International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 6, June 2014

Optical method for Images Encryption Based on Chaotic BakerMap and Double Random Phase Encoding

Anusha G. K[1], Nilajkar R. M[2]

Abstract: ***This paper presents a new optical technique for 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, with the chaotic Baker map on the original image. In the second layer, the DRPE is utilized. Matlab simulation experiments show that the this technique enhances the security level of the DRPE, and at the same time it has a better immunity to noise.***

Keywords: Chaotic Bakermap, DRPE, optical image, Fourier domain, Random Phase Mask key

1. Introduction

Optical information-processing systems have emerged as a very promising means of encryption, securing and validation of data. They exploit the advantage of the inherent parallelism of optical systems, the processing of information at the speed of the light, and its versatility for manipulating the information in the spatial domain or in the spatial frequency domain. Under these circumstances, optical systems are considered to be a good solution for real-time secure 3D television and video-conference systems, where a digital communication channel transmits encrypted digital holograms and then this information is retrieved and displayed by means of secure 3D display systems. To encrypt the data, one of the most popular techniques is the double random phase encryption scheme.

This scheme uses a classical 4-f correlator and two random phase masks. The first mask is placed in the input plane immediately after the image to be encrypted. The second mask is located in the Fourier domain. Up to now, a complete analysis regarding the security of this technique has not been performed. To meet the requirements of modern applications with high levels of security, DRPE with chaotic map pre-processing is proposed in this paper.

2. The DRPE

The DRPE presented by Refregier and Javidi 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 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 " "). The decryption process uses the same Fourier Random Phase Mask (RPM) as in the encryption process. The DRPE, when applied in an 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.

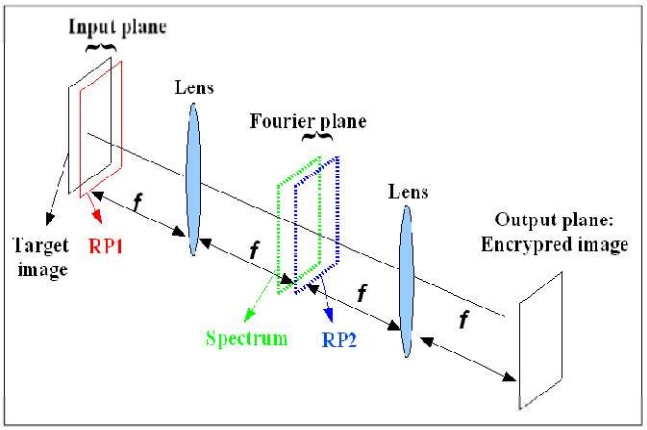

Figure 1: Optical setup for DRPE method

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 image.

The DRPE method in detail consider a primary intensity image f(x, y) with positive values where x and y denote the spatial domain coordinates. Also v and ŋ denote the Fourier domain coordinates. Let Ψ(x, y) denote the encrypted image and n(x, y) and m(x, y) denote two independent white sequences uniformly distributed in

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 6, June 2014

[0,2π] to encode f(x, y) into a white stationary sequences two RPMs are used $\Psi_n(x, y)= \exp [2i \pi n(x, y)]$ and $\Psi_m(x, y)=\exp[2i \pi m(x, y)]$ h(x, y)=m(x, y) is a phase function uniformly distributed in [0,2π].The second RPM, $\Psi_m(v, \eta)$ is the Fourier transform of the function h(x, y), that is;

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

The encryption process consists of multiplying the primary image by the first RPM $\Psi_n(x, y)$. 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.

$$\Psi(x, y)= \{f(x, y) \Psi_n(x, y)\} * IFT \{ \Psi_m(v, \eta)\} \quad (2)$$

Where the symbol (*) denote the 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 Ψ(x, y) is Fourier transformed, multiplied by the complex conjugate of the second RPM Ψm(v,ŋ) that acts as a key and then inverse Fourier transferred then the output is

$$IFT\{FT[\Psi(x, y)] \Psi_m^{*}(v, \eta)\}$$
$$=IFT\{FT[f(x, y) \Psi_n(x, y)] \Psi_m(v, \eta) \Psi_m^{*}(v, \eta)\}$$
$$= f(x, y) \Psi_n(x, y)\} \quad (3)$$

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 -processor shown in Fig. 1. In the encryption process, the -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 -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 Ψ(x, y) are complex (amplitude and phase) functions, such as those described in the method originally proposed by Refregier and Javidi 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, invisibility to the naked eye, and more security than the amplitude. Towghi et al. modified the linear encoding technique of the DRPE by introducing a nonlinear (full-phase) encoding, for which a phase-only version of the primary image is encoded. Thus, the fully phase-encrypted image is given by the following equation:

$$\Psi_p(x, y) = \{\exp [i \pi f(x, y)] \Psi_n(x, y) \} * h(x, y) =\{\exp [i \pi f(x, y)] \Psi_n(x, y) \}*IFT \{\Psi_m(v, \eta) \} \quad (4)$$

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

3. 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 × M by changing the pixel positions based on a secret key. It assigns a pixel to another pixel position in a bijective manner. The discretized Baker map is denoted by $B(v_1,v_2\ldots.v_k)$, where the sequence of k integers v1.v2,v3,….vk is chosen such that each integer v_i divides M, and $M_i=v_1+v_2\ldots\ldots+v_i$

The pixels at indices (l, s), with $M_i \leq l < M_i + v_i$ and $0 \leq s < M$ is mapped to $B_{(n1,\ldots..nk)}(l, s)$

$$=[M/vi(l- M_i) + s \bmod M/v_i ,v_i/M(s- s \bmod M/v_i) +M_i] \quad (5)$$

This formula is implemented in the following steps;

1) The square matrix is divided into k rectangles of width vi 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.

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 2 Issue 6, June 2014

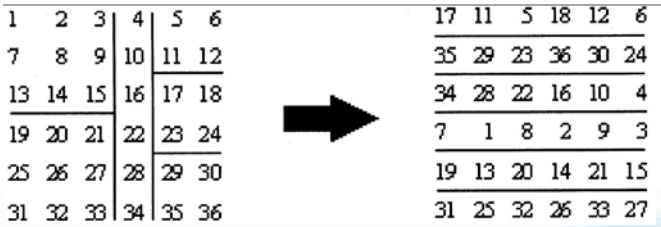

Figure 2: An example for the chaotic randomization of an (6× 6) square matrix (i.e. M=6). The secret key S = [3 12]

4. 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 cannot 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.

The encryption process is described mathematically as:

$$\Psi_b(x, y) = FT'[FT(fb(x, y)\varphi n(x, y))\varphi m(v, \eta)] \quad (6)$$

The decryption process is described as

$$IFT(FT(\varphi b(x, y)\varphi m * (v, \eta)) = fb(x, y)\varphi n(x, y) \quad 7$$

Eliminate $\varphi n(x, y)$ by taking the magnitude, and then perform chaotic Baker map decryption.

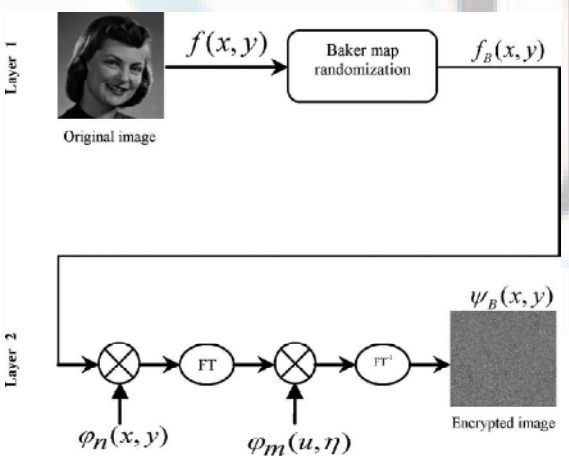

Figure 3: Block diagram of proposed encryption process

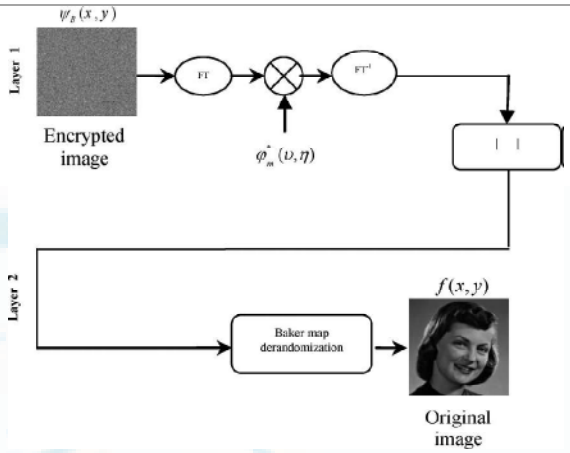

Figure 4: Block diagram of proposed decryption process

5. 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 Lena image are shown in the paper.

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

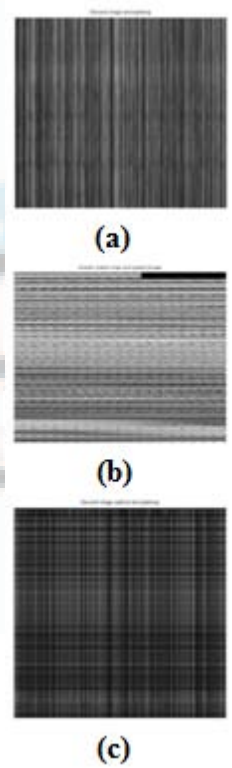

Figure 6: Encrypted Lena image of (a) DRPE (b) Baker map (c) Proposed method

Figure 6 shows the encryption results of the Lena image with different algorithms. One of the important factors in examining the encrypted image is the visual inspection.

6. 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.

Acknowledgement

It is a pleasure to recognise Mr Ramesh Nilajkar (G.M.I.T Davangere) for all technical guidance encouragement and analysis of data throughout this process.

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 FourierOptics, 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, andM. Yuankao, "An image encryption algorithm based on two dimensional Baker map," in Proc. ICICTA, 2009.
[14] F. Elashry, O. S. Farag Allah, A.M. AbbasS. 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.

Author Profile

Anusha G. K. is currently doing M. Tech in Digital Electronics in G.M Institute of technology Engineering College, Davangere Visvesvaraya Technological University, Belagum, Karnataka, India

Nilajkar R. M is currently working as Assistant Professor in the department of Electronics and Communication Engineering in G.M Institute of Technology Engineering College, Davangere .Visvesvaraya Technological University, Belagum, Karnataka, India

