1-1-2013

Optical image encryption based on chaotic baker map and double random phase encoding

Ahmed M. Elshamy
Menoufia University, Egypt

Ahmed N. Z Rashed
Menoufia University, Egypt

Abd El-Naser A. Mohamed
Menoufia University, Egypt

Osama S. Faragalla
Menoufia University, Egypt

Yi Mu
University of Wollongong, ymu@uow.edu.au

See next page for additional authors

Recommended Citation

Elshamy, Ahmed M.; Rashed, Ahmed N. Z; Mohamed, Abd El-Naser A.; Faragalla, Osama S.; Mu, Yi; Alshebeili, Saleh A.; and El-Samie, F E Abd, "Optical image encryption based on chaotic baker map and double random phase encoding" (2013). *Faculty of Engineering and Information Sciences - Papers: Part A*. 1583.
https://ro.uow.edu.au/eispapers/1583

Optical image encryption based on chaotic baker map and double random phase encoding

Abstract

This paper presents a new technique for optical image encryption based on chaotic Baker map and Double Random Phase Encoding (DRPE). This technique is implemented in two layers to enhance the security level of the classical DRPE. The first layer is a pre-processing layer, which is performed with the chaotic Baker map on the original image. In the second layer, the classical DRPE is utilized. Matlab simulation experiments show that the proposed technique enhances the security level of the DRPE, and at the same time has a better immunity to noise.

Keywords

encoding, phase, random, double, image, map, optical, baker, chaotic, encryption

Disciplines

Engineering | Science and Technology Studies

Publication Details

Elshamy, A. M., Rashed, A. N. Z., Mohamed, A. A., Faragalla, O. S., Mu, Y., Alshebeili, S. A. & El-Samie, F. E Abd. (2013). Optical image encryption based on chaotic baker map and double random phase encoding. Journal of Lightwave Technology, 31 (15), 2533-2539.

Authors

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

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

***Abstract*—This paper presents a new technique for optical image encryption based on chaotic Baker map and Double Random Phase Encoding (DRPE). This technique is implemented in two layers to enhance the security level of the classical DRPE. The first layer is a pre-processing layer, which is performed with the chaotic Baker map on the original image. In the second layer, the classical DRPE is utilized. Matlab simulation experiments show that the proposed technique enhances the security level of the DRPE, and at the same time has a better immunity to noise.**

***Index Terms*—Chaotic Baker map, DRPE, optical image encryption.**

I. Introduction

OPTICAL encryption techniques have played a vital role in the field of optical information processing over the past decade. Special and reliable security in the transmission and storage of images is needed in several applications like pay TV, medical or biometric images for storage or transmission, confidential video conferencing over optical fiber, military applications, police identification procedures, online banking systems, governmental services, identity (ID) cards, etc.

The problem with images with unauthorized use is more and more serious as digital image information can be easily invaded by hackers through transmission via the Internet or other communication media. Optical encryption can provide a better and safe method for image communication. To retrieve the original optical information at the receiver side, the encryption method and keys are required.

In the past decade, several optical encryption methods have been proposed. Among them, the most widely used and highly successful optical encryption scheme is the DPRE proposed by Refregier and Javidi [1]. This method uses two random phase masks, one in the input plane and the other in the Fourier plane, to encrypt the primary image into stationary white noise [1], [2].

Several optical encryption methods have also been presented in the literature depending on the DRPE concepts [1]–[7]. Some other methods are based on digital holography [8], [9], Fresnel domain [10], [11], multiplexing [12], [13], polarized light [14], and interferometery [15], [16]. It is important to mention here that the 2-D Discrete Fourier Transform (DFT) is essential to perform a large number of the optical encryption algorithms.

To meet the requirements of modern applications with high levels of security, DRPE with chaotic map pre-processing is proposed in this paper. The objective of the pre-processing layer is to increase the level of security. The rest of this paper is organized as follows. Section II gives an explanation of the DRPE. Section III gives an explanation of the chaotic Baker map used in the pre-processing step. Section IV discusses the proposed technique. Section V presents the simulation results with a discussion of the encryption quality metrics. Finally, Section VI gives the concluding remarks.

II. The DRPE

The DRPE presented by Refregier and Javidi [1] is based on the modification of the spectral distribution of the image. Without any prior information about this spectral modification or the target image at the receiver, the image decoding cannot be done. The main idea of this approach, as shown in Fig. 1, depends on inserting two encoding keys (random phase) in a setup called "4f". The 4f Setup is an optical system consisting of two cascaded lenses separated by two focal lengths as in Fig. 1, with each of the input and output image planes one focal length outside the lens system from different directions (i.e., the total length is four focal lengths, hence "4f").

The decryption process uses the same Fourier Random Phase Mask (RPM) as in the encryption process. The DRPE, when applied in a 4f optical processor, requires the complex conjugate Fourier phase key to decrypt the image.

The DRPE consists mainly of three stages:

1. The first key, i.e., the RPM1, is multiplied by the target image to be encrypted. The resulting image should be displayed in the input plane of the "4f" setup and lighted with a parallel coherent light resulting from a Laser generator. This procedure introduces the first modification to the spectrum of the target image.

Manuscript received September 23, 2012; revised March 29, 2013; accepted May 28, 2013. Date of publication June 12, 2013; date of current version July 03, 2013.

A. M. Elshamy, A. N. Z. Rashed, and A. E. A. Mohamed are with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt (e-mail: a.alshamy@fujairah.ae; ahmed_733@yahoo.com; d_elnaser6@yahoo.com).

O. S. Faragallah is with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt (e-mail: osm_sal@yahoo.com).

Y. Mu is with the Centre of Computer and Information Security Research (CCISR), School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia (e-mail: ymu@uow.edu.au).

S. A. Alshebeili is with the Electrical Engineering Department, KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICS), King Saud University, KSA (e-mail: dsaleh@ksu.edu.sa).

F. E. Abd El-Samie is with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt, and also with the KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICS), King Saud University (e-mail: fathi_sayed@yahoo.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JLT.2013.2267891

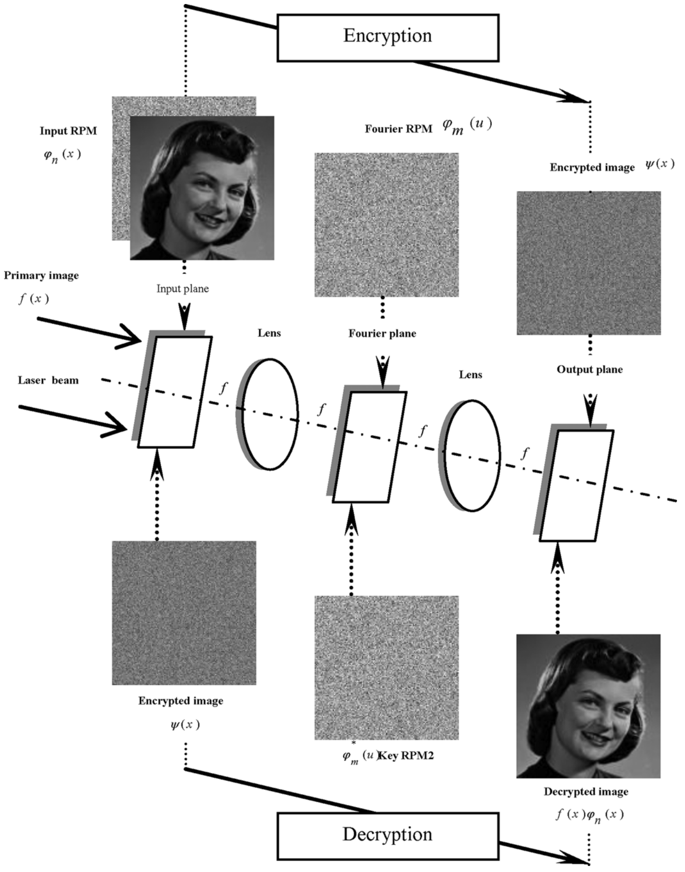


Fig. 1. Optical setup for DRPE encryption (top) and decryption (bottom).

2. The second key, i.e., RPM2, is directly inserted into the image spectrum in the Fourier plane. The multiplication of the RPM2 by the spectrum obtained in the first stage can introduce the second modification into the spectrum of the target image.
3. A second optical Fourier transform is carried out using a second lens to obtain the encoded image in the original 2-D space of images.

To explain the DRPE in detail, we consider a primary intensity image $f(x,y)$ with positive values, where x and y denote the spatial domain coordinates. Also, υ and η denote the Fourier domain coordinates. Let $\psi(x,y)$ denote the encrypted image, and $n(x,y)$ and $m(x,y)$, denote two independent white sequences uniformly distributed in $[0,2\pi]$. To encode $f(x,y)$ into a white stationary sequence, two RPMs are used, $\varphi_n(x,y)=\exp[2i\pi n(x,y)]$ and $\varphi_m(x,y)=\exp[2i\pi m(x,y)]$. $h(x,y)=m(x,y)$ is a phase function uniformly distributed in $[0,2\pi]$. The second RPM, $\varphi_m(\upsilon,\eta)$, is the Fourier transform of the function $h(x,y)$, that is,

$$FT\{h(x,y)\}=\hat{h}(\upsilon,\eta)=\varphi_m(\upsilon,\eta)=\exp[2i\pi m(\upsilon,\eta)] \quad (1)$$

The encryption process consists of multiplying the primary image by the first RPM $\varphi_n(x,y)$. The result is then convolved with the function $h(x,y)$. The encrypted function is complex, with amplitude and phase, and is given by the following expression:

$$\psi(x,y)=\{f(x,y)\varphi_n(x,y)\}*FT^{-1}\{\varphi_m(\upsilon,\eta)\} \quad (2)$$

where the symbol $(*)$ denotes convolution. The encrypted function in (2) has a noise-like appearance that does not reveal the content of the primary image. Regarding the amplitude-coded primary image $f(x,y)$, (2) is a linear operation.

In the decryption process, $\psi(x,y)$ is Fourier transformed, multiplied by the complex conjugate of the second RPM $\varphi_m(\upsilon,\eta)$ that acts as a key, and then inverse Fourier transformed. As a result, the output is

$$\begin{aligned}&FT^{-1}\{FT[\psi(x,y)]\varphi^*_m(\upsilon,\eta)\}\\&\quad=FT^{-1}\{FT[f(x,y)\varphi_n(x,y)]\varphi_m(\upsilon,\eta)\varphi^*_m(\upsilon,\eta)\}\\&\quad=f(x,y)\varphi_n(x,y)\end{aligned} \quad (3)$$

whose absolute value turns out the decrypted image $f(x,y)$. The whole encryption–decryption method can be implemented either digitally or optically. The optical hardware can be the classical 4f-processor shown in Fig. 1 [11]. In the encryption process, the 4f-processor has the first RPM stuck to the primary image in the input plane and the second RPM in its Fourier plane. In the output plane, the encrypted function is recorded, in amplitude and phase, using holographic techniques. In the decryption process, the 4f-processor has the encrypted function in the input plane and the key, that is the complex conjugate of the second RPM, in its Fourier plane. In the output plane, the decrypted image is recovered using an intensity-sensitive device such as a CCD camera.

Optical information can be hidden either in the complex-amplitude form or in the phase-only form or in the amplitude-only form. If the encrypted data $\psi(x,y)$ are complex (amplitude and phase) functions, such as those described in the method originally proposed by Refregier and Javidi [1], then there are some practical constraints to encode them. However, if the encrypted data can be either phase or amplitude only, then the recording and storage is easier.

The phase is often chosen to encode, convey, and retrieve information for many reasons such as higher efficiency, invisiblity to the naked eye, and more security than the amplitude. Towghi *et al.* [7] modified the linear encoding technique of the DRPE [1] by introducing a nonlinear (full-phase) encoding, for which a phase-only version of the primary image $f(x,y)$ is encoded. Thus, the fully phase-encrypted image is given by the following equation:

$$\begin{aligned}\psi_p(x,y)&=\{\exp[i\pi f(x,y)]\varphi_n(x,y)\}*h(x,y)\\&=\{\exp[i\pi f(x,y)]\varphi_n(x,y)\}*FT^{-1}\{\varphi_m(\upsilon,\eta)\}\end{aligned} \quad (4)$$

and it can be generated either optically or electronically in a way similar to that described in (2). The same optical setup shown in Fig. 1 is used for decryption, but in this case, the complex conjugate of both RPMs $\varphi^*_n(x,y)=\exp[-2i\pi n(x,y)]$ and $\varphi^*_m(\upsilon,\eta)=\exp[-2i\pi m(\upsilon,\eta)]$, referred to as keys, are necessary for decryption. The Fourier phase key $\varphi^*_m(\upsilon,\eta)$ is placed in the Fourier plane, whereas the phase key $\varphi^*_n(x,y)$ is placed at the output plane of the optical processor. The phase-only version of the primary image $\exp[i\pi f(x,y)]$ is recovered in the spatial domain. The primary image $f(x,y)$ can be visualized as an intensity distribution by extracting the phase of $\exp[i\pi f(x,y)]$ and dividing it by π.

The simplicity and the ease of implementation of DRPE have made it very attractive, but it has some drawbacks emphasized in the literature [9], [10]. Recently, the authors of [9] meticulously analyzed the DRPE and mentioned a large number of possible attacks. They also suggested few propositions to increase the encoding rate either with an increased number of keys or with the addition of another security layer. We adopt their second proposition in this paper.

III. Chaotic Baker Map

The chaotic Baker map is well-known to the image processing community as a tool of encryption. It is a permutation-based tool, which performs the randomization of a square matrix of dimensions $M \times M$ by changing the pixel positions based on a secret key [12]. It assigns a pixel to another pixel position in a bijective manner. The disretized Baker map is denoted by $B(v_1, \ldots, v_k)$, where the sequence of k integers, $v_1, v_2, \ldots, v_k$ is chosen such that each integer v_i divides M , and $M_i = v_1 + \cdots + v_i$.

The pixel at indices (l, s), with $M_i \leq l < M_i + v_i$ and $0 \leq s < M$ is mapped to [12], [13]:

$$B_{(n_1,\ldots,n_k)}(l,s) = \left[\frac{M}{v_i}(l-M_i)+s \bmod \frac{M}{v_i}, \frac{v_i}{M}\left(s-s \bmod \frac{M}{v_i}\right)+M_i\right] \quad (5)$$

This formula is implemented in the following steps [12], [13]:

1. The $M \times M$ square matrix is divided into k rectangles of width v_i and number of elements M.
2. The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from right to left beginning with upper rectangles, and then lower ones.
3. Inside each rectangle, the scan begins from the bottom left corner towards upper elements.

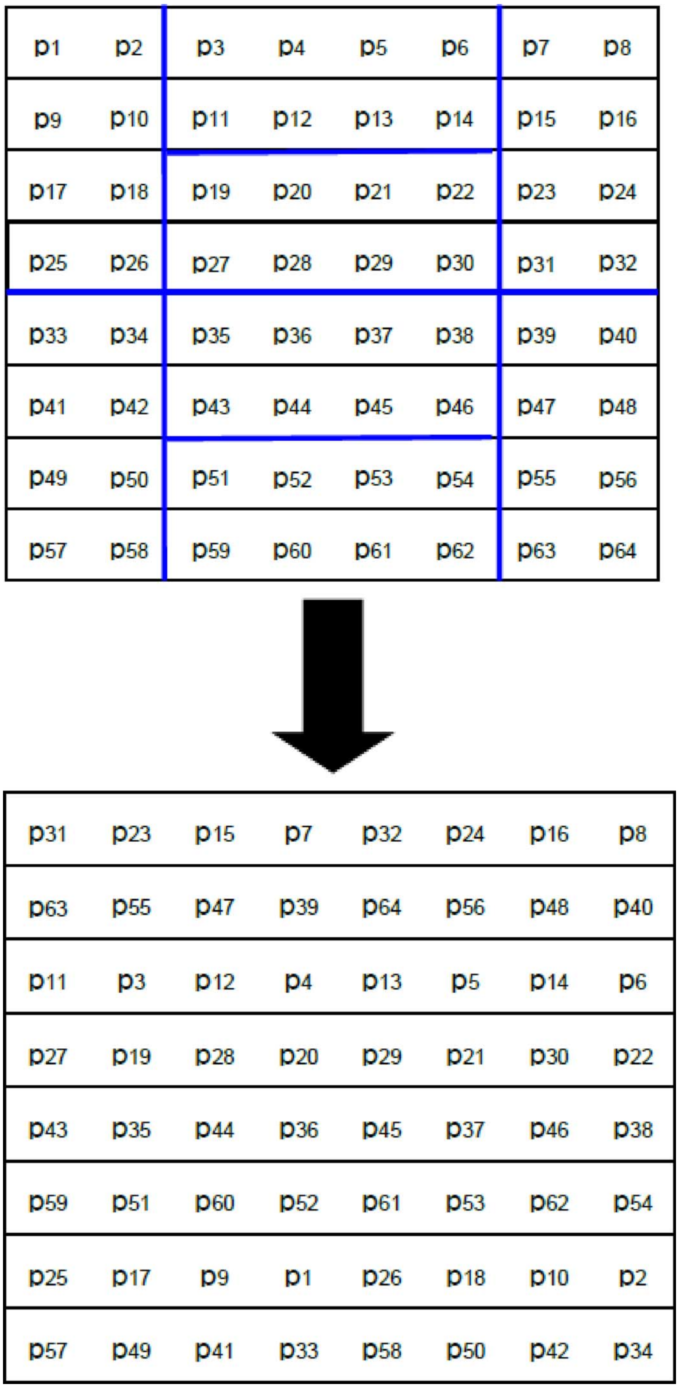
Fig. 2 shows an example for the chaotic randomization of an (8×8) square matrix (i.e., $M = 8$). The secret key $S = [2, 4, 2]$.

IV. The Proposed Technique

The proposed technique is based on adding a pre-processing chaotic Baker map layer to allow for the randomization of the image pixels prior to optical encryption. This layer can be performed numerically to avoid the complexity of the all-optical implementation. The second layer is the classical DRPE. Figs. 3 and 4 show the encryption and decryption processes of the proposed technique, respectively.

With this proposed implementation, we can achieve the following gains:

1. Cracking or hacking the encrypted images becomes harder. Let us imagine the case when a hacker may crack the DRPE key, i.e., the second RPM, he still can not obtain the target image as it is protected by the first auxiliary key of the chaotic Baker map.
2. All acts of piracy on the encrypted image could affect the chaotic randomized pixels. In this case, we can easily notice if the received image has been intercepted or modified.
3. The proposed technique could also be used as a water-marketing technique. Some useful information can be hidden in the image prior to optical encryption.



p1	p2	p3	p4	p5	p6	p7	p8
p9	p10	p11	p12	p13	p14	p15	p16
p17	p18	p19	p20	p21	p22	p23	p24
p25	p26	p27	p28	p29	p30	p31	p32
p33	p34	p35	p36	p37	p38	p39	p40
p41	p42	p43	p44	p45	p46	p47	p48
p49	p50	p51	p52	p53	p54	p55	p56
p57	p58	p59	p60	p61	p62	p63	p64

p31	p23	p15	p7	p32	p24	p16	p8
p63	p55	p47	p39	p64	p56	p48	p40
p11	p3	p12	p4	p13	p5	p14	p6
p27	p19	p28	p20	p29	p21	p30	p22
p43	p35	p44	p36	p45	p37	p46	p38
p59	p51	p60	p52	p61	p53	p62	p54
p25	p17	p9	p1	p26	p18	p10	p2
p57	p49	p41	p33	p58	p50	p42	p34

Fig. 2. Chaotic randomization of an 8×8 matrix with a secret key $S = [2, 4, 2]$.

The encryption process is described mathematically as:

$$\psi_B(x,y) = FT^{-1}[FT(f_B(x,y)\varphi_n(x,y))\varphi_m(\upsilon,\eta)] \quad (6)$$

The decryption process is described as:

$$FT^{-1}[FT(\psi_B(x,y))\varphi^*_m(\upsilon,\eta)] = f_B(x,y)\varphi_n(x,y) \quad (7)$$

We can eliminate $\varphi_n(x,y)$ by taking the magnitude, and then perform chaotic Baker map deryption.

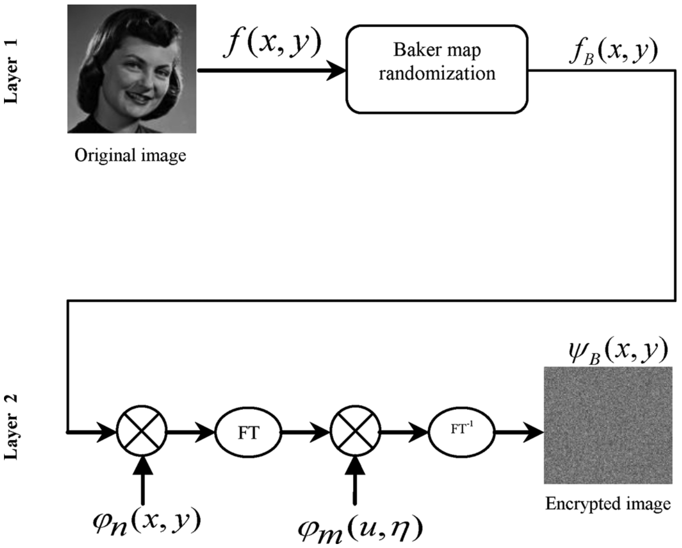


Fig. 3. Block diagram of proposed encryption process.

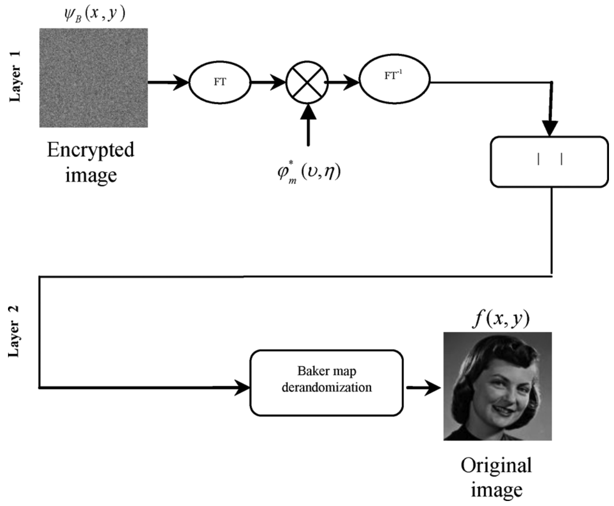


Fig. 4. Block diagram of proposed decryption process.

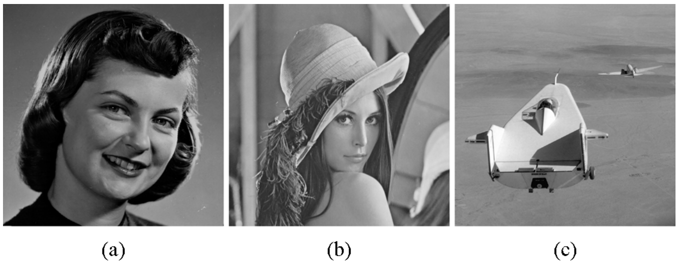


Fig. 5. Girl, Lena, and Plane images. (a) Girl. (b) Lena. (c) Plane.

V. Simulation Experiments

Several Matlab experiments have been carried out to test the proposed technique and compare its performance with those of the DRPE and chaotic Baker map encryption. The three images of the Girl, Lena, and Plane shown in Fig. 5 have been used in the experiments. Visual results for the Girl image only are shown in he paper, and the other results are tabulated.

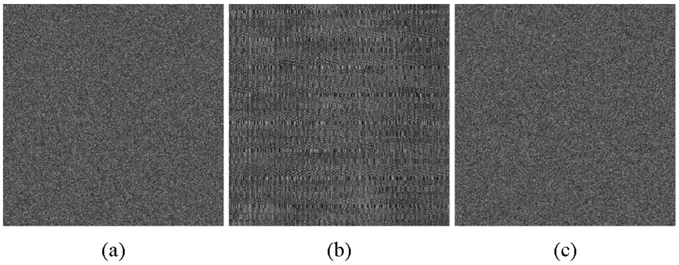


Fig. 6. Encrypted Girl image with (a) DRPE, (b) chaotic Baker map, (c) the proposed technique.

Fig. 6 shows the encryption results of the Girl image with different algorithms. One of the important factors in examining the encrypted image is the visual inspection. But, depending on the visual inspection only is not enough in judging the data hiding process. So, other metrics are considered to evaluate the degree of encryption, quantitatively.

A. Histogram Analysis

Histogram analysis of the decrypted and the original images has also been performed to validate the proposed method. For image encryption algorithms, the histogram of the encrypted image should be totally different from the histogram of the original image [14]. Fig. 7 shows the histograms of the encrypted images in Fig. 6 and their decrypted versions. It is clear from this figure that the histograms of the original and decrypted images are identical. It is also clear that the histograms of the encrypted images are different from that of the original image for the DRPE and the proposed technique.

B. Correlation Cofficient Analysis

The correlation coefficient between the original and the encrypted images has been used as a tool for encryption quality evaluation. The correlation coefficient is estimated as:

$$\begin{aligned} r &= \frac{\operatorname{cov}(f,\psi)}{\sqrt{D(f)}\sqrt{D(\psi)}} \\ \text{and}\quad D(f) &= \frac{1}{L}\sum_{l=1}^{L}(f_l - E(f))^2 \\ \operatorname{cov}(f,\psi) &= \frac{1}{L}\sum_{l=1}^{L}(f_l - E(f))(\psi_l - E(\psi)), \\ E(f) &= \frac{1}{L}\sum_{l=1}^{L} f_l \end{aligned} \tag{8}$$

where f and ψ are gray-scale pixel values of the original and encrypted images. Table I shows the correlation coefficient values between the original image and the encrypted image for the DRPE and the proposed technique. The low correlation values reflect the strength of the encryption algorithm.

C. Maximum Deviation Analysis

The maximum deviation measures the quality of encryption in terms of how it maximizes the deviation between the original

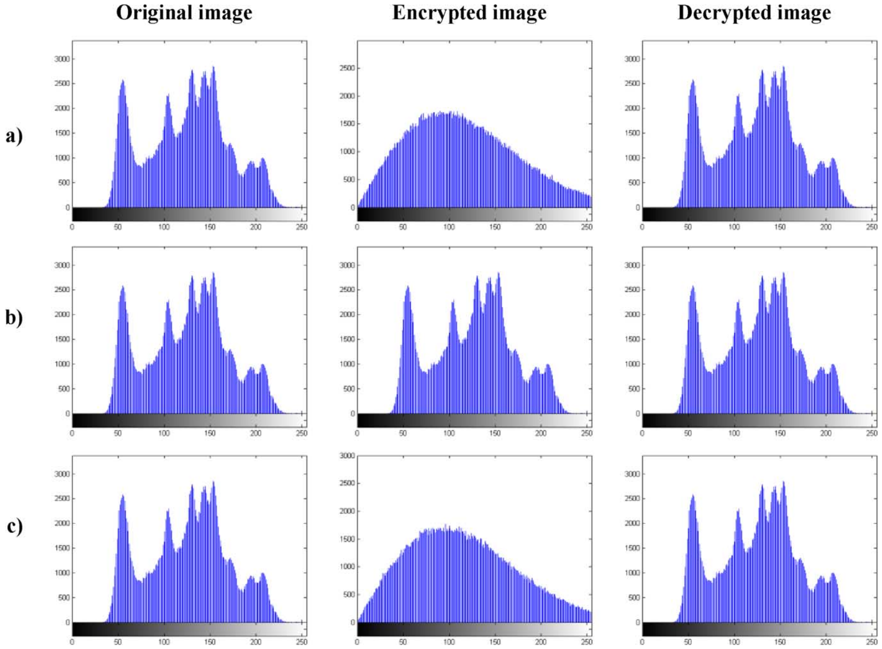


Fig. 7. The histograms of the images for (a) DRPE, b) chaotic Baker map encryption, and c) proposed technique. a) DRPE. b) Chaotic Baker map. c) Proposed technique.

TABLE I
CORRELATION COEFFICIENT BETWEEN THE ORIGINAL IMAGE AND THE ENCRYPTED IMAGE FOR THE DRPE AND THE PROPOSED TECHNIQUE.

Encryption technique	Lena	Girl	Plane
DRPE	- 0,0027	0.0026	- 0.0023
Proposed technique	- 0,0011	0.0019	- 0.0011

TABLE II
MAXIMUM DEVIATION METRIC VALUES FOR THE CLASSICAL DRPE AND THE PROPOSED TECHNIQUE.

Encryption technique	Lena	Girl	Plane
DRPE	127966	188230	283213
Proposed technique	127790	188470	283426

and the encrypted images. The steps of calculating this metric are:

1. Count the number of pixels for each gray-scale value in the range of 0 to 255 and present the results graphically for both the original and encrypted images (i.e.,; get their histogram distributions).
2. Compute the absolute difference or deviation between the two curves and represent it, graphically.
3. Estimate the area under the absolute difference curve, which is the sum of deviations.

Of course, the higher the estimated value, the more the encrypted image is deviated from the original image. Table II shows the maximum deviation metric values for the DRPE and the proposed technique for different images. The results are in favor of the proposed technique for the Girl and the Plane images.

D. Irregular Deviation Analysis

This analysis is based on how much the deviation caused by encryption on the encrypted image is irregular. It gives an attention to each individual pixel value and the deviation caused at every pixel position of the input image before getting the histogram, which does not preserve any information about the positions of the pixels. To evaluate this metric, we follow the steps:

1. Construct the 'D' matrix, which represents the absolute values of the difference between pixel values at the same position before and after encryption. So, D can be represented as:

$$D = |f - \psi| \tag{9}$$

2. Construct the histogram distribution 'H' of the matrix D.
3. Get the average value of this histogram as:

$$H_{av} = \frac{1}{255}\sum_{i=0}^{255} H_i \tag{10}$$

4. Subtract this average from the deviation histogram, and then take the absolute value of the result to obtain a modified histogram.

$$H_{i,m} = |H_i - H_{av}| \tag{11}$$

TABLE III
IRREGULAR DEVIATION METRIC VALUES FOR THE DRPE AND PROPOSED TECHNIQUE.

Encryption technique	Lena	Girl	Plane
DRPE	220078	241970	234900
Proposed technique	220296	241976	235190

5. Estimate the area under modified histogram curve, which is the sum of deviations of the histogram from the uniformly distributed histogram.

$$D_I = \sum_{i=0}^{255} H_{i,m} \tag{12}$$

The lower the value of D_I, the better the encryption quality [14]. Table III shows the irregular deviation metric values for the DRPE and the proposed technique. Both techniques have close values.

E. Noise Immunity

To evaluate the reliability of an encryption technique, the Mean Square Error (MSE) between the decrypted and original images is calculated. It is defined as:

$$MSE = \frac{1}{XY} \sum_{x=1}^{X} \sum_{y=1}^{Y} \left| f(x,y) - \hat{f}(x,y) \right|^2 \tag{13}$$

where X and Y are the image dimensions. $f(x,y)$ and $\hat{f}(x,y)$ represent the original and the decrypted images, respectively. The Peak Signal-to-Noise Ratio is estimated from the MSE as follows:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{14}$$

A comparison between the original image and the decrypted image in the PSNR in the presence of Additive White Gaussian Noise (AWGN) before decryption is presented in Fig. 8 and Table IV. From this table, we notice that the proposed technique is more immune to noise than the DRPE, which makes it a good candidate for communication applications.

F. Time Analysis

The processing time is the time required to encrypt/decrypt data. The smaller the processing time, the higher the speed of encryption. We have tested the DRPE and proposed technique and estimated the decryption time as both the encryption and decryption processes have approximately the same time. The results are shown in Table V. It is clear from this table that the complexity resulting from adding the chaotic Baker map randomization layer is slight.

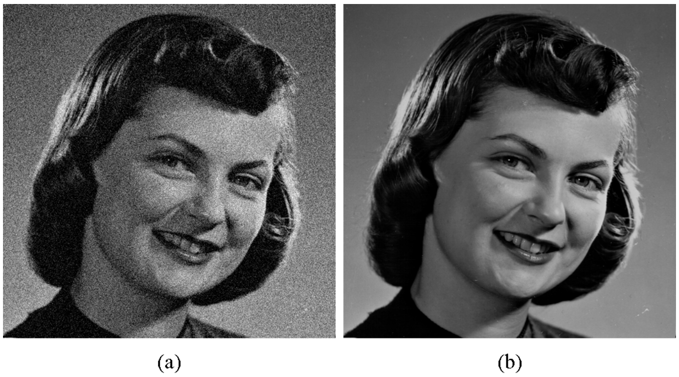


Fig. 8. Decrypted images for the DRPE and the proposed technique in the presence of noise on the encrypted image with variance 0.01. (a) DRPE. (b) Proposed technique.

TABLE IV
PSNR VALUES (DB) OF THE DECRYPTED IMAGES FOR THE DRPE AND THE PROPOSED TECHNIQUE IN THE PRESENCE OF NOISE WITH VARIANCE 0.01 ON THE ENCRYPTED IMAGE.

Encryption technique	Lena	Girl	Plane
DRPE	5.6831	8.3098	5.0077
Proposed technique	10.2918	10.8824	10.6846

TABLE V
PROCESSING TIME (SEC) FOR THE DRPE AND THE PROPOSED TECHNIQUE.

Encryption technique	Lena	Girl	Plane
DRPE	0.5259	0.4937	0.5274
Proposed technique	3.7621	3.6348	3.8194

VI. CONCLUSION

In this paper, an encryption technique based on chaotic Baker map and the DRPE has been presented. The chaotic Baker map is used as a pre-processing layer to increase the security level. The implementation of the proposed technique is simple, and achieves good permutation and diffusion mechanisms in a reasonable time with large immunity to noise, which is a required property for communication applications.

REFERENCES

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

[2] 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.

[3] F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," *J. Opt. Soc. Amer. A*, vol. 15, pp. 2629–2638, 1998.

[4] 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, 2000.

[5] S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," *Appl. Opt.*, vol. 41, pp. 5462–5470, 2002.

[6] L. G. Neto and Y. Sheng, "Optical implementation of image encryption using random phase encoding," *Opt. Eng.*, vol. 35, no. 9, pp. 2459–2463, 1996.

[7] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Amer. A*, vol. 16, pp. 1915–1927, 1999.

[8] G. Unnikrishnan and K. Singh, "Optical encryption using quadratic phase systems," *Opt. Commun.*, vol. 193, pp. 51–67, 2001.

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

[10] 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.

[11] J. W. Goodman*, Introduction to Fourier Optics*, 2nd ed. New York, NY, USA: McGraw-Hill, 1996.

[12] J. Fridrich*, Symmetric Ciphers Based on Two-Dimensional Chaotic Maps*. Singapore: World Scientific, 1998.

[13] Y. Honglei, W. Guang-shou, W. Ting, L. Diantao, Y. Jun, M. Weitao, F. Y. Shaolei, and M. Yuankao, "An image encryption algorithm based on two dimensional Baker map," in *Proc. ICICTA*, 2009.

[14] I. F. Elashry, O. S. Farag Allah, A. M. Abbas, S. El-Rabaie, and F. E. A. El-Samie, "Homomorphic image encryption," *J. Electron. Imag.*, vol. 18, no. 3, pp. 033002-1–033002-14, 2009.

[15] B. Javidi, Ed., Optical and Digital Techniques for Information Security New York, Springer Verlag, 2005.

[16] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi, "Optical techniques for information security," *Proc. IEEE*, vol. 97, no. 6, pp. 1128–1148, Jun. 2009.

Ahmed Mohamed Elsayed Elshamy received the B.Sc. degree in electronics and electrical communications engineering from Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2010. He has got the best project award in communications engineering from the Smart Village in the EED event. He is now working Dubai e-Government, UAE. His areas of interest include network security, optical communication systems, and optical encryption.

Ahmed Nabih Zaki Rashed received the B.Sc., M.Sc., and Ph.D. degrees from the Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menoufia University in 1999, 2005, and 2010, respectively. His research interests include optoelectronic devices, passive optical access communication networks, optical communication systems, advanced optical communication networks, wireless optical access networks, analog communication systems, optical filters and sensors, digital communication systems, advanced material science, network management systems, multimedia databases, network security, encryption, biometrics, acoustic communication systems, under-water communications, and optical access computing systems.

Abd-Elnaser A. Mohamed received the Ph. D degree from the faculty of Electronic Engineering, Menofia University in 1994. Now, he is a Professor at Electronics and Electrical Communications Engineering department, Faculty of Electronic Engineering, Menofia University, Egypt. His research interests include passive optical communication networks, digital communication systems, advanced optical communication wireless access networks, analog communication systems, optoelectronic devices, advanced material science, network management systems, multimedia databases, network security, optical encryption, and biometrics.

Osama Salah Faragallah received the B.Sc., M.Sc., and Ph.D. degrees in Computer Science and Engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently Associate Professor with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was a Demonstrator from 1997 to 2002 and has been Assistant Lecturer from 2002 and to since 2007 and since 2007 he has been a Teaching Staff Member with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. His research interests include network security, cryptography, internet security, multimedia security, image encryption, optical encryption, watermarking, steganography, data hiding, medical image processing and chaos theory.

Yi Mu received his PhD from the Australian National University in 1994. Prior to joining University of Wollongong, he was a senior lecturer in the Department of Computing, Macquarie University. He also worked in Department of Computing and IT, University of Western Sydney as a lecturer. He has been with the University of Wollongong since 2003. His current research interest includes cryptography, network security, access control, and computer security. He also previously worked in the areas of quantum cryptography, quantum computers, atomic computations, and quantum optics. Professor Mu is Editor-in-Chief of International Journal of Applied Cryptography and serves as associate editor or guest editor for many international Journals. He has served in program committees for a number of international security conferences, including ACM CCS, ACM AisaCCS, ESORICS, ACISP, CANS, EuroPKI, ICICS, ICISC, ProvSec, ISPEC, etc. He is a senior member of the IEEE and a member of the IACR.

Saleh A Alshebeili is professor and chairman (2001–2005) of Electrical Engineering Department, King Saud University. He has more than 20 years of teaching and research experience in the area of *communications* and *signal processing*. Dr Alshebeili is member of the board of directors of Prince Sultan Advanced Technologies Research Institute (PSATRI), the Vice President of PSATRI (2008–2011), the director of Saudi-Telecom Research Chair (2008–2012), and the director (2011-Present) of the Technology Innovation Center, *RF and Photonics in the e-Society* (RFTONICS), funded by King Abdulaziz City for Science and Technology (KACST). Dr Alshebeili has been in the editorial board of *Journal* of *Engineering Sciences* of King Saud University (2009–2012). He has also an active involvement in the review process of a number of research journals, KACST general directorate grants programs, and national and international symposiums and conferences.

Fathi E. Abd El-Samie received the B.Sc.(Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. He is currently a researcher at KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICs). He is a coauthor of about 200 papers in international conference proceedings and journals, and four textbooks. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. Dr. Abd El-Samie was a recipient of the Most Cited Paper Award from the *Digital Signal Processing* journal in 2008.