

Simultaneous multiplexing & encoding of multiple images based on a double random phase encryption system

Ayman Alfalou^{*a} and Ali Mansour^b

^a Département optoélectronique, Laboratoire L@BISEN, ISEN-BREST, 20 rue cuirassé Bretagne, CS 42807, 29228 Brest Cedex 2, France

^b Department of Electrical and Computer Engineering, Curtin University, GPO Box U1987, Perth, WA, 6845, Australia

ABSTRACT

Nowadays, protecting information is a major issue in any transmission system, as showed by an increasing number of research papers related to this topic. Optical encoding methods, such as a Double Random Phase encryption system i.e. DRP, are widely used and cited in the literature. DRP systems have very simple principle and they are easily applicable to most images (B&W, gray levels or color). Moreover, some applications require an enhanced encoding level based on multienryption scheme and including biometric keys (as digital fingerprints). The enhancement should be done without increasing transmitted or stored information. In order to achieve that goal, a new approach for simultaneous multiplexing & encoding of several target images is developed in this manuscript. By introducing two additional security levels, our approach enhances the security level of a classic "DRP" system. Our first security level consists in using several independent image-keys (randomly and structurally) along with a new multiplexing algorithm. At this level, several target images (multienryption) are used. This part can reduce needed information (encoding information). At the second level a standard DRP system is included. Finally, our approach can detect if any vandalism attempt has been done on transmitted encrypted images.

Keywords: Optical encryption, optical compression, DRP, Simultaneous multiplexing & encoding.

1. INTRODUCTION

The growing interest in modern communication tools urges us to reduce and protect processed and transmitted information. To achieve these two goals, two main operations are required:

1. Compression operation which is used to reduce redundant information in a given message.
2. Encryption which is used to hide or to protect information. This can be done by changing the characteristic of a message in connection with few encryption keys.

To meet the above new needs much work has been made in recent years [1]. At L@BISEN, we focus on optical techniques to implement and develop image processing and encryption systems such as the DRP proposed by Refregier *et al.* [2]. Recently, there has been much interest in DRP thanks to its very simple principle which is based on the famous setup of "4f" [3] and the multiplication by two random phase masks [4-10]. However, this system has some weaknesses against some types of attacks [11]. To increase the robustness of this system several research works have been done in the literature. In [12] the authors increased the encryption level of a classical "DRP" system by using iterative fractional Fourier transforms.

To compress transmitted or stored information, many research documents can be proposed in the literature. In [13], Daraki *et al.* optimized the coding of complex amplitudes necessary to reconstruct a hologram-PSI. Other optical compression techniques consists in implementing modified versions of JPEG and JPEG2000 [14,15].

* ayman.al-falou@isen.fr; phone + 33 2 98 03 84 09; fax + 33 2 98 03 84 10

However, the above two mentioned operations should be performed in cascade, without taking into consideration their mutual effects. A first attempt to realize such system was proposed in [16]. A compression and encryption technique consists in combining together various images using "DCT" transformation. Recently, we proposed a new method of simultaneously encryption and multiplexing multi-images [17].

In this manuscript, our previous method [17] is briefly described. Several simulations and experimental setups have been performed in order to corroborate the performance of our algorithm. Its compression capability has been tested. In order to improve this capacity, we propose hereafter a modified version. This version can increase the rate of a classic "DRP" standard system, by using an additional security level (i.e. the multiplexing level) based on iterative Fourier transformations and several encryption keys. Moreover, this approach can also encrypt several target images (multiencryption) and compress requested information.

2. DOUBLE RANDOM PHASE ENCRYPTION SCHEME TO MULTIPLEX & SIMULTANEOUS ENCODE MULTIPLE IMAGES

The synoptic diagram of our approach with two encoding independently levels is illustrated in figure 1. The target image (I_0) is introduced at the input of the first level (figure 3). In the first stage, the image " I_0 " is multiplied by a selected phase function: " $I_0 e^{i\varphi_{01}}$ ". By carrying out, a first Fourier Transform "FT", we obtain " $I_1 e^{i\varphi_{11}}$ ". Then, we carry out successively several Fourier Transformations (FT(n)) by modifying at each iteration the phase function until " ρ_1 " (i.e. the amplitude of the target image spectrum I_0 modulated with a function phase) converges towards " I_1 " which is a known image (for example, a digital fingerprint). After "N-iterations", we obtain at the output of our first level " $I_1 e^{i\varphi_{1n}}$ ": a digital fingerprint modulated with a function phase (Equation 1).

$$I_1 e^{i\varphi_{1n}} = FT_n(I_0 e^{i\varphi_{0n}}) \tag{1}$$

With (φ_{0n} & φ_{1n}) are two pure phase functions necessary to tend the amplitude of the target image spectrum towards the desired digital fingerprint. The algorithm, used to find these two functions, is described in [17]. The obtained complex image " $I_1 e^{i\varphi_{1n}}$ " is introduced at the input of a classical DRP (as a second stage of our approach). Thus, the latter complex image is multiplied by a first random phase key " $I_1 e^{i(\varphi_{1n} + \varphi_{A1})}$ ". After a Fourier transform, we multiply its spectrum by a second random phase key " $e^{i(\varphi_{A2})}$ ". Finally, another Fourier transform gives, at the output of our system, the doubly encrypted image with two different and independent levels ($I_c e^{i\varphi_c}$).

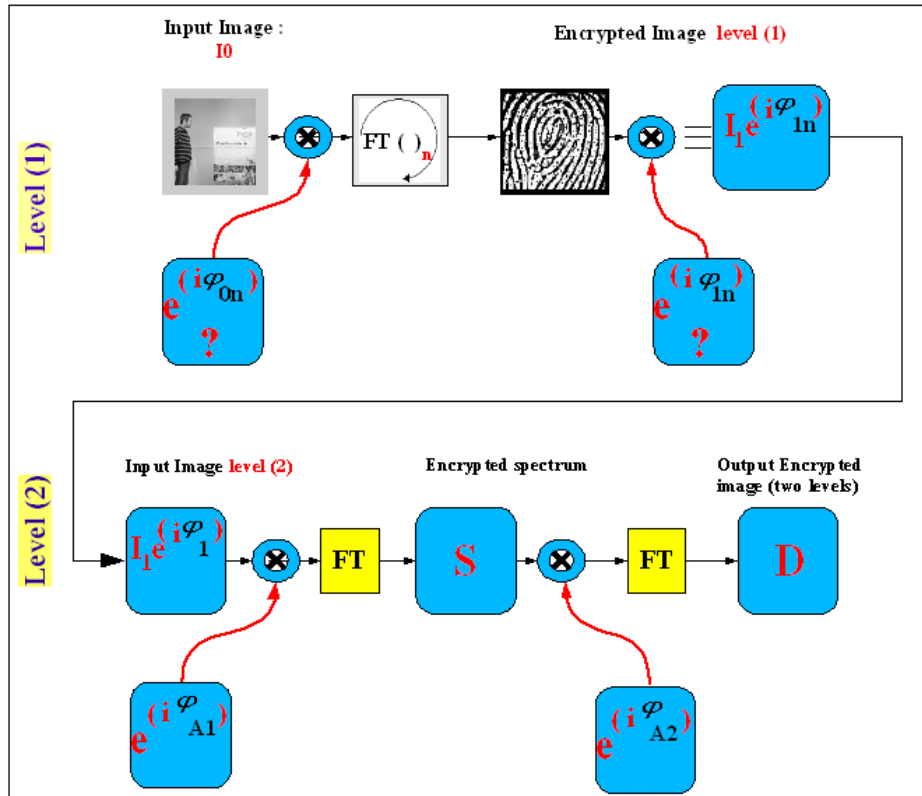


Figure 1. A double random phase encryption system enforced by two encryption levels

3. COMPRESSION

In the previous paragraph, we briefly described the main idea of the double random phase encryption scheme to multiplex & simultaneous encode multiple images. Thus, to encrypt and multiplex « N » images (I_1, I_2, \dots, I_N), we propose the synoptic diagram presented in figure (2). At first, we should consider a couple of images (I_1, I_2), after the multiplication of image I_1 by the phase (ϕ_1) followed by the application of several Fourier Transforms, our algorithm converges to the image I_2 with a phase function (ϕ'_2) . Applying the same procedure to another couple of images (I_2, I_3), we can obtain two different phases (ϕ''_2, ϕ'_3) . This procedure should be repeated several times to consider all the N images. The final couple of images (I_{N-1}, I_N) will generate a complex image $(I_m e^{i\phi^m})$ which should be introduced into a classic DRP algorithm. In the latest stage, the image is multiplied by a first random phase mask. After applying a Fourier transformation, we should multiply the result with a second random phase mask. The obtained image should be again introduced to another Fourier Transform module to get the final image. This final image contains all necessary information to reconstruct the multiple original images. It is worth to be mentioned that the reconstruction is only possible if we know (Figure 2):

- The two random phase masks used in the classical DRP,

- Various phase functions used to converge the iterative Fourier Transforms $(\phi_2, \phi_3, \dots, \phi_{m-1})$, with $(\phi_i = \phi_i'' - \phi_i')$.

As it was previously mentioned, to reconstruct the various images, we must transmit the various phase functions in $[-\pi, \pi]$. The operation may lead to huge amount of data. Therefore, a compression stage is required. In this section we propose to reduce the size of the different phases by coding them by using different bit numbers. To achieve that, all phases should be translated to $[0, 2\pi]$. Then we quantize and normalize the values to be in $[0, 2^N]$ with "N" the number of desired bits using the following equation:

$$V_{estimated} = Fix \left(V_{origine} \times \frac{2^N}{2 \times \pi} \right) \quad (2)$$

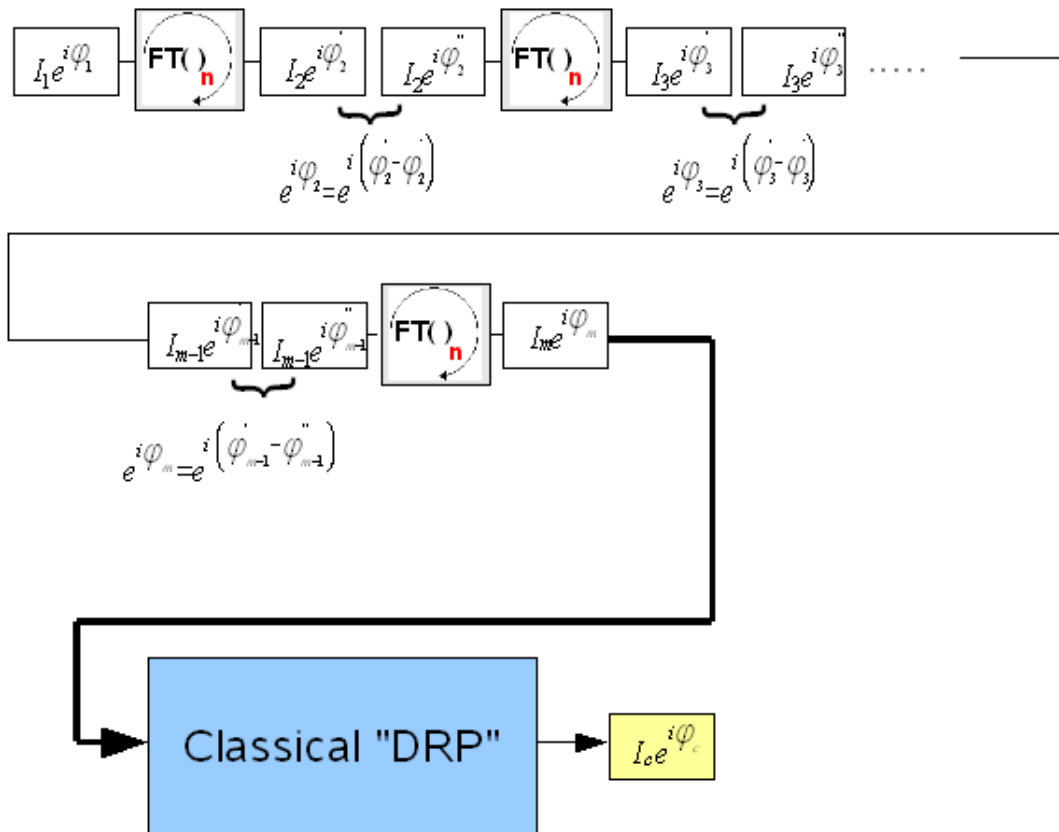


Figure 2. Encryption of a multiple target images using a DRP system

4. SIMULATION RESULTS

In this section, we present a procedure to encrypt multiple images while reducing the size of the information necessary for their reconstruction. At first, we consider two images (I_0 (1) and I_0 (2))

with (256x256) pixels and several grayscale level table (1). These images should be quantized using firstly a huge quantization number (up to 64 as used to be in Matlab, the quantization number is given in the first column of table 1). Then, lower quantization numbers are considered till reaching a binary encoding (with a single bit). The second column of table 1 contents the compression ratio achieved for every phase function. The compression rate is defined as the ratio between the size of the final phase function (with respect to the quantization number) and the original size coded on 8-bit (equation 3).

$$C_R = \left(1 - \frac{256 \times 256 \times 2^N}{256 \times 256 \times 2^8} \right) \times 100 \quad (3)$$

Columns 3 and 4 of the table (1) present different reconstructed images with their corresponding MSEs values (defined in equation 4). The convergence of the algorithm is given in table (2). Various simulations have been conducted. Based on our simulation results, we can notice that:

1. A good compression power has been achieved. Indeed, reconstructed images of good quality have been achieved, even when only two bits were used.
2. It seems that the convergence of our algorithm is not affected by the quantization number.

$$MSE = \frac{1}{M \times N} \sum \sum |I_{rebuilt}(i,j) - I_0(i,j)|^2 \quad (4)$$

5. CONCLUSION AND PERSPECTIVES

A new modified version of a double random phase encryption scheme with compression has been presented. The new approach allows us to simultaneously multiplex & encode multiple images. Various simulations have been conducted to corroborate the performance of our algorithm. Our experimental results show the efficiency our compression procedure. In addition, we tested this new version (with compression) on different Kinds of images including binary images. Actually, we are working on a dynamic quantization approach which means that the quantization number will not be the same for all phase functions. The robustness and the experimental results of the latter approach will be shown in our future works.








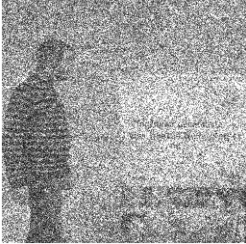
| Phase bits number | Compression Ratio : C_R |  Image $I_0(1)$ |  Image $I_0(2)$ |
|-------------------|---------------------------|---|---|
| 64 | | $MSE_1 = 8.82 \cdot 10^{-5}$ | $MSE_2 = 6.54 \cdot 10^{-4}$ |
| 16 | | $MSE_1 = 1.64 \cdot 10^{-4}$ | $MSE_2 = 5.82 \cdot 10^{-4}$ |
| 8 | $C_R = 0\%$ |  $MSE_1 = 5.74 \cdot 10^{-4}$ |  $MSE_2 = 4.48 \cdot 10^{-3}$ |
| 7 | $C_R = 12.5\%$ | $MSE_1 = 1.11 \cdot 10^{-3}$ | $MSE_2 = 7.31 \cdot 10^{-3}$ |
| 6 | $C_R = 25\%$ | $MSE_1 = 6.62 \cdot 10^{-3}$ | $MSE_2 = 2.21 \cdot 10^{-2}$ |
| 5 | $C_R = 37.5\%$ |  $MSE_1 = 3.80 \cdot 10^{-2}$ |  $MSE_2 = 3.68 \cdot 10^{-2}$ |
| 4 | $C_R = 50\%$ | $MSE_1 = 8.11 \cdot 10^{-2}$ | $MSE_2 = 5.91 \cdot 10^{-2}$ |
| 3 | $C_R = 62.5\%$ | $MSE_1 = 1.11 \cdot 10^{-1}$ | $MSE_2 = 9.64 \cdot 10^{-2}$ |
| 2 | $C_R = 75\%$ |  $MSE_1 = 1.25 \cdot 10^{-1}$ |  $MSE_2 = 1.34 \cdot 10^{-1}$ |
| 1 | $C_R = 87.5\%$ | $MSE_1 = 4.94 \cdot 10^{-1}$ | $MSE_2 = 1.41 \cdot 10^{-1}$ |

Table (1) : simulation results



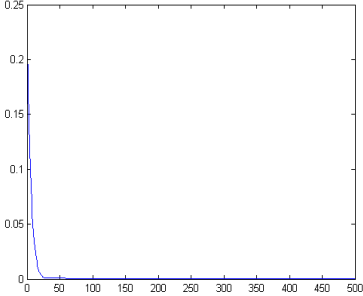
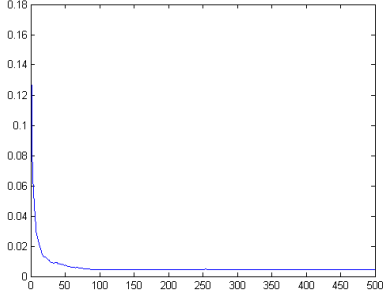
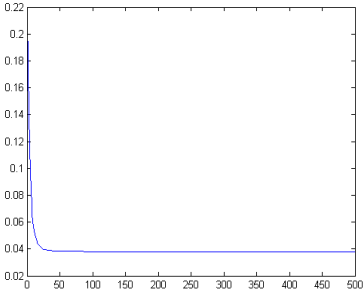
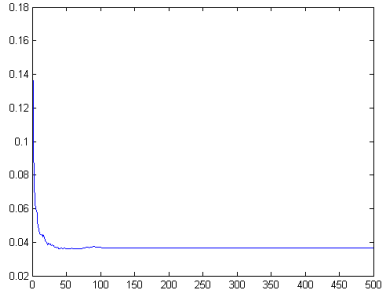
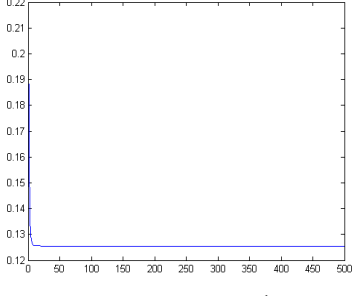
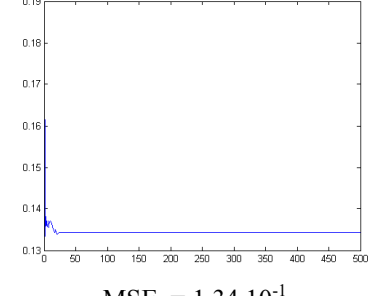
| | | | |
|-----------------------|----------------|---|--|
| Phase bits number r | $C_R \%$ |  |  |
| | | Image $I_0(1)$ | Image $I_0(2)$ |
| 64 | | $MSE_1 = 8.82 \cdot 10^{-5}$ | $MSE_2 = 6.54 \cdot 10^{-4}$ |
| 16 | | $MSE_1 = 1.64 \cdot 10^{-4}$ | $MSE_2 = 5.82 \cdot 10^{-4}$ |
| 8 | $C_R = 0\%$ |  |  |
| | | $MSE_1 = 5.74 \cdot 10^{-4}$ | $MSE_2 = 4.48 \cdot 10^{-3}$ |
| 7 | $C_R = 12.5\%$ | $MSE_1 = 1.11 \cdot 10^{-3}$ | $MSE_2 = 7.31 \cdot 10^{-3}$ |
| 6 | $C_R = 25\%$ | $MSE_1 = 6.62 \cdot 10^{-3}$ | $MSE_2 = 2.21 \cdot 10^{-2}$ |
| 5 | $C_R = 37.5\%$ |  |  |
| | | $MSE_1 = 3.80 \cdot 10^{-2}$ | $MSE_2 = 3.68 \cdot 10^{-2}$ |
| 4 | $C_R = 50\%$ | $MSE_1 = 8.11 \cdot 10^{-2}$ | $MSE_2 = 5.91 \cdot 10^{-2}$ |
| 3 | $C_R = 62.5\%$ | $MSE_1 = 1.11 \cdot 10^{-1}$ | $MSE_2 = 9.64 \cdot 10^{-2}$ |
| 2 | $C_R = 75\%$ |  |  |
| | | $MSE_1 = 1.25 \cdot 10^{-1}$ | $MSE_2 = 1.34 \cdot 10^{-1}$ |
| 1 | $C_R = 87.5\%$ | $MSE_1 = 4.94 \cdot 10^{-1}$ | $MSE_2 = 1.41 \cdot 10^{-1}$ |

Table (2) : simulation results

REFERENCES

- [1] A. Alfalou, C. Brosseau "The nuts and bolts of optical image compression and encryption methods," **submitted**.
- [2] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, **20**, 767-769 (1995).
- [3] J. W. Goodman, [Introduction to Fourier Optics], McGraw-Hill, New York, (1968).
- [4] L. G. Neto, and Y. Sheng, "Optical implementation of image encryption using random phase encoding," *Optical engineering*, **35**, n°9, 2459-2463 (1996).
- [5] G. Unnikrishnan, J. Joseph and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," *Optics Letters*, **25**, 887-889 (2000).
- [6] N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," *J. Opt. Soc. Am. A*, **16**, 1915-1927 (1999).
- [7] G. Unnikrishnan and K. Singh, "Optical encryption using quadratic phase systems," *Optics Communications*, **193**, 51-67 (2001).
- [8] G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters*, **29**, 1584-1586 (2004).
- [9] F. Goudail, F. Bollaro, B. Javidi, and P. Réfrégier, "Influence of a perturbation in a double phase-encoding system," *J. Opt. Soc. Am. A*, **15**, 2629- 2638 (1998).
- [10] S. Kishk and B. Javidi, "Information Hiding Technique with Double Phase Encoding," *Applied Optics*, **41**, 5462-5470 (2002).
- [11] Y. Frauel, A. Castro, T. J. Naughton, and B. Javidi, "Resistance of the double random phase encryption against various attacks," *Opt. Express* **15**, 10253-10265 (2007).
- [12] Z. Liu, S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Opt. Commun.* **275**, 324-329 (2007).
- [13] E. Darakis and J. J. Soraghan, "Reconstruction domain compression of phase-shifting digital holograms," *Applied Optics* **46**, 351-356 (2007).
- [14] A. Alkholidi, A. Alfalou, and H. Hamam, "A new approach for optical colored image compression using the JPEG standards," *Signal Processing* **87**, 569-583 (2007).
- [15] A. Alkholidi, A. Cottour, A. Alfalou, H. Hamam, and G. Keryer, "Real-time optical 2D wavelet transform based on the JPEG2000 standards," *Eur. Phys. J. Appl. Phys.* **44**, 261-272 (2008) .
- [16] A. Loussert, A. Alfalou, R. El Sawda, and A. Alkholidi, "Enhanced System for image's compression and encryption by addition of biometric characteristics", *Int. J. Software Eng. and Appl.* **2**, 111-118 (2008).
- [17] A. Alfalou, A. Mansour, "A new double random phase encryption scheme to multiplex & simultaneous encode multiple images," **Submitted**.