Image Cryptosystem Based on Digital Signature and Double Random Phase Encoding

HAYAM ABDEl-MORDY[1], EMAD S. HASSAN[1,2], SAMI A. El-DOLIL[1], AND FATHI E. ABD El-SAMIE[1]

[1]Dept. of Electronics and Electrical Communications
Menoufia University
Faculty of Electronic Engineering, Menouf, 32952
EGYPT

[2]Dept. of Electrical Engineering
Jazan University
JAZAN
SAUDI ARABIA

hayamabdalmordy@yahoo.com, emad.hassan@el-eng.menofia.edu.eg, msel_dolil@yahoo.com, fathi_sayed@yahoo.com.

Abstract: - This paper presents a new technique of multi-level security for image transmission based on image signature by Discrete Cosine Transform (DCT2) and image encryption by Double Random Phase Encoding (DRPE). This technique is implemented in two successive steps to enhance the security level of the transmitted image. The proposed technique exploits the benefits of signature and encryption, which make it robust to image processing attacks such as speckle, impulsive and Gaussian noise. Several experiments have been carried out to test the performance of the proposed technique in the terms of Peak Signal-to-Noise Ratio (PSNR), processing time and correlation coefficients. The obtained results show that, the proposed technique enhances the security level of the transmitted images with better immunity to noise when compared to stand-alone signature or DRPE.

Key-Words: - Digital image signature, Discrete Cosine Transform (DCT), Image encryption, Double Random Phase Encoding (DRPE).

1 Introduction

Recently, the interest in digital communications has increased rapidly, and its influence on our advanced electronic world has grown largely. Thus, the security of information must be increased and multi-level security systems are has become badly needed. The problem with images is more serious as digital images are attacked through transmission via the Internet or other communication media. To guarantee trustworthiness and security for image transmission, image authentication techniques have been proposed to confirm content integrity and prevent forgery attacks [1-5]. These techniques need to be robust to image processing and transmission errors, while being able to detect noise and attacks on the images. Digital signature and encryption techniques are the most famous techniques that provide security to image transmission [1-12].

Digital signature provides secure methods for image transmission [1-4], where it protects the copyright information of the users, and provides also high resistance to image processing. Digital signature is the process of embedding information into digital media such as images (binary, gray-scale or color), audio, and video by using any type of transforms. The most famous and favourite transform is the discrete cosine transform (DCT2) [4]. Based on the simplicity of the DCT and its energy compaction property, it will be chosen for signature in this paper.

Several encryption techniques have been proposed during past decades [5-12]. However, any cryptosystem is claimed to be secure only if it is able to endure attacks. Much effort has been exerted to enhance encryption. One of the most popular encryption techniques is the DRPE presented by Refregier and Javidi [13]. Encryption by DRPE is highly successful and is widely used [14-16]. It is implemented using two random phase masks. One mask is inserted in the input plane and the other in the Fourier plane to encrypt the image to a stationary white noise [13], [17]. At the receiver side to retrieve the original information, the encryption method and keys are required to be known. Without these keys, no one can get original image.

In this paper, we propose a new technique to improve the security of image transmission. The proposed technique is a hybrid technique that combines image signature by DCT and image encryption by DRPE. This technique can work on both the integrity protection for the images and the repudiation prevention for the sender. The combination of DCT and DRPE provides several advantages such as enhancement of the security level of the transmitted image, simplicity, high speed, and copyright protection. The proposed technique is implemented in two successive steps. The first step is to generate a digital signature on the original image with DCT. In the second step, encryption is performed with DRPE. The detection process of the proposed technique has to be robust to intentional and unintentional distortions. These distortions are called attacks [18]. The aim of these attacks is not always to destroy or remove the image. This distortion can introduce degradations in the system.

The rest of this paper is organized as follows. Section 2 explains the image signature using DCT2. Section 3 explains the DRPE process. Section 4 discusses the proposed technique. Section 5 presents the simulation results and discussion. Finally, Section 6 gives the concluding remarks.

2 The DCT Technique

The DCT is a general orthogonal transform for digital image / signal processing with several advantages such as energy compaction, good information integration ability, high compression ratio and good synthetic effect of calculation complexity [4]. One-dimensional DCT is described with the help of equations (1) and (2) [19]:

$$F(0)=\frac{1}{\sqrt{N}}\sum_{x=0}^{N-1} f(x) \tag{1}$$

$$F(u)=\sqrt{\frac{2}{N}}\sum_{x=0}^{N-1} f(x) Cos\frac{2(x+1)u\pi}{2N} \tag{2}$$

where $F(u)$ is the cosine transform coefficient, u is a general frequency variable, u =1, 2, 3…, N-1, N is the signal length, and $f(x)$ is the time-domain sequence, x = 1, 2, 3… N-1. the one-dimensional Inverse Discrete Cosine Transform (IDCT) is defined as [19]:

$$f(x)=\sqrt{\frac{1}{N}}F(u)+\sqrt{\frac{2}{N}}\sum_{x=0}^{N-1} F(u) Cos\frac{2(x+1)u\pi}{2N} \tag{3}$$

Two- dimensional DCT is defined analogously as:

$$f(x,y)=C(u)C(v)*\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} F(u,v)Cos[\frac{(2x+1)u\pi}{2N}]Cos[\frac{(2y+1)v\pi}{2N}] \tag{4}$$

The inverse of two- dimensional DCT is defined as:

$$f(u,v)=\frac{2}{N}C(u)C(v)*\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} F(x,y)Cos[\frac{(2x+1)x\pi}{2N}]Cos[\frac{(2y+1)y\pi}{2N}] \tag{5}$$

For x, y = 0, 1, 2… N −1, generally N = 8. If N is greater than 8, efficiency is increased a little but complexity is increased a lot [20]. The DCT allows the image block to be broken up into different frequency bands, namely the high, middle and low frequency bands. This makes it easier to choose the band in which the signature is to be inserted [21].

Many literature papers use the middle frequency bands for embedding signature, because embedding the signature in the middle frequency band does not scatter the information to most visual important parts of the image. The low frequencies are subject to removal through compression and noise attacks, where high frequency components are targeted [21]. The frequency bands of an 8 × 8 DCT block are shown in Fig. 1. The DCT block consists of three frequency bands: Low frequency band (F_L), High frequency band (F_H) and Mid frequency band (F_M).

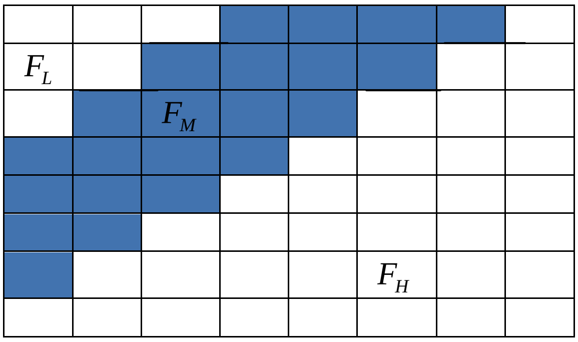


Fig. 1: DCT regions.

The DCT output for a block of size of 8 × 8 is shown in Fig. 2. This figure illustrates the 1st and 5th bands (enclosed with rectangles) [4].

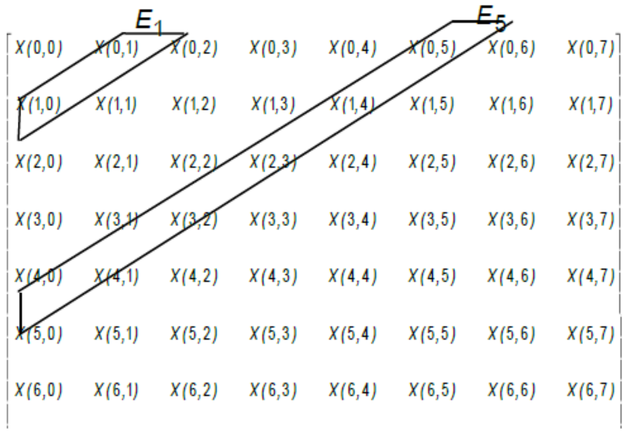

E1
E5
X(0,0) X(0,1) X(0,2) X(0,3) X(0,4) X(0,5) X(0,6) X(0,7)
X(1,0) X(1,1) X(1,2) X(1,3) X(1,4) X(1,5) X(1,6) X(1,7)
X(2,0) X(2,1) X(2,2) X(2,3) X(2,4) X(2,5) X(2,6) X(2,7)
X(3,0) X(3,1) X(3,2) X(3,3) X(3,4) X(3,5) X(3,6) X(3,7)
X(4,0) X(4,1) X(4,2) X(4,3) X(4,4) X(4,5) X(4,6) X(4,7)
X(5,0) X(5,1) X(5,2) X(5,3) X(5,4) X(5,5) X(5,6) X(5,7)
X(6,0) X(6,1) X(6,2) X(6,3) X(6,4) X(6,5) X(6,6) X(6,7)

Fig. 2: DCT output for a block of size 8×8.

3 Double Random Phase Encoding

The DRPE presented by Refregier and Javidi [13] is based on modification of the spectral distribution of the images. The DRP encryption scheme presents some weakness against attackers [22–24]. The image decoding cannot be done at the receiver without any prior information about the spectral modification or the target image. The main idea of this scheme is illustrated in Fig. 3.

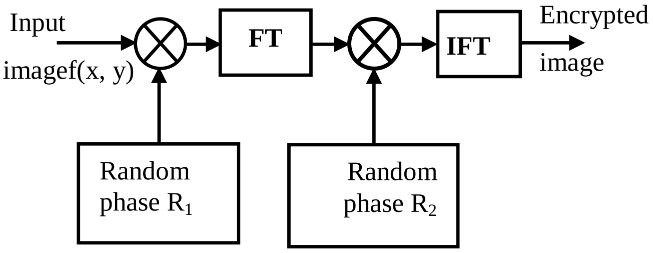


Fig. 3: DRPE encoding.

The input function *f*(*x*, *y*) denotes the original two-dimensional image to be encrypted, where *x* and *y* denote the space coordinates, the original image *f*(*x*, *y*) is multiplied by a random phase function $R_1(x, y)$ and is then Fourier transformed. In the next step, the Fourier transformed image is multiplied with another phase mask $R_2(u, v)$, which is independent of $R_1(x, y)$, where *u* and *v* the coordinates in the Fourier domain [25]. The two random phase functions $R_1(x, y)$ and $R_2(u, v)$ are used during the process of encryption as keys for data security during decryption. The inverse Fourier transform is performed on this image to get the encrypted image in space domain. In the decryption process, the encrypted image is Fourier transformed and then multiplied with the complex conjugate of $R_2(u, v)$. The obtained image is inverse Fourier transformed to get the decrypted image as shown in Fig. 4.

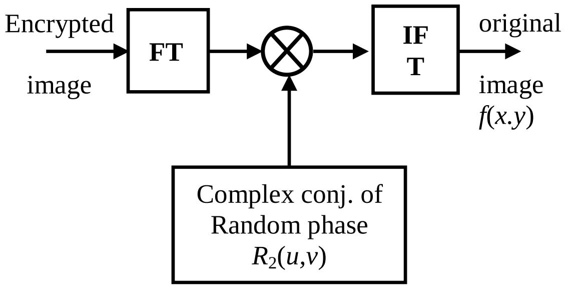


Fig. 4: DRPE decoding.

To explain the DRPE mathematically, let the encrypted image to be Ψ(*x*, *y*), and let *n*(*x*, *y*) and *m*(*x*, *y*) denote two independent sequences uniformly distributed in[0, 2*π*]. The two RPMs are $R_1(x,y)=\exp\big(2i\pi n(x,y)\big)$, and $R_2(x,y)=\exp(2i\pi m(x,y))$ are used to encode *f*(*x*,*y*) into a white stationary sequence. The encrypted function is complex, with magnitude and phase [26], and is given by:

$$\Psi(x,y) \;=\; \{f(x,y)R_1(x,y)\} * FT^{-1}\{R_2(u,v)\} \qquad (6)$$

where the symbol (*) denotes convolution. *h*(*x*, *y*) = *m*(*x*,*y*), which is a phase function uniformly distributed in [0, 2*π*]. Thus $R_2(u,v)$ is the Fourier transform of the function *h*(*x* ,*y*) given by:

$$FT\{h(x,y)\} = R_2(u,v) = \hat{h}\,(u,v) = \exp[2i\pi m(u,v)] \qquad (7)$$

In the decryption process, the encrypted image Ψ(*x*, *y*) is Fourier transformed and then multiplied by the conjugate of $R_2(u, v)$, and the result is inverse Fourier transformed. The output is given by:

$$\begin{aligned} &FT^{-1}\{FT[\Psi(x,y)]R_2^*(u,v)\} \\ &= FT^{-1}\{FT[f(x,y)R_1(x,y)]R_2(u.v)R_2^*(u,v)\} \\ &= f(x,y)R_1(x,y) \qquad (8) \end{aligned}$$

The absolute value of the output gives the decrypted image *f*(*x*, *y*).

4 The Proposed Multi-Level Security Technique

The proposed technique achieves multi-level security based on applying encryption using DRPE on the image with signature. We use DCT for signature embedding. In our work, the signature means embedding some information about a part or parts of the image into another part or parts. The proposed technique exploits the benefits of signature and encryption showing robustness to image degradations. The hacking becomes harder as the RPMs are new factors introduced into the security. In addition, the proposed technique leads to complete reconstruction of the transmitted images.

The steps of the proposed technique are shown in figure 5 and listed below:

1. Read the original image.
2. Divide original image into two similar parts.
3. Break each part in this image into 8×8 block of pixels.
4. Apply DCT to each block.
5. Replace the last column/row in each block of the first part by the last column/row in the corresponding block of the second part in the image, and vice versa.
6. After replacement, apply IDCT to each block.
7. Multiply the obtained image with signature by a random phase function $R_1(x, y)$ as shown in Fig. 3.
8. Apply Fourier transform on the resulting image.
9. Multiply the Fourier transformed image with the second phase mask $R_2\ (u, v)$.
10. Apply Inverse Fourier transform.

The steps to retrieve original image are shown in figure 6 and listed below:

1. Apply Fourier transform on the encrypted image as in Fig. 4.
2. Multiply the resulting image with the complex conjugate of $R_2\ (u,v)$.
3. Apply Inverse Fourier transform to the obtained image to get the decrypted image with signature.
4. Break the image with signature to 8×8 blocks of pixels
5. Apply DCT to each block.
6. Calculate correlation coefficients for the extracted columns and rows with their corresponding ones.

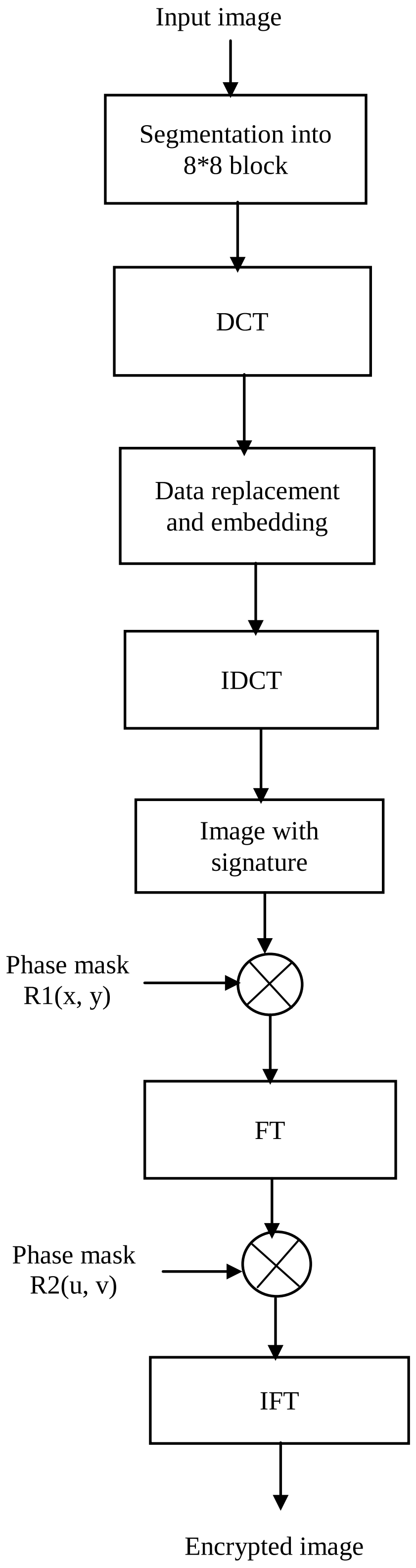


Fig. 5: Block diagram of the proposed technique.

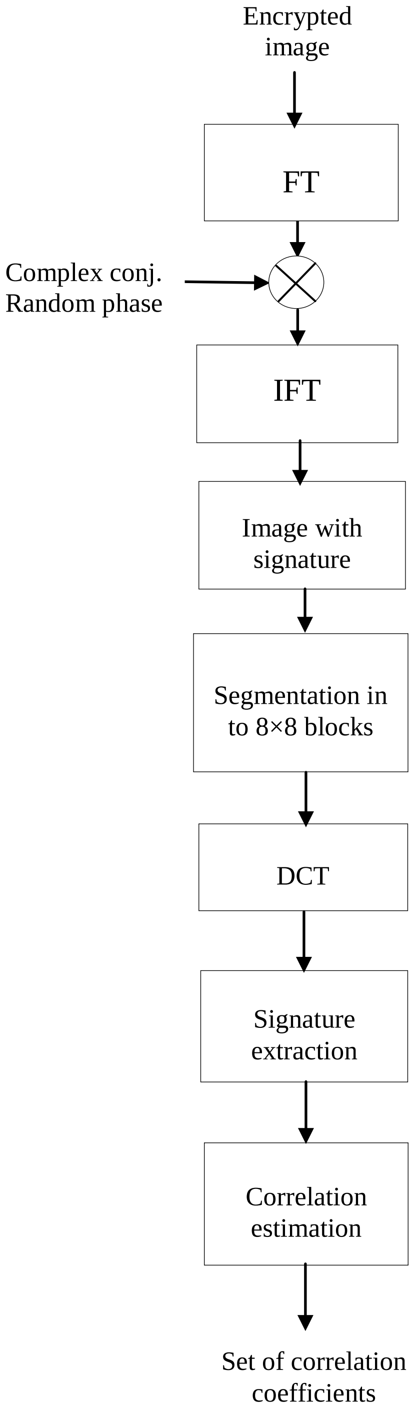


Fig. 6: Block diagram of signature verification.

5 Simulation Results and Discussion

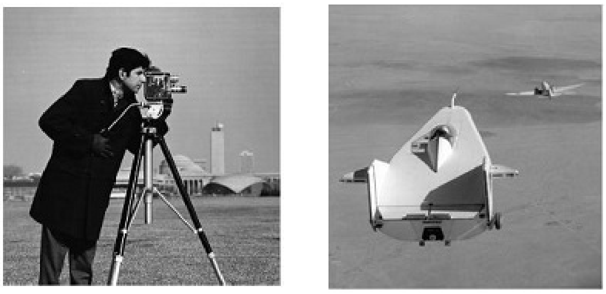
Several experiments have been carried out to test the performance of the proposed technique. Three different metrics have been utilized for quality assessment. The first metric is the PSNR, which is used to measure the quality of the reconstructed images at the receiver to guarantee that the image is not distorted. The PSNR for an image with size N x N is expressed as follows in eq.(9) [27-28].

$$PSNR = 10Log_{10} \frac{255^2}{\frac{1}{N \times N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}(f(x,y) - \psi(x,y))^2} \tag{9}$$

The second metric is the correlation coefficient between extracted rows or columns representing the embedded signatures and their corresponding ones. The third metric is the processing time.

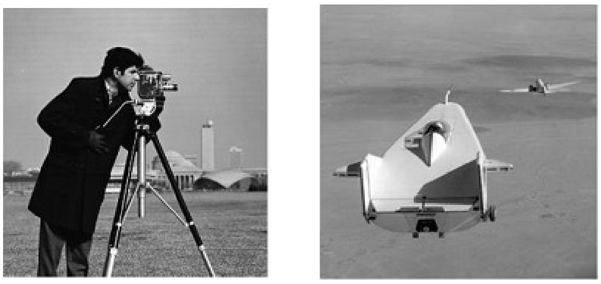
Matlab simulation has been carried out to test the performance of the proposed multi-level security technique in the absence of attacks. Figures (7) to (10) show the results of these experiments on two images; Cameraman and Plane images as shown in Fig. 7(a & b). The original images are signature firstly using DCT2 as shown in Fig. 8 (a & b). Secondly signature images are encrypted using DRPE as shown in Fig. 9(a & b). The encrypted images with signature are tested with some typical attacks such as salt & pepper noise, speckle noise and Gaussian white noise of variances 0.02, 0.05 and 0.08 are shown in table (3), (4) and (5), respectively.

The results in these figures ensure that the proposed technique is reversible in the absence of attacks. Comparative analysis of PSNR for signature, encryption and proposed technique without noise are shown in table (1) which explain that Encryption values are so different from the other techniques because images are totally encrypted and there details are disappeared but signature enter the images without masking features. Comparative analysis of processing time for signature, encryption and proposed technique are shown in table (2) ensure that, the complexity resulting from adding DRPE to signature in the proposed technique is slight. The results in Tables (3) to (5) show the effect of different types of noise on the performance of the proposed multi-level security systems. These results ensure the robustness to noise. Tables (6) and (7) show the probability distributions of estimated correlation coefficient values for rows and columns in the presence and absence of noise. These results clarify the possibility to detect the existence of signatures even in the presence of noise.



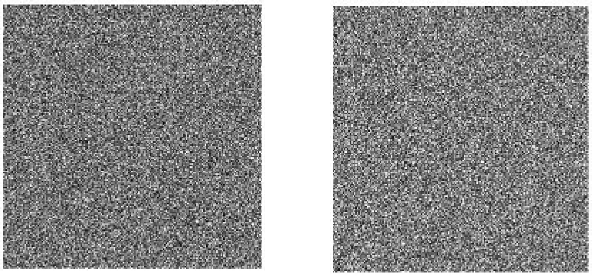
(a) (b)

Fig 7: Original images, (a) Cameraman, and (b) Plane.



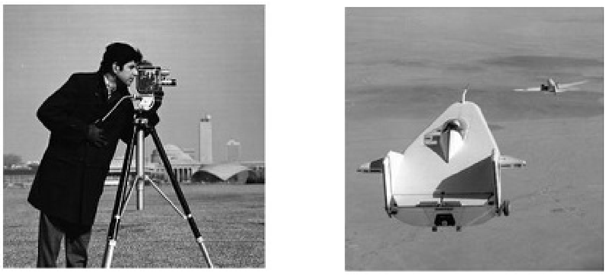
(a) (b)

Fig 8: Images with signature for (a) Cameraman, and (b) Plane.



(a) (b)

Fig 9: Encrypted images for (a) Cameraman, and (b) Plane.



(a) (b)

Fig 10: Decrypted images for (a) Cameraman, and (b) Plane.

5 CONCLUSION

This paper presented an efficient multi-level security system for image communication. This system employs digital signature with the DCT and DRPE. Simulation results have proved that the system is reversible. In addition, the system is robust to the presence of different types of noise, and the processing time is acceptable.

Table 1: PSNR values in dB for signature, encryption, and proposed technique without noise.

	Signature	**Encryption**	**Proposed**
Cameraman	35.33	311.34	35.48
Plane	45.8	310.70	45.82

Table 2: Processing time values in sec for signature, encryption, and proposed technique.

	Signature	**Encryption**	**Proposed**
Cameraman	2.05	0.50	2.50
Plane	2.50	0.68	2.84

Table 3: PSNR values in dB for signature, encryption, and proposed technique with noise of variance 0.02.

		Signature	**Encryption**	**Proposed**
Cameraman	Gaussian	5.64	10.38	10.35
	Salt & pepper	5.64	10.55	10.56
	Speckle	5.64	10.67	10.64
Plane	Gaussian	5.03	13.14	13.17
	Salt & pepper	5.04	13.46	13.51
	Speckle	5.03	13.52	13.55

Table 4: PSNR values in dB for signature, encryption, and proposed technique with noise of variance 0.05.

		Signature	**Encryption**	**Proposed**
Cameraman	Gaussian	5.63	10.04	10.05
	Salt&pepper	5.64	10.46	10.44
	Speckle	5.63	10.56	10.56
Plane	Gaussian	5.03	12.66	12.74
	Salt& pepper	5.04	13.26	13.33
	Speckle	5.03	13.33	13.37

Table 5: PSNR values in dB for signature, encryption, and proposed technique with noise of variance 0.08.

		Signature	**Encryption**	**Proposed**
cameraman	Gaussian	5.63	9.81	9.80
	Salt&pepper	5.64	10.34	10.35
	Speckle	5.63	10.47	10.44
Plane	Gaussian	5.03	12.33	12.37
	Salt & pepper	5.03	13.04	13.14
	Speckle	5.03	13.21	13.21

Table 6: Correlation coefficient PDFs in the case of Cameraman image.

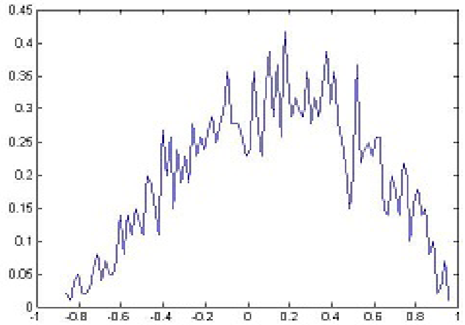
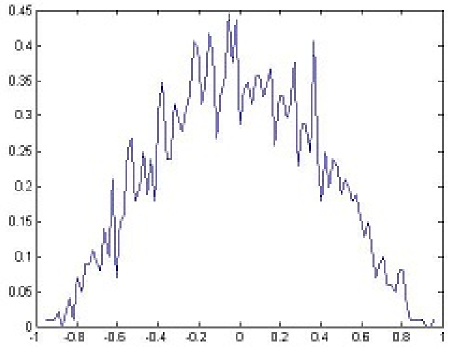
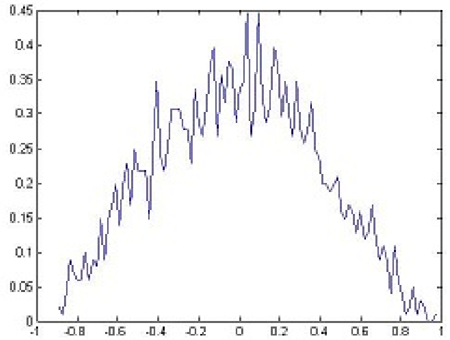
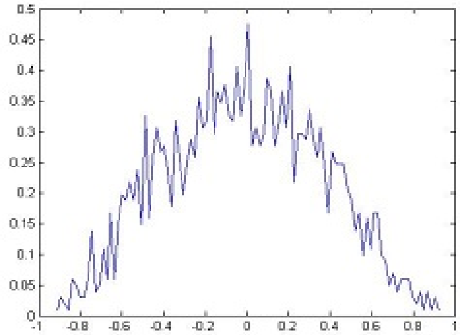
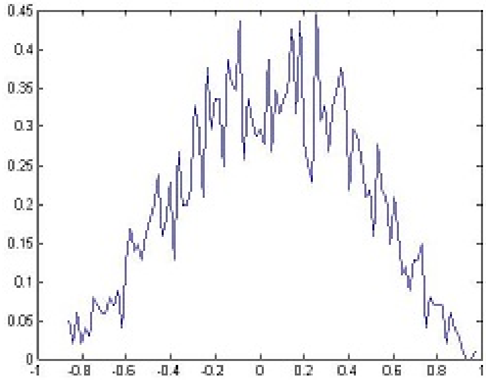
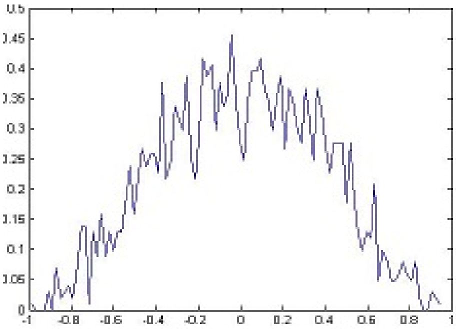
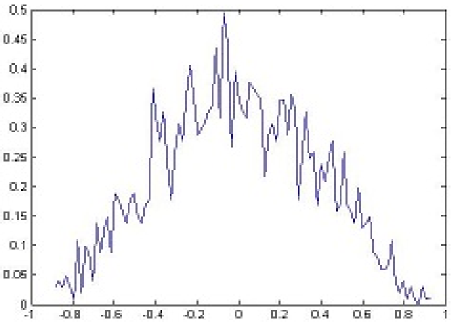
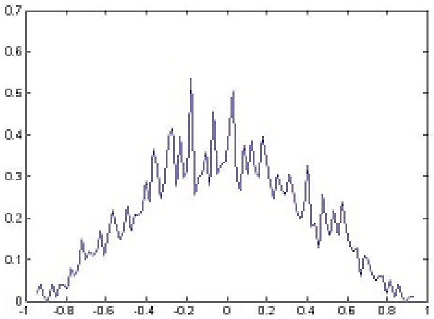
	Proposed algorithm with DCT signature and DRPE
No attack	
Salt& Pepper	
Speckle noise	
Gaussian noise	

Table 7: Correlation coefficient PDFs in the case of Plane image.

	Proposed algorithm with DCT signature and DRPE
No attack	
Salt & pepper	
Speckle noise	
Gaussian noise	

References

[1] J Sravanthi, Dr. MHM Krishna Prasad, “Robust and secure digital signature for image authentication over wireless channels", International Journal of Computer Trends and Technology, pp.245-250, 2011.

[2] SEITZ J., Digital watermarking for digital media, (Idea Group Publishing, 2005), Ch. 2.

[3] Schneider M., Chang S.-F., A content based digital signature for image authentication, Proc. IEEE Int. Conf. Image Processing (ICIP’96), 1996, pp. 227–230.

[4] Hayam A. Abdelhameed, Emad S. Hassan, Sami A. El-Dolil, and F.E. Abd El-Samie “ A Discrete Cosine Transform (DCT) based Watermarking Scheme for Confidence Guarantee Image Transmission,” Digital Image Processing, vol. 6, no. 3, pp. 131-138, 2014**.**

[5] G. H. Situ and J. Zhang, “Double random-phase encoding in the Fresnel domain,” Opt. Lett., vol. 29, pp. 1584-1586, July 2004.

[6] G. Unnikrishnan and K. Singh, “Double random fractional Fourier domain encoding for optical security,” Opt. Eng., vol. 39, pp. 2853-2859, November 2000.

[7] J. W. Han, C. S. Park, D. H. Ryu, and E. S. Kim, “Optical image encryption based on XOR operations,” Opt. Eng., vol. 38, pp. 47-54, January 1999.

[8] P. K. Wang, L. A. Watson, and C. Chatwin, “Random phase encoding for optical security,” Opt. Eng., vol. 35, pp. 2464-2469, September 1996.

[9] Y. Li, K. Kreske, and J. Rosen, “Security and Encryption Optical Systems Based on a Correlator with Significant Output Images,” Appl. Opt., vol. 39, pp. 5295-5301, October 2000.

[10] N. Towhgi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” J. Opt. Soc. Am. A, vol. 16, pp. 1915-1927, August 1999.

[11] T. Nomura and B. Javidi, “Optical encryption using a joint transform correlator architecture,” Opt. Eng., vol. 39, pp. 2031-2034, August 2000.

[12] X. F. Meng, L. Z. Cai, and X. L. Yang, “Information security system by iterative multiple-phase retrieval and pixel random permutation,” Appl. Opt., vol. 45 pp. 3289-3297, May 2005.

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

[14] G. Unnikrishnan, J. Joseph and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain,” Opt. Lett., vol.25, pp. 887–889, December 2000.

[15] F.M. Liu, H.C. Zhai and X.P. Yang, “Kino form-based iterative random phase encryption,” Acta. Phys., Sin.52, pp.2462–2465, October 2003 (in Chinese).

[16] X.P. Yang and H.C. Zhai, “Optimization of kino form in double-random-phase encryption,” Acta. Phys., Sin.54, pp. 1578–1582, April 2005 (in Chinese).

[17] B.Javidi, A.Sergent, G.Zhang, and L.Guibert,“Fault tolerance properties of a double phase encoding encryption technique,” Opt. Eng., vol. 36, pp. 992–998, 1997.

[18] Xiaojun Qi and KokSheik Wong, “An Adaptive DCT-Based MOD-4 Steganography Method**”,** Proceedings of the IEEE, pp.7803-9134, 2005.

[19] Blossom Kaur, Amandeep Kaur, Jasdeep Singh,“Steganographic approach for hiding image in DCT domain**”**, International Journal of Advances in Engineering & Technology, ISSN: 2231-1963, Vol. 1, Issue 3, pp.72-78, , July 2011.

[20] Frank Hartung and Martin Kutter, “Multimedia Watermarking Techniques”, Proceedings of the IEEE, Vol. 87, No. 7, July 1999.

[21] LOU D.C., LIU J.L. and LI C.-T.: ‘Digital Signature-Based Image Authentication’, in LU C.S. (EDS.):‘Multimedia security: steganography and digital watermarking techniques for protection of intellectual property’ (Idea Group Inc., 2003)**.**

[22] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” Opt. Express, vol.15, pp.10253–10265, (2007).

[23] A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, “Vulner ability to chosen-cypher text attacks of optical encryption schemes based on double random phase keys,” Opt. Lett., Vol.30, pp.1644–1646, (2005).

[24] X. Peng, P. Zhang, H. Wei, and B. Yu, “Known-plaintext attack on optical encryption based on double random phase keys,” Opt. Lett., Vol.31, pp.1044–1046, (2006).

[25] Karuna Kesavan K and Ratheesh kumar M," Optical color image encryption based on Hartley transform and double random phase encoding system,"7-77- 8111- pp.963-978

[26] Ahmed M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragalla, Yi Mu, Saleh A. Alshebeili, and F. E. Abd El-Samie "optical image encryption based on chaotic baker map and double random phase encoding", Journal of light wave technology IEEE, vol. 31, no. 15, pp. 0733-8724, August 2013.

[27] E. M. El-Bakary, E. S. Hassan, O. Zahran, S. A. El-Dolil, and F. E. Abd El-Samie “Efficient image transmission with multi-carrier CDMA”, wireless personal Commu. , DOI 10.1007/s11277-012-0622-6. 2012.

[28] E. S. Hassan, “Performance Enhancement of Continuous-Phase Modulation Based OFDM Systems Using Chaotic Interleaving”, WSEAS Transactions on Systems, vol. 12, no. 1, pp. 1-10, Jan. 2013.