In [17], a color image ciphering scheme based on using fractional chaotic techniques was introduced. The ciphered images introduced zero autocorrelation, uniform histogram, and a high entropy value. A new encryption method for a color image was suggested in the Fresnel domain [18]. The color plainimage is split into three phase masks utilizing Gerchberg Saxton Phase Iterative scheme with another pre-defined phase key.

In [19], a color image ciphering/deciphering method based on masking and shuffling was suggested. The proposed method utilized the chaotic Baker map and the fractional dual random phase masking to improve the security level. The tests ensured that the proposed cipher has high efficiency and reliable for image transmission.

In [20], a two-stage image ciphering method using DRPE and baker mapping was introduced. The plainimage is split into detail and approximate components utilizing DWT. After that, the details components are ciphered utilizing the chaotic Baker map scheme. Then, the DRPE method is employed utilizing two various keys for increasing the security of the transmitted images and to minimize the correlation between the ciphered pixels. The tested results demonstrated good noise resistance, and key sensitivity.

This research paper introduces a DRPE block-based opto-color cipher with different block sizes. The security examination of the DRPE block-based opto-color cipher is analyzed in terms of visual inspection, information entropy, histograms, differential analysis, encryption quality analysis, and effect of noise. All the simulation and experimental results demonstrate a high confusion efficiency of the suggested technique with respect to literature methods.

The paper remainder is marshaled as follows. Section II explores DRPE as an optical encryption technique. Section III explains in detail the proposed DRPE block-based opto-color cipher with different block sizes. Simulation and performance tests are explored in section IV. Noise effect on the deciphering system is discussed and investigated in section V. In section VI, the comparative analysis between the proposed scheme and the recent literature schemes is introduced. Section VII summarizes the conclusions.

II. THE DRPE

The DRPE utilizes a pair of Random Phase Mask (RPM) or keys in a setup called "4F". The first key RPM1 is bonded by the color plainimage in time domain. The second key, RPM2, is also bonded by the result obtained in the first stage in Fourier plane. Then, a second OFT is employed to reconstruct the color cipherimage in time domain.

Let $I(i, j)$ and $F(i, j)$ be plain and cipher color images, and $x(u, v)$ and $h(i, j)$ stand for key pair functions in frequency/spatial domains, where their estimations are located in the range of [0-1] with uniform distribution probability. The DRPE ciphering mechanism may be formulated as [4]:

$$F(i, j) = FT\{FT[I(i, j) \exp(j2\pi\theta(i, j))] \exp(j2\pi\omega(u, v))\} \quad (1)$$

By the same way, the DRPE deciphering mechanism can be formulated as [4]:

$$I(i, j) = \{FT^{-1}[FT^{-1}(F(i, j)) \exp(-j2\pi\omega(u, v))] \times \exp(-j2\pi\theta(i, j))\} \quad (2)$$

Here, $\exp(j2\pi\theta(i, j))$ and $\exp(-j2\pi\omega(u, v))$ are the keys transmitted in conjunction to the resulted encrypted image.

III. THE PROPOSED DRPE BLOCK-BASED OPTO-COLOR CIPHER

Fig. 1 illustrates the framework of the ciphering mechanism.

The color plainimage is divided into equal blocks [21], [22] and then converted from electrical signal to optical signal using an optical emitter (optical source). The resulted optical image is encrypted by employing the DRPE technique with two types of phase modulation on the optical image, one in time domain and the other in Fourier domain. Finally, the image is detected by using a CCD digital camera and then converted to the digital format that can be processed through computer.

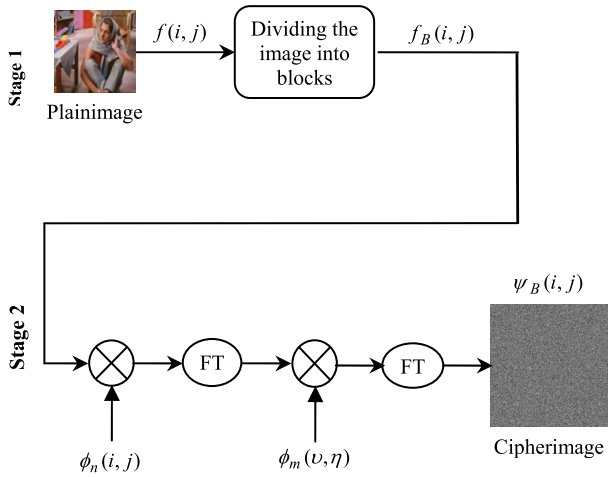


FIGURE 1. The framework of the ciphering mechanism.

The ciphering mechanism can be formulated mathematically as:

$$\psi_B(i, j) = FT^{-1}[FT(f_B(i, j)\phi_n(i, j))\phi_m(v, \eta)] \quad (3)$$

On the other hand, Fig. 2 shows the framework of the suggested deciphering mechanism, which can be represented mathematically as:

$$FT^{-1}[FT(\psi_B(i, j)\phi_m^*(v, \eta))] = f_B(i, j)\phi_n(i, j) \quad (4)$$

The conjugate of RPMs are applied to the optical signal to decrypt the image in two stages: (1) the optical signal is converted to the electrical signal by using the optical detector, and then (2) the image blocks are collected to get the color plainimage.

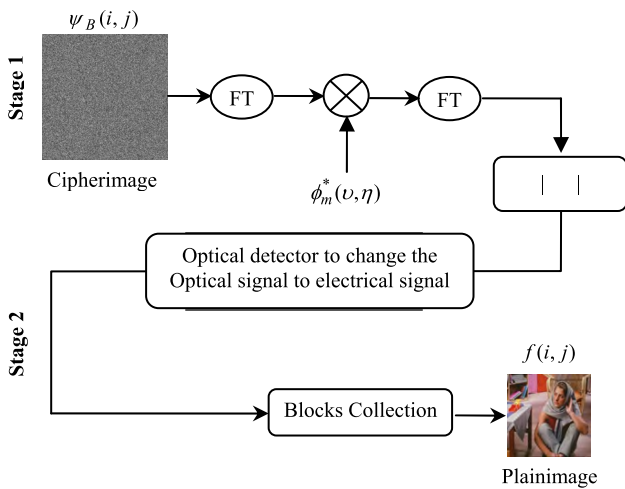


FIGURE 2. The framework of the deciphering mechanism.

IV. SIMULATION RESULTS

To evaluate the proposed encryption technique, two color plainimages ‘Barbara’ and ‘House’, are sized to 512 × 512,



FIGURE 3. Different samples of color plainimages.

256 × 256, 128 × 128, 64 × 64, 32 × 32, 16 × 16, 8 × 8, and 4 × 4 as illustrated in Fig. 3. The simulation tests are evaluated through visual testing, entropy, histogram, ciphering quality, and differential analysis [23]–[25].

A. VISUAL TESTING

The visual testing may be considered as one of the almost remarkable methods for evaluating the encryption quality. The more characteristics of a cipherimage disappear, the more a ciphering technique is recommended. The results of the cipherimages are shown in Fig. 4 for the Barbara and House images. It is noticed that the proposed encryption technique succeeds in ciphering and hiding the main details of the color plainimages. Fig. 5 shows the ciphered images produced by DRPE block-based opto-color cipher using different block sizes of 512 × 512, 256 × 256, 128 × 128, 64 × 64, 32 × 32, 16 × 16, 8 × 8 and 4 × 4. It is clear that the encryption efficiency of DRPE block-based opto-color cipher improves with increasing block size of the color plainimages.

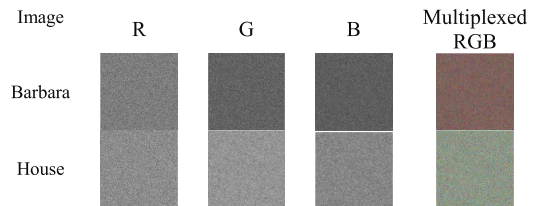


FIGURE 4. Visual tests of ciphered Barbara and House color component images using DRPE block-based opto-color cipher.

B. ENTROPY ANALYSIS

The structural property of the color plainimage should be hidden in the color cipherimage. Therefore, disappearing structural property leads to unpredictability of secret information of an enciphered image. Entropy analysis is used to measure this unpredictability by the following mathematical formula [26]:

$$E(x) = - \sum_{i=1}^{2^N-1} P(x_i) \log_2 P(x_i) \quad (5)$$

where $E(x)$ denotes the entropy for cipherimage x , $P(x_i)$ represents the occurrence probability of symbol x_i ; x_i in the cipherimage x , N denotes the bits number to assign the symbol x_i ; and $\log_2 \log_2$ will be applied to get the entropy value as a function of bits. The resulted pixel value may be located in the range from 0 to 255. It is known that the optimum

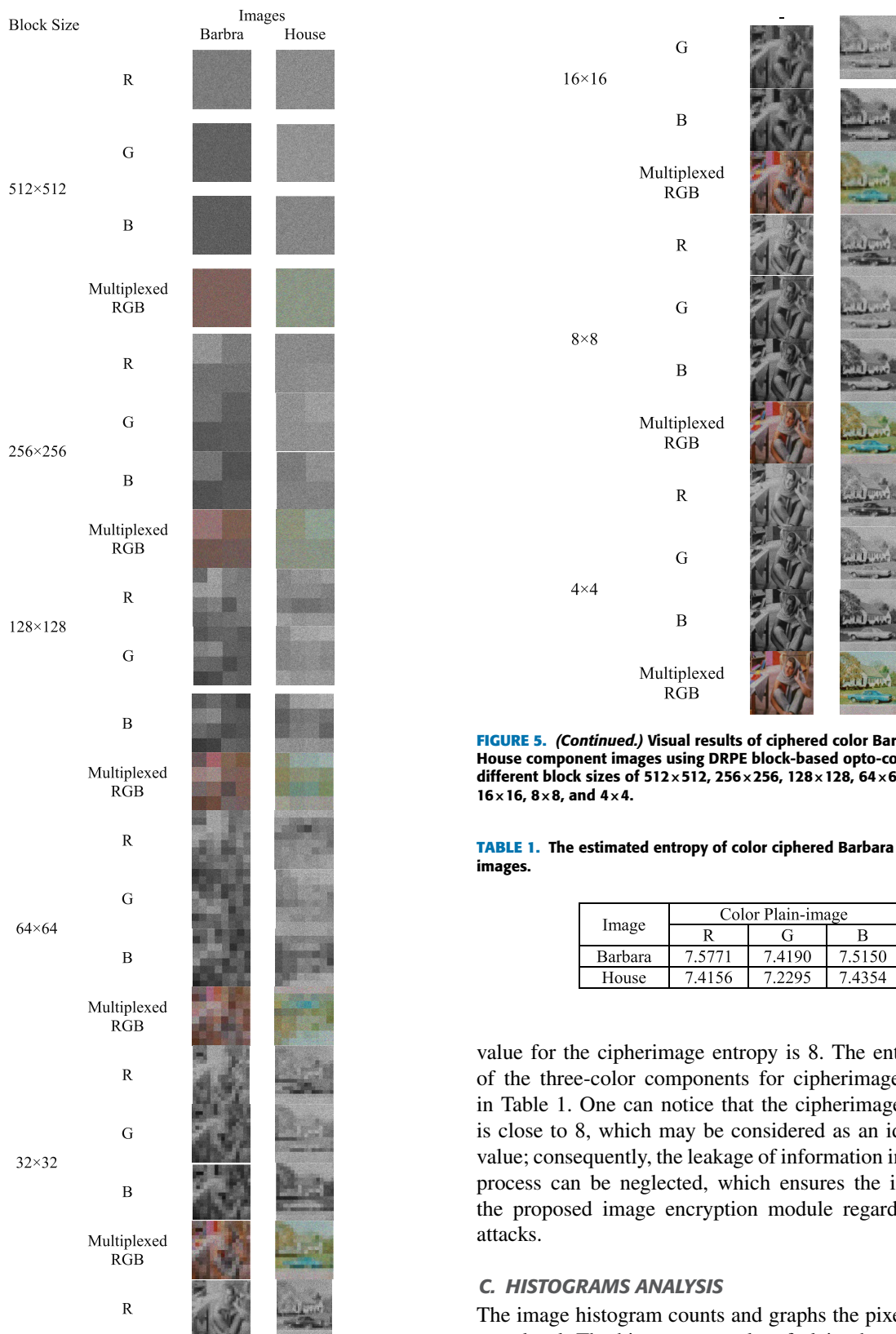


FIGURE 5. Visual results of ciphered color Barbara and House component images using DRPE block-based opto-color cipher with different block sizes of 512×512 , 256×256 , 128×128 , 64×64 , 32×32 , 16×16 , 8×8 , and 4×4 .

FIGURE 5. (Continued.) Visual results of ciphered color Barbara and House component images using DRPE block-based opto-color cipher with different block sizes of 512×512 , 256×256 , 128×128 , 64×64 , 32×32 , 16×16 , 8×8 , and 4×4 .

TABLE 1. The estimated entropy of color ciphered Barbara and House images.

Image	Color Plain-image		
	R	G	B
Barbara	7.5771	7.4190	7.5150
House	7.4156	7.2295	7.4354

value for the cipherimage entropy is 8. The entropy values of the three-color components for cipherimages are listed in Table 1. One can notice that the cipherimage entropy of is close to 8, which may be considered as an ideal entropy value; consequently, the leakage of information in encryption process can be neglected, which ensures the immunity of the proposed image encryption module regarding entropy attacks.

C. HISTOGRAMS ANALYSIS

The image histogram counts and graphs the pixels for every gray level. The histogram results of plain channels are presented in Fig. 6 for the color plainimages, and Fig. 7 illustrates the histogram results of ciphered RGB channels using the DRPE block-based opto-color cipher. As the DRPE

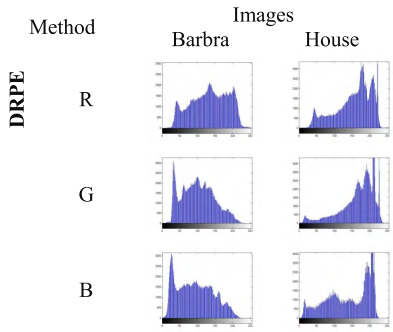


FIGURE 6. Histogram results of color Barbara and House component images.

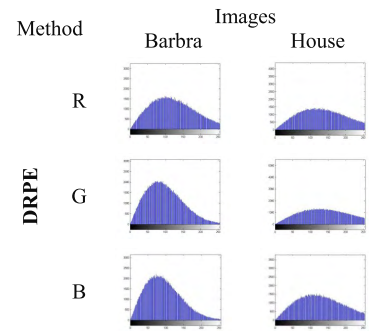


FIGURE 7. Histogram results of encrypted color Barbara and House component images using DRPE block-based opto-color cipher.

block-based opto-color cipher includes a diffusion procedure, pixel values must be changed. So, it is noticed from the histogram results presented in Fig. 7 that the color cipher-image histograms are completely distinct compared to their corresponding color plainimage histograms. Fig. 8 shows the histogram outcomes of color Barbara and House component images using the DRPE block-based opto-color cipher with different block sizes of 512×512 , 256×256 , 128×128 , 64×64 , 32×32 , 16×16 , 8×8 , and 4×4 . The resulted histograms confirm that with increasing plainimage block sizes, the histogram results are positively enhanced.

D. CIPHERING QUALITY ANALYSIS

The ciphering quality of the DRPE block-based opto-color cipher can be estimated using three parameters: (1) correlation coefficient (r_{xy}), (2) histogram deviation (D_H) between the color plainimage and the color cipherimage, and (3) the irregular deviation (D_I) of the color cipherimage.

The correlation coefficient (r_{xy}) can be calculated in 1-D sequences as follows [27]:

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{6}$$

where x is color plainimage and y is the color cipherimage, $\text{cov}(x, y) = \frac{1}{L} \sum_{i=1}^L (x(i) - E(x))(y(i) - E(y))$,

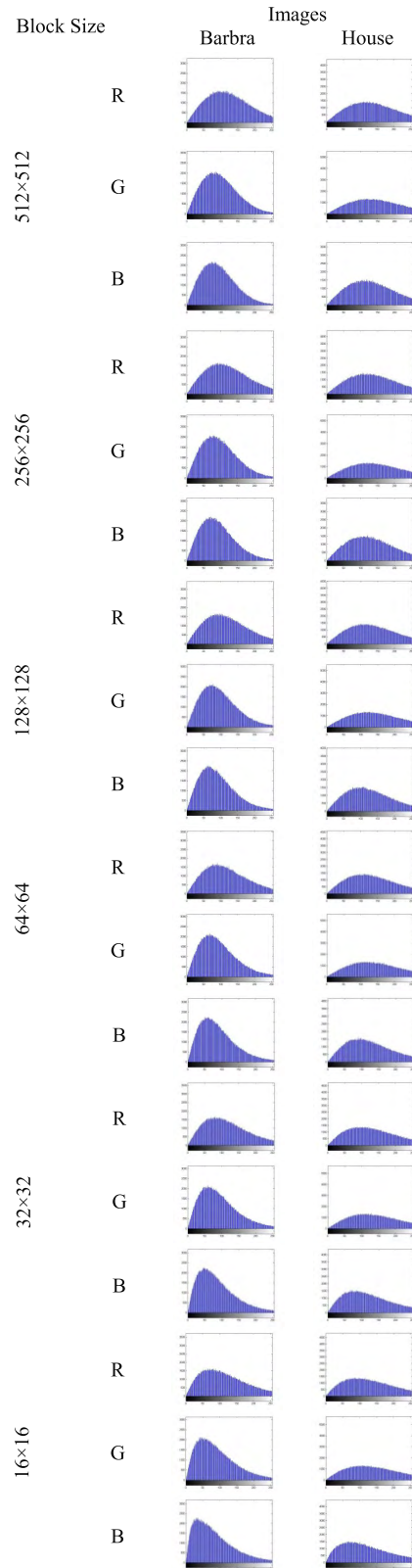


FIGURE 8. The histogram outcomes of color Barbara and House component images using DRPE block-based opto-color cipher with different block sizes of 512×512 , 256×256 , 128×128 , 64×64 , 32×32 , 16×16 , 8×8 and 4×4 .

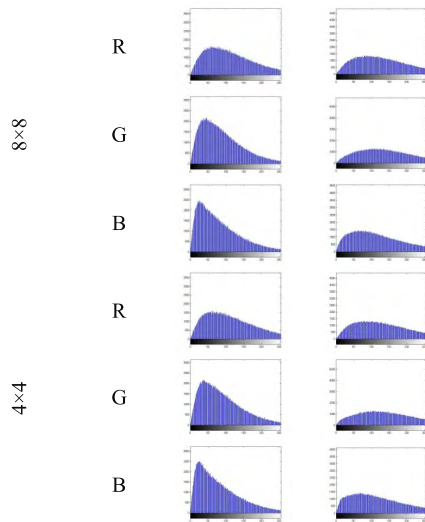


FIGURE 8. (Continued.) The histogram outcomes of color Barbara and House component images using DRPE block-based opto-color cipher with different block sizes of 512×512 , 256×256 , 128×128 , 64×64 , 32×32 , 16×16 , 8×8 and 4×4 .

$$D(x) = \frac{1}{L} \sum_{i=1}^L (x(i) - E(x))^2, D(y) = \frac{1}{L} \sum_{i=1}^L (y(i) - E(y))^2, \text{ and } L \text{ is image total pixels.}$$

The histogram deviation (D_H) between the plainimage and the cipherimage is obtained by estimating the difference between the areas under the histogram curves using the formula [28]:

$$D_H = \frac{\left(\sum_{i=0}^{255} d(i) \right)}{WxH}, \tag{7}$$

where $d(i)$ is absolute variance among the amplitude values of the obtained histograms of plain and encrypted images at the pixel level i with dimensions $W \times H$.

Finally, irregular deviation (D_I) of the color cipherimage is estimated using the following equations [29]:

$$D_I = \frac{\left| \sum_{i=0}^{255} h_d(i) \right|}{WxH}, \tag{8}$$

$$h_d(i) = |h(i) - M|, \tag{9}$$

where $h(i)$ is color cipherimage histogram at i -level and M is average of a pre-assumed uniform histogram distribution for ideal cipherimage.

The values of the correlation coefficient (r_{xy}), histogram deviation (D_H) and the irregular deviation (D_I) are presented in Table 2. The r_{xy} and D_H values are both close to zero and the D_I values are low. Consequently, the color plainimage and the color cipherimage are uncorrelated.

E. DIFFERENTIAL ANALYSIS

The underlying principle of a differential attack relates to modifying a pixel or bit in the plainimage and discovers

TABLE 2. The results of the entropy, correlation coefficient, deviations, NPCR, and UACI for the encrypted RGB of Barbara and House images using the DRPE block-based opto-color cipher.

Image	Encrypted color image with the suggested DRPE ciphering technique						
	Entropy	Cr	D_H	D_I	NPCR	UACI	
Barbara	R	7.7368	-6.67×10^{-5}	0.4090	0.7612	99.5468	0
	G	7.6325	-0.0011	0.2591	0.9124	99.4095	0
	B	7.5725	2.15×10^{-4}	0.2971	0.8941	99.4610	0
House	R	7.5985	-0.0019	0.6464	0.7218	99.6033	0
	G	7.4510	-8.24×10^{-5}	0.8065	0.7095	99.6281	0
	B	7.6759	0.0010	0.5934	0.6574	99.5970	0

the difference between the two resulted cipherimages. The immunity of the DRPE block-based opto-color cipher against differential attacks can be analyzed through calculating the UACI and the NPCR values. Consider two cipherimages $C1$ and $C2$ of the two plainimages $S1$ and $S2$, which have 2-D matrix of size $H \times W$ with only one-pixel value variation such that $D(i, j) = 1$. UACI and NPCR values are estimated for the cipherimages $C1$ and $C2$ using the following two equations [28], [29]:

$$UACI_{R/G/B} = \frac{1}{W \times H} \left[\sum_{i=1}^W \sum_{j=1}^H \frac{C1_{R/G/B}(i, j) - C2_{R/G/B}(i, j)}{255} \right] \times 100\%, \tag{10}$$

$$NPCR_{R/G/B} = \frac{\sum_{i=1}^W \sum_{j=1}^H D_{R/G/B}(i, j)}{W \times H} \times 100\%, \tag{11}$$

where W and H represent the color cipherimage width and height. The ideal value for the $UACI$ and $NPCR$ are 33.46% and 99.60%, respectively. Table 3 gives the numerical estimations of $NPCR$, and $UACI$, which indicate that the suggested ciphering technique is secure and robust against a differential attack.

Tables 3 and 4 put all together the metrics of image entropy, correlation coefficient, deviations (D_H and D_I), NPCR, and UACI for the encrypted Barbara and House component images using the DRPE block-based opto-color cipher at different block sizes. It is observed that the DRPE block-based opto-color cipher with different block sizes becomes more secure as increasing the color plainimage block size.

V. EFFECT OF NOISE

The PSNR values are calculated for evaluating the visual quality and the robustness efficiency of the proposed technique in channel noise existence.

The performance efficiency of the deciphering mechanism is tested with PSNR values (in dB) using the following

TABLE 3. Barbara image quality metrics using the DRPE block-based opto-color cipher with different block sizes.

Blocks	Layer	Encrypted DRPE Barbara Image Quality Metrics					
		Entropy	Cr	D _H	D _I	NCPR	UACI
512×512	R	7.7357	0.00005	0.4023	0.7608	99.5560	0
	G	7.6322	0.0018	0.2605	0.9146	99.4129	0
	B	7.5730	-0.0008	0.2979	0.8933	99.4556	0
256×256	R	7.7148	0.0906	0.4306	0.7990	99.5281	0
	G	7.6302	0.0517	0.2818	0.9292	99.3988	0
	B	7.5742	0.0804	0.3188	0.9213	99.4537	0
128×128	R	7.6969	0.1724	0.4538	0.8327	99.5354	0
	G	7.6250	0.1451	0.3168	0.9599	99.3744	0
	B	7.5758	0.1713	0.3305	0.9497	99.3954	0
64×64	R	7.6777	0.2414	0.4806	0.8606	99.4553	0
	G	7.6225	0.2431	0.3555	0.9894	99.3702	0
	B	7.5789	0.2990	0.3479	0.9951	99.3217	0
32×32	R	7.6651	0.3378	0.5146	0.8988	99.4785	0
	G	7.6248	0.3484	0.3951	1.0256	99.2859	0
	B	7.5864	0.4102	0.3639	1.0340	99.2390	0
16×16	R	7.6654	0.4313	0.5453	0.9357	99.4053	0
	G	7.6285	0.4649	0.4390	1.0645	99.2302	0
	B	7.5914	0.5358	0.3787	1.0837	99.0360	0
8×8	R	7.6602	0.4977	0.5704	0.9652	99.3668	0
	G	7.6284	0.5354	0.4601	1.0965	99.1497	0
	B	7.5832	0.6075	0.3931	1.1144	98.9311	0
4×4	R	7.6701	0.5444	0.5658	0.9947	99.3365	0
	G	7.6383	0.5871	0.4649	1.1226	99.0700	0
	B	7.5948	0.6528	0.3973	1.1442	98.8277	0

TABLE 4. House image quality metrics using the DRPE block-based opto-color cipher with different block sizes.

Blocks	Layer	Encrypted DRPE Barbara Image Quality Metrics					
		Entropy	Cr	D _H	D _I	NCPR	UACI
512×512	R	7.5959	-7.1*10 ⁻¹	0.6515	0.7209	99.5937	0
	G	7.4476	-0.0017	0.8086	0.7102	99.6243	0
	B	7.6792	0.0020	0.5930	0.6597	99.6181	0
256×256	R	7.5969	0.0078	0.6482	0.7250	99.5884	0
	G	7.4526	0.0165	0.8138	0.7149	99.6216	0
	B	7.6694	0.0254	0.5965	0.6685	99.6128	0
128×128	R	7.5845	0.0914	0.6727	0.7571	99.6021	0
	G	7.4464	0.0731	0.8233	0.7354	99.6265	0
	B	7.6356	0.1734	0.6115	0.7368	99.5911	0
64×64	R	7.5743	0.1730	0.6920	0.7853	99.5678	0
	G	7.4450	0.1163	0.8305	0.7504	99.5876	0
	B	7.6140	0.2623	0.6227	0.7779	99.5383	0
32×32	R	7.5623	0.2928	0.7221	0.8286	99.5262	0
	G	7.4311	0.2152	0.8525	0.7861	99.6033	0
	B	7.5920	0.3945	0.6242	0.8414	99.4881	0
16×16	R	7.5553	0.3641	0.7409	0.8579	99.5026	0
	G	7.4371	0.2898	0.8632	0.8107	99.5510	0
	B	7.5898	0.4812	0.6311	0.8902	99.4251	0
8×8	R	7.5585	0.4224	0.7495	0.8833	99.4614	0
	G	7.4342	0.3539	0.8673	0.8369	99.5338	0
	B	7.5900	0.5399	0.6342	0.9232	99.3835	0
4×4	R	7.5546	0.4806	0.7482	0.9165	99.4228	0
	G	7.4396	0.4207	0.8650	0.8684	99.4839	0
	B	7.5874	0.5961	0.6317	0.9648	99.2378	0

formula:

$$PSNR = 10 \log \frac{(255)^2}{\sum_{i=0}^{W-1} \sum_{j=0}^{H-1} [f_1(i, j) - f_2(i, j)]^2} \quad (12)$$

where $f_1(i, j)$, $f_2(i, j)$ denotes pixels gray values positioned in the i^{th} row and j^{th} column plainimage and cipherimage, respectively.

TABLE 5. The PSNR results of deciphered images using the DRPE block-based opto-color cipher with different block sizes.

Image	Technique	PSNR (dB)						
		$\mu=0$ $\sigma=0.01$	$\mu=0$ $\sigma=0.05$	$\mu=0$ $\sigma=0.1$	$\mu=0$ $\sigma=0.15$	$\mu=0$ $\sigma=0.20$		
Barbara	DRPE block 512×512	R	12.1069	10.5810	9.5276	8.8293	8.3848	
		G	13.3756	11.4687	10.0964	9.2263	8.7142	
		B	12.3141	10.9379	9.8418	9.1092	8.6092	
	DRPE block 128×128	R	11.3361	10.0669	9.2233	8.6371	8.2524	
		G	12.4870	10.9424	9.7435	9.0331	8.5193	
		B	11.5852	10.4609	9.5163	8.8776	8.4040	
	House	DRPE block 64×64	R	11.1313	9.9104	9.1160	8.5567	8.1790
			G	12.1365	10.7068	9.5895	8.8759	8.4234
			B	11.1983	10.1568	9.2948	8.7072	8.3181
DRPE block 32×32		R	10.7873	9.7284	8.9983	8.4806	8.1462	
		G	11.8005	10.4645	9.4441	8.8010	8.3763	
		B	10.9526	9.9722	9.2948	8.7072	8.3181	
House		DRPE block 512×512	R	7.1461	6.7057	6.3908	6.1694	6.0113
			G	7.0591	6.6553	6.3613	6.1404	5.9960
			B	6.7556	6.3839	6.1231	5.9678	5.8719
	DRPE block 128×128	R	9.2766	8.4436	7.8303	7.4398	7.1392	
		G	8.3819	7.7846	7.3423	7.0648	6.8814	
		B	9.2494	8.4142	7.7584	7.4168	7.1407	
	DRPE block 64×64	R	9.1236	8.3670	7.7688	7.3859	7.1150	
		G	8.3716	7.7860	7.3619	7.0628	6.8771	
		B	8.9900	6.2803	7.7399	7.3570	7.1010	
DRPE block 32×32	R	9.0492	8.2961	7.7260	7.3896	7.1367		
	G	8.3201	7.7949	7.3741	7.0801	6.8813		
	B	8.9558	8.2875	7.7357	7.3698	7.1118		
DRPE block 32×32	R	8.8178	8.0898	7.6056	7.2814	7.0478		
	G	8.1725	7.6724	7.2750	7.0141	6.8369		
	B	8.6550	8.0505	7.5526	7.2458	7.0120		

For better noise immunity, a higher value (than 5) of PSNR is a requirement in cipherimage. The PSNR values for several cipherimages generated using the DRPE block-based opto-color cipher at different block sizes are calculated and given in Tables 5 and 6. These numerical and subjective outcomes confirm and support the efficiency and robustness of the DRPE block-based opto-color cipher in the existence of channel noise.

VI. COMPARATIVE ANALYSIS AND DISCUSSIONS

To verify the efficiency of the DRPE block-based opto-color cipher for reliable color transmission over insecure channels, test experiments are employed for comparing results of DRPE block-based opto-color cipher with the state-of-the-art schemes [9], [11], [14]–[17], [19], [20]. We compared the statistical security analysis of the entropy, correlation coefficient, UACI, NPCR, and PSNR results of the proposed encryption scheme with the recent literature encryption related schemes in [9], [11], [14]–[17], [19], and [20].

The entropy values of the three-color components for the Lena cipherimage are listed in Table 7 of the DRPE block-based opto-color cipher compared to the proposed schemes in [14] and [17]. We noticed that the entropies of the cipherimage for the DRPE block-based opto-color cipher are more closely to 8 compared to other literature methods in [14] and [17], which is the ideal entropy value; consequently, the leakage of information in encryption process can be

TABLE 6. Decrypted Barbra and House images using the DRPE block-based opto-color cipher with different block sizes in the existence of channel noise with various noise variances on the encrypted images.

Image	Technique		Deciphered image				
			$\mu=0$ $\Sigma = 0.01$	$\mu=0$ $\Sigma = 0.05$	$\mu=0$ $\Sigma = 0.1$	$\mu=0$ $\Sigma = 0.15$	$\mu=0$ $\Sigma = 0.20$
Barbara	DRPE block 512×512	R					
		G					
		B					
		RGB					
	DRPE block 128×128	R					
		G					
		B					
		RGB					
	DRPE block 64×64	R					
		G					
		B					
		RGB					
	DRPE block 32×32	R					
		G					
		B					
		RGB					
House	DRPE block 512×512	R					
		G					
		B					
		RGB					

TABLE 6. (Continued.) Decrypted Barbra and House images using the DRPE block-based opto-color cipher with different block sizes in the existence of channel noise with various noise variances on the encrypted images.

	DRPE block 128×128	R				
		G				
		B				
		RGB				
	DRPE block 64×64	R				
		G				
		B				
		r RGB				
	DRPE block 32×32	R				
		G				
		B				
		RGB				

TABLE 7. The estimated entropy of ciphered RGB Lena image for the DRPE block-based opto-color cipher and the literature schemes in [14] and [17].

Scheme	R	G	B
DRPE block-based opto-color cipher	7.7771	7.7190	7.7150
Ref. [14]	7.5872	7.6251	7.6296
Ref. [17]	7.2596	7.5890	6.9734

neglected, which ensures the immunity of the DRPE block-based opto-color cipher regarding the entropy attack compared to the literature schemes.

The comparison values of correlation coefficient for the DRPE block-based opto-color cipher and the proposed schemes in [9], [14]–[16], [19], and [20] for the Lena image are presented in Table 8. The correlation coefficient values for the DRPE block-based opto-color cipher are more closely to zero compared with correlation coefficient values of the state-of-the-art schemes. Consequently, the color plainimage and the color cipherimage are uncorrelated.

Table 9 lists NPCR/UACI numerical values of the DRPE block-based opto-color cipher compared to the proposed

TABLE 8. The correlation coefficient of ciphered RGB Lena image for the DRPE block-based opto-color cipher and the literature schemes in [9], [14]–[16], [19], and [20].

Scheme	R	G	B
DRPE block-based opto-color cipher	$-6.67 \cdot 10^{-5}$	0.0367	0.0247
Ref. [9]	0.1955	0.1806	0.1574
Ref. [14]	0.0435	0.0519	0.0675
Ref. [15]	0.1204	0.0985	0.1002
Ref. [16]	0.0219	0.0419	0.0259
Ref. [19]	0.0001	0.0021	0.0251
Ref. [20]	-0.0006	0.0246	0.0306

schemes in [14] and [19]. The results indicate that the suggested ciphering technique in this paper is more secure and robust against a differential attack.

The PSNR results (dB) of the deciphered Lena image using the DRPE block-based opto-color cipher compared to the proposed schemes in [19] and [20] are presented in Table 10. The DRPE block-based opto-color cipher is more efficient than the proposed schemes in [19] and [20].

TABLE 9. The NPCR and UACI results of ciphered Lena image for the DRPE block-based opto-color cipher and the literature schemes in [14] and [19].

Scheme	NPCR	UACI
DRPE block-based opto-color cipher	0.9973	0
Ref. [14]	0.9971	0.3345
Ref. [19]	0.9956	0.3117

TABLE 10. The PSNR (dB) results of the deciphered Lena image using the DRPE block-based opto-color cipher compared to the proposed schemes in [19] and [20].

Scheme	PSNR
DRPE block-based opto-color cipher	44.62
Ref. [19]	41.51
Ref. [20]	42.88

VII. CONCLUSION

The paper presented a DRPE block-based opto-color cipher with different block sizes. In the DRPE block-based opto-color cipher, the color plainimage is split into equal sized blocks and converted to optical signal, and then encrypted using the DRPE scheme. Several experiments using MATLAB were carried out on four color plainimages with different block sizes. The experimental tests obtained and the security analysis demonstrated that the DRPE block-based opto-color cipher with increased block size of the input color plainimage is secure and effective, including a good immunity to channel noise.

REFERENCES

- [1] L. Xinyu and Y. Wang, "Optical encryptions and decryptions based on all-optical shift register," in *Proc. IEEE Int. Conf. Opt. Commun. Netw. (ICOCN)*, Aug. 2017, pp. 1–3.
- [2] A. Ritika, Y. Xiong, and C. Quan, "Optical image encryption using radon transform," in *Proc. IEEE Prog. Electromagn. Res. Symp.-Fall (PIERS-FALL)*, 2017, pp. 1235–1238.
- [3] W. Zamrani, E. Ahouzi, A. Lizana, J. Campus, and M. J. Yzuel, "Towards the growth of optical security systems for image encryption by polarized light," in *Proc. IEEE Int. Conf. Comput. Syst. Appl. (AICCSA)*, Nov./Dec. 2016, pp. 1–6.
- [4] Z. Liu, S. Li, W. Liu, Y. Wang, and 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, no. 1, pp. 8–14, Jan. 2013.
- [5] S. Narendra and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Opt. Lasers Eng.*, vol. 46, no. 2, pp. 117–123, 2008.
- [6] Z. Nanrun and T. Dong, "Optical image encryption scheme based on multiple-parameter random fractional Fourier transform," in *Proc. IEEE Int. Symp. Electron. Commerce Secur. (ISECS)*, vol. 2, 2009, pp. 48–51.
- [7] J. Li, X. Di, X. Liu, and X. Chen, "Image encryption based on quantum-CNN hyperchaos system and anamorphic fractional Fourier transform," in *Proc. IEEE Int. Conf. Image Signal Process., Biomed. Eng. Inform. (CISP-BMEI)*, Oct. 2017, pp. 1–6.
- [8] R. Hui, J. Wang, and Q. Wang, "Optical encryption of gray image based on the computer-generated hologram and logical modulation," in *Proc. IEEE Int. Conf. Opt. Photon. Eng. (ICOPEN)*, Oct. 2017, pp. 1–6.
- [9] S. Shrija and M. A. Hussain, "A novel image encryption technique using RGB pixel displacement for color images," in *Proc. IEEE Int. Conf. Adv. Comput. (IACC)*, Feb. 2016, pp. 275–279.
- [10] H. Chen, X. Du, Z. Liu, and C. Yang, "Color image encryption based on the affine transform and gyrator transform," *Opt. Lasers Eng.*, vol. 51, no. 6, pp. 768–775, 2013.
- [11] B. Awdun and G. Li, "The color image encryption technology based on DNA encoding & sine chaos," in *Proc. IEEE Int. Conf. Smart City Syst. Eng. (ICSCSE)*, Nov. 2016, pp. 539–544.
- [12] E. M. El-Bakary, E.-S. M. El-Rabaie, O. Zahran, and F. E. A. El-Samie, "DRPE encryption with chaotic interleaving for video communication," *Wireless Pers. Commun.*, vol. 97, no. 1, pp. 1373–1384, 2017.
- [13] X. Z. Luo, N. R. Zhou, Q. M. Zhao, and J. H. Wu, "Color image encryption based on the multiple-order discrete fractional cosine transform and chaos in YCbCr space," *Appl. Mech. Mater.*, vol. 182, pp. 1839–1843, Jun. 2012.
- [14] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.
- [15] X. Kang and R. Tao, "Color image encryption using pixel scrambling operator and reality-preserving MPFRHT," *IEEE Trans. Circuits Syst. Video Technol.*, to be published, doi: 10.1109/TCSVT.2018.2859253.
- [16] F. Han, X. Liao, B. Yang, and Y. Zhang, "A hybrid scheme for self-adaptive double color-image encryption," *Multimedia Tools Appl.*, vol. 77, no. 11, pp. 14285–14304, 2018.
- [17] T. Dasgupta, P. Paral, and S. Bhattacharya, "Colour image encryption based on multiple fractional order chaotic systems," in *Proc. IEEE Int. Conf. Control, Instrum., Energy Commun. (CIEC)*, Jan./Feb. 2014, pp. 583–587.
- [18] Z. Liu et al., "Securing color image by using phase-only encoding in Fresnel domains," *Opt. Lasers Eng.*, vol. 68, pp. 87–92, May 2015.
- [19] R. Jain and J. B. Sharma, "Symmetric color image encryption algorithm using fractional DRPM and chaotic baker map," in *Proc. IEEE Int. Conf. Recent Trends Electron., Inf. Commun. Technol. (RTEICT)*, May 2016, pp. 1835–1840.
- [20] R. Jain and J. B. Sharma, "Multi-domain image encryption using chaotic map with DRPE," in *Proc. IEEE Int. Conf. Adv. Inf. Commun. Technol. Comput.*, Aug. 2016, pp. 10–16.
- [21] G. R. G. King and C. Christopher, "Improved block-based segmentation algorithm for compression of compound images," *J. Intell. Fuzzy Syst.*, vol. 27, no. 6, pp. 3213–3225, 2014.
- [22] G. R. G. King and H. Haennah, "Hybrid compression scheme using pre-coding block and fast stationary wavelet transformation," *J. Intell. Fuzzy Syst.*, vol. 31, no. 1, pp. 415–421, 2016.
- [23] S. Ergin, "Security analysis of a chaos-based random number generator for applications in cryptography," in *Proc. IEEE Int. Symp. Commun. Inf. Technol. (ISCIT)*, Oct. 2015, pp. 319–322.
- [24] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, 2011.
- [25] Y. Zhang and D. Xiao, "Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform," *Opt. Lasers Eng.*, vol. 51, no. 4, pp. 472–480, Apr. 2013.
- [26] P. Pauline and W. Puech, "Reversible data hiding in encrypted images based on adaptive local entropy analysis," in *Proc. IEEE Int. Conf. Image Process. Tools Appl. (IPTA)*, Nov./Dec. 2017, pp. 1–6.
- [27] B. Nini, A. Zitouni, and A. Ounzar, "Analysis of the use of some statistical measures in deciding about the efficiency of an image encryption algorithm," in *Proc. IEEE Int. Conf. Image Process., Appl. Syst. (IPAS)*, Nov. 2016, pp. 1–6.
- [28] Y. Xie, J. Li, Z. Kong, Y. Zhang, X. Liao, and Y. Liu, "Exploiting optics chaos for image encryption-then-transmission," *J. Lightw. Technol.*, vol. 34, no. 22, pp. 5101–5109, Nov. 15, 2016.
- [29] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.



OSAMA S. FARAGALLAH received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in computer science and engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He was with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was a Demonstrator from 1997 to 2002 and an Assistant Lecturer from 2002 to 2007. Since 2007, he has been a Teaching Staff Member with the

Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he is currently an Associate Professor. He has co-authored about 100 papers in international journals and conference proceedings, and two textbooks. His current research interests include network security, cryptography, Internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.



MOHAMMED A. ALZAIN received the bachelor's degree in computer science from King Abdulaziz University, Saudi Arabia, in 2004, the master's degree in information technology from La Trobe University in 2010, and the Ph.D. degree from the Department of Computer Science and Computer Engineering, La Trobe University, Melbourne, Australia, in 2014. His Ph.D. research was on cloud computing security. His dissertation title was Data Security, Data Management, Performance

Evaluation for a Multi-Cloud Computing Model. He is currently a Vice Dean and an Assistant Professor with the College of Computers and Information Technology, Taif University, Saudi Arabia. His areas of interests are cloud computing security and multimedia security.



HALA S. EL-SAYED received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electrical engineering from Menoufia University, Shebin El-Kom, Egypt, in 2000, 2004, and 2010, respectively. She was with the Department of Electrical Engineering, Faculty of Engineering, Menoufia University, where she was a Demonstrator from 2002 to 2004 and an Assistant Lecturer from 2004 to 2010. Since 2010, she has been a Teaching Staff Member with the Department of Electrical Engineering,

Faculty of Engineering, Menoufia University, where she is currently an Assistant Professor. She has co-authored about 40 papers in international journals and conference proceedings, and one textbook. Her research interests cover database security, network security, data hiding, image encryption, wireless sensor network, secure building automation systems, medical image processing, and biometrics.



JEHAD F. AL-AMRI received the degree from the Centre for Computing and Social Responsibility, De Montfort University. He is currently an Assistant Professor with the Department of Information Technology, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. He is an Assistant Professor of computer informatics.



WALID EL-SHAFAI was born in Alexandria, Egypt, in 1986. He received the B.Sc. degree in electronics and electrical communication engineering from the Faculty of Electronic Engineering (FEE), Menoufia University, Menouf, Egypt, in 2008, and the M.Sc. degree from the Egypt–Japan University of Science and Technology in 2012. He is currently a Teaching Assistant and a Ph.D. Researcher with the Electrical Communications Engineering Department, FEE, Menoufia

University. His research interests are in the areas of wireless mobile and multimedia communications systems, image and video signal processing, efficient 2-D video/3-D multi-view video coding, multi-view video plus depth coding, 3-D multi-view video coding and transmission, quality of service and experience, digital communication techniques, 3-D video watermarking and encryption, error resilience, and concealment algorithms for H.264/AVC, H.264/MVC, and H.265/HEVC video codecs standards.



ASHRAF AFIFI received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in electronic and communication engineering from Zagazig University, Egypt, in 1987, 1995, and 2002, respectively. He is currently an Associate Professor with the Department of Computer Engineering, Faculty of Computers and Information Technology, Taif University, Saudi Arabia. He has co-authored about 30 papers in international journals and conference proceedings. His research interests cover communication

security, image processing, and image encryption.



ENSHERAH A. NAEEM received the B.Sc., M.Sc., and Ph.D. degrees in electronics and communications engineering from the Faculty of Engineering, Tanta University, Tanta, Egypt, in 2006, 2012, and 2017, respectively. Since 2018, she has been a Teaching Staff with the Department of Electronics and Electrical Communications, Higher Institute of Engineering and Technology, Kafr El Sheikh, Egypt. Her current research areas of interests include wireless communications, image and

video compression, image encryption, image processing, and watermarking.



BEN SOH (S'89–M'92–SM'03) received the Ph.D. degree in computer science and engineering from La Trobe University, Melbourne, Australia, in 1995. He is currently an Associate Professor with the Department of Computer Science and Computer Engineering, La Trobe University. He had numerous successful Ph.D. graduates. He has authored more than 150 peer-reviewed research papers. He has made significant contributions in various research areas, including fault-tolerant and

secure computing, and Web services.

...