Optical Color Images Encryption based on Double Random Phase Encoding

M. A. Mohamed
Associate Professor at ECE Department, Faculty of Engineering, Mansoura University, Egypt

A. S. Samrah
Professor at ECE-Department, Faculty of Engineering, Mansoura University, Egypt

M. I. Fath Allah
Assist Lecturer at ECE-Department, Faculty of Engineering, Delta University, Egypt

ABSTRACT
Extensive studies have been carried out to develop strong encryption techniques that have played a vital role in communications and multimedia transmission. The main requirement of any encryption techniques is to get high robustness. One of the most common techniques for optical encryption is Double Random Phase Encoding (DRPE), but it was found that it suffers from weak performance against attacks especially with color images. In this paper, we will introduce three techniques, traditional, modified, and proposed one for optical encryption of colored images with various extensions and different sizes based on DRPE. As a result of the extensive comparative study, it was found that the Discrete Wavelet Transform (DWT) based DRPE provides the best experimental results from the point of view of differential attacks and statistical attacks.

General Terms
Image Encryption, Optical Encryption, RGB.

Keywords
Double Random Phase Encoding (DRPE), Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT).

1. INTRODUCTION
With the fast development of image transmission through computer networks especially the Internet, medical imaging and military message communication, intensive research has been directed toward coherent optics, especially the issues of compression and encoding, because of the potential for new technological applications in telecommunications [1]. Optical techniques appear as effective practical tools in securing and validating information [2, 3]. Optical encryption has reached a level of maturity recently with the publication of realistic attacks that exploit its inherent weakness of linearity [4-6]. To encourage widespread use, the field of optical encryption should offer a cohesive and fully featured suite of practical and unique applications [4]. It has been found that optical encryption techniques have the best performance for image encryption because of the optical nature of an image as well as some other advantages of optical encryption. One of the most attractive advantages of optical systems is the possibility to provide many degrees of freedom to handle parameters such as amplitude, phase, wavelength, and polarization [7]. The image encryption technique has attracted a growing attention since the DRPE technique was proposed by Refregier and Javidi in 1995 [8]. The main weakness of DRPE was bad performance when imposing the transmitted image to different types of attacks specifically rotation and cropping attacks. Most practical life information is represented by color images, and it was found that DRPE isn't effective technique for color image encryption against attacks.

This paper introduces a novel DWT based DRPE technique that has been compared with other traditional techniques based on DRPE. DRPE technique was simple to be applied to gray scale image, but it was needed to some modifications to be suitable for color images encryption. Towards this aim we have introduced an optical encryption scheme using Fast Fourier Transform (FFT) based DRPE as a traditional technique. After that a modified DCT based DRPE encryption technique have been presented. Finally, we will present for our proposed DWT based DRPE algorithm that has given high performance and high robustness against all types of attacks that have been imposed to encrypted image during transmission which makes it more realistic than other stated techniques.

The next of this paper is organized as follows; section-2 provides survey and related work, section-3 introduces DRPE overview, section-4 presents encryption algorithms and data collection, section-5 shows the simulation results and discussions, and section-6 gives the conclusions.

2. SURVEY AND RELATED WORK
Kanchana and Annapurna have introduced an approach of image encryption using the concept of sieving, dividing and shuffling which was robust to withstand brute force attacks [9]. Li, et al. have proposed a performance-enhanced image encryption schemes based on depth-conversion integral imaging and chaotic maps, aiming to meet the requirements of secure image transmission [10]. Lee, et al. have presented much works on analyzing security level of existing image encryption techniques [11-13]. Shao, et al. have described a novel algorithm to encrypt double color images into a single undistinguishable image in quaternion gyrator domain using an iterative phase retrieval algorithm [14]. Wang, et al. have introduced recent works presented color image encryption algorithms in a fully vector form that rely on the discrete quaternion Fourier transform and the quaternion gyrator transform [15, 16]. Multiple-image encryption algorithm capable to fuse more than one target image into a single illegible image has attracted great interest in the research field of [17-34]. Kester has developed a cipher algorithm for colored image encryption of size m*n by shuffling the RGB pixel values [35]. Z. Liu and Chen have designed a color image encryption algorithm using Arnold transform and Discrete Cosine Transform (DCT) [36]. Deng and Zhu have proposed a simple color image encryption with the help of quick response (QR) code [37].

3. DRPE OVERVIEW
In this section, the main optical encryption technique based on DRPE will be discussed. This implementation has been performed using an optical setup called 4f system as depicted in Fig. (1) [1, 8].

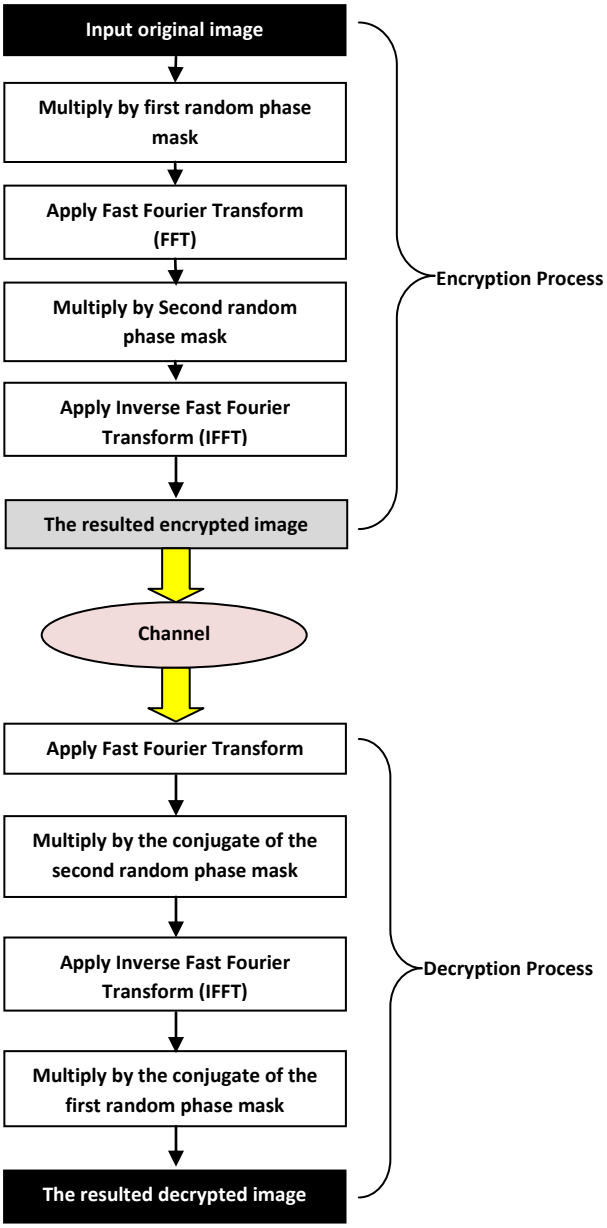

Fig 1: Flow Chart of traditional DRPE

As shown from Fig 1, the original image is first multiplied by the first random phase mask, then FFT is applied. After that, the resulted cypher text is multiplied by the second random phase mask. The last step in encryption process is applying Inverse Fast Fourier Transform (IFFT), then we get the encrypted image, coated from [8]. As depicted from the same figure, the steps of encryption are reversed for decryption process to get the resulted decrypted image (original image), coated from [8]. It was found that the implementation of FFT and IFFT could be applied using 2 lenses; one for FFT and another one for IFFT, coated from [1, 8].

4. ENCRYPTION ALGORITHMS AND DATA COLLECTION

4.1 Encryption Algorithms

In this subsection we will introduce the main steps of our three techniques represented by flow charts. The first technique is the traditional technique which has been represented by FFT based DRPE. This only the same as traditional DRPE scheme stated in the previous section with little modifications to be mare suitable for colored images. The flow chart of this technique is illustrated in Fig. (2).

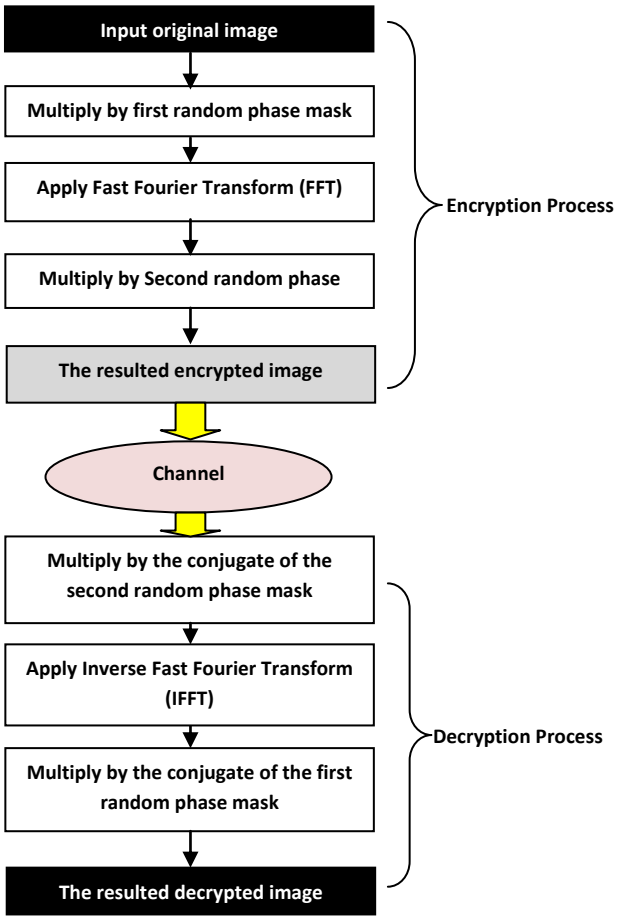

Fig 2: Flow Chart of FFT Based DRPE Technique

As shown from Fig 2, the original image is first multiplied by the first random phase mask, then FFT has been applied. After that, the resulted cipher text is multiplied by the second random phase mask to get the encrypted image. So the reversed steps could be done for decryption process to get the resulted decrypted image. We can overcome the problem of dealing with colored images with 3 color components (red, green, and blue) by using the green component for encryption process. Note that this problem doesn't exist for gray scale images.

The second scheme is the modified technique that has been designed using DCT based DRPE as depicted in Fig 3.

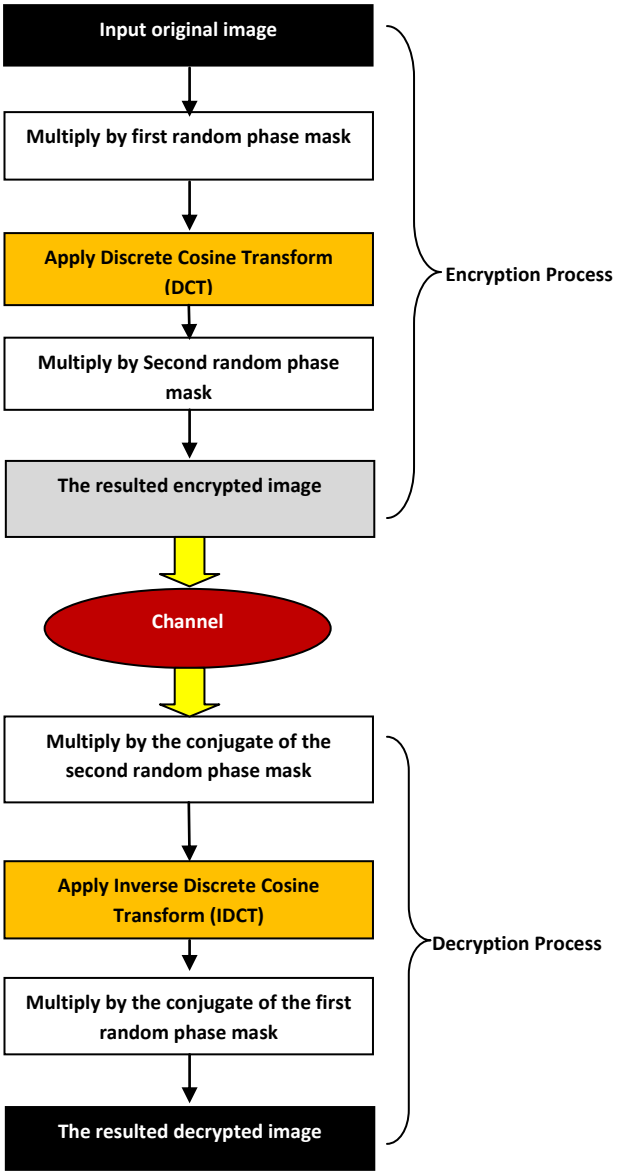

Fig 3: Flow Chart of DCT Based DRPE Technique

As obtained from Fig 3, the only modification is the use of DCT instead of FFT in the traditional technique stated before. The last algorithm is our novel proposed one that is represented by DWT based DRPE. The main flow chart of our approach is observed in Fig 4. As demonstrated from this figure, the original image is first multiplied by the first random phase mask and this stage is followed by multiplying by the second random phase mask. After that, the Discrete Wavelet Transform (DWT) has been applied to end the encryption process by obtaining the encrypted image. Here, for the first time FFT is replaced by DWT in which we have get a very good technique that is robust to most types of attacks as shown in the following section. The decryption process has been started by applying Inverse Discrete Wavelet Transform (IDWT) to the received encrypted image followed by multiplying by the conjugate of the second random phase mask and finally multiplying by the conjugate of the first random phase mask to get the resulted decrypted image.

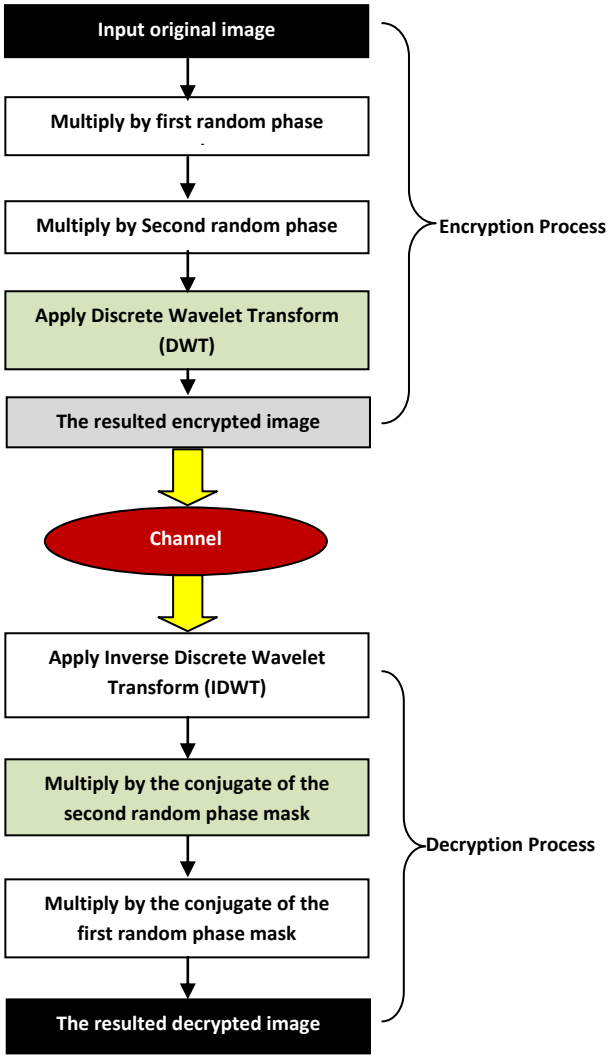

Fig 4: Flow Chart of DWT Based DRPE Technique

In the previous techniques, we use the green component of RGB colored image for encryption and decryption process. On the other hand, in our proposed technique, first the true color image RGB has been converted to the equivalent National Television System Committee (NTSC) image. The main components of NTSC image are; luminance (Y component), and chrominance (I and Q components). So NTSC image is also called YIQ image. We have used the luminance component (Y component) for encryption as well as decryption processes in our proposed algorithm. So that the final stage in programming our algorithm was to convert the NTSC image (YIQ components) again to the true color image (RGB components). For all the previous schemes, the channel could be ideal (without attacks) or real channel (in the presence of attacks) which is more practical. In the following section, the performance of all three techniques will be measured for real channels.

4.2 Data Collection

The main database of color images that has been used for our simulation is observed in Table 1 showing the name, the extension, the size, and the entropy of each plain image.

The original images as well as their histogram are illustrated in the following figures.

Table 1. Plain Images Database

Image	Name	Extension	Size	Entropy
1	Peppers	png	384 * 512	7.3785
2	Board	tif	648 * 306	7.2368
3	My picture	JPEG	450 * 300	6.0302
4	Water lilies	JPEG	600 * 800	7.0650
5	Greens	jpg	300 * 500	7.3743

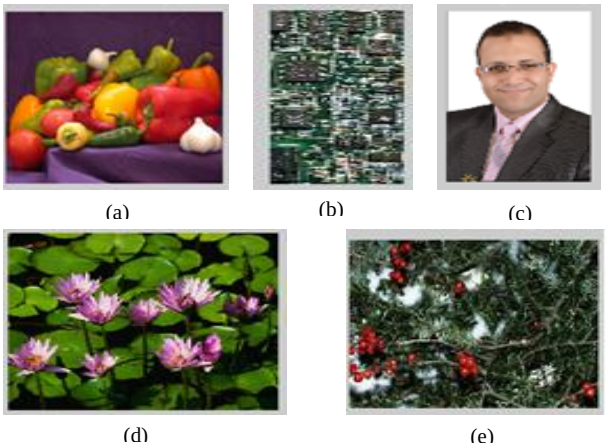

Fig 5: The original image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5)

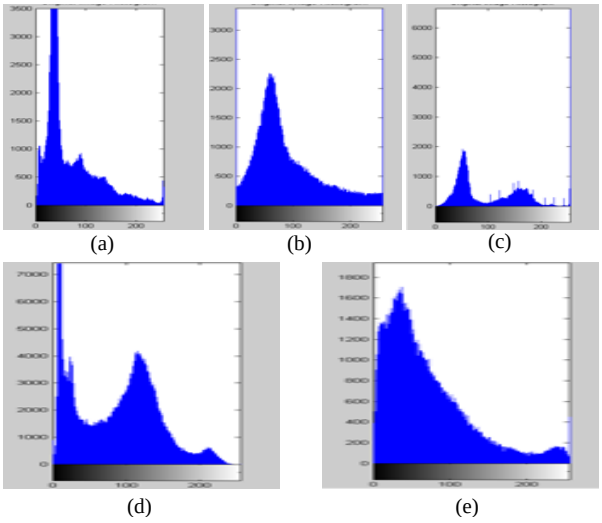

Fig 6: The original image Histogram for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5)

5. SIMULATION RESULTS AND DISCUSSIONS

The presented optical encryption techniques in the above section will be simulated using MATLAB-2009 on a personal computer of the following specifications: (i) Intel processor 3.2 GHZ Pentium-four; (ii) 2MB cache RAM; (iii) 2 GB RAM; (iv) SATA hard disk 250GB. The performance has been examined for practical channel case using different performance metrics. So we can divide this section into two subsections; performance metrics, and simulation results for real channel techniques.

5.1 Performance Metrics

We have used six performance metrics to measure the performance of all of three techniques stated in the previous section; elapsed time, entropy analysis, Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), cross correlation coefficient between original and decrypted images, and the histogram analysis for both plain and resulted decrypted images. Besides all of the above performance metrics, the simulation results for original, encrypted, and decrypted images for each technique will be observed. First we must present for the basic definitions for all the above performance metrics as follows.

5.1.1 Elapsed Time

Elapsed time has represented the total computational time for encryption as well as decryption processes in seconds for each trial of experiments. All of our experiments have been done using the same computer and the same version of MATLAB Program. Our device was connected to internet most of time. All experiments have been applied more than one time and hence the elapsed time has represented the average simulation time for all trials for each experiment.

5.1.2 Entropy Analysis

The entropy of a message source could be defined as in Eq. (1):

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i)\, log_2(p(m_i)) \qquad (1)$$

Where, $p(m_i)$ is the probability of symbol m_i, and N represents the number of bits for each symbol. The entropy represents the most outstanding feature of randomness [38]. For our techniques we concentrate on the difference between the entropy of original images listed in table (1) and the entropy of decrypted images that will be presented for each technique.

5.1.3 Mean Square Error (MSE)

The Mean Square Error between the original and decrypted images could be computed as in Eq. (2):

$$MSE=\frac{1}{MxNxf}\sum_{k=1}^{f}\sum_{i=1}^{M}\sum_{j=1}^{N}[OI(i,j,k)-DI(i,j,k)]^2 \quad (2)$$

Where, M is the number of rows, N is the number of columns, f is the number of image frames, OI is the original image, and DI is the decrypted image [38].

5.1.4 Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio is used to measure the degradation between the plain and decrypted images. It can be computed as in Eq. (3):

$$PSNR = 10log_{10}\left(\frac{Max_{OI}{}^2}{MSE}\right) dB \qquad (3)$$

Where, Max_{OI} represents the maximum possible pixel value of the original image [38].

5.1.5 Cross Correlation Coefficient (R)

The cross correlation between the original and decrypted images can be defined as in Eq. (4):

$$R = \frac{\sum_m \sum_n (OI_{mn}-\overline{OI})(DI_{mn}-\overline{DI})}{\sqrt{(\sum_m \sum_n (OI_{mn}-\overline{OI})^2)(\sum_m \sum_n (DI_{mn}-\overline{DI})^2)}} \qquad (4)$$

Where, m is the row number, n is the column number, $\overline{OI}$ is the mean value of the pixels of original image, and $\overline{DI}$ is the mean value of the pixels of decrypted image.

5.1.6 Histogram Analysis

The histogram analysis clarifies that, how the pixel values of original or decrypted image are distributed. For good encryption technique, the histogram of decrypted image must be similar to the histogram of original image with slightly little difference [38]. The main equation of histogram of an image is obtained as follows;

$$P_n = \frac{Number\ of\ pixels\ with\ intensity\ n}{Total\ number\ of\ pixels}, \quad n = 0, 1, \ldots, L - 1 \qquad (5)$$

Where, for f is a given image represented as a r by c matrix of integer pixel intensities ranging from 0 to L − 1. L is the number of possible intensity values, usually 256, and pn denote the normalized histogram of image f [39].

5.2 Simulation Results for Real Channel Techniques

In this subsection, the simulation results as well as performance metrics measurements in the case of real channel will be depicted. The results for all three techniques will be demonstrated in the following figures and tables. The performance of each technique will be measured against various types of attacks as; salt and pepper noise, Gaussian noise, speckle noise, rotation by different degrees, and cropping as will be mentioned in the following few subsections.

5.2.1 Noise Attacks

Here we will present for simulation results and performance measurements for three techniques in which the encrypted image has been imposed to salt and pepper noise.

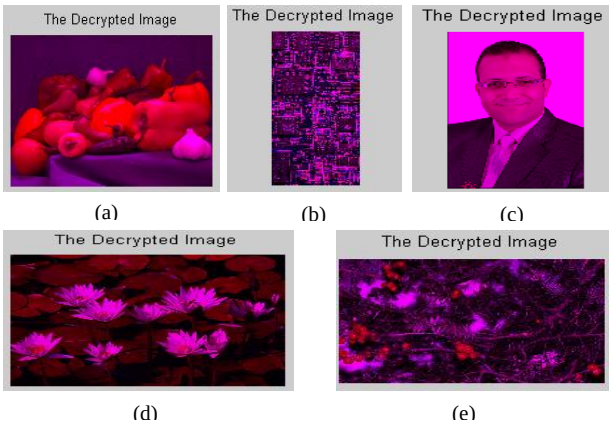

Fig 7: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using traditional or modified schemes

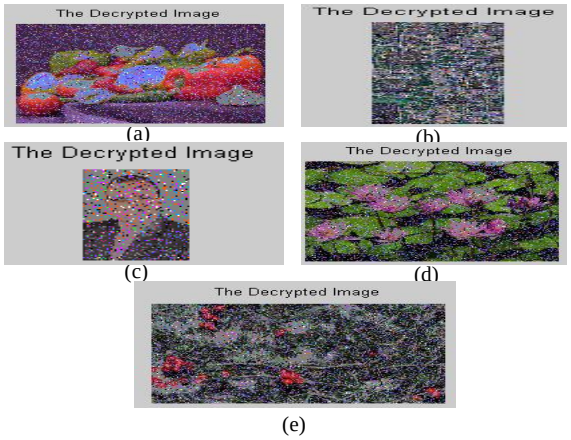

Fig 8: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using proposed technique

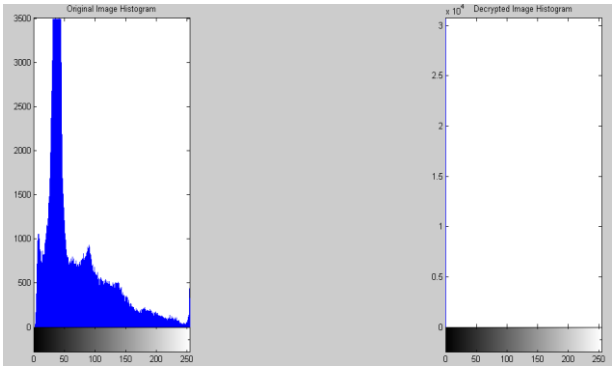

Fig 9: Histogram Analysis of image (1) for traditional or modified technique

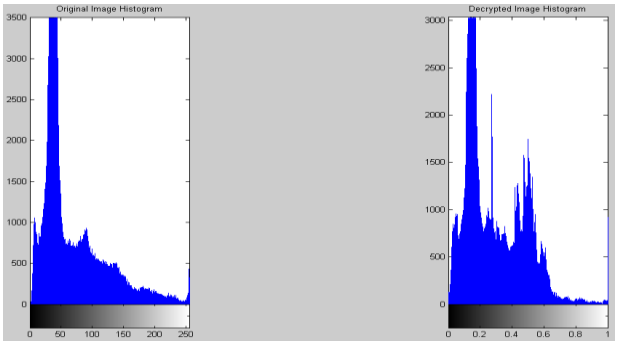

Fig 10: Histogram Analysis of image (1) for our proposed Technique

Table 2. Performance Metrics in Case of 10% Salt & Pepper Noise

Metrics	Traditional Technique	Modified Technique	Proposed Technique
Elapsed Time (Sec)	0.3082	0.9646	3.3424
Entropy of Decrypted Image	5.6491	0.4502	7.5516
MSE	1	0.998	0.0666
PSNR (dB)	9.6615	9.6692	59.8939
R	-0.0016	0.0031	0.6021

Table 3. Performance Metrics in Case of Gaussian Noise (mean=0, variance = 0.01)

Metrics	Traditional Technique	Modified Technique	Proposed Technique
Elapsed Time (Sec)	0.3439	1.0004	3.4275
Entropy of Decrypted Image	0.000097	0.5505	7.5057
MSE	1	0.997	0.0483
PSNR (dB)	9.6615	9.6717	61.2915
R	-0.0016	-0.0036	0.7946

The performance metrics for image (1) for all three techniques in case of different types of noise will be introduced in the following tables.

Table 4. Performance Metrics in Case of Speckle Noise (mean = 0, variance =0.4)

Metrics	Traditional Technique	Modified Technique	Proposed Technique
Elapsed Time (Sec)	0.3625	0.9685	3.3785
Entropy of Decrypted Image	0	0.5466	7.4687
MSE	1	0.997	0.0408
PSNR (dB)	9.6615	9.6715	62.0219
R	0	-0.0062	0.8010

From the previous tables, it is clearly found that our proposed technique has given great enhancement in performance than other traditional and modified techniques against various types of noise when imposed to encrypted image. This result can appear more obvious from the following figure.

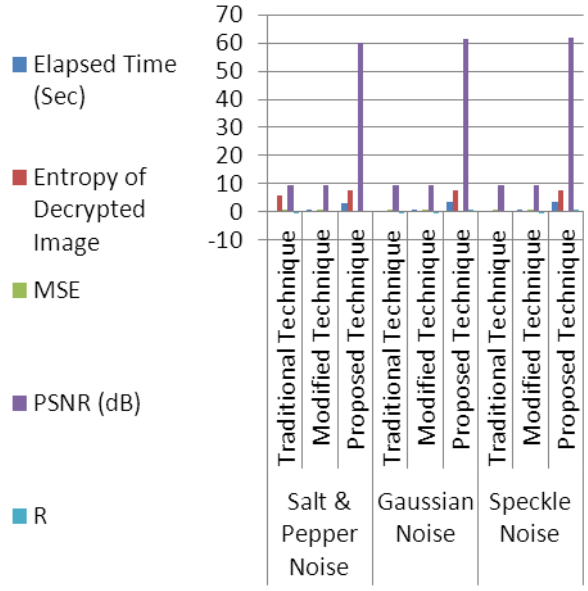

Fig 11: Performance Metrics of Image (1) against Different Types of Noise Attacks

5.2.2 Rotation by different degrees

One of the most famous attacks that must be taken into account is the rotation of the encrypted image by specific degree during transmission. In this paper the rotation of encrypted images by different degrees will be studied. The decrypted images for original images illustrated in Fig 5 will be observed for all three techniques in case of rotation by 10 degrees as an example. After that the performance metrics measurements will be introduced for image (1) through Excel graph that will be shown in Fig 15.

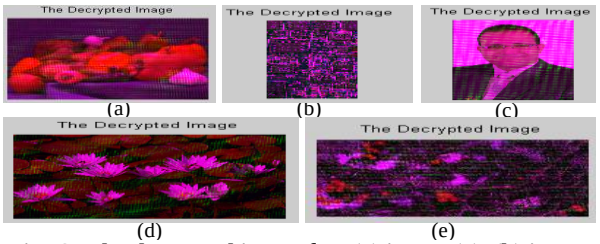

Fig 12: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using traditional scheme

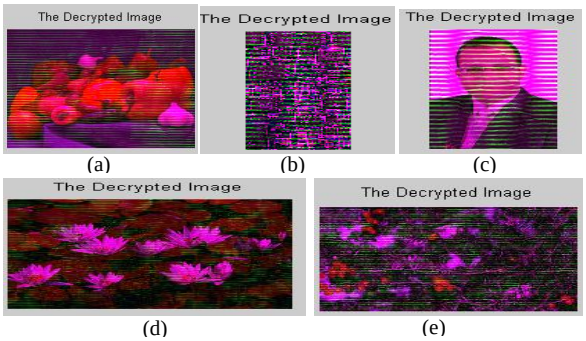

Fig 13: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using modified scheme

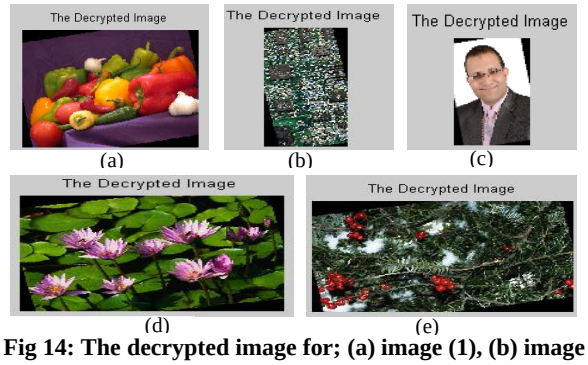

Fig 14: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using proposed scheme

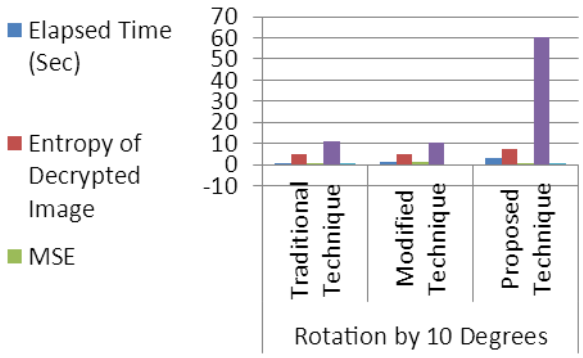

Fig 15: Performance Metrics of Image (1) against Rotation by 10 Degrees

From the previous figure, it is obviously noticed that our proposed technique stills the best robust scheme against not only noise attacks but also rotation attacks by different degrees. Until now our novel technique gives the minimum MSE, max PSNR, max entropy for decrypted image, and max cross correlation coefficient. Only the elapsed time doesn't belong to this result in which our proposed method gave slightly larger elapsed than other methods, but this can be ignored besides all other perfect measurements. The histogram analysis for original and decrypted image (1) for all three techniques is shown in the following figures.

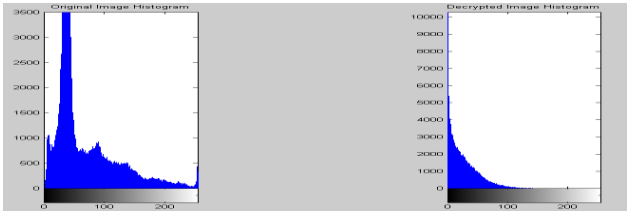

Fig 16: Histogram Analysis for image (1) using traditional technique against rotation by 10 degrees

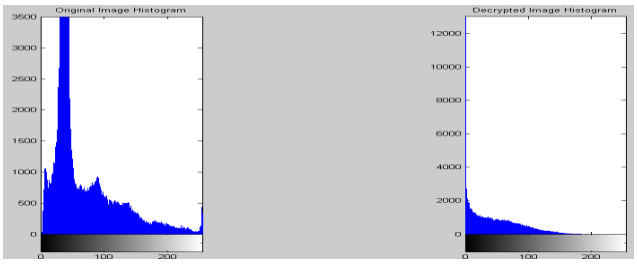

Fig 17: Histogram Analysis for image (1) using modified technique against rotation by 10 degrees

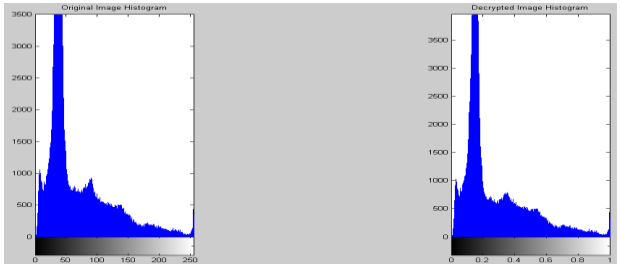

Fig 18: Histogram Analysis for image (1) using proposed technique against rotation by 10 degrees

5.2.3 Cropping Attacks

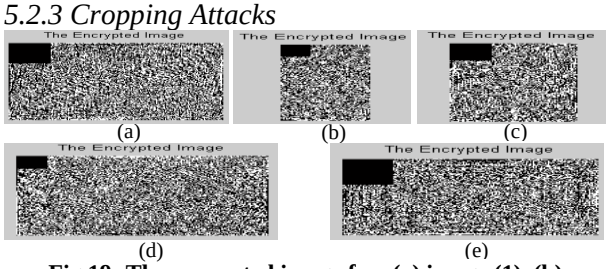

Fig 19: The encrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using traditional scheme

In this subsection, the simulation results as well as performance metrics measurements will be depicted for three techniques against cropping attack. Here a cropping of size 100 x 100 will be imposed to encrypted images during transmission.

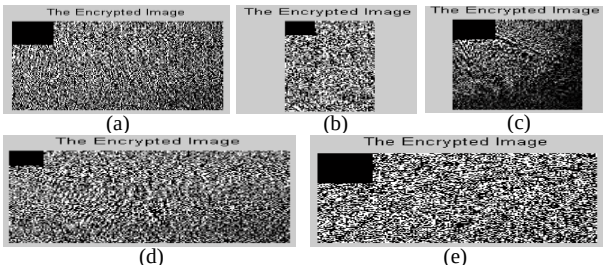

Fig 20: The encrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using modified scheme

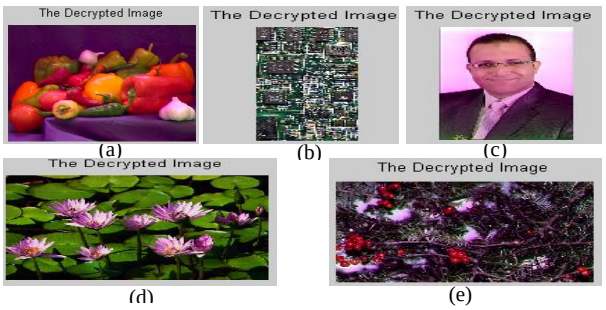

Fig 21: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using traditional scheme

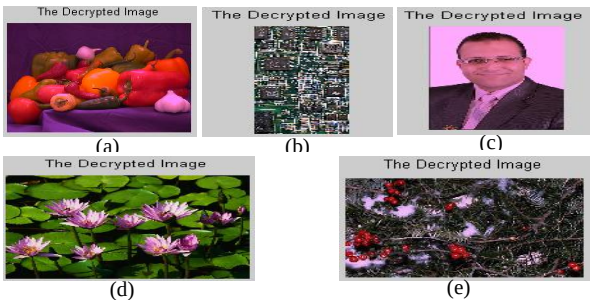

Fig 22: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using modified scheme

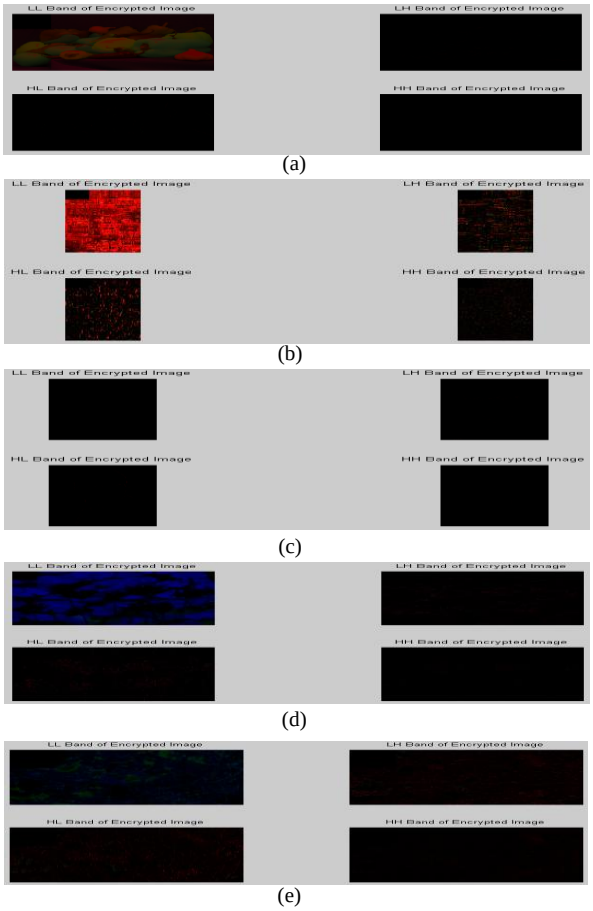

Fig 23: The encrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using proposed scheme

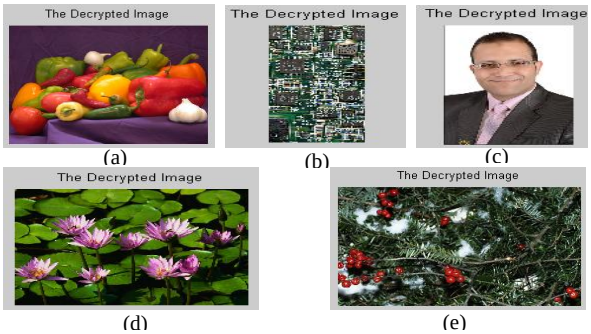

Fig 24: The decrypted image for; (a) image (1), (b) image (2), (c) image (3), (d) image (4), and (e) image (5) using proposed scheme

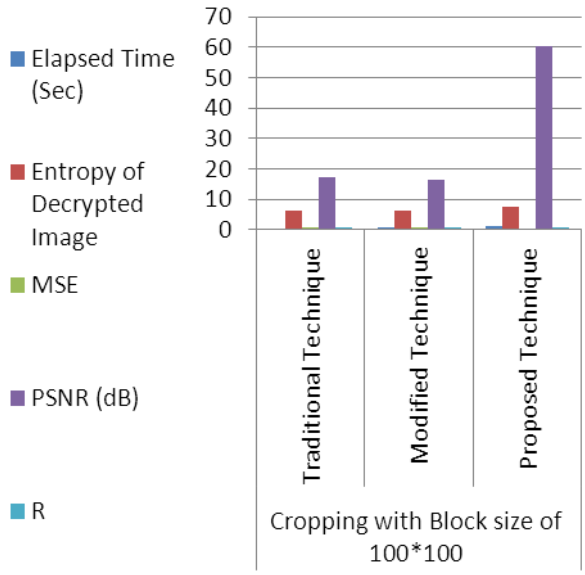

Fig 25: Performance Metrics of Image (1) against Cropping of Size 100*100

From the previous figures, it is obvious that our proposed technique has given better resolution for the decrypted images against cropping of the encrypted images. The performance metrics for image (1) in case of cropping attacks has been illustrated in Fig 25. The effectiveness of our proposed technique against cropping of encrypted image could be noticed from that figure except for elapsed time measurements. Now we will present for the histogram of the original as well as decrypted images for image (1) as an example to study histogram analysis for all three methodologies.

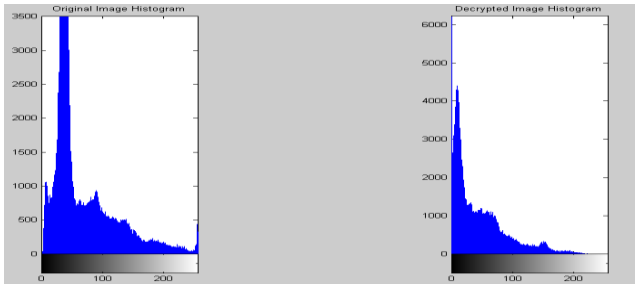

Fig 26: Histogram Analysis for image (1) using traditional technique against cropping

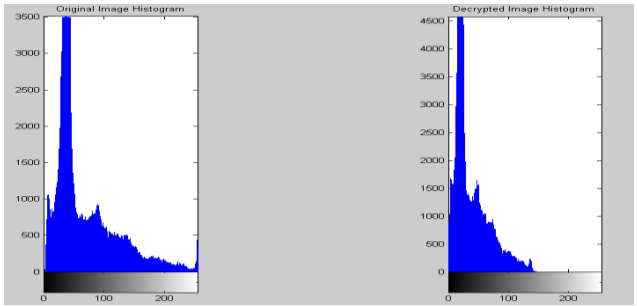

Fig 27: Histogram Analysis for image (1) using modified technique against cropping

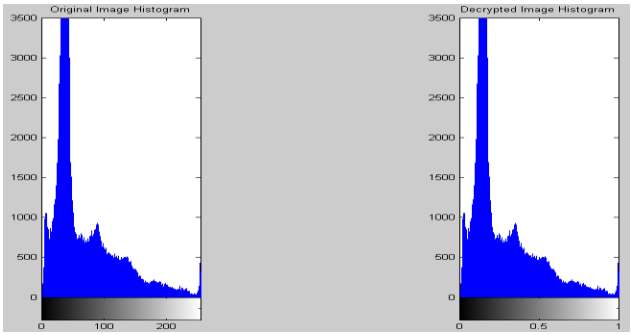

Fig 28: Histogram Analysis for image (1) using proposed technique against cropping

Again we could find from the previous figures that our proposed technique has given the best histogram matching between the plain and decrypted images.

6. CONCLUSIONS

The main problem in this paper was to get a reasonable optical encryption technique robust to various types of attacks. Three optical color images encryption techniques have been introduced: (i) traditional; based on FFT; (ii) modified; based on DCT, and (iii) proposed; based on DWT. All of these techniques have been applied on five different images with various extensions and dimensions in the case of real channel system. As a result of the extensive simulation study, it was found that the proposed technique provided superior performance with respect to the two other techniques in all performance metrics except the elapsed time against all different types of attacks. The first technique; FFT based DRPE, has given the least elapsed time due to the reduction of multiplication processes that are executed through Fourier Transform. So to achieve high robustness with slightly increasing in elapsed time, we advise to use our proposed technique; DWT based DRPE. In the future the proposed technique can be implemented using suitable hardware platform as Field Programmable Gate Array (FPGA).

7. REFERENCES

[1] A. Alfalou and C. Brosseau, "Optical Image Compression and Encryption Methods," Adv. Opt. Photon, Vol.1, hal-00516980, pp: 589-636, 2010.

[2] M. A. Mohamed, A.S. Samarah, and M.I. Fath Allah, "Optical Encryption Techniques: An Overview," International Journal for Computer Science Issues (IJCSI), Vol. 11, Issue 4, No. 2, pp: 125-129, 2014.

[3] F. Mosso and M. Tebaldi, "All-Optical Encrypted Movie," Optical Society of America, Vol. 19, No. 6, pp: 5706-5712, 2011.

[4] N. K. Neshchal and T. J. Naughton, "Flexible Optical Encryption with Multiple Users and Multiple Security Levels," ELSEVIER, Optics Communication 284, pp:735-739, 2011.

[5] A. Carnicer, M. Montes-Usategui, S. Arcos, I. Juvells, Opt. Lett. 30 (2005) 1644.

[6] G. Situ, G. Pedrini, W. Osten, Appl. Opt. 49 (2010) 457.

[7] Y. Liu, J. Lin, J. Fan, and N. Zhou, "Image Encryption Based on Cat Map and Fractional Fourier Transform," Journal of Computational Information Systems 8:18, pp: 7485:7492, 2012.

[8] P. R´efr´egier and B. Javidi, "Optical Image Encryption Based on Input Plane and Fourier Plane Random Encoding," Optics. Letters., Vol. 20, pp: 767-769, 1995.

[9] M. V. Kanchana and V. K. Annapurna, "An Enhanced VCS of Image Encryption using SDS Algorithm without Secret Keys," International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), Vol. 2, Issue 7, pp: 1794-1798, 2014.

[10] X. Li, C. Li, S. T. Kim, and I. K. Lee, "An Optical Image Encryption Scheme Based on Depth Conversion Integral Imaging and Chaotic Maps," arXiv: 1501. 04167v1 [cs. CR], pp: 1-18, 2015.

[11] Y.-L. Lee and W. H. Tsai, "A New Secure Image Transmission Technique via Secret-Fragment-visible Mosaic Images by Nearly Reversible Color Transformations," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 24, No. 4, pp: 695-703, 2014.

[12] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-Gray Code for Image Systems," IEEE Transactions on Cybernetics, Vol. 43, No. 2, pp: 515-529, 2013.

[13] C. Li and K.T. Lo, "Optimal Quantitative Cryptanalysis of Permutation-only Multimedia Ciphers Against Plain-text Attacks," Signal Processing, Vol. 91, No. 4, pp: 949-954, 2011.

[14] Z. Shao, H. Shu, J. Wu, and Z. Dong, "Double Color Image Encryption using Iterative Phase Retrieval Algorithm in Quaternion Gyrator Domain," Optics Express, inserm-00951570, Version 1, 2014.

[15] X. L. Wang, H. C. Zhai, Z. L. Li, and Q. Ge, “Double Random-Phase Encryption based on Discrete Quaternion Fourier-Transforms,” Optik 122(20), pp: 1856-1859, 2011.

[16] Z. H. Shao, J. S. Wu, J. L. Coatrieux, G. Coatrieux, and H. Z. Shu, “Quaternion Gyrator Transform and its Application to Color Image Encryption,” in Proceedings of IEEE International Conference on Image Processing (Institute of Electrical and Electronics Engineers, New York, pp: 4579-4582, 2013.

[17] G. H. Situ, and J. J. Zhang, “Multiple-Image Encryption by Wavelength Multiplexing,” Opt. Lett. 30(11), pp: 1306-1308, 2005.

[18] Y. S. Shi, G. H. Situ, and J. J. Zhang, “Multiple-Image Hiding in the Fresnel Domain,” Opt. Lett. 32(13), pp: 1914-1916, 2007.

[19] H. Hwang, H. T. Chang, and W. Lie, “Multiple-image Encryption and Multiplexing using a Modified Gerchberg-Saxton Algorithm and Phase Modulation in Fresnel-Transform Domain,” Opt. Lett. 34(24), pp: 3917-3919, 2009.

[20] H. T. Chang, H. Hwang, and C. Lee, “Position Multiplexing Multiple-image Encryption using Cascaded Phase-only Masks in Fresnel Transform Domain,” Opt. Commun. 284(18), pp: 4146-4151, 2011.

[21] H. T. Chang, H. E. Hwang, C. L. Lee, and M. T. Lee, “Wavelength Multiplexing Multiple-image Encryption using Cascaded Phase-only Masks in The Fresnel Transform Domain,” Appl. Opt. 50(5), pp: 710-716, 2011.

[22] A. Alfalou and A. Mansour, "Double Random Phase Encryption Scheme to Multiplex and Simultaneous Encode Multiple Images," Appl. Opt. 48(31), pp: 5933-5947, 2009.

[23] X. P. Deng and D. M. Zhao, "Multiple-Image Encryption using Phase Retrieve Algorithm and Intermodulation in Fourier Domain," Opt. Laser Technol. 44(2), pp: 374-377, 2012.

[24] X. G. Wang and D. M. Zhao, "Fully Phase Multiple-image Encryption Based on Superposition Principle and The Digital Holographic Technique," Opt. Commun. 285, pp: 4280-4284, 2012.

[25] L. S. Sui, M. T. Xin, and A. L. Tian, "Multiple-image Encryption Based on Phase Mask Multiplexing in Fractional Fourier transform domain," Opt. Lett. 38(11), PP: 1996-1998, 2013.

[26] D. Z. Kong, X. J. Shen, Q. Z. Xu, W. Xin, and H. Q. Guo, "Multiple-image Encryption Scheme Based on Cascaded Fractional Fourier transform," Appl. Opt. 52(12), pp: 2619-2625, 2013.

[27] R. Tao, Y. Xin, and Y. Wang, "Double Image Encryption Based on Random Phase Encoding in The Fractional Fourier Domain," Opt. Express 15(24), pp: 16067-16079, 2007.

[28] Z. J. Liu and S. T. Liu, "Double Image Encryption Based on Iterative Fractional Fourier Transform," Opt. Commun. 275(2), pp: 324-329, 2007.

[29] Z. J. Liu, J. M. Dai, X. G. Sun, and S. T. Liu, "Triple Image Encryption Scheme in Fractional Fourier Transform Domains," Opt. Commun. 282(4), pp: 518-522, 2009.

[30] J. H. Wu, X. Z. Luo, and N. R. Zhou, "Four-image Encryption Method Based on Spectrum Truncation, Chaos and the MODFrFT," Opt. Laser Technol. 45, pp: 571-577, 2013.

[31] M. Joshi, C. Shakher, and K. Singh, "Color Image Encryption and Decryption for Twin Images in Fractional Fourier Domain," Opt. Commun. 281(23), pp: 5713-5720, 2008.

[32] M. Joshi, C. Shakher, and K. Singh, "Fractional Fourier Transform Based Image Multiplexing and Encryption Technique for Four-color Images using Input Images as Keys," Opt. Commun. 283(12), pp: 2496-2505, 2010.

[33] Z. J. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. T. Liu, "Double Image Encryption by Using Iterative Random Binary Encoding in Gyrator Domains," Opt. Express 18(11), pp: 12033-12043, 2010.

[34] H. J. Li and Y. R. Wang, "Double-image Encryption Based on Iterative Gyrator Transform," Opt. Commun. 281(23), pp: 5745-5749, 2008.

[35] Q. A. Kester, "Image Encryption based on The RGB Pixel Transposition and Shuffling," I. J. Computer Network and Information Security DOI: 10.5815/ijcnis.2013.07.05, pp: 43-50, 2013.

[36] Z. Liu and H. Chen, "Color image encryption by using Arnold Transform and Color-blend Operation in Discrete Cosine Transform Domains," Optics Communications 284 (2011), pp: 123–128, 2015.

[37] X. Deng and X. Zhu, "A Simple and Practical Color Image Encryption with the Help of QR Code," Optica Applicata, Vol. XLV, No. 4, pp: 513-521, 2015.

[38] M. A. Mohamed, H. M. Abdel-Atty, A. M. Abutaleb, M. G. Abdel-Fattah, and A. S. Samrah, "Hybrid Watermarking Scheme for Copyright Protection Using Chaotic Maps Cryptography," International Journal of Computer Applications (0975 – 8887), Vol. 128, No. 1, pp: 1:14, 2015.

[39] R. C. Gonzalez and R. E.Woods, "Digital Image Processing," Third Edition, 2008.