Optical information hiding by combining image scrambling techniques in fractional Fourier domains

Shi Liu[†] and John T. Sheridan[*]

School of Electrical, Electronic and Mechanical Engineering,
Communications and Optoelectronic Research Centre,
The SFI-Strategic Research Cluster in Solar Energy Conversion,
College of Engineering, Mathematical and Physical Sciences,
University College Dublin, Belfield, Dublin 4, Ireland.

E-mail: [†]Shi.Liu@ucdconnect.ie [*]John.Sheridan@ucd.ie

Abstract — **In this paper, we propose a novel scheme for optical information hiding (encryption) of two-dimensional images by combining image scrambling techniques in fractional Fourier domains. The image is initially random shifted using the jigsaw transform algorithm, and then a pixel scrambling technique based on the Arnold transform (ART) is applied. Then, the scrambled image is iteratively encrypted in the fractional Fourier domains using randomly chosen fractional orders. The parameters of the architecture, including the jigsaw permutations indices, Arnold frequencies, and fractional Fourier orders, form a huge key space enhancing the security level of the proposed encryption system. Optical implementations are discussed and numerical simulation results are presented to demonstrate the flexibility and robustness of the proposed method.**

Keywords — **Optical security, Optical encryption, Image scrambling, Jigsaw transform, Arnold transform, Fractional Fourier transform, Optical signal processing.**

I Introduction

Optical information hiding techniques have received significant attention recently, due to their considerable advantages, such as inherent capabilities for parallel ultra-fast processing, and the possibility of their applications to biometrics, optical security and product authenticity verification [1–5]. Using these techniques, information can be hidden or secured in many different kinds of dimensions offering many degrees of freedom. Refregier and Javidi [1] proposed a double random phase encoding (DRPE) method to encode an amplitude image into a stationary white noise pattern. This includes multiplication of the image by random phase screens both in the input (space) and Fourier (spatial frequencies) planes. Furthermore, fully phase-based encryption provides much better performance than amplitude-based (linear) encryption because of the secure properties of nonlinear encryption [2]. In addition, several other algorithms, for instance, digital optical stream cipher [3], optical XOR image encryption [4], and information encryption with phase-shifting interferometry [5] have also yielded theoretical and experimental results that indicate a high level of security can be achieved by applying optically inspired hiding techniques.

The fractional Fourier transform (FRT) and its optical implementations have been studied for several years. Various algorithms and optical hardwares configurations for many different applications have been reported [6–10]. With the introduction of the fractional order, a, indicating the domain into which it transforms, the FRT broadens signal representation possibilities, while still including in the limiting cases both the spatial and frequency domains [6]. The FRT is a generalization of the conventional Fourier Transform (FT) for which the order $a = 1$ [7]. More importantly, in optical encryption, it provides different ways in which to encrypt two-dimensional information. The extra degrees of freedom it provides, i.e.,

the fractional orders and scaling factors in both the x-axis and the y-axis, improves the systems performance (security and robustness) to blind decryption attacks [8].

Image scrambling techniques are normally applied during digital image processing, information cryptography, digital watermarking, and optical image encryption [11–17]. Depending on the image pixel arrangements, image scrambling techniques can be categorized into matrix transformations and coordinate movements [11]. Considering the first type, the Arnold transform [12], Fibonacci transformation [13] and generalized 2D matrix transformation [14] have been shown to provide excellent robustness. On the other hand, cellular automata [15], the torus automorphism [16], and chaotic Kolmogoroc flows are used to produce the second coordinate movements type [11]. Different applications can benefit from image scrambling technologies, for example, analog TV, confidential video conferencing, facsimile transmission, and medical data. [17].

In this paper, we propose a novel optical encryption architecture based on a combination of two image scrambling techniques in fractional Fourier domains. We apply the jigsaw and Arnold transforms as pre-processing image scrambling algorithms in each iteration, and we utilize iterative multi-stage fractional Fourier transforms employing random fractional orders. This architecture does not require the use of random phase keys, reducing the time taken and algorithm complexity. The many random parameters used in the iterative scheme provide more degrees of freedom and thus more secure cryptography.

The paper is arranged as follows: Section II presents the theory of double random phase encoding (DRPE), the fractional Fourier transform (FRT), as well as describing the jigsaw and Arnold transform (ART) algorithms. Section III describes our new optical encryption scheme, which we refer to as the "scrambled FRT image encryption algorithm" or SFRT. Section IV discusses the flexibility and robustness of our proposed method. The last section gives a brief conclusion.

II Theoretical Analysis

a) Double random phase encoding (DRPE)

In this section, we review the DRPE [1]. This method is also called amplitude-based encryption (AE) as opposed to fully phase-based encryption (PE) [2]. Let $f(x, y)$ denote the two-dimensional input data (intensity, phase). Two random phase-only masks are applied in this encoding scheme. Let $n(x, y)$ and $b(\mu, \nu)$ denote two statistically independent white sequences uniformly distributed in $[0, 1]$. Here, (x, y) are the coordinates in the space domain, and (μ, ν) are the coordinates in the Fourier domain. The input image is first multiplied by the first random phase function $\varphi_1(x, y) = \exp[jn(x, y)]$ and then multiplied by the second random phase function $\psi_2(\mu, \nu) = \exp[jb(\mu, \nu)]$ in the Fourier domain. The encrypted image $g(x, y)$ can be represented by:

$$g(x, y) = \{f(x, y)\exp[jn(x, y)]\} * h(\mu, \nu) \tag{1}$$

The $*$ denotes the convolution operation and $h(\mu, \nu)$ is the inverse Fourier transform of $\exp[jb(\mu, \nu)]$, which is described in equation (2), where $\mathcal{F}$ denotes as the Fourier transform:

$$h(\mu, \nu) = \mathcal{F}^{-1}\{\exp[jb(\mu, \nu)]\} \tag{2}$$

The first random phase mask serves to make the input image into white noise and the second serves to make the image stationary and encoded. Therefore, for AE, when $f(x, y)$ is real, the random phase key located in the Fourier domain of this algorithm is the only key necessary to decrypt the original image. To decrypt, the inverse process is applied using the complex conjugate of the corresponding phase masks used in the encryption process. This method can be implemented optically. Fig. 1 shows a 4-f optical setup, using two fixed random-phase masks located in the input plane and Fourier plane, to implement the DRPE.

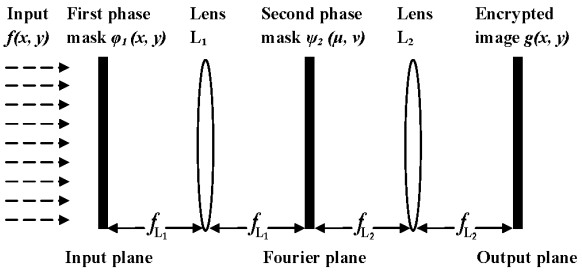

Fig. 1: Optical architecture of the 4-f imaging system used to implement the DRPE.

b) The fractional Fourier transform (FRT)

The FRT is a mathematical tool that has attracted significant attention owing to its simple optical implementation and wide range of applications [6–10]. The concept of FRT domains is of critical importance to our scheme. A continuum of domains, referred to as *fractional domains*, exist between the typically examined time (or space) and frequency (or spatial frequency) domain, frequently met in signal processing (optics). We follow the notations in Ref. [9]. The a-th order FRT $f_a(x_a)$ of a function $f(x)$ is defined as:

$$\begin{aligned} f_a(x_a) =& F_a\{f(x)\}(x_a) \\ =& \int_{-\infty}^{+\infty} K_a(x, x_a) f(x) dx \end{aligned} \tag{3}$$

The kernel function is given by:

$$K_a(x,x_a) = A_\varphi[i\pi(x^2\cot\varphi - 2xx_a + x_a^2\cot\varphi)], \quad 0<|a|<2 \tag{4}$$

where,

$$A_\phi = \exp[-i\pi\ \mathrm{sgn}(\sin\phi)/4 + i\phi/2] \tag{5}$$

x_a represents the a-th domain coordinates, and $\phi = a\pi/2$. A_ϕ is described in equation (5) and is a constant phase factor that is dependent on only the fractional order. In addition, the definition in equation (3) is only valid for values of a not equal to 0 or ± 2. In our algorithm, we apply the FRT in both the x and y axes.

c) The jigsaw transform

The jigsaw transform for optical encryption was originally proposed in Ref. [10]. $J_p\{\}$ is defined and used to describe the jigsaw transform which juxtaposes different subsections of the complex image, where p indicates the permutation. Correspondingly, $J_{-p}\{\}$ denotes the inverse jigsaw transform. This image scrambling algorithm involves the arrangement of randomly distributed sub-image blocks and has many advantages. For example, it is unitary and can be reconstructed perfectly if the user knows the permutation used in the encryption process. Energy is conserved through the transform. Importantly, no phase keys are used to encrypt the image. Fig. 2 illustrates an application of the jigsaw transform.

(a) Original Image (b) Output Image

Fig. 2: Illustration of the jigsaw transform of an image.

d) The Arnold transform (ART)

The ART, also known as cat mapping, was introduced by Arnold in the study of ergodic theory [12]. This transform is a process of clipping and splicing which realigns the pixel matrix of a digital image. Given an $N \times N$ image $f(x,y)$, the ART of a pixel (x,y) in the image is calculated using equation (6).

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\mathrm{mod}\ N),\ (x,y) \in N \tag{6}$$

where x and y are the coordinates of the pixel before the Arnold transform, and x' and y' denote a new position afterwards.

Accordingly, the ART of an image can be described as:

$$ART(f,N) = \{(v,(x',y')) \mid (x',y')^T = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} (x,y)^T (\mathrm{mod}\ N)\} \tag{7}$$

where $(v,(x,y)) \in f$, v denotes a value at the pixel (x,y) in the original image $f(x,y)$. $(x,y)^T$ is the transpose of (x,y). The term on the right-hand side of "|" indicate the algorithm conditions or operation procedures.

Based on previous studies, the ART is periodic. The original image will reappear after a certain number of iterations, as in equation (8). The period of the Arnold transform is determined by

$$Period = \min\{n \mid \{ART[f(x,y),N]\}^n = f(x,y)\} \tag{8}$$

where 'min' denotes a minimum value, and n is the iteration number. In our scheme, N is larger than 2 and usually the $Period \leq N^2/2$.

The ART can be regarded as a process of image shearing and stitching in which points of the discrete digital image matrix are rearranged. Fig. 3 illustrates the effect of applying an Arnold transform with the frequency $\omega = 2$, where the frequency ω stands for the number of iterations and is normally less than the Period value. We use ω as a key in the proposed encryption scheme. The original image can be reconstructed by an inverse ART using the correct ω value.

(a) Original Image (b) ART with $\omega = 2$

Fig. 3: Illustration of the Arnold transform of an image.

III Scrambled FRT image (SFRT)

A schematic of the proposed SFRT encryption architecture is presented in Fig. 4. $f(x,y)$ denotes the input two-dimensional image to be encrypted. K is the number of iterations, and k indicates the kth iteration where $1 \leq k \leq K$. g_k is the encrypted image after the kth iteration. Each iteration of the encryption process in our method involves the following steps:

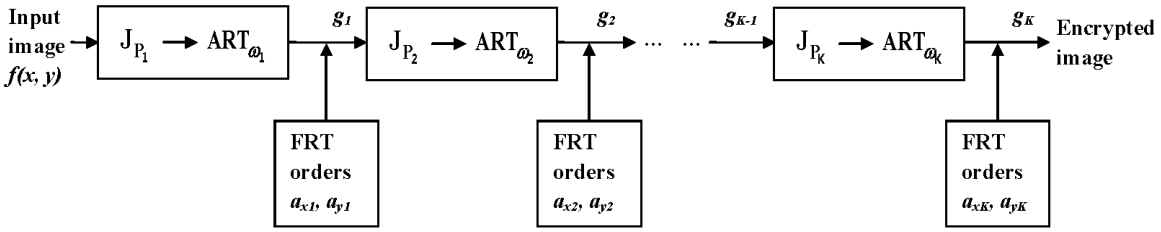

Fig. 4: Image encryption for the proposed scrambled FRT (SFRT) architecture.

1. In the kth iteration, the two dimensional data, g_{k-1}, is divided into sub-images. The sizes of these sub-images are randomly chosen, one at a time, from a list of four possibilities $\{2\times 2, 4\times 4, 8\times 8, 16\times 16\}$. Thus a random list is generated. If $k > 4$, then the number of sub-images is determined by returning to the random list. These sub-images undergo a permutation, p_k, by the jigsaw transform, and we can obtain:

$$J_{p_k}\{g_{k-1}\} \tag{9}$$

2. $J_{p_k}\{g_{k-1}\}$ is then subsequently scrambled by the ART using a frequency ω_k randomly chosen from $\{1, 2, 3, 4, 5\}$, giving:

$$ART_{\omega_k}\{J_{p_k}\{g_{k-1}\}\} \tag{10}$$

3. Perform an FRT of order a_k, i.e., a_{xk} in x and a_{yk} in y, randomly chosen from a fractional orders range defined by the user. Finally, the encrypted image for this iteration is given by:

$$g_k = FRT_{a_k}\{ART_{\omega_k}\{J_{p_k}\{g_{k-1}\}\}\} \tag{11}$$

We apply these three steps iteratively to encrypt the image into uniformly random distributions as discussed in Section IV. The jigsaw and Arnold transforms are implemented and applied to the complex image field. Optically, the resulting scrambled complex image could be displayed after each iteration using a spatial light modulator (SLM) located at the input plane of the architecture, which can display both the phase and the amplitude of a waveform. A single-lens of focal length f_L is used to implement the FRT, while adjusting the distances (z_1, z_2) to control the fractional orders. After the FRT, we can capture the encrypted complex information as a hologram using a reference beam at the surface of the Charge-coupled device (CCD). Fig. 5 gives an optical setup for the proposed SFRT.

The decryption is the exact inverse of the encryption process. It can also be achieved using the same configuration by exchanging the input and

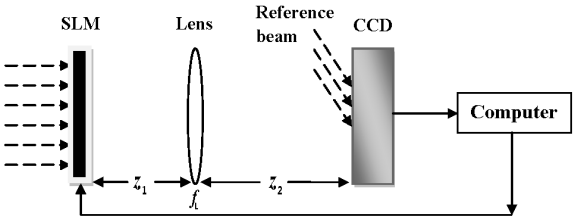

Fig. 5: Optical architecture for SFRT. with distances (z_1, z_2) and lens focal length f_L.

output planes of the optical architecture. The decryption for the kth iteration is described in equation (12).

$$g_{k-1} = J_{-p_k}\{ART_{-\omega_k}\{FRT_{-a_k}\{g_k\}\}\} \tag{12}$$

After all the iterations, the original image $f(x, y)$ can be extracted.

In our proposed algorithm, we use a large number of randomly chosen key parameters to increase the system security. The key space includes: the number of iterations K, the choice of the jigsaw divided subsections $\{2\times 2, 4\times 4, 8\times 8, 16\times 16\}$ for each iteration, the jigsaw transform permutation p for each iteration, the ART frequency ω chosen from $\{1, 2, 3, 4, 5\}$ for each iteration, as well as the FRT order keys: a_x in x and a_y in y. The following key data set KEY is an example of one key we used for encryption.

$$\begin{aligned} KEY = \{&[4], [16, 4, 8, 2], \{[7, 9, 14, 16, 11, 15, \\ &12, 4, 10, 1, 3, 5, 13, 6, 8, 2], [2, 4, 3, 1], \\ &[3, 6, 7, 1, 2, 4, 8, 5], [2, 1]\}, [5, 1, 3, 4], \\ &[0.2, 1.8, 1.3, 0.6], [1.2, 1.7, 0.6, 0.1]\} \end{aligned} \tag{13}$$

In this key, $K = 4$ iterations. The image is divided into 16×16, 4×4, 8×8, and 2×2 sequentially, and these undergo the jigsaw permutations indicated. The next key parameter $[5, 1, 3, 4]$ indicates the frequencies of the ARTs used for each successive iteration. The last two lists are the fractional orders used both in the x and y axes.

The security level of our encryption system is increased by the large number of randomly chosen keys which increases with each iteration added. Only when all the correct keys are simultaneously

used for decryption can information be extracted. This provides significant robustness to blind decryption.

IV Simulation results

In this section, numerical simulations performed to examine the validity and robustness of our algorithm are discussed. We use the image of Lena with 256×256 pixels as our original input image Fig. 6(a). Then we present a sample result with $K = 10$ in Fig. 6(b). It can been seen that the encrypted image appears as white noise.

(a) Original Image (b) Encrypted Image

Fig. 6: Sample encryption result with $K = 10$ and randomly generated key values.

During decryption, only the application of all the correct keys will reveal the original information. Thus, it is difficult for an unauthorized person to attack the system to obtain the original image. Fig. 7(a) and Fig. 7(b) show correctly decrypted images for the cases when $K = 2$ and $K = 5$ respectively. In order to demonstrate the robustness of this algorithm, we examine the sensitivities to errors in one of the fractional order keys in one domain by calculating the mean square errors (MSEs) between the decrypted image and the original image. MSE is defined by

$$MSE = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} | f^{'}(i,j) - f(i,j) |^{2} \quad (14)$$

where $N \times N$ is the size of the image, $f^{`}(i,j)$ and $f(i,j)$ denotes the decrypted and original images at the (i,j) pixel.

(a) Decrypted Image with K=2 (b) Decrypted Image with K=5

Fig. 7: Sample decryption results with matched keys.

The MSE is plotted against the deviation of a_y from the correct fractional order value. We present the results in Fig. 8 and Fig. 9 for $K = 4$ and $K = 9$ respectively. The thick solid curve corresponds to varying the value of the last encryption, first decryption, Kth fractional order in the y-axis, i.e., $-a_{yK}$, while all the other keys are correct. The dashed curve corresponds to varying the value of the first encryption fractional order in the y-axis, i.e., $-a_{y1}$. As the fractional order a_y deviates from the correct key, the value of MSE increases extremely quick. Apparently, the decryption procedure is more sensitive to the fractional order $-a_{yK}$ than $-a_{y1}$, which means a slight deviation from the Kth fractional order produces errors which are accumulated and eventually result in high MSE.

We have also analyzed the sensitivities to use of an incorrect number of iterations K, a wrong ART frequencies ω, or a wrong jigsaw permutation p. The MSE results versus the deviation from the correct keys always indicate good robustness in these cases.

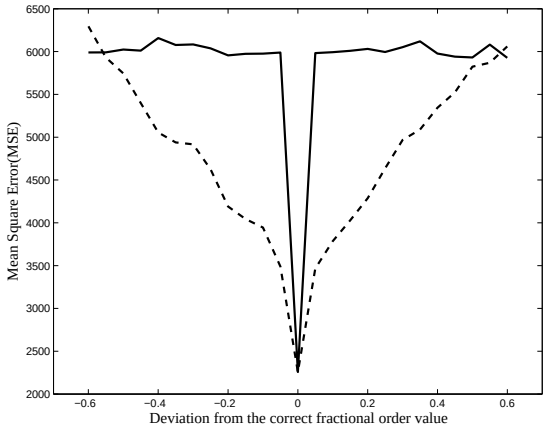

Fig. 8: MSE versus the deviation of fractional orders for: $K = 4$. The thick solid curve corresponds to the wrong $-a_{yK}$; The dashed curve corresponds to the wrong $-a_{y1}$.

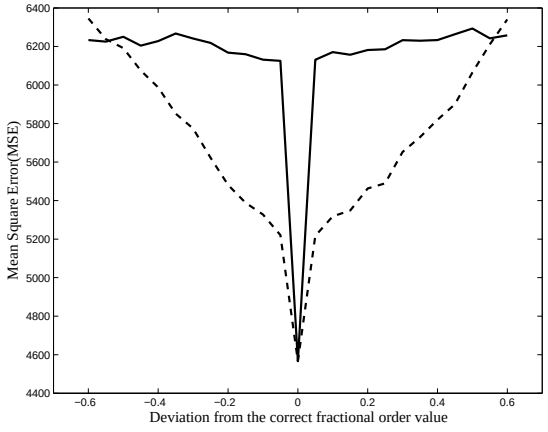

Fig. 9: MSE versus the deviation of fractional orders for: $K = 9$. The thick solid curve corresponds to the wrong $-a_{yK}$; The dashed curve corresponds to the wrong $-a_{y1}$.

V Conclusion

In summary, we have proposed a new optical information hiding technique for two-dimensional image encryption by using a combination of image scrambling techniques and fractional Fourier transforms. The image is first scrambled by applying the jigsaw and Arnold transforms sequentially. Then, the scrambled image is encrypted iteratively in random fractional domains. Comparing to previous FRT image encryption architectures, our algorithm can provide an enlarged key space which by choosing random keys enhances the security level. One needs to specify all the keys to decrypt the information correctly. Optical implementation and numerical simulation results have demonstrated the flexibility and robustness of the proposed methods.

We acknowledge EI, SFI, and IRCSET funding under the NDP and thank Dr. B. Hennelly, Dr. M. Gleeson and Mr Dayan Li. SL is supported by an Erasmus Mundus scholarship.

References

[1] P. Refregier and B. Javidi. "Optical image encryption based on input plane and fourier plane random encoding". *Opt. Lett.*, 20(7):767–769, 1995.

[2] N. Towghi, B. Javidi, and Z. Luo. "Fully phase encrypted image processor". *J. Opt. Soc. Am. A*, 16(8):1915–1927, 1999.

[3] M. Madjarova, M. Kakuta, M. Yamaguchi, and N. Ohyama. "Optical implementation of the stream cipher based on the irreversible cellular automata algorithm". *Opt. Lett.*, 22(21):1624–1626, 1997.

[4] J. W. Han, C. S. Park, D. H. Ryu, and E. S. Kim. "Optical image encryption based on XOR operations". *Opt. Eng.*, 38:47–54, 1999.

[5] E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi. "Optoelectronic information encryption with phase-shifting interferometry". *Appl. Opt.*, 39(14):2313–2320, 2000.

[6] H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay. The Fractional Fourier Transform with Applications in Optics and Signal Processing. *Wiley, New York*, 2001.

[7] H. M. Ozaktas, O. Arikan, M. A. Kutay, and G. Bozdagt. "Digital computation of the fractional fourier transform". *IEEE Trans. on Signal Process*, 44(9):2141–2150, 1996.

[8] Y. Zhang, C. H. Zheng, and N. Tanno. "Optical encryption based on iterative fractional fourier transform". *Opt. Commun.*, 202(4-6):277–285, 2002.

[9] B. M. Hennelly and J. T. Sheridan. "Image encryption and the fractional fourier transform". *Optik*, 114(6):251–265, 2003.

[10] B. M. Hennelly and J. T. Sheridan. "Optical image encryption by random shifting in fractional fourier domains". *Opt. Lett.*, 28(4):269–271, 2003.

[11] K. T. Lin. "Information hiding based on binary encoding methods and pixel scrambling techniques". *Appl. Opt.*, 49(2):220–228, 2010.

[12] M. A. Arnold and G. W. Small. "Determination of physiological levels of glucose in an aqueous matrix with digitally filtered fourier transform near-infrared spectra". *Analytical Chemistry*, 62(14):1457–1464, 1990.

[13] Y. Zhou A, S. Agaian, V. M. Joyner A, and K. Panetta. "Two fibonacci p-code based image scrambling algorithms". *Proc. SPIE*, 6812, 2008.

[14] D. Qi, J. Zou, and X. Han. "A new class of scrambling transformation and its application in the image information covering". *Science in China Series E: Technological Sciences*, 43:304–312, 2000. 10.1007/BF02916835.

[15] O. Lafe. "Data compression and encryption using cellular automata transforms". *Engineering Applications of Artificial Intelligence*, 10(6):581–591, 1997.

[16] C. C. Chang and J. C. Chuang. "An image intellectual property protection scheme for gray-level images using visual secret sharing strategy". *Patt. Reco. Let.*, 23(8):931–941, 2002.

[17] L. Shao, Z. Qin, B. Liu, J. Qin, and H. Li. "Image scrambling algorithm based on random shuffling strategy". In *ICIEA 2008.*, pages 2278–2283, 2008.