



A new double random phase encryption scheme to multiplex and simultaneous encode multiple images

Ayman Alfalou, Ali Mansour

► To cite this version:

Ayman Alfalou, Ali Mansour. A new double random phase encryption scheme to multiplex and simultaneous encode multiple images. Applied optics, 2009, 48 (31), pp.5933-5947. hal-00579204

HAL Id: hal-00579204

<https://hal.science/hal-00579204>

Submitted on 23 Mar 2011

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

A new double random phase encryption scheme to multiplex & simultaneous encode multiple images

Ayman Alfalou^{1,*} and Ali Mansour²

¹ *Département optoélectronique, Laboratory L@BISEN, ISEN-BREST, 20 rue cuirassé Bretagne,
CS 42807, 29228 Brest Cedex 2, France*

² *Department of Electrical and Computer Engineering, Curtin University of Technology,
GPO Box U1987, Perth, WA, 6845, Australia*

**Corresponding author: ayman.al-falou@isen.fr*

Abstract:

In this manuscript, a new approach of multiplexing & simultaneous encoding of target images is presented. Our approach can enhance the encryption level of a classical “DRP” system, by adding a supplementary security layer. The new approach can be divided into two security layers. The first layer is called the multiplexing level which consists in using iterative Fourier transformations along with several encryption key-images. These latter can be a set of biometrical images. At the second layer, we are using a classical DRP system. The two layers enable us to encoding several target images (multi-encryption) and to reduce, at the same time, the requested decoded information (transmitted or storage information).

OCIS codes: 070.0070, 070.4560, 100.2000, 200.4560, 999.9999 (optical encryption).

1. Introduction

In the last two decades, the development of secure transmission systems becomes the priority of many research and engineering institutions. In fact, many approaches can be found in the literature. Among these methods, cryptography methods are very attractive ones which consist in transforming original information to an illegible format (encrypted information). To retrieve the original information, encryption keys and encryption methods are required. To reduce the processing time, an increase attention has been recently paid to optical encoding methods. In addition, multi-encryption and a very good encoding level including a biometric key (as digital fingerprints) are required in many recent applications. The study proposed in this manuscript deals with the latest mentioned problems.

In [1-7], methods using a double random phase have been proposed. Different other methods can be found in the literature. The latter methods are based on: Digital holography [8,9], Fresnel domain [10,11], multiplexing [12,13], polarized light [14], and interferometer [15,16]. We should mention here that Fractional Fourier transform is essential to perform some optical encryption algorithms, further details can be found in [17-19]. To support modern applications, multiple image encryption methods have been recently proposed [20]. The main idea of the multi-encryption methods consists in encoding the phase and the amplitude of two original images and combines them into a single image.

To meet the requirements of modern applications with a high encoding level, a modified and an improved version of a **Double Random Phase** encryption system “**DRP**” is proposed in this manuscript. **DRP** systems are very attractive thanks to their simple implementation, robustness

and their easily application on several different image formats (B&W, gray level or colored images). To increase the security level of a classic DRP system, we firstly use several and independently keys. In fact, we are using two different kinds of image-keys: random and structural images. Secondly, we are using different multiplexing algorithms. We should mention that at least one image-key can be a biometric image. Our modified method can be summarized as following:

- The first level consists in multiplexing several target images using a set of iterative Fourier transformations. In this stage, several encoding-keys, including known biometric images, should be used. This level can be done off-line (numerically) to avoid the complexity of an all optical implementation.
- The second level, more traditional, is based on the use of double random keys.

We should mention that the DRP and the IFTA are two techniques well know in the literature. Should we mention here that, to the best of our knowledge, these two techniques have been never employed in tandem. Besides that, our new algorithm has shown very good results in various scenarios: using mono-dimensional signals (as speech, music and other acoustic signals) as well as bi-dimensional data (as black and white, grayscale or colored images). Many experiments have been conducted to corroborate the performances and the convergence of our approach.

The principal idea of our approach consists in using two encryption levels to avoid implementing a simple phase mask as the input of a classical DRP. In fact, by using IFAT and a known image (such as the fingerprint), we can encrypt at same time the amplitude and the phase of target image or mixed images. By doing so, mainly three advantages can be obtained:

- 1- Cracking and hacking the encrypted images become harder. Let us imagine the case when a hacker may crack the DRP key, i.e. the second mask which is the random phasis, he could still not obtain the target image as it is protected by the first mask and the other auxiliary keys (i.e the mixed images).
- 2- All acts of piracy on the encrypted image could affect the first mask, i.e. the hidden fingerprint. In this case, we can easily notice if the received image has been intercepted and modified.
- 3- This approach could be also used as a water-marketing technique. Some useful information (copyright, version, etc) can be easily hidden in the encrypted image.

This manuscript is organized as follows: Section 2 describes classical DRP systems. In section 3, our modified algorithm is presented. To corroborate our new approach, simulations are shown in that section. Section 4 presents the multiplexing and simultaneous encryption of several target images. Finally, conclusions and future works are given in section 5.

2. Classical Double Random Phase “DRP”: Mono-encryption system

In the last two decades, various optical encoding approaches have been proposed. These works can be traced back to the original work proposed initially by Ph. Refergier and B. Javidi [1]. In their approach, Ph. Refergier and B. Javidi proposed an image encryption scheme based on the modification of the spectral distribution. Without any prior information about the spectral modification or the target image, the image decoding cannot be done. The main idea of their

approach, see figure 1, consists in inserting two encoding-keys (**random phase**) in a setup called “**4f**”. The proposed approach consists mainly of three stages:

- The first key, i.e. the first Random Phase Mask **RP₁**, is multiplied by a target image (the image which should be encrypted). The latest image should be displayed in the input plane of a “**4f**” setup and lighted with a parallel coherent light resulting from a Laser generator. This procedure introduces a first modification to the spectrum of the target image.
- The second key (i.e. **RP₂**) is directly inserted into the image spectrum in the Fourier plane. The multiplication of the **RP₂** by the spectrum obtained at the first stage can introduce a second modification into the spectrum of the target image.
- Finally, a second optical Fourier transformation is carried out using a second lens to obtain the encoded image in original 2D space images.

This approach can generate a high-noise encrypted image. We should mention that the simplicity and the easy implementation of this approach make it very attractive. On the other hand, its drawbacks are emphasized in the literature [21-23]. Recently, the authors of [21] meticulously analyzed this approach and they proposed a large number of possible attacks. In the same work, they suggested few propositions to increase the encoding rate of **DRP** systems: One should use a huge number of encoding keys and we should very often change them. In this manuscript, a new scheme satisfying their propositions is proposed. In addition, another security layer has been added. Further details are provided in the following.

3. Multiplexing and simultaneous images encryption: multi-encryption **DRP** system

In specific applications (such as military applications, police identification procedures, online banking systems, etc.), a robust encoding systems are highly required. Here, we reinforce the encoding rate of a classical “mono-**DRP**” system by adding another security layer. The main idea of our approach (multi-encryption system), consists in multiplexing target images (I_0, I_1, I_2 etc which are images to be encrypted) with at least a key-image. The latest procedure realizes our first security level, see figure 2-a. At our second encoding level, we introduce the outcomes of our first encoding level as the input of a classical **DRP** system. The result of the first layer is a complex image “ $I_i e^{i\varphi_i}$ ” which is completely different from the original target image (figure 2-b), where “ I_i ” is a known image used in our **DRP** stage. This image could be a bio-metric image such as a digital fingerprint. Finally, as shown in figure 2, the output of our system is a two layer encrypted image “ $I_c e^{i\varphi_c}$ ” obtained by two independent sub-systems.

To simplify the principle of our new scheme and without any loss of generality, only two images (I_0 and I_1) will be used in the first encoding level: I_0 is a grayscale digital image and I_1 is a known white-black image of a fingerprint or a photo. Before applying the iterative Fourier transform algorithm, the target image I_0 should be multiplied by a pure random phase function $[0, \pi]$.

3.1 Encryption

The synoptic diagram of our approach with two encoding independently levels is illustrated in figure 3. 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 “ $\rho_1 e^{i\varphi_{11}}$ ”. Then, we carry out successively several

Fourier Transformations ($\mathbf{FT}(\cdot)_n$) by modifying for each iteration the phase function until “ ρ_1 ” (amplitude of the target image spectrum I_0 modulated with a function phase) converges towards “ I_1 ” (with I_1 could be a known black and white image as fingerprint (its own fingerprint for example) or grayscale image as a photo, *etc*). After “ $\mathbf{N}$ -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):

$$I_1 e^{i\varphi_{1n}} = \mathbf{FT}_n(I_0 e^{i\varphi_{0n}}) \quad (1)$$

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, will be detailed in the following paragraph. Then, this complex image “ $I_1 e^{i\varphi_{1n}}$ ” is introduced at the input of the classical **DRP** (second level). Thus, this complex image is multiplied by a first random phase key “ $I_1 e^{i(\varphi_{1n} + \varphi_{A1})}$ ”. After a Fourier transform, we multiply this spectrum with a second random phase key “ $e^{i(\varphi_{A2})}$ ”. Finally, a last Fourier transform gives, in the output of our system, the doubly encrypted image with two different and independently layers “ $I_c e^{i\varphi_c}$ ”.

3.2 Mathematical Concepts and Convergence

In [19] Z. Liu and Sh. Liu proposed a double encryption based on iterative fractional Fourier transform. This approach is similar to the first layer of our encryption system. In fact, in this manuscript, an iterative Fourier transform is considered. To get benefit of the high security level offered by these methods and the simplicity of the Fourier transform which can be done optically using a single convergent lens. The convergence of the iterative Fourier transform could indeed be similar to the convergence of the algorithm proposed by [19]. We should

mention that the convergence analysis has not been considered in [19]. Indeed, the authors showed the convergence of their algorithm through the outcomes of their conducted simulations. In this section, this analysis of the convergence will be discussed. Without loss of generality and for seek simplicity, the convergence of the iterative 1D Fourier transform is considered instead of the 2D Discrete Fourier transform. The case of 2D Fourier transform required in our algorithm is just straightforward [24-26]. Fig. 4 shows the results of applying our algorithm on speech signals. We should just mention that the absolute value of the signals should only be considered instead of the original real zero-mean signals. Fig. 5 shows the convergence of the Mean Square Error (MSE). Let $x(t)$ and $Y(f)$ respectively be the target signal and the key signal. The main loop of the iterative Fourier transform can be simplified as following; further details can be founded in the Matlab code provided in appendix A:

$$\begin{aligned}
& \text{for } i = 1:T \\
& X_1(f) = TF(x(t)\exp(j\varphi_1(t))) \\
& \varphi_s(f) = \text{angle}(X_1(f)) \\
& y(t) = TF^{-1}(Y(f)\exp(j\varphi_s(f))) \\
& \varphi_1(t) = \text{angle}(y(t)) \\
& \text{end}
\end{aligned} \tag{2}$$

By considering the above equations, we can roughly consider that at each iteration the amount of information in “ $\varphi_1(t)$ ” and related to $Y(f)$ will be increased [27]. At the same time, $\varphi_1(t)$ will also contain more information about $x(t)$. In the following, we will give some hints to prove the previous basic reasoning.

The mean square error (**MSE**) is considered as the convergence criterion of our algorithm. In this case, one should prove that the nonlinear “angle” function of the Fourier transform of target signal is an optimal solution of **MSE**:

$$\underset{\varphi(t)}{\text{Min}} E \left\| TF^{-1}(Y(f)\exp(j\varphi(f))) - x(t) \right\|^2 \tag{3}$$

It is obvious that the minimisation of equation (3) is a minimization of energy functional [28-30]. We should mention here that there is no general or unique solution for such problem. However, few approximation numerical methods can be founded in the literature [31-33]. The main idea of the latter methods consists in approximating the solution using a projection in a set of kernel functions. These numerical methods can't be used to prove that the nonlinear "angle" function (i.e. the phasis of the Fourier transform) is a solution that belongs to the set of optimal solutions of equation (3). However, by using Taylor series and the previous methods, we can approximate the solution. The proof using the minimisation of energy functional is beyond the scope of this manuscript.

We mention that intensive simulations have been conducted to corroborate the performance and the convergence of the proposed algorithm. In following sections, some simulations are shown and discussed.

3.3 Algorithm

Figure (6) shows the flowchart of our algorithm which can mix multiple target images together and modify them towards a single known image-key. At first a random and a pure phase " $e^{i\varphi_0}$ " should be selected. The multiplication of the latter phase function by the first target image " I_0 " gives us a modulated image equal to: " $I_0 e^{i\varphi_0}$ ". Once the multiplication is done, a first Fourier Transformation of this modulated image is carried out. Then, a comparison test (i.e. a convergence criterion) is required to compare the amplitude of the obtained spectrum " ρ_1 " and the key-image " I_1 " (which is a black and white known image or it could be a grayscale image, as its own digital fingerprint or a photo). The Mean square error "**MSE**" is widely used as a

convergence criterion. Therefore in our algorithm, we evaluated the MSE between the amplitude of the spectrum “ ρ_1 ” obtained at the first stage and the image-key “ I_1 ” as that is shown in equation (4), with (M, N) are the pixel size of the images.

$$MSE = \frac{1}{M \times N} \sum_i^N \sum_j^M |\rho_1(i, j) - I_1(i, j)|^2 \quad (4)$$

The encryption is considered achieved when the value of obtained **MSE** becomes lower than a preselected threshold “**C**”. The value of the threshold should be wisely adjusted. In fact, a very small value of “**C**” means a better performance but more computing efforts and processing time are needed. If the convergence is achieved, the first level output image can be written as: “ $\rho_1 e^{i\phi_{1n}} = I_1 e^{i\phi_{1n}}$ ”. Otherwise, if ($\rho_1 \neq I_1$), we change “ ρ_1 ” by “ I_1 ” and we apply an inverse Fourier transform. This Inverse Fourier transform enables us to return our obtained image in the image domain. In a similar way, we should compare the amplitude “ ρ_0 ” of the inverse Fourier transform with the target image “ I_0 ”. For that, we estimated another **MSE** between “ ρ_0 ” and “ I_0 ” and we compared its value with a second threshold “**CC**”. If “ $\rho_0 \neq I_0$ ”, we replaced “ ρ_0 ” by “ I_0 ” and another iteration should be done. The convergence of our algorithm is achieved when a measurement error applied to image I_0 and respectively to I_1 becomes less than a fixed threshold “ $\epsilon_0 = C$ ” and respectively “ $\epsilon_1 = CC$ ”.

3.4 Effect of the iteration number

We should mention here that in all conducted simulations, good results have been obtained in less than 50 iterations. For this reason, we implemented a simplified version of the proposed algorithm mainly to decrease the processing time. The simplified version is given in appendix A. in that version a fixed number of iterations is used instead of the output of the **MSE**.

However, the first version can obviously be implemented. In order to fix the needed number of iterations to obtain optimal performance, a heuristic analysis is conducted. In this section, the effect of the iteration number on the performance of our proposed algorithm is emphasized.

The following example shows the effect of the iteration number on the quality of obtained images using the algorithm described in Fig. 6. Let us consider two images: A black-white image and a gray level image; see Fig. 7. Figure 8 shows the **MSE** values between the origin image and the image obtained after “**500**” iterations and “**3000**” iterations.

Figure 8 emphasizes the strong convergence of our algorithm. Once the MSE becomes less than our threshold, then the convergence of our algorithm is achieved. In this case, the spectrum of processed image becomes a real image multiplied by a phase function. This result proves that we finally can get:

$$I_0 e^{i\varphi_{0n}} \approx I_1 e^{i\varphi_{1n}} ; \quad I_1 e^{i\varphi_{1n}} = FT(I_0 e^{i\varphi_{0n}}) \quad (5)$$

The previous equation is the solution of equation (3). As mentioned before, in many simulations, 50 iterations were enough to obtain satisfactory or good results. Hereinafter, we select 500 as the maximum number of iterations.

3.4 Validation by numerical simulations

Many simulations were conducted to show the effectiveness and the performance of our algorithm. Figure (9) presents one target image and one known image-key, both of them are grayscale images: The target image is “Florent” and “Lena” is the known key-image. After **N = 25** iterations, our algorithm converges and we obtain the image shown in figure (9-c) with a “**MSE = 0.0014**”. After “**500**” iterations, a slightly improved image was obtained, with “**MSE =**

$1.2869 \cdot 10^{-4}$ " (figure 9-d). In the second stage of our encryption approach, the outcome of the first stage, i.e. the image shown in Fig 9-c or Fig 9-d, is used as the input of a classical **DRP**. In the **DRP** part, two random phase masks are used. The final encrypted image is shown in figure (10). The final result presented in Fig. 10 shows the high quality of encryption that could be obtained by two stage encryption scheme. The iterative Fourier transform could reinforce the encryption done by a classical DRP system. In the following, the influence of algorithm parameters will be investigated.

3.6 Decryption

The main advantage of our proposed algorithm is its ability to be implemented using an all-optical system. In fact, once the convergence is attained, our system can be considered as a simple Fourier transform applied to the product by phase functions of input images. Besides, the classical **DRP** system could be realized using an all-optical system. The decryption system could also be implemented by mainly using an all-optical system. The latter system is described in the next section. We should mention here that all-optical systems have many advantages comparing to classical digital systems. The main advantages are:

- 1- High speed (almost the light speed) processing.
- 2- A Fourier transform or an inverse Fourier transform can be realized using a simple convergent lens
- 3- Compact systems: While classical digital systems require digital cameras, processing unites, memories, power supplies, etc.; optical systems can be made very compact.

A powerful encryption system becomes useless without the existence of a corresponding decryption system which allows us to retrieve the hidden transmitted information. Hereinafter, we will describe a decryption system that could retrieve the target image from the final two level encrypted image $(I_c e^{i\varphi_c})$. At the receiver, we assume that various encryption keys: $e^{(i\varphi_{A2})}$ & $e^{(i\varphi_{A1})}$ are known. Fig. 11 presents a synoptic diagram of our decryption system:

- At first, an inverse Fourier Transform of the encrypted image $(I_c e^{i\varphi_c})$ should be conducted.
- Then, we multiply the obtained spectrum by the second phase random key conjugate “ $e^{-(i\varphi_{A2})}$ ”.
- Later on, we should carry out a second inverse FT.
- The outcome of the inverse Fourier transform should be multiplied by a second phase random key conjugate “ $e^{-(i\varphi_{A1})}$ ”. In this step, the digital fingerprint, modulated with a phase function “ $(I_1 e^{i\varphi_{1n}})$ ”, is obtained.
- Finally, the decrypted image I_0 could be obtained as the modulus of another inverse Fourier transform “ $|I_0 e^{i\varphi_{0n}}| = I_0$ ”.

By introducing a known key-image (as a digital fingerprint) at the first stage of our algorithm, two main benefits could be observed:

- One could perform the multiplex of various target images to reinforce the encryption result.
- Any unauthorized modification on the transmitted encrypted image $(I_c e^{i\varphi_c})$. (i.e. an image attack) could be easily detected at the reception stage. Indeed, any vandalism attempt (attacks) results in a modification of the encrypted image

$(I_c e^{i\varphi_c})$. The latter modification could be detected at the output of the first decryption stage as the digital fingerprint is well known to all authorized users.

Fig. 12 presents the outcomes of our encryption-decryption systems. These results were obtained after “25” iterations. We should mention that we succeeded in decrypting the encrypted image with a very low **MSE** =0.0173. The low value of MSE proves the good decryption performances obtained by our approach. This low value makes possible the encryption-decryption of multiple target images.

3.7 Hacking

Previous sections show good experimental results which are obtained using our proposed algorithm with two layers of encryption security. In this section, the robustness of our approach to cracking or hacking procedure is considered. Several modifications of classic DRP can be found in the literature [34]. Most of them can be straightforward included in our system to improve the robustness of our DRP stage. We should mention that the major weakness of a classic DRP is the possibility for a hacker to crack the second key, i.e. the random phase mask. In this case, the hacker can easily retrieve the decrypted image. This problem could be solved using our approach. In fact, at the first stage of our algorithm, the principal image has been intentionally modified. Therefore, without priori information, the hacker can’t obtain the other keys (the mixed images) by simply intercepting and processing the encrypted image. On the other hand, without the knowledge of all used keys, the original image can’t be clearly retrieved. In order to prove the latter statement, many simulations results have been conducted.

In the following simulation, the target image is a real greyscale image shown in figure (13-a). Let us consider “Lena’s” photo as the known image, i.e. the first key shown in fig (13-b). The encrypted image is shown in figure (13-c). If the hacker has successfully found the key of the classical DRP, he will be able to find the known image up to a phase function as shown in figure 13-d. By applying a Fourier transform on the retrieved image, one can obtain the image shown in figure 13-e. This result clearly shows that the original image can’t be obtained without knowing the second key of the DRP. The task of hacking becomes more and more difficult when the number of mixed images is increased.

4. Multiplexing and simultaneous encryption of multiple target images.

In previous sections, the case of two target images has been discussed. Here, a most general case, with a set of target images, is considered. Hereinafter, the extension of our approach to encrypt simultaneously several target images is described. The encryption system is based on DRP-Multi-encryption. To illustrate the power of our proposed approach comparing to the classical Mono-DRP system, we compared the outcomes of both algorithms applied to encrypt same real target images $(I_1, I_2, \dots, I_m)$.

4.1. Mono-DRP system

From a practical point of view, the encoding of multiple target images can be simply obtained by successively encrypt various target images using the classical mono-DRP system. Two cases can be distinguished, see figure (14):

1. The first case illustrated in figure (14-a) consists in the encryption of all target images ($I_1, I_2, \dots, I_m$) using the same phase random keys “ $e^{(i\varphi_{A2})}$ & $e^{(i\varphi_{A1})}$ ”. In the decryption system, all encrypted images $I_{c1}e^{(i\varphi_{c1})}, I_{c2}e^{(i\varphi_{c2})}, \dots, I_{cm}e^{(i\varphi_{cm})}$ and one key “ $e^{(i\varphi_{A2})}$ ” are needed. However according to [21] this case does not offer a high encoding rate because the same encryption keys are used in the whole process.
2. The second case, shown in figure (14-b), consists in using different encryption keys for every target image. This case offers a higher encoding rate. However, it seriously increases the required transmitted information. In fact, the decryption stage necessities all encrypted images $I_{c1}e^{(i\varphi_{c1})}, I_{c2}e^{(i\varphi_{c2})}, \dots, I_{cm}e^{(i\varphi_{cm})}$ as well as all keys $e^{(i\varphi_{A12})}, e^{(i\varphi_{A22})}, \dots, e^{(i\varphi_{Am2})}$.

4.2. The proposed Multi-encryption-DRP system

Using classic **DRP** to encrypt a set of N_t target images has two major drawbacks:

- $2 N_t$ random phase keys should be used.
- N_t encrypted images should be processed.

It is clear that this procedure involves huge amount of data which requires huge memories, enormous transmission time and computing efforts. These problems can be solved by considering our approach. In fact, the target images could be mixed together to form one mixed image using the first layer of our approach. Later on, the mixed image should be considered as the input of standard **DRP**. The mixing procedure can be achieved using various methods. One of them is the method proposed in [35] and it is based on the fusion of relevant information in the Fourier plane. However, the latter approach doesn't achieve good performances. In fact, this approach is mainly based on the extraction of critical spectrum information from each target image. Therefore, the spectrum space should be shared by all these spectrum information. When

the number of target images increases the reserved spectrum information for every target image will decrease. This can result in important deterioration of reconstructed images [34].

Hereinafter, an alternative method to mix multiple target images is proposed. A multi-encryption is performed by multiplexing various target images together. This multiplexing is realized using our algorithm which is based on iterative Fourier transformations. We called this approach the Multi-encryption-DRP system, see Figure (15). Our encryption system consists of two stages:

1. At first, various independent target images should be jointly equalized to a single image “ $I_m e^{i\varphi_m}$ ”. This multiplexing can be done using adequate phase functions which are making it possible to write: $I_j e^{i\varphi_j} = FT(I_{j-1} e^{i\varphi_{j-1}})$. The algorithm is discussed in section 4.3.
2. A second encryption level is obtained as the output of a traditional DRP-system.

In our approach, the mixing of various target images can result in a unique image which contains all necessary information for the decryption process. The obtained mixed image should be used as the input of a classical DRP. In this case, we are getting double encryption layers. Our simulation results show very good performances of our approach. Other aspects of our algorithm, such as the convergence and the compression ability, are also studied.

4.3. Multi-Layer Encryption-Decryption Algorithm

Hereinafter, an extend version of our algorithm proposed in figure 6 is presented, see Fig. 16. Let us considered m target images ($I_1, I_2, \dots, I_m$). At first only two target images (I_1, I_2) is considered as the input of the first layer. At the convergence, we obtained two other

images $(I_1 e^{i\varphi_1}, I_2 e^{i\varphi_2})$. The second step is similar to the first one except for the two considered images $(I_2 e^{i\varphi_2}, I_3)$. The convergence of the second step generates two new images $(I_2 e^{i\varphi_2}, I_3 e^{i\varphi_3})$. This procedure should be continued until the last image, i.e I_m , has been taken into consideration. The final obtained image $(I_m e^{i\varphi_m})$ is used as the input of the **DRP** algorithm. The outcome of the **DRP** is the doubled encrypted image. The multi-encryption can be resumed using the following steps:

- At first, two phase functions (φ_1, φ_2') have been adjusted to satisfy the following relationship: $I_2 e^{i\varphi_2'} = FT(I_1 e^{i\varphi_1})$.
- Another iterative Fourier transforms should be carried out to find two new phase functions $(\varphi_2'', \varphi_3')$ which satisfy similar relationship correspond to other target images (I_2, I_3) : $I_3 e^{i\varphi_3'} = FT(I_2 e^{i\varphi_2''})$.
- A difference phase function $\varphi_2 = \varphi_2' - \varphi_2''$, corresponding to the second image I_2 , is evaluated.
- Using similar way, the other phase functions $(\varphi_3, \varphi_4, \dots, \varphi_{m-1})$ could be calculated.
- After the fourth step, a new image $I_m e^{i(\varphi_m)}$ is obtained. This latter is used as the input of our second level (classical **DRP**) after multiplying it with a first phase random mask. The output of the **DRP**, i.e. the final encrypted image $I_c e^{i(\varphi_c)}$ is obtained. The final encrypted image contains different keys and necessary information to decrypt target images.

The decryption system necessities the knowledge of:

- $I_c e^{i(\varphi_c)}$: encrypted image at output of our multi-encryption system,

- φ_{A2} : the second random encryption key using a traditional **DRP** system,
- φ_{A1} : the first random key of traditional **DRP** system,
- $\varphi_3, \varphi_4, \dots, \varphi_{m-1}$: Various phase functions which have been used in the multiplexing of various target images.

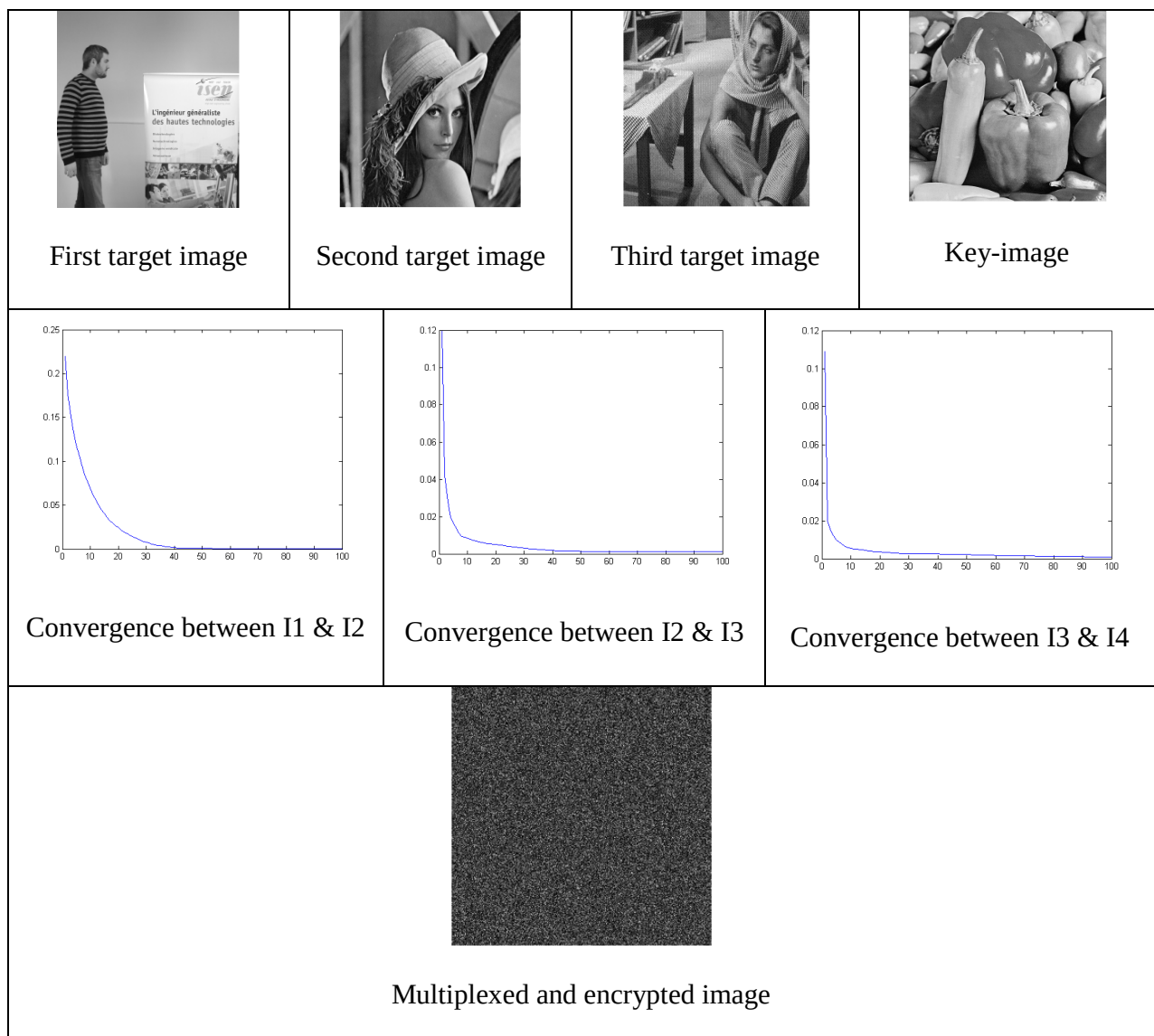
4.4. Convergence of Multi-Layer -Encryption-Decryption Algorithm.

Various simulations have been conducted to show the performance and the convergence of our algorithm as well as the impact of an increasing number of target images on the quality of decrypted images. It is obvious that an increasing number of target images is the most important issue to the stability, the convergence of our algorithm and the quality of reconstructed images. In this section, we emphasize the impact of this number. Using three images (two target images and one key image), encryption and decryption parts of our algorithm have shown very good results: very weak values of **MSE**, 1.014×10^{-4} and 5.15×10^{-5} , are obtained. When the number of target images is increased to three, once again, the convergence is reached and good results are observed; see the second row of table 1. The encrypted image is shown in the third row of the same table. By increasing further the number of target images, we notice a small deterioration of decrypted images. However, the convergence has been always obtained and the quality of the reconstructed images could be improved by increasing the number of iterations.

Other simulations have proved that our algorithm is more sensitive to the bit number. To better compress the involved images, the number of bits should be decreased. On the other hand, the reduction of this number has a big impact of the quality of reconstructed images. This effect

has been emphasized in our recent study presented in SPIE conference Europe Security and Defence / September 2009 in Berlin. A resume of that study is given in the following.

Hereinafter, a comparison between a standard **DRP** and the proposed algorithm is given. This comparison takes into consideration the required information, the image quality among other performance indexes to encrypt-decrypt multi target images.



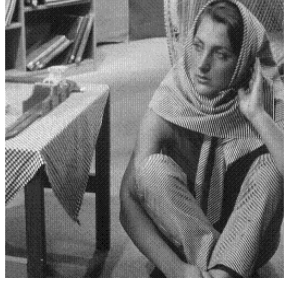
 $MSE = 1.738 \cdot 10^{-5}$	 $MSE = 4.6182 \cdot 10^{-4}$	 $MSE = 9.3561 \cdot 10^{-4}$
---	--	--

Table (1): The outcomes of our multi-encryption approach: multiplexed, encrypted, decrypted and demultiplexed images.

4.5. Comparison between two encryption techniques: Successive classical DRP and the proposed multi-encryption DRP.

It is clear that in our approach, we considerably reduce the size of transmitted information necessary to carry out the decryption of multiple target images. To highlight this fact, we compared the two techniques described in this section to encrypt and decrypt a set of real target images. Many simulations have been conducted. Table (2) shows one of the obtained results. In Table (2), four target images (256,256) pixels have been used.

The results presented in table (2), show that we considerably reduced the size of encrypted information (storage information and/or transmitted information), needed to encrypt a multiple target images. Indeed, a rate factor of 2 has been observed. Finally, we should notice that the compression ratio (between the two previously described techniques) increases according to the number of images. We are conducting studies to evaluate the reconstruction quality of the different target images according to the compression ratio.

Multi-encryption	Required information to decrypt “4” target images	Quantity express in K-Bytes	MSE between the target and decrypted images
Approaches using a classical DRP system	$I_{c1}e^{i(\varphi_{c1})}, \square, I_{cm}e^{i(\varphi_{cm})},$ $\varphi_{A21}, \varphi_{A22}, \square, \varphi_{A2m}$	$1048,5 + \dots + 1048,5$ + $524,2 + \dots + 524,2$ = 6 291.1 KBytes	0.0259
Approaches using a DRP system with two levels	$I_c e^{i(\varphi_c)},$ $\varphi_{A2}, \varphi_{A2}, \varphi_2, \square, \varphi_{m-1}$	$1048,57$ + $524,2 + \dots + 524,288$ = 3 145.7 KBytes	0.0264
		Compression rate between this tow methods equal to: « 2 ».	

Table(2): Comparison between two encryption techniques: Successive classical DRP and the proposed multi-encryption DRP.

4.6. Reduction of the bit number

In this section, we emphasize the impact of reducing the bit number on necessary information required to reconstruct target images. To clarify our idea and simplify the study, we only consider two grayscale images ($\mathbf{I}_0$ (1) and $\mathbf{I}_0$ (2)) with (256x256) pixels, see table (3). These images should be quantized using firstly a huge quantization number (up to 64 as usually used in Matlab, the quantization number is given in the first column of table 3). Then, lower quantization numbers are considered till reaching a binary encoding (with a single bit). The second column of table 2 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 6).

$$C_R = \frac{\sum_{i=1}^N \sum_{j=1}^M \sum_{k=1}^L |I_{0,i,j,k} - I_{R,i,j,k}|}{256 \times 256 \times 2} \times 100 \quad (6)$$

Columns 3 and 4 of table (3) present different reconstructed images with their corresponding MSEs values. We should mention that an optimal bit number should be used. This number should be resulted as a compromised solution to achieve good compression ratio and good encryption-decryption quality.

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	$C_R = 62.5\%$	$MSE_1 = 1.11 \cdot 10^{-1}$	$MSE_2 = 9.64 \cdot 10^{-2}$

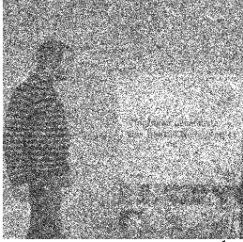
2	$C_R = 75 \%$	 $MSE_1 = 1.25 \cdot 10^{-1}$	 $MSE_2 = 1.34 \cdot 10^{-1}$
1	$C_R = 87.5 \%$	$MSE_1 = 4.94 \cdot 10^{-1}$	$MSE_2 = 1.41 \cdot 10^{-1}$

Table (3): simulation results

5. Conclusions and prospects

In this manuscript, a new all-optical and two level encryption/decryption system is proposed. The new proposed system has several advantages compared to the classical system. Indeed, while the new algorithm is faster, it can achieve two level encryption securities, enables us to obtain better compression / transmission information rate, realizes a joint encryption of various target images and enables us to use biometrical key images. Many simulations have been conduct to corroborate the effectiveness and the good performance of the proposed algorithm. Our future works will emphasize the relationship between the reconstruction qualities of different target images according to the increase of compression ratio.

References

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, **20**, 767-769 (1995).
2. 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).
3. 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).
4. S. Kishk and B. Javidi, "Information Hiding Technique with Double Phase Encoding," *Applied Optics*, **41**, 5462-5470 (2002).
5. L. G. Neto, and Y. Sheng, "Optical implementation of image encryption using random phase encoding," *Optical engineering*, **35**, n°9, 2459-2463 (1996).
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. B. Javidi, N. Takanori, "Securing information by use of digital holography," *Optics Letters*, **25**, Issue 1, 28-30 (2000).
9. E. Tajahuerce, B. Javidi, "Encrypting three-dimensional information with digital holography," *Applied Optics*, **39**, Issue 35, 6595-6601 (2000).
10. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," *Optics Letters*, **29**, 1584-1586 (2004).
11. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimensional keys in the Fresnel domain," *Optics Letters*, **24**, 762-764 (1999).
12. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, "Multiple image encryption using an aperture-modulated optical system," *Optics Communications*, **261**, 29-33 (2006).
13. O. Matoba and B. Javidi, "Encrypted Optical Storage with Angular Multiplexing," *Applied Optics*, **38**, 7288-7293 (1999).
14. J. F. Barrera, R. Henao, M. Tebaldi, N. Bolognini, R. Torroba, "Multiplexing encrypted data by using polarized light", *Optics communications*, **260**, n°1, 109-112 (2006).
15. L. Cai, M. He, Q. Liu, and X. Yang, "Digital Image Encryption and Watermarking by Phase-Shifting Interferometry," *Applied Optics*, **43**, 3078-3084 (2004).
16. M. He, L. Cai, Q. Liu, and X. Yang, "Phase-only encryption and watermarking based on phase-shifting interferometry," *Applied Optics*, **44**, 2600-2606 (2005).
17. Z. Xin, Y. Sheng Wei and X. Jian, "Affine cryptosystem of double-random-phase encryption based on the fractional Fourier transform," *Applied optics*, **45**; 8434- 8439 (2006).
18. B. M. Hennelly and J.T. Sheridan, "Image encryption techniques based on fractional Fourier transform," *Proc. SPIE* **5202**, 76-87 (2003).
19. Z. Liu, S. Liu, "Double image encryption based on iterative fractional Fourier transform," *Optics Communications*, **275**, Issue 2, 324-329 (2007).
20. M. Z. He, L. Z. Cai, Q. Liu, X.C. Wang, X.F. Meng, "Multiple image encryption and watermarking by random phase matching," *Optics Communications*, **247**, Issues 1-3, 29-37 (2005).
21. 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).

22. A. Carnicer, M. Montes-Usategui, S. Arcos, and I. Juvells, "Vulnerability to chosen-cyphertext attacks of optical encryption schemes based on double random phase keys," *Optics Letters*, **30**, 1644-1646 (2005).
23. X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Optics Letters*, **31**, 1044-1046 (2006).
24. G.B. Folland, *Fourier Analysis and Its Applications* (Wadsworth & Brooks/ Cole, Pacific Grove, 1992).
25. M.A. Pinsky, *Introduction to Fourier Analysis and Wavelets* (Brooks/Cole, Pacific Grove, 2002).
26. C. Ioana, A. Mansour, A. Quinquis and E. Radoi, *Digital signal processing using matlab* (Wiley Science, UK, ISBN: 978-1-84821-011-0, 2008).
27. I. Yamaguchi, K. Yamamoto, G. A. Mills and M. Yokota, "Image reconstruction only by phase in phase-shifting digital holography," *Applied Optics*, **45**, 975-983 (2006).
28. J.E. Rubio, *The global control of nonlinear diffusion equations* (Manchester University Press; John Wiley, Manchester; New York, London, 1986).
29. H.L. Langhaar, *Energy Methods in Applied Mechanics* (John Wiley & Sons, New York, 1962).
30. T. J.Asaki, P. R. Campbell, R. Chartrand, C. E. Powell, K. R. Vixie, and B. Wohlberg, "Abel inversion using total variation regularization: applications," *Inverse Problems in Science and Engineering*. **14**, 873-885 (2006).
31. J. Van Kan; A. Segal; F. Vermolen, *Numerical Methods in Scientific Computing* (VSSD, Netherlands, ISBN 90-71301-50-8).
32. K. Atkinson and W. Han, *Theoretical Numerical Analysis* (Springer-Verlag, New York, 2001).
33. A.R. Alghofari, *Problems in Analysis Related to Satellites* (Ph.D. Thesis, The University of New South Wales, Sydney, 2005).
34. A. Alfalou and C. Brosseau "Optical Image Compression and Encryption Methods," *Advances in Optics and Photonics*, submitted (2009).
35. S. Soualmi, A. Al Falou and H. Hamam, "Optical image compression based on segmentation of the Fourier plane: new approaches and critical analysis," *J. Optics A, Pure and Applied Optics*, **9**, 73-80 (2007).

Figure Captions

FIG. 1: Synoptic diagram of classical **Double Random Phase** encrypted system: “Mono-encryption **DRP** system”

FIG. 2: Synoptic diagram of our multi-encryption approach

FIG. 3: A double random phase encryption system enforced by two encryption levels

FIG. 4: The outcomes of our algorithm applied on positive speech signals

FIG. 5: Convergence of the Mean Square Error (MSE)

FIG. 6: Proposed multiplexing Algorithm used in the first level of our multi-encryption scheme.

FIG. 7: Two input images (a target image and a key-image).

FIG. 8: Mean square errors with respect to iteration numbers.

FIG. 9: The outcomes of the first stage of our encryption algorithm

FIG. 10: The final encrypted Image $I_c e^{i\varphi_c}$ after 500 iterations

FIG. 11: A synoptic diagram of the decryption system.

FIG. 12: The outcomes of the encryption - decryption algorithm

Fig 13: Pirated image

FIG. 14: Encryption of a multiple target images using a **DRP** system.

FIG. 15: Synoptic diagram of Multi-encryption-**DRP** system

FIG. 16: Main ideas of our algorithm.

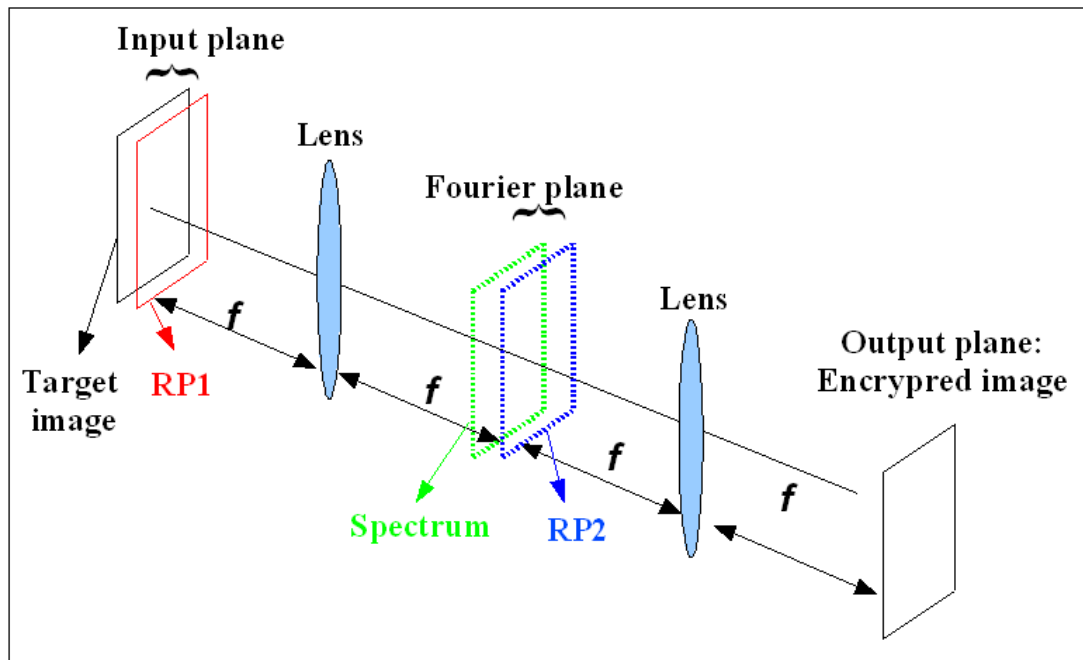


FIG. 1: Alfalou and Mansour

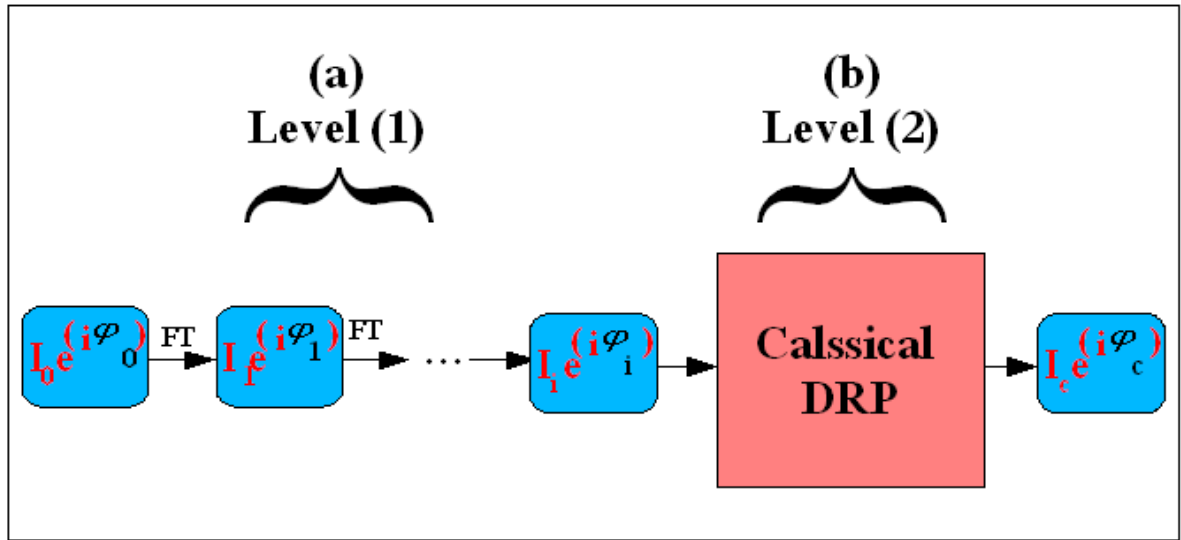


FIG. 2: Alfalou and Mansour

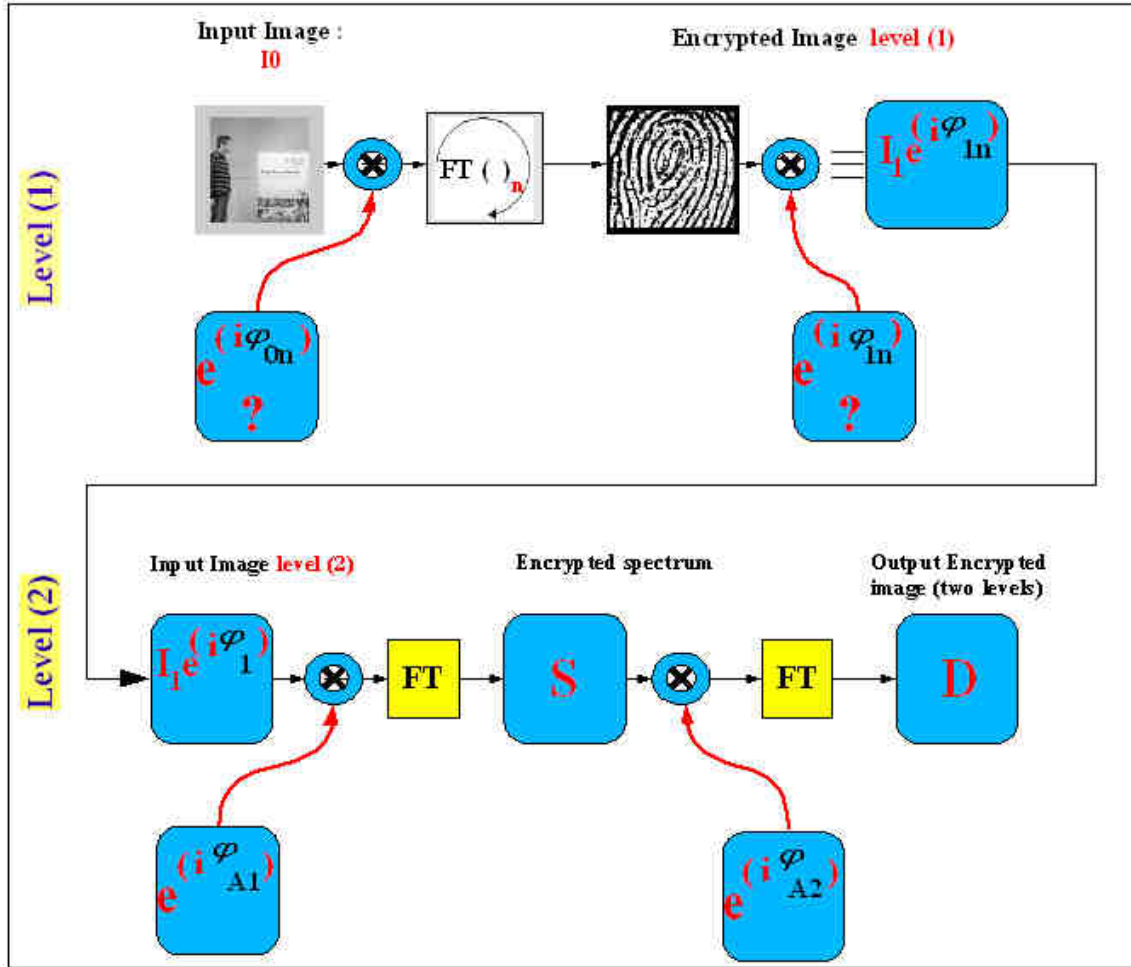
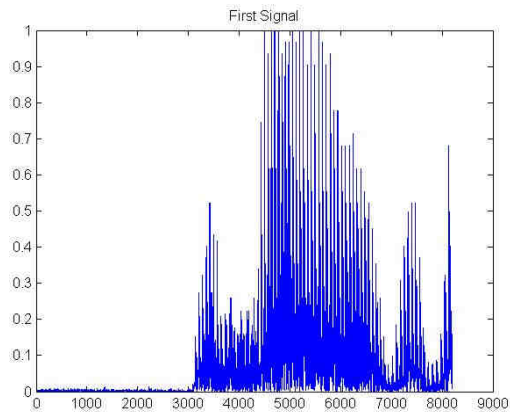
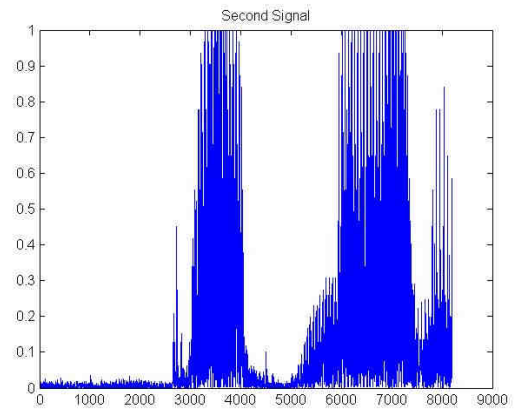


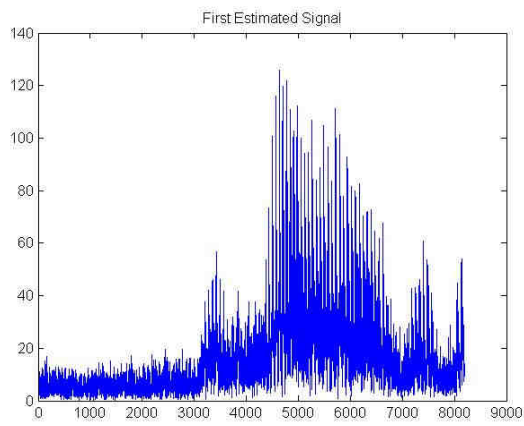
FIG. 3: Alfalou and Mansour



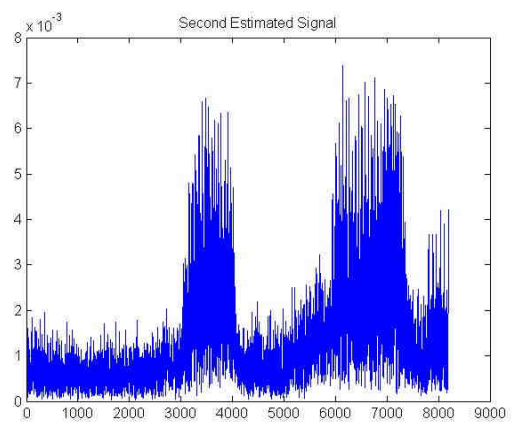
a) First Positive Signal



b) A Target Positive Signal



c) First Encrypted Signal



d) 2nd Encrypted Signal

FIG. 4: Alfalou and Mansour

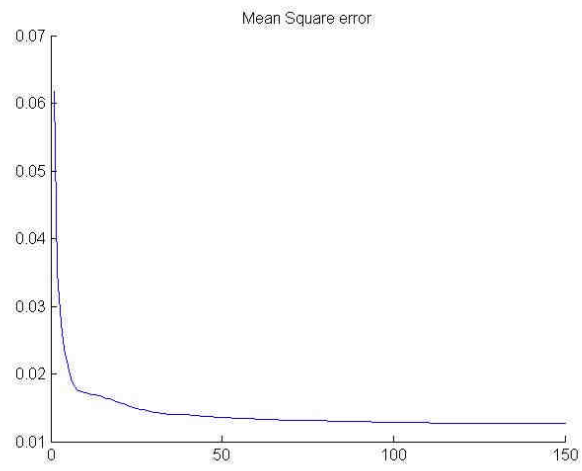


FIG. 5: Alfalou and Mansour

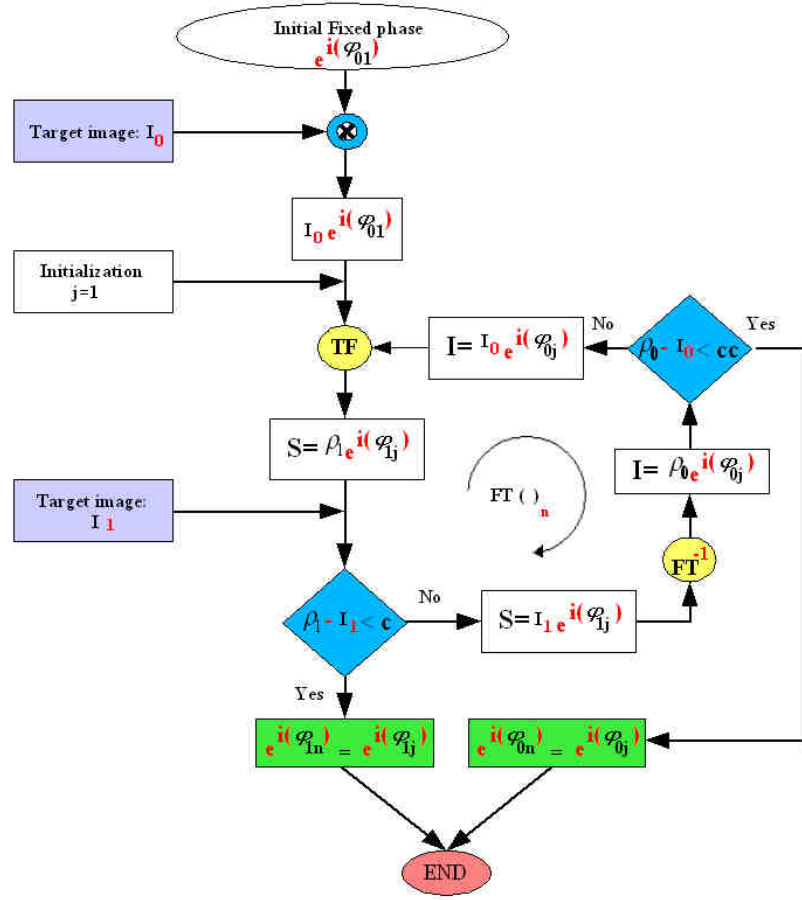


FIG. 6: Alfalou and Mansour



FIG. 7: Alfalou and Mansour

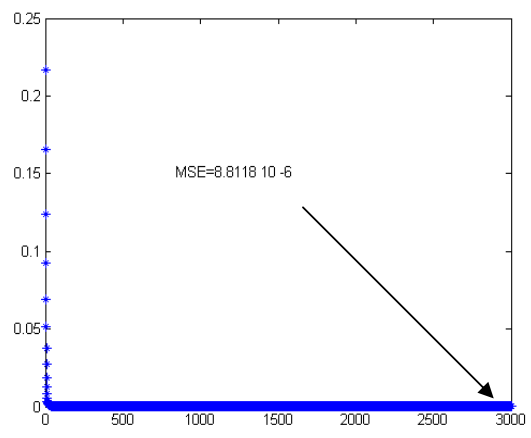
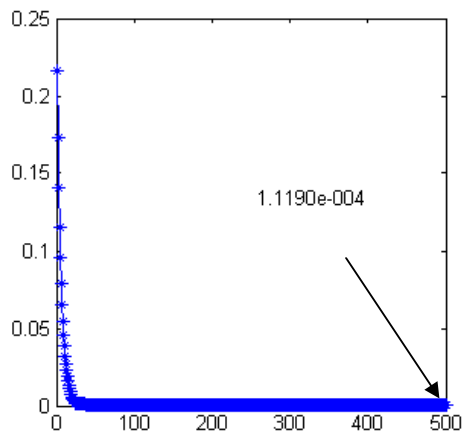


FIG. 8 Alfalou and Mansour



(a) Origin Target Image: I_0



(b) Know Key-image: I_1



(c) First level output image
MSE = 0.0014 (using 25 iterations)



(c) First level output image
MSE = $1.2869 \cdot 10^{-4}$ (using 500 iterations)

FIG. 9 Alfalou and Mansour

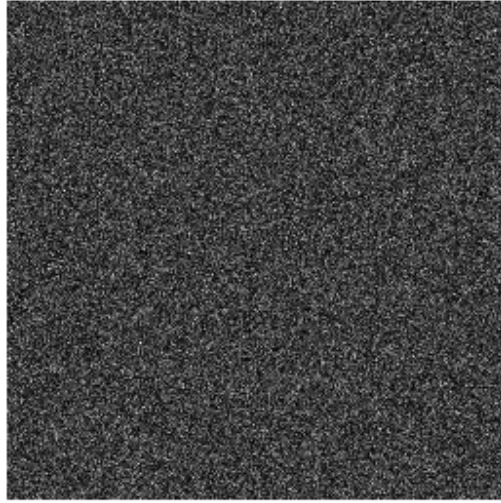


FIG. 10 Alfalou and Mansour

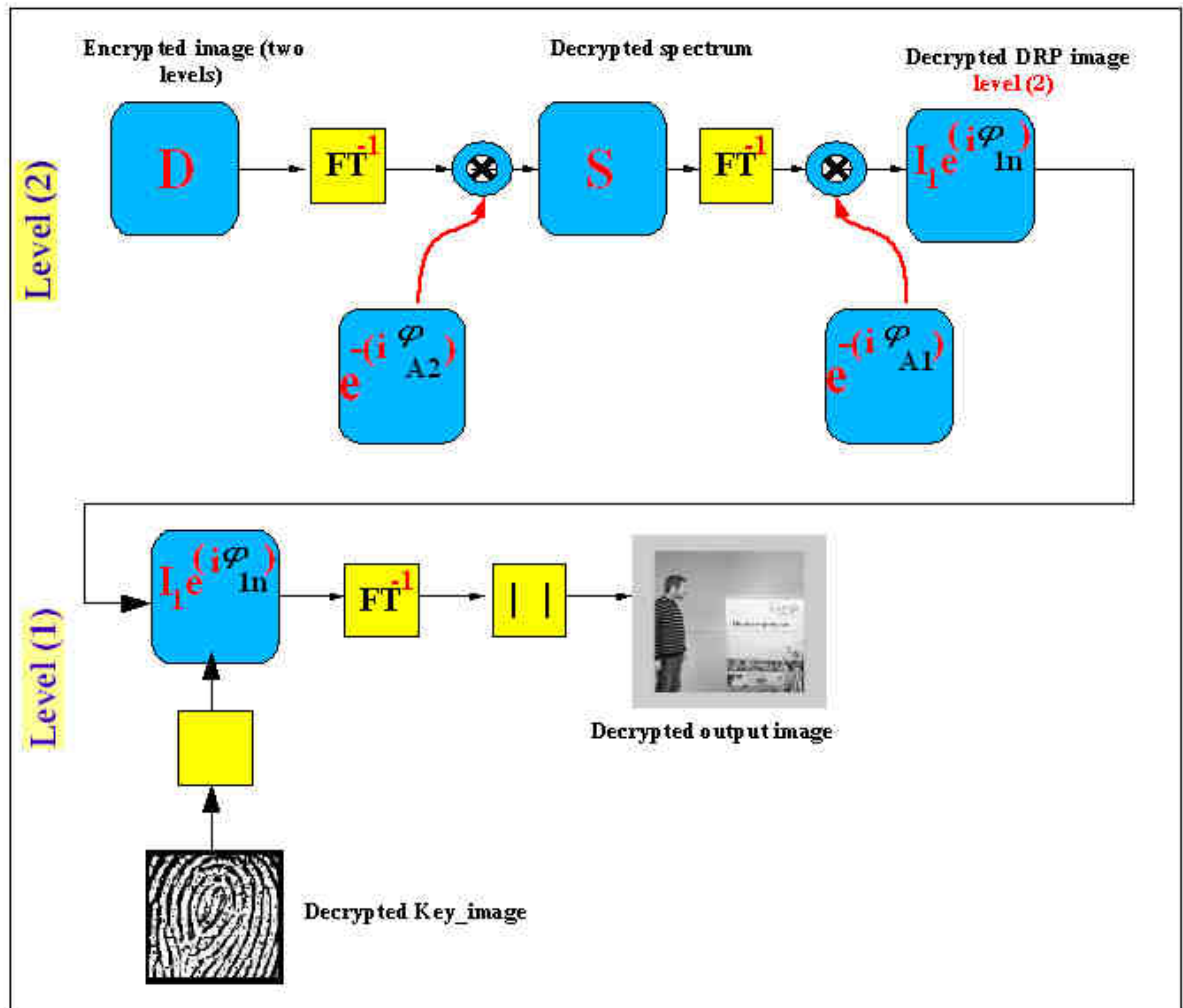


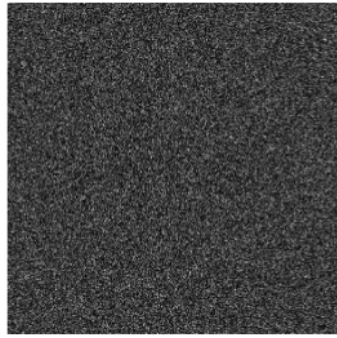
FIG. 11 Alfalou and Mansour



(a) Input target image: I_0



(b) Known Key-Image: I_1



(c) Encrypted image at the output of our tow level encrypted system: $(I_c e^{i\varphi_c})$



(d) Decrypted image $MSE' = 0.0173$

FIG. 12 Alfalou and Mansour

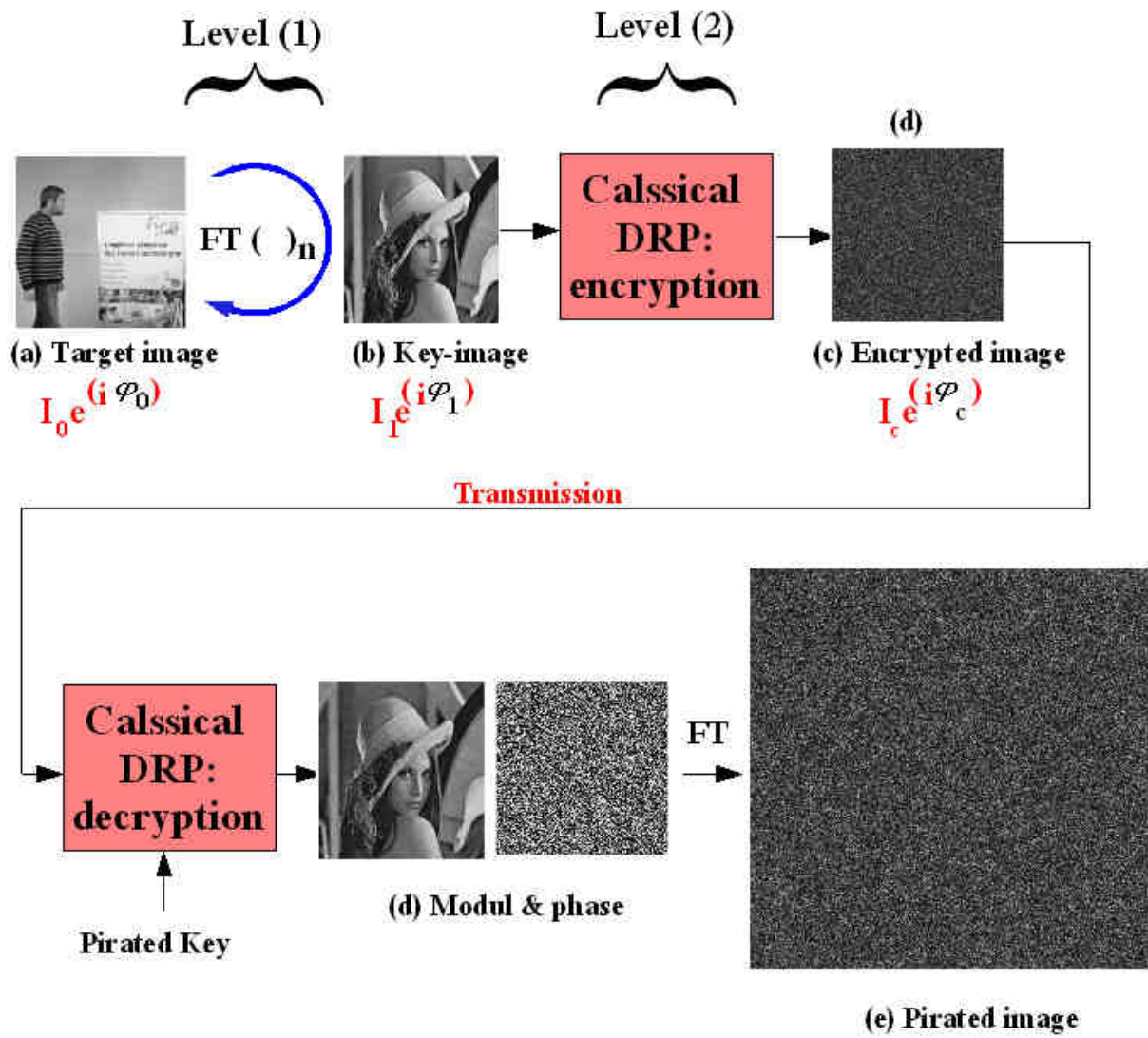


FIG. 13 Alfalou and Mansour

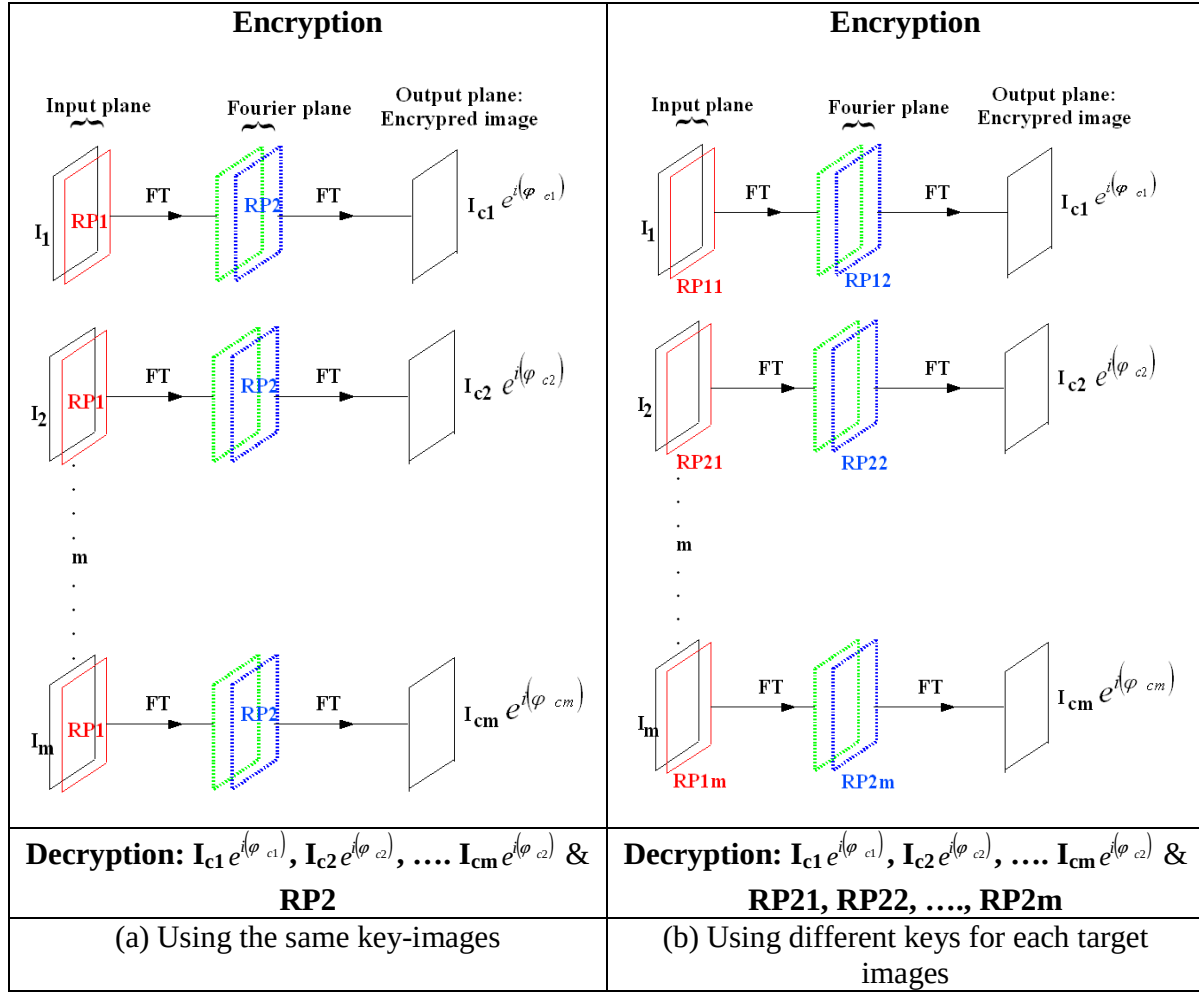


FIG. 14 Alfalou and Mansour

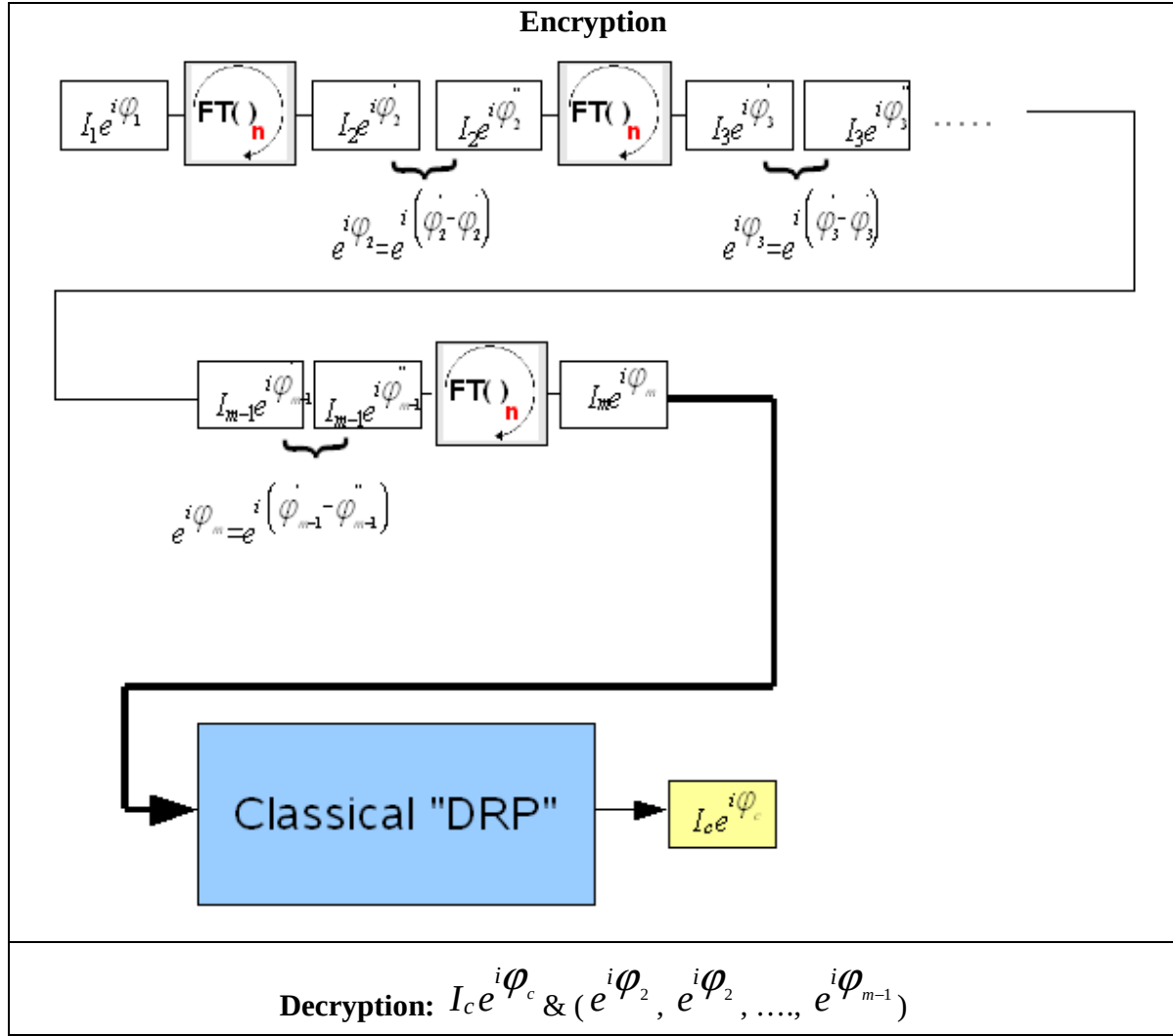


FIG. 15 Alfalou and Mansour

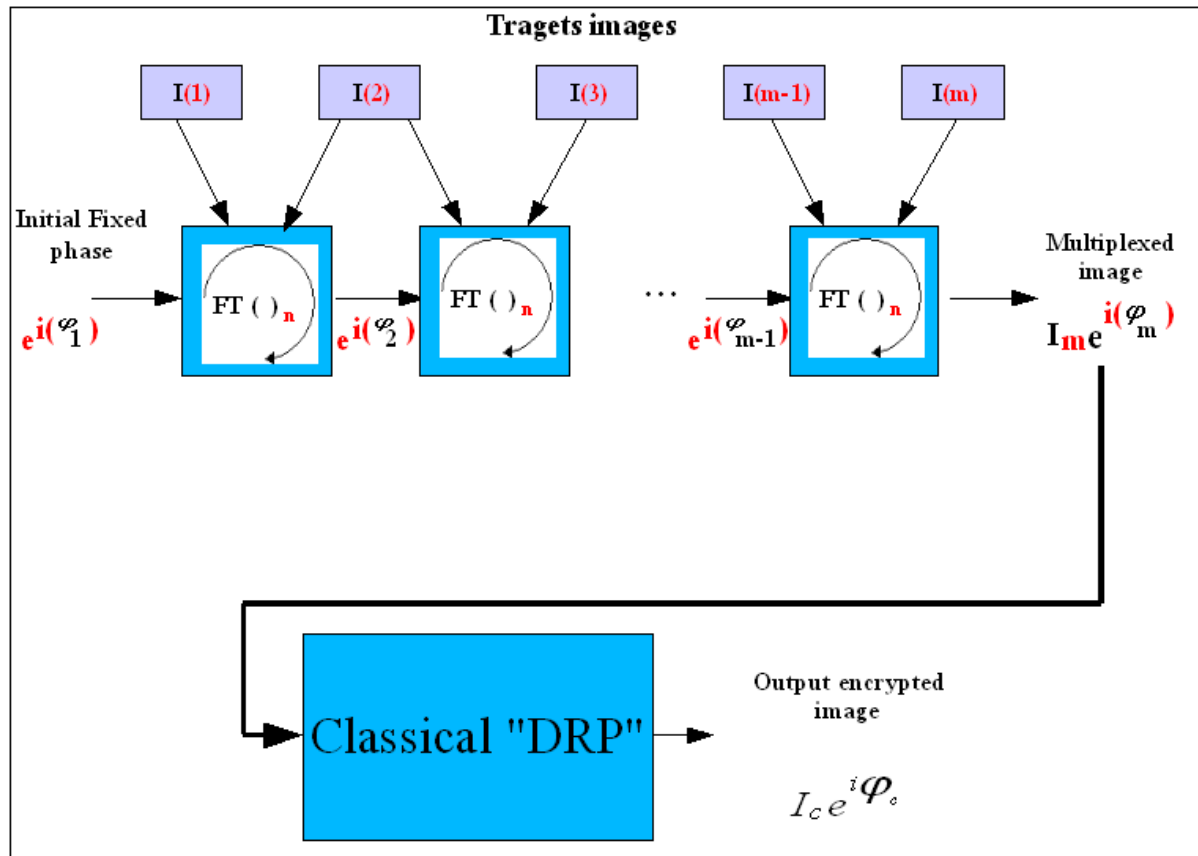


FIG. 16 Alfalou and Mansour