Optik 114, No. 6 (2003) 251–265

http://www.urbanfischer.de/journals/optik

Optik Optics
International Journal for Light and Electron Optics

Image encryption and the fractional Fourier transform

B. M. Hennelly, J. T. Sheridan

Department of Electronic and Electrical Engineering, Faculty of Architecture and Engineering, University College Dublin, Belfield, Dublin 4, Ireland

Abstract: A number of method have been recently proposed in the literature for the encryption of 2-D information using optical systems based on the fractional Fourier transform, FRT. In this paper a brief review of the methods proposed to date is presented. A measure of the strength/robustness of the level of encryption of the various techniques is proposed and a comparison is carried out between the methods. Optical implementations are discussed. Robustness of system with respect to misalignment and blind decryption are also discussed.

Key words: Fractional Fourier transform – optical image encryption – random phase mask – optical security

1. Introduction

The Fractional Fourier Transform (FRT) is a generalisation of the Fourier Transform (FT). The Fourier Transform can be understood as a linear transformation, which allows a signal, originally captured in the position or time domain to be rotated through $\pi/2$ radians into the orthogonal spatial frequency or frequency domain. It can be shown that four successive applications of the FT (2π radians) are equivalent to the identity function. In an analogous way, the FRT can be seen as a linear transformation, which rotates the signal through any arbitrary angle into a mixed frequency – space domain.

The rigorous mathematical formulation for the FRT dates back, at least, to the Fractional Order Fourier Transform introduced by Namias for use in the field of quantum mechanics [1]. This work was further developed in [2]. In [3] and [4] the FRT was applied to describe wave propagation in Graded Index (GRIN) media and given an optical interpretation similar to that of the FT. The GRIN media has the property of combining propagation and continuous refocusing. Over a particular distance of GRIN the input plane repeats, equivalent to four applications of the FT. At half this distance we find the inverse of the input plane, equivalent to two applications of the FT. At one quarter the distance we find the Fourier plane. The FRT of any non-integer order is defined as the field distribution at some other distance of GRIN. In [5] the FRT was given a novel yet equivalent interpretation in terms of phase space. It was shown that, while a FT operation could be described as the rotation of the Wigner Distribution Function (WDF) by an angle of $\pi/2$, the FRT describes the rotation of the WDF by an angle equal to $a\pi/2$ where a represents the order of the FRT. Two optical implementations were proposed, which shall be shown shortly. The implementation is no more complex than that of the FT. Since then, the FRT has allowed for new applications in many areas where the FT has importance, for example, phase retrieval [6, 7], beam shaping [8], filtering [9] and many others, including optical encryption.

Information security has been receiving increasing attention in recent years. Because optical processes have the distinct advantage of sending 2-D complex data in parallel and carrying out otherwise time costly operations at great speeds, they have found growing importance in data encryption. In [10] an optical encryption scheme is proposed dubbed "double random phase encoding" which involves multiplying by two random phases in the input plane and in the Fourier domain. It can be shown that if these random phases are statistically independent white noises then the encrypted image is also a stationary white noise. The random phase key located at the Fourier plane serves as the only key in this encryption scheme but it was not long until the extra degree of freedom offered by the FRT was utilised as a new key in similar encryption schemes, which shall be discussed shortly.

The outline of this paper is as follows: In section 2 we discuss the FRT in more detail outlining a mathematical definition. In section 3 we will present a review of the recent FRT encryption algorithms, which have emerged and we shall go on in section 4 to discuss some other possible algorithms. All of these algorithms are compared briefly in section 5 and this is followed by a conclusion.

Received 4 April 2003; accepted 28 May 2003.

Correspondence to: J. T. Sheridan
Fax: ++353-1-283-0921
E-mail: John.Sheridan@ucd.ie

0030-4026/03/114/06-251 $ 15.00/0

2. The fractional Fourier transform

Conventionally, the a-th order FRT $f_a(x_a)$ of a function $f(x)$ is defined as

$$f_a(x_a) = F_a\{f(x)\}(x_a) = \int_{-\infty}^{+\infty} K_a(x, x_a)\, f(x)\, \mathrm{d}x\,. \quad (1)$$

The kernel is given by

$$\begin{aligned} K_a(x, x_a) &= A_\varphi \exp\left[\mathrm{i}\pi(x^2 \cot\varphi - 2xx_a \right. \\ &\quad \left. + x_a^2 \cot\varphi\right] \quad 0 < |a| < 2 \\ &= \delta(x - x_a) \qquad a = 0 \\ &= \delta(x + x_a) \qquad a = \pm 2\,, \end{aligned} \quad (2)$$

where,

$$A_\varphi = \exp\left[-\mathrm{i}\pi\, \mathrm{sgn}(\sin\varphi)/4 + \mathrm{i}\varphi/2\right] \quad \text{and} \quad \varphi = \pi/2 \quad (3)$$

and x and x_a represent the coordinate systems for the input or zeroth order domain and output a-th fractional domain respectively. The FRT has the property that it is index additive,

$$F_a\{F_b\{f(x)\}\} = F_{a+b}\{f(x)\}\,. \quad (4)$$

It is possible to extend this definition of the FRT for orders beyond ± 2 by noting that

$$F_a\{f(x)\} = F_{a+4n}\{f(x)\} \quad \forall\, n = \text{integer}\,. \quad (5)$$

The eigenfunctions of the FRT can be shown to be Hermite-Gaussian functions, the solutions to the Hermite-Gaussian polonomials. However, the eigenvalues can be chosen in different ways resulting in different definitions of the FRT, which all obey the characteristic laws of index additivity and reduce to the FT for an order of 1. This is mentioned because two of the encryption schemes discussed in the proceeding sections are based on different definitions of the FRT. The definition above is the one that has found the most applications in general and it has a simple optical implementation. In terms of arrangement of eigenfunctions and eigenvalues

$$F_a\{\varphi_n(x)\} = \exp(-\mathrm{i}an\pi)\, \varphi_n(x)\,, \quad (6)$$

$$\varphi_n(x) = \frac{2^{1/4}}{\sqrt{2^n n!}}\, H_n(\sqrt{2\pi}\, x) \exp(-\pi x^2)\,, \quad (7)$$

where, H_n is the n-th Hermite-Gaussian polynomial. The definition of the kernel given in eq. (2) can be shown to be equivalent with the following spectral expansion of the linear transform kernel

$$K_a(x, x_a) = \sum_{n=0}^{\infty} \exp(-\mathrm{i}an\pi/2)\, \psi_n(x)\, \psi_n(x_a)\,. \quad (8)$$

In image encryption, we will of course be dealing with two-dimensional signals. The 2-D FRT has separable kernels in both dimensions and so the above definition can be extended naturally in this way. All of the mathematical derivations in this paper are in one dimension for simplicity.

2.1. Optical implementation

Having shown that the FRT of order a corresponded to a rotation of the WDF by an angle $a\pi/2$ in [5], Lohmann went on to describe the rotation of the WDF using three shearing operations of the WDF – one in the x direction the next in the y direction followed by another one in the x direction $(x - y - x)$ (this is equivalent to $y - x - y$ shearing). This leads to two optical implementations, Type I and Type II, see fig. 1, where each of the shearing operations is performed by either free space propagation or the action of a lens. We will represent all optical FRT operations using a single lens.

For Type I we require the following conditions to be met,

$$f = \frac{f_1}{\sin\varphi}\,, \quad z = f_1 \tan\varphi \quad (9)$$

and for Type II we require,

$$f = \frac{f_1}{\tan\varphi}, \quad z = f_1 \sin\varphi\,, \quad (10)$$

where, f represents the focal length of the lens and z is shown in the diagrams and f_1 is a virtual focal length. The resulting optical transform is given by

$$\begin{aligned} &f_a(x_a) \\ &= \int_{-\infty}^{+\infty} f(x) \exp\left\{\frac{\mathrm{i}\pi}{\sqrt{\lambda f_1}}\left\{\cot\varphi(x^2 + x_a^2) - 2xx_a \sin\varphi\right\}\right\} \mathrm{d}x\,, \end{aligned} \quad (11)$$

where we have omitted a constant phase factor since it is different for both optical implementations and also different from the constant phase factor in the mathematical definition given in eq. (3). A FRT with different orders in both the x and y directions could be implemented with two orthogonally situated cylindrical thin lenses with different focal lengths.

2.2. Numerical implementation

The first method [11] used to digitally calculate the FRT decomposed the signal to be transformed into a summation of the eigenfunctions of the FRT – the Her-

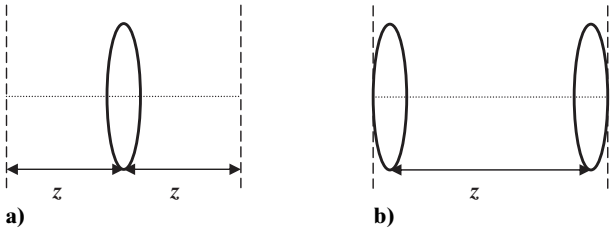

Fig. 1. Lohmann's a) Type I and b) Type II optical implementations of the FRT.

mite-Gaussian functions and then weighted them with the appropriate eigenvalues. This method proved to be time consuming requiring $O(N^2)$ calculations. Various methods utilising the fast Fourier algorithm (FFT) emerged [12–14] enabling digital calculation of the FRT in $O(N \log N)$.

Two algorithms were presented in [12]. The preferable of these two uses the Shannon interpolation formula and a series of mathematical manipulations to arrive at a convolution summation that can be determined using the FFT algorithm. This algorithm has the disadvantage of requiring a increase in data points by a factor of 2, due to interpolation and decimation, to allow for the shearing of the WDF when the signal is multiplied by the first chirp term (in the FRT kernel). This algorithm is not very accurate for small orders due to the sampling of rapid oscillations.

In [13] an algorithm is derived based on a numerical implementation of the Type II optical set up proposed by Lohmann. It has a simple interpretation and provides better results for low orders than [12]. Two FFTs and multiplication by three quadratic phase factors are needed.

In [14] an algorithm using only a single FFT operation is derived. This algorithm assumes that the highest spatial frequency due to the quadratic phase factor is larger than that of the signal to be transformed. This allows the sampling period to be related to the inverse of the maximum frequency of the quadratic phase term. This algorithm can improve upon [13] for determination of FRTs of low orders. However, constraints are placed on the sampling period, which can lead to the need for zero padding. Also, if we wish to apply the inverse of a transform of order a, we must first apply a transform of $(1 - a)$ and then apply an inverse FFT. This amounts to an exact inverse transformation.

All three of these algorithms were used to simulate the encryption/decryption schemes outlined in this paper but the results presented here have been calculated using [13]. An important factor in our simulations is the need for a completely reversible FRT calculation. Without an exact inverse, we could not simulate ideal decryption. In [8] a unitary condition is derived for fractional Fourier systems. We can use this result to vary the optical scaling factor $s = \sqrt{f_1 \lambda}$ in eq. (11) so that the algorithms given in [12] and [13] are exactly unitary discrete transforms for one order only.

An exactly unitary index additive discrete FRT has been derived [15], based on the discrete counterparts of the Hermite-Gaussian functions. No closed form definition has been given and the transform requires N^2 calculations.

3. The measurement of encryption

The input image used in the simulations below is a 256×256 sized grayscale (levels ranging from 0 to 255) Lena image, see fig. 2.

Fig. 2. The input image.

As a measure of the level of encryption of an image we calculate the Mean Square Error (MSE) between our original image and our decrypted image. Mathematically,

$$\mathrm{MSE} = \|\mathrm{in} - \mathrm{out}\|^2 = \frac{1}{N^2} \sum_{i=1}^{N} \sum_{j=1}^{N} |\mathrm{out}\,(i, j) - \mathrm{in}\,(i, j)|^2 \tag{12}$$

out (i, j) represents our decrypted image and in (i, j) represent the pixel values of our decrypted and encrypted images respectively.

4. Encryption Algorithms

4.1. Method 1

We begin this section reviewing the first Fourier based optical encryption scheme presented in [10]. This makes use of the FT, which a FRT of order 1. Two phase masks are used in the encryption scheme, which are in the form of two statistically independent white sequences uniformly distributed in $[0, 1]$. We will denote these random functions as n_1 and n_2. The scheme is as follows; the input image to be encoded is multiplied by one Random Phase Mask (RPK). The resulting complex wave field is Fourier transformed using a convex lens and in the Fourier domain, it is multiplied by the second RPK. The resulting image is again Fourier transformed through the use of a second lens. This is equivalent to a convolution operation, where the encrypted image can be represented by

$$g(x) = \{f(x) \exp[\mathrm{i}2\pi n_1(x)]\} * h(x)\,. \tag{13}$$

The $*$ denotes the convolution operation and $f(x)$ represents the signal to be encrypted.

$$F\{h(x)\} = \exp[\mathrm{i}2\pi n_2(x)]\,. \tag{14}$$

The resulting encrypted image, which is complex valued, can be shown to be a stationary white noise. The first RPK serves to make the input image white but nonstationary and not encrypted. The second serves to make the image stationary and encoded. Because the encrypted image is complex valued, both the real and

imaginary parts are needed to decode the image. In order to record such a signal we must use holographic methods. Decryption is simple. We apply the exact inverse of what was done to encrypt the image: first we return to the Fourier domain through the action of a lens. Then comes multiplication by a phase mask, which is the conjugate of the corresponding phase mask used in the encryption process. One last Fourier transforming lens follows this. The resulting wave field will have an amplitude distribution equal to the original image so holographic techniques are not necessary to capture it. There is only one key in this encryption scheme – the second random phase function, without which, blind decryption is very difficult. An optical encryption/decryption implementation can be seen in fig. 3. The Spatial Light Modulators (SLM) can display both amplitude and phase information. For encryption, SLM1 displays the input image multiplied by the first random phase, while SLM2 displays the second random phase mask. For decryption, SLM1 displays the encrypted complex image and SLM2 displays the conjugate of the second random phase key. Note, that we do not need a coherent reference beam at the CCD for decryption since we only require the intensity of the image.

The properties of such an encryption-decryption system have been investigated in [16], [17] and [18]. It is worth noting that since the FRT operation is a linear transform, it exhibits identical behaviour to that of the FT with regard to additive and multiplicative noise in optical implementations. This optical encoding scheme has also been extended to use a phase (only) modulated signal as the input to the system instead of an amplitude based image [19]. Such a system can be shown to have an improvement in robustness to additive noise but the first phase mask must be included in decryption and the final decrypted image must be recorded using interferometric methods. A numerical simulation of the above system was carried out. Fig. 4a shows the results of encryption. Fig 4b shows the results for an ideal decryption while decryption using an incorrect phase key is illustrated in fig. 4c. Fig. 5 shows the effect of decryption as the random phase mask is misaligned in one direction in steps of one pixel. Analogous results are found for all the encoding phase masks used in the following sections. If the phase mask is translationally out of place by one pixel the image

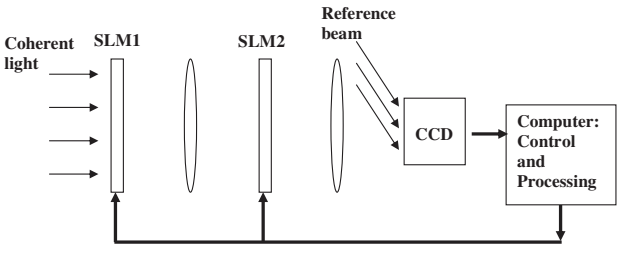

Fig. 3. General optical encryption/decryption set up for method 1 and method 2.

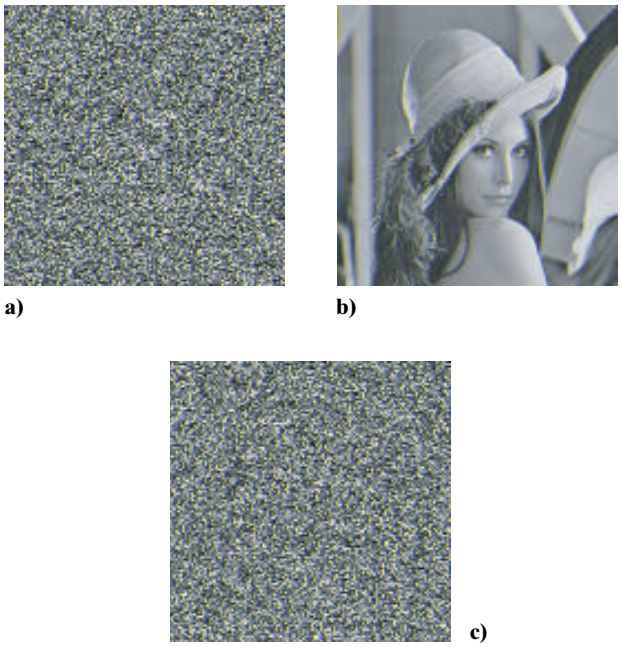

Fig. 4. Method 1: a) Encrypted image, MSE = 6010.50; b) decrypted correctly MSE = 0.00; c) decrypted with wrong phase key, MSE = 5871.19.

remains fully encrypted. For movement Δ less than one pixel in one direction, the shift tolerance is found to give a Signal to Noise Ratio (SNR) of the form,

$$\mathrm{SNR} = \frac{N(D-\Delta)^2}{\Delta^2}\,. \tag{15}$$

Here, N denotes the pixel number of the mask and D is the pixel size of the mask. However, aligning the phase mask is not as serious a problem as one might imagine due to a property outlined in [16]. We note that all of the FRT based optical encryption methods, which used random phase keys as keys, showed similar behaviour to misalignment and therefore further results will not be presented here.

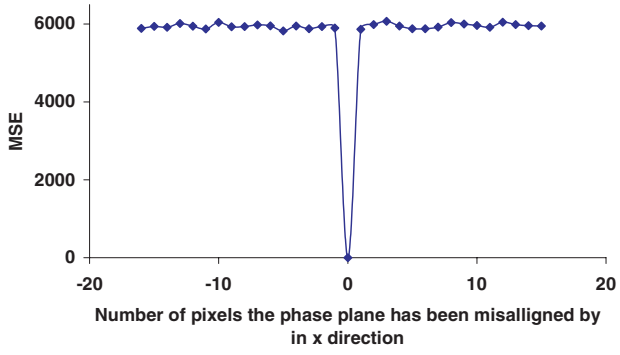

Fig. 5. The number of pixels the phase plane SLM2 has been misaligned by in x dir during decruption versus the resultant MSE.

4.2. Method 2

Before we begin, we note the following. In all the following sections we refer to FRTs of order a. We are dealing with 2-D transforms and in the most general case, two independent orders, a_x and a_y, for the x and y directions exist. This is due to the 2-D FRT having separable kernels in both directions. In our figures we use a symmetric lens to signify a FRT of order a. For simplicity we do not discuss the two dimensions referring to them only in relation to the simulated results.

In [20], the authors propose an optical encryption scheme very similar to the one described above, making use of the extra degree of freedom offered by the FRT. Fig. 3 is again used to represent the encryption and decryption schemes. The lenses in this diagram now representing optical FRT operations.

For the encryption process, the first lens represents a FRT operation of order a_1 and the second lens represents a FRT operation of order a_2. For the decryption process, the first lens represents a FRT operation of order $-a_2$ and the second lens represents a FRT operation of order $-a_1$. Again, two phase masks are used which are in the form of two statistically independent white sequences uniformly distributed in $[0, 1]$. The encryption scheme is as follows; the input image to be encoded is multiplied by one RPK to give us

$$f(x)\,\exp\left[\mathrm{i}2\pi n_1(x)\right]. \tag{16}$$

A FRT operation of order a_1 was applied through a convex lens to give,

$$F_{a1}\{f(x)\,\exp\left[\mathrm{i}2\pi n_1(x)\right]\}. \tag{17}$$

Now, in this fractional domain, the image is multiplied by the second RPK

$$F_{a1}\{f(x)\,\exp\left[\mathrm{i}2\pi n_1(x)\right]\}\,\exp\left[\mathrm{i}2\pi n_1(x)\right]. \tag{18}$$

The resulting image is again transformed by a FRT operation, this time of order a_2, through the use of a second lens

$$g(x) = F_{a2}\{F_{a1}\{f(x)\,\exp\left[\mathrm{i}2\pi n_1(x)\right]\}\,\exp\left[\mathrm{i}2\pi n_1(x)\right]\}. \tag{19}$$

The result is that we have buried our phase key in some fractional domain. It is shown in [20] that the result of this method of encryption is to encode our input signal into a white stationary noise.

Once again, decryption is the exact inverse of encryption. To $g(x)$ we apply an FRT of order $-a_2$ to obtain eq. (18). We now multiply by the conjugate of the second RPK to obtain eq. (17). A second FRT of order $-a_1$ is finally used to decrypt into a signal whose amplitude is equal to our original image. Decryption requires the knowledge of five keys in total, namely; the encoding RPK and the four fractional orders used $-a_{1x}$, a_{1y}, a_{2x} and a_{2y}.

The procedure was simulated for ($a_{1x} = a_{1y} = 0.5$, and $a_{2x} = a_{2y} = 0.5$). The simulated results showing the encrypted image, correct and incorrect decryption are shown below in fig. 6. The robustness of these fractional order keys to blind decryption is shown in fig. 7, where we graph error in a_{1x} (thick line) and a_{2x} (thin line) used in the decryption process, against the MSE of the resulting decrypted image. It can be seen that a_2 is the more robust of these two sets of fractional keys. The reason for this is that an incorrect a_2 will result in multiplication by the conjugate phase mask in the wrong fractional domain.

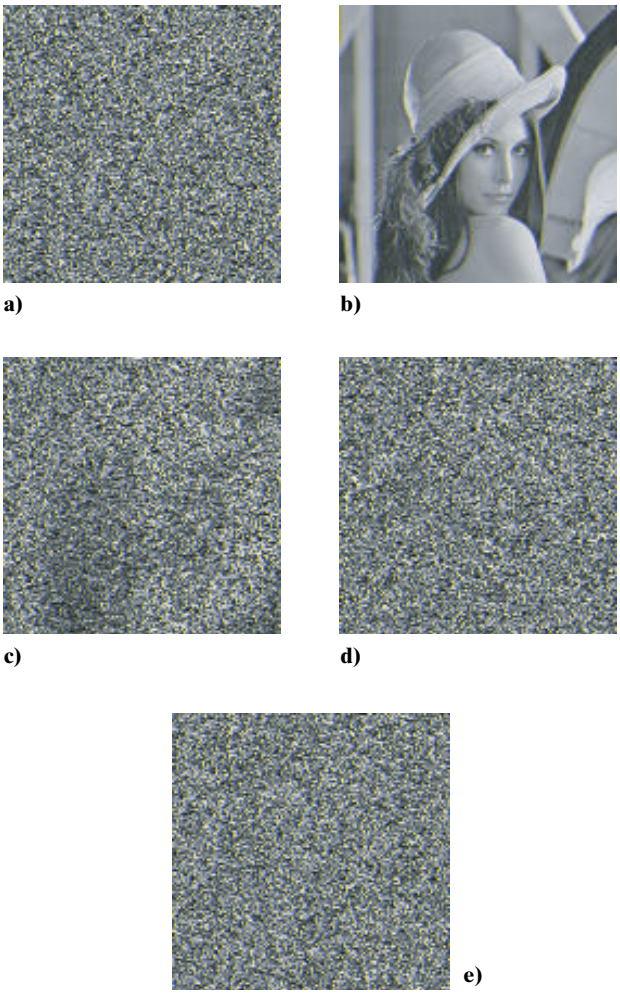

Fig. 6. Method 2: a) The encrypted image (0.5, 0.5, 0.5, 0.5) with a MSE = 5944.08; b) correctly decrypted (0.5, 0.5, 0.5, 0.5) with MSE = 0.00; c) incorrectly decrypted (0.7, 0.5, 0.5, 0.5) with MSE = 5013.74; d) incorrectly decrypted (0.5, 0.5, 0.7, 0.5) with MSE = 5858.68; e) decrypted using incorrect phase with MSE = 5921.15.

An optical method was proposed by the author to implement this algorithm in [21]. However, this allows for a scaling of the input image before applying an FRT operation followed by a scaling of the output image. This operation is referred to by the author as an 'extended fractional Fourier transform'. Such a transform can also be referred to as a Linear Canonical Transform (LCT), which finds its optical implementa-

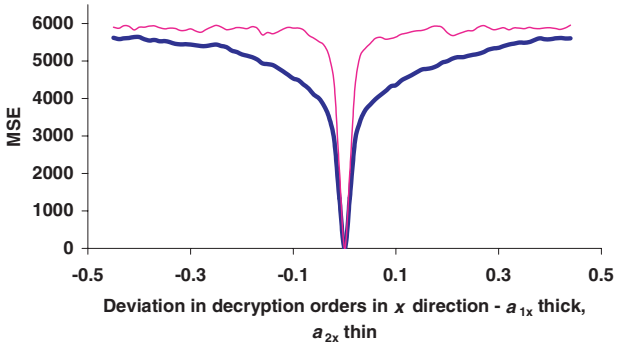

Fig. 7. Graph of deviation in decryption order keys for method 2 in the x direction from the correct values against the resultant MSE.

tion in the form of Quadratic Phase Systems (QPS), which are also in the form of bulk lens systems. The LCT is a generalisation of the FRT [22]. The scaling factors in the input and output planes are additional keys in the encryption system. Therefore, each QPS has three keys in each dimension. Analysis of QPS encryption systems is covered extensively in [23].

4.3. Method 3

The optical encryption scheme proposed in [24] is an extension of that proposed in [20] above. The only difference is, an additional random phase key and an additional FRT operation have been added in the encryption and decryption, to further encrypt the data.

Encryption consists of multiplying the input image by RPK 1, applying a FRT of order a_1, multiplying by RPK 2, applying a FRT of order a_2, multiplying by RPK 3, and finally applying a FRT of order a_3.

Decryption consists of applying a FRT of order $-a_3$, multiplying by the conjugate of random phase mask 3, applying a FRT of order $-a_2$, multiplying by the conjugate of random phase mask 2, and finally applying a FRT of order $-a_1$. The resultant has an amplitude distribution equal to our original image. An optical implementation of this encryption/decryption scheme is shown in to fig. 8. We note that it is almost identical to that given in fig. 3 except for the additional SLM and lens representing the additional RPK and fractional operation.

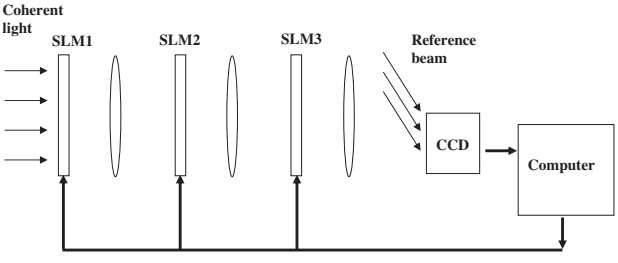

Fig. 8. Optical encryption/decryption scheme for method 3.

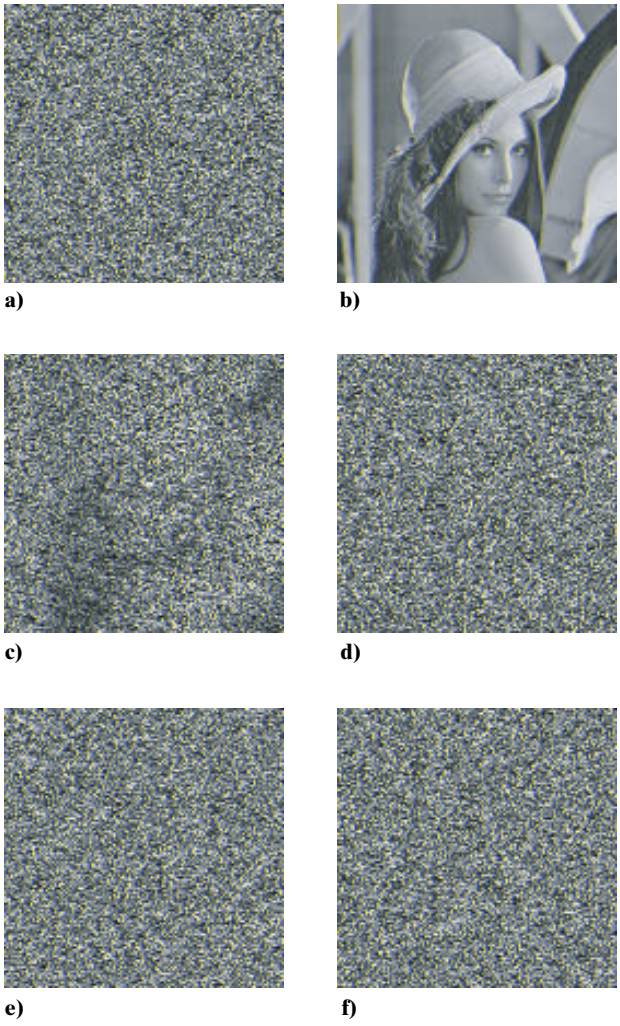

Fig. 9. Method 3: a) The encrypted image (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with a MSE = 5930.87; b) correctly decrypted (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 0.00; c) incorrectly decrypted (0.7, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 5063.37; d) incorrectly decrypted (0.5, 0.5, 0.7, 0.5, 0.5, 0.5) with MSE = 5841.08; e) incorrectly decrypted (0.5, 0.5, 0.5, 0.5, 0.7, 0.5) with MSE = 5896.61; f) decrypted using incorrect phase (second RPK in encryption process i.e. SLM3) with MSE = 5972.89.

The procedure was simulated for ($a_{1x} = a_{1y} = 0.5$, $a_{2x} = a_{2y} = 0.5$, and $a_{3x} = a_{3y} = 0.5$). The simulated results showing the encrypted image, and both a correct and an incorrect decryption are shown in fig. 9. The robustness of these fractional order keys to blind decryption is shown in fig 10. where we graph error in a_{1x} (thick line), a_{2x} (thinner line) and a_{3y} (thinnest line) used in the decryption process, against the MSE of the resulting decrypted images. The result of this additional phase key and FRT operation is that our image is further encrypted with 3 additional phase keys – the new phase key and the additional fractional order keys in the x and y directions. Also, it can be seen in fig. 10 that the robustness of the third order key a_3 is slightly better than that of a_2 and significantly better than that

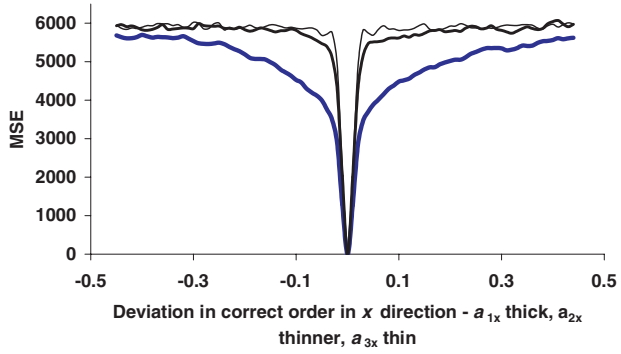

Fig. 10. Graph of deviation in decryption order keys for method 3 in the x direction from the correct values against the resultant MSE.

of a_1. This is due to the cummulative effect of the error early in our decryption process, leading to the two RPKs being applied in incorrect fractional domains.

4.4. Method 4

The optical encryption scheme outlined in [25] is a generalisation of the two previously described encryption schemes. We use some arbitrary number, n, of phase keys and n FRT operations to encrypt our data.

The number of keys needed to decrypt the data is given by $3n-1$, which is made up of $n-1$ phase keys and $2n$ FRT order keys. Graphical representations of encryption and decryption are shown in fig. 11 and fig. 12.

The case for $n=2$ is described by method 2 above and the case for $n=3$ is given by method 3 above. Optical implementation of the encryption/decryption scheme is given in fig 13. Here, multiplying by the random phases is carried out digitally within the computer. To carry out successive FRT operations we record the results using holographic techniques and send this

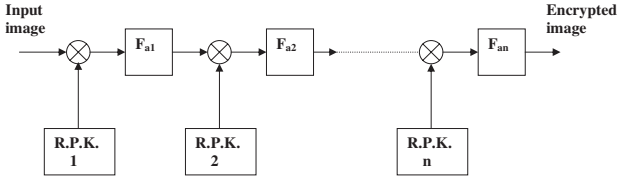

Fig. 11. Method 4, general interative encryption scheme.

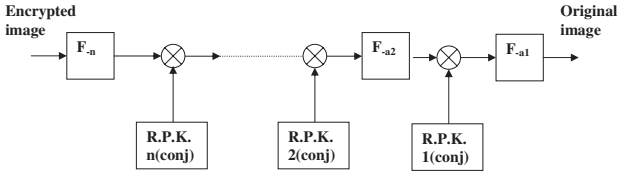

Fig. 12. Method 4, the corresponding iterative decryption scheme.

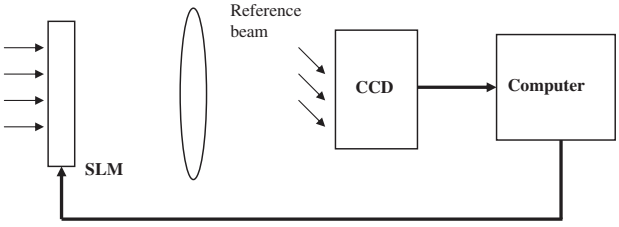

Fig. 13. Optical encryption/decryption scheme for method 4 and method 9.

to the input of the system which is a SLM, capable of displaying both amplitude and phase information.

It should be noted that as we further encrypt the image with more and more FRT operations the robustness of the orders as decryption keys increases. However, the increase in robustness is only significant for the first two FRT operations. Simulations of this method have already been presented for $n=2$ and $n=3$ above.

4.5. Method 5

In [26], the authors propose a new type of fractional convolution integral. We wish to fractionally convolve two functions $f(x)$ and $h(x)$ and the fractional convolution operation has three parameters a_1, a_2 and a_3. The fractional convolution operation is defined as follows

$$g(x) = f(x) \overset{a_1, a_2, a_3}{*} h(x)\,, \tag{20}$$

$$\begin{aligned} g(x) = {} & \exp\left\{-\mathrm{i}\cot\left(a_3\,\frac{\pi}{2}\right)x^2\right\} \\ & \times\left[f(x)\exp\left\{\mathrm{i}\cot\left(a_1\,\frac{\pi}{2}\right)\right\} * h(x)\right. \\ & \left.\times\exp\left\{\mathrm{i}\cot\left(a_2\,\frac{\pi}{2}\right)\right\}\right], \end{aligned} \tag{21}$$

where the $*$ in the above expression denotes the convolution operation in the traditional sense.

It is possible to deduce another interpretation of this operation in terms of FRT operations. First, we calculate the FRT of order a_1 of $f(x)$ and also the FRT of order a_2 of the function $h(x)$

$$f_{a1}(x_{a1}) = F_{a1}\{f(x)\}\,, \qquad h_{a2}(x_{a2}) = F_{a2}\{h(x)\}\,. \tag{22}$$

We multiply these functions together and multiply the result by X, a phase term, dependent on a_1, a_2 and a_3, which we do not define here. Finally we apply a FRT of order $-a_3$ to the result to give us,

$$g(x) = F_{-a3}\{X f_{a1}(x_{a1})\, h_{a2}(x_{a2})\}\,. \tag{23}$$

The encryption scheme is based on the convolution operation outlined above, where $f(x)$ represents our image to be encrypted and $h(x)$ is a random phase or intensity function. In the following simulations we have set $h(x)$ equal to a random phase function. In the previous sections outlined above, we have noted the

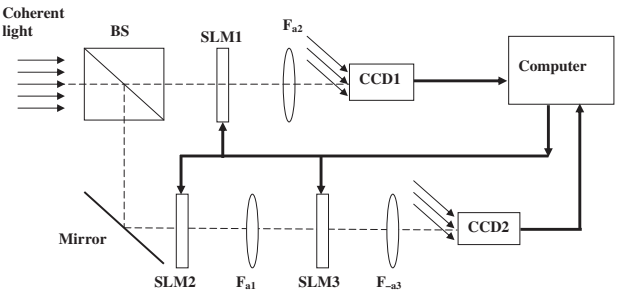

Fig. 14. Optical encryption/decryption scheme for method 5.

importance of a phase mask, which is multiplied by our original image at the input to the encryption process. This random phase, which is not required during decryption, serves to further encrypt the image and also to strengthen the robustness of the fractional order keys. Since there is no extra cost in terms of hardware, we add this feature to this encryption process, improving upon the results presented in [26]. The optical implementation for encryption is shown in fig. 14. SLM1 displays $h(x)$. SLM2 displays $f(x)\exp(in(x))$. We use a CCD and a computer to display $XH_{a2}(x_{a2})$. We can use the same set-up for decryption. SLM1 will again display $h(x)$, SLM2 will display our encrypted complex image and SLM3 will display $1/XH_{a2}(x_{a2})$. The lens that carried out FRT a_1, now applies an FRT of order a_3 while the lens that carried out FRT $-a_3$ will now applies an FRT of order $-a_1$.

The procedure was simulated for ($a_{1x} = a_{1y} = 0.5$, $a_{2x} = a_{2y} = 0.5$, and $a_{3x} = a_{3y} = 0.5$). The simulated results showing the encrypted image, correct and incorrect decryption are shown below in fig. 15. The robustness of these fractional order keys to blind decryption is shown in fig. 16. where we graph error in a_{1x} (thick line), a_{2x} (thinner line) and a_{3x} (thinnest line) used in the decryption process, against the resulting MSE.

4.6. Method 6

In [27], the authors outline a new and very different method of encryption using the FRT. First, we will present a diagram displaying the encryption scheme to aid in our explanation, see fig. 17 below.

Each H_n represents a randomly coded pure intensity filter and H_{-n} represents its complement. By this we mean $H_n + H_{-n} = 1$. We have n channels with n outputs $g_n(x)$. Each of these outputs is necessary to decrypt the image. To carry out decryption, we apply a FRT of order $-a_{n-1}$ to all the outputs. We add $F_{-a_{n-1}}\{g_1(x)\}$ and $F_{-a_{n-1}}\{g_2(x)\}$. H_n, and its complement H_{-n}, disappear since they add up to 1. We now apply a FRT of order $-a_n$ to the result of this addition and to all the other channels. The procedure repeats n times until we have eliminated all the H filters and arrive back at our original image. The optical implementation of this encryption/decryption scheme is not shown here. Each FRT operation would again be car-

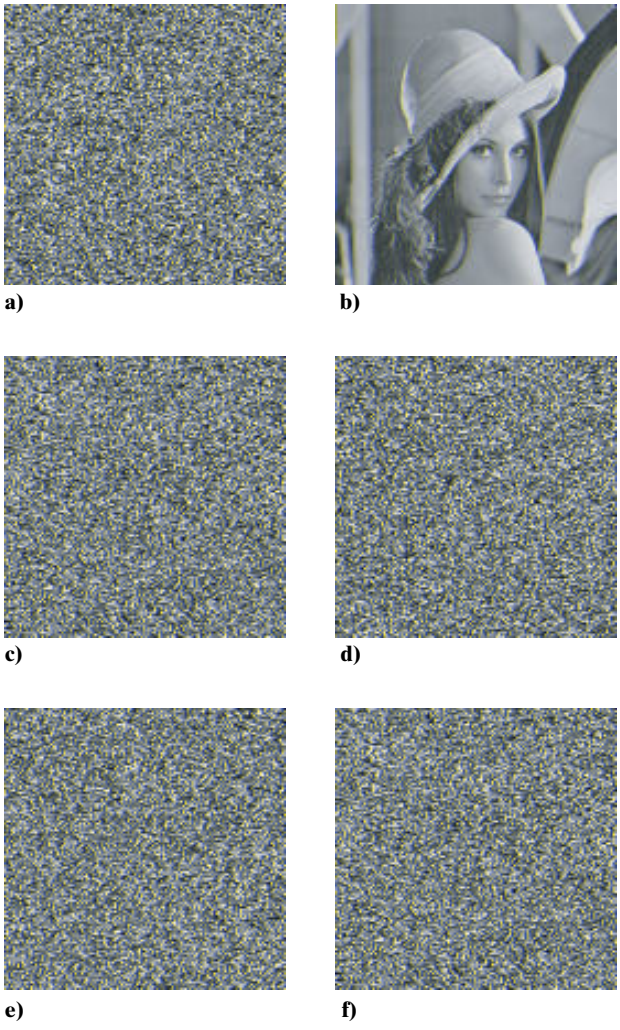

Fig. 15. Method 5: a) The encrypted image (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with a MSE = 5918.06; b) correctly decrypted (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 0.00; c) incorrectly decrypted (0.7, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 4987.03; d) incorrectly decrypted (0.5, 0.5, 0.7, 0.5, 0.5, 0.5) with MSE = 5982.17; e) incorrectly decrypted (0.5, 0.5, 0.5, 0.5, 0.7, 0.5) with MSE = 5907.84; f) decrypted using incorrect phase key with MSE = 5753.07.

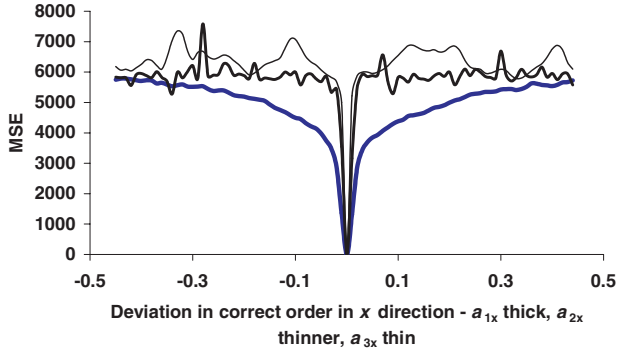

Fig. 16. Graph of deviation in decryption order keys for method 5 in the x direction from the correct values against the resultant MSE.

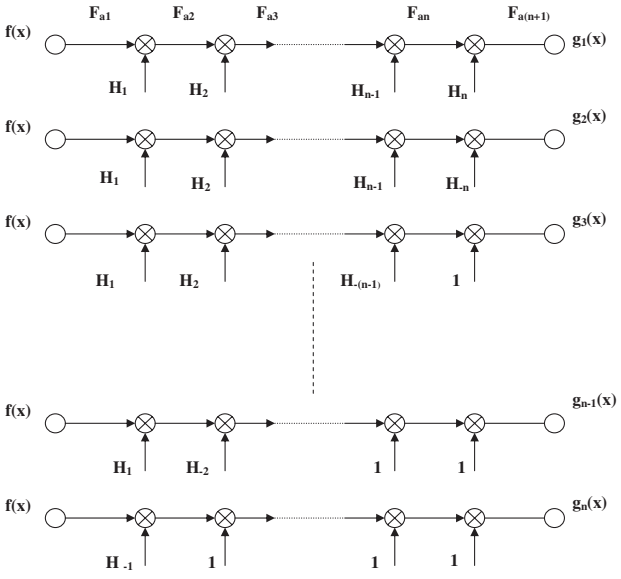

Fig. 17. Diagram representation of encryption algorithm in method 6.

ried out using a lens. The filtering would be carried out either digitally or using SLMs. Addition would have to be carried out digitally which means we would have to record the result of each FRT stage in each channel during the decryption process. The main advantage of this method is that the effect of multiplicative noise is decreased by a factor equal to the number of channels. There is no effect on additive noise. Disadvantages include that the resulting encrypted signal from an n channel system is made up of n image signals and the robustness of the fractional order keys less than that of most of the other methods reviewed in this paper.

A three-channel system was simulated with ($a_{1x} = a_{1y} = 0.5$, $a_{2x} = a_{2y} = 0.5$, and $a_{3x} = a_{3y} = 0.5$) and the H functions were chosen to be white random intensity functions. The encrypted image, correct and incorrect decryptions are presented in fig. 18. The robustness of these fractional order keys to blind decryption is shown in fig 19. where we graph error in a_{1x} (thick line), a_{2x} (thinner line) and a_{3x} (thinnest line) used in the decryption process, against the resulting MSE.

4.7. Method 7

In [28], the author derives a different fractional Fourier transform than the one previously presented in this paper in eq. (1) and applied in all of the previous encryption schemes. Making use of the times four periodicity of the Fourier transform he derives a transform which has the following form,

$$F_a\{f(x)\} = A_0(a)\, f(x) + A_1(a) F\{f(x)\} + A_2(a)\, F\{F\{f(x)\}\} + A_3(a)\, F\{F\{F\{f(x)\}\}\}, \quad (24)$$

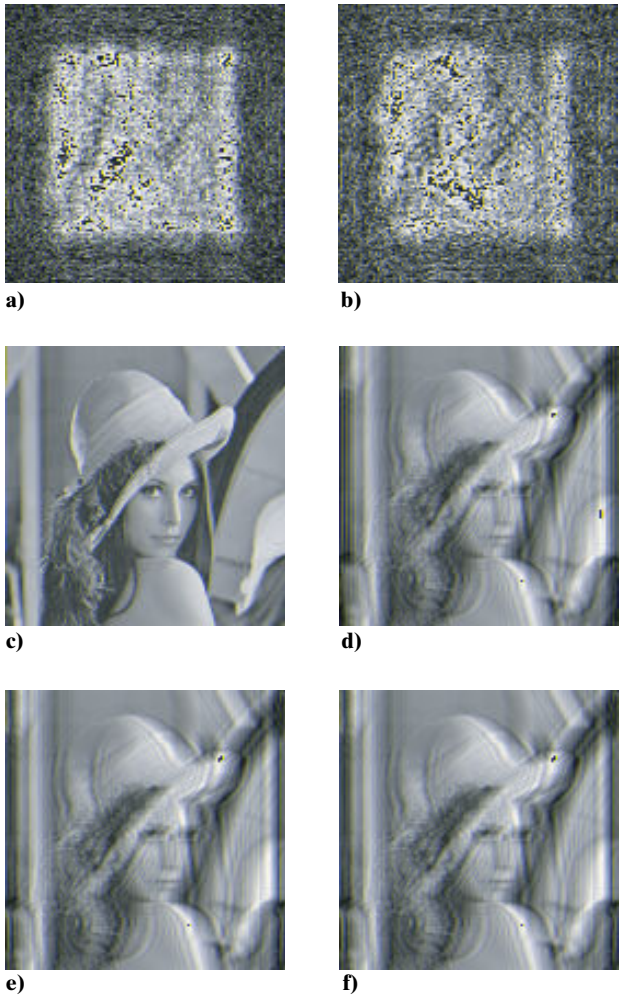

Fig. 18. Method 6: a) Second part of encrypted image (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with a MSE = 7736.56; b) third part of encrypted image (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with a MSE = 7531.03; c) correctly decrypted (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 0.00; d) incorrectly decrypted (0.7, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 1119.72; e) incorrectly decrypted (0.5, 0.5, 0.7, 0.5, 0.5, 0.5) with MSE = 1088.40; f) incorrectly decrypted (0.5, 0.5, 0.5, 0.5, 0.7, 0.5) with MSE = 5390.98; f) decrypted using incorrect phase key with MSE = 2622.07.

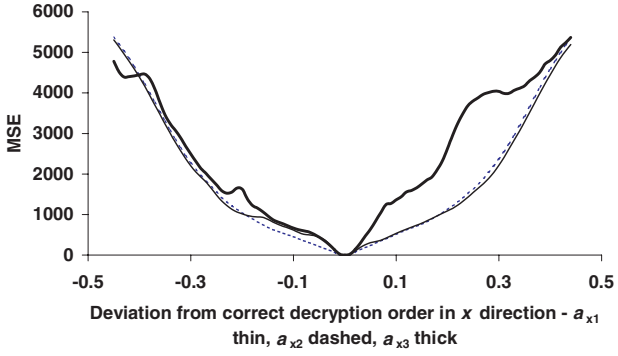

Fig. 19. Graph of deviation in decryption order keys for method 6 in the x direction from the correct values against the resultant MSE.

where F denotes the Fourier transform. On the basis of a being a continuous variable, the fact that any fractional Fourier transform should obey the index additive property and should reduce to the FT for $a = 1$ he formulates an expression for $A_i(a)$, the weighting factors shown above. The resulting fractional Fourier transform is given by,

$$F_a\{f(x)\} = \exp(\mathrm{i}\pi a/2)\,[\cos(\pi a/2)\,f(x) - \mathrm{i}\sin(\pi a/2)\,F\{f(x)\}]\,. \tag{25}$$

It should be noted that this transform has the same eigenfunctions as the definition presented earlier. However the eigenvalues are different. The author goes on to generalize the above result for any transform, which has a periodicity of N ($N = 4$ for the FT). It is demonstrated that any transform operator K which, has a periodicity of N can be fractionalized as follows:

$$K_a\{f(x)\} = \frac{1}{N}\sum_{n=0}^{N-1} K_n\{f(x)\}\exp[\mathrm{i}(N-1)\,\pi(a-n)/N] \times \frac{\sin[\pi(a-n)]}{\sin[\pi(a-n)/N]}\,. \tag{26}$$

In [29], the authors go on to use this result to define a new type of generalised FRT. They let K denote the FRT of order $4/N$. This is best clarified by example: for a periodicity $N = 8$, we have the FRT of order 0.5. Applying an FRT of order 0.5 eight succession times is equivalent to application of the identity operator. K_n, in this case, denotes n applications of the FRT 0.5 operator. They go on to use this expression to develop an encryption scheme. The keys to decrypting the data are a and N. An optical implementation of the above is shown in fig. 20. We begin with the image to be encrypted, displayed on an SLM. The FRT of order $4/N$ is recorded using holographic methods, on the CCD. It is stored in the computer and it is displayed on the SLM. Now the FRT of order $2(4/N)$ is recorded and so on until we have all the F_n terms. Then these complex images are weighted as defined by eq. (26) above and they are all added together to give us our encrypted complex image. Decryption uses an identical set-up, but we replace a with $-a$ in our calculations. Simulations of this optical encryption scheme were carried out for $N = 8$ in both x and y directions and with $a_x = a_y = 0.5$. An encrypted image, a decrypted image and an incorrectly decrypted image are shown in fig. 21. Note that the correctly decrypted image has a MSE of 60, this is due to difficulty in simulating this algorithm and not due to any difficulties inherent to the encryption scheme itself. We also graph the effect of incorrect N in the x direction in fig. 22 and incorrect order in x direction in fig. 23. We note that the robustness of these keys improves the larger the value of N used in the encryption process.

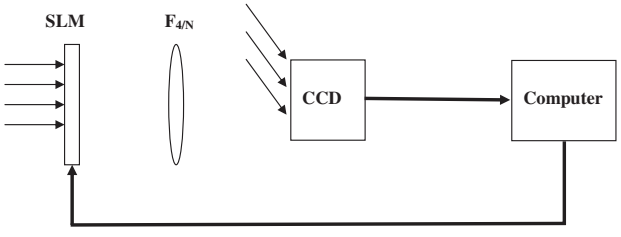

Fig. 20. Optical encryption/decryption scheme for method 7.

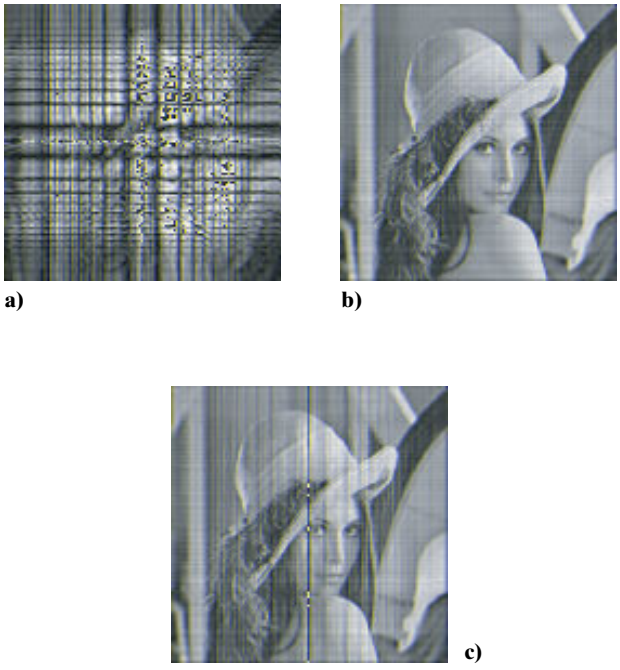

Fig. 21. Method 8: a) The encrypted image $N_x = N_y = 8$, $a_x = a_y = 0.5$, with a MSE = 6663.08; b) correctly decrypted MSE = 60.27; c) incorrectly decrypted $a_x = 0.7$ with MSE = 424.68.

4.8. Method 8

In [30] a new technique based on a random shifting or Jigsaw algorithm is proposed. The main advantage of this algorithm is that we do not need to use any phase keys in order to decrypt the image and yet we encrypt

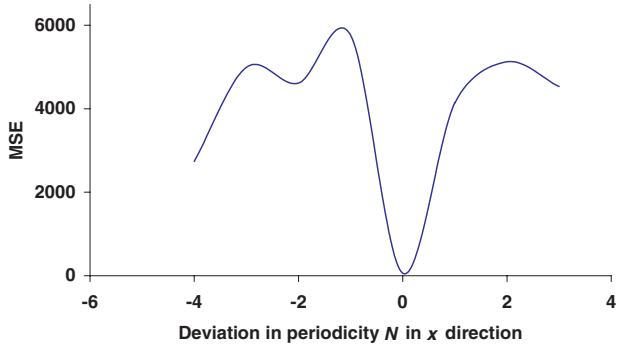

Fig. 22. Error in value of N used in decryption process in method 7 against the resultant MSE.

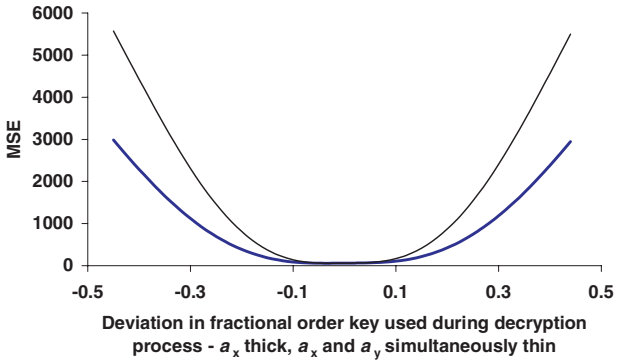

Fig. 23. Graph of deviation in decryption order keys for method 7 from the correct values against the resultant MSE.

the image in a very similar way. The encryption scheme is as follows. First, the input image is multiplied by a random phase function giving us

$$f(x)\,\exp\left[\mathrm{i}2\pi n(x)\right], \tag{27}$$

where $n(x)$ is a white sequences uniformly distributed in [0, 1]. The authors define a Jigsaw transform, $J\{\,\}$, which juxtaposes different sections of the complex image. A simple two-dimensional case is shown in fig. 24. We show the effect of this transform on our input image in fig. 25a. In this case the image was broken up into 64 subsections of 8×8 pixels, which were repositioned relative to each other according to some permutation. The permutation used is random. The Jigsaw transform is unitary, energy being conserved through the transform and it also has an inverse. In the case shown in fig. 25b, there are 64! possible Jigsaw transform permutations. Each particular Jigsaw transform is denoted by some index e.g. $J_b\{\,\}$ and its inverse is denoted by $J_{-b}\{\,\}$. The Jigsaw transform is applied to eq. (27)

$$J_{b1}\{f(x)\,\exp\left[\mathrm{i}2\pi n(x)\right]\}. \tag{28}$$

The resulting complex information can be displayed using SLMs, which have the capability of modulating both the phase and intensity of a waveform. Now we apply a FRT operation of order a_1 which gives us

$$F_{a1}\{J_{b1}\{f(x)\,\exp\left[\mathrm{i}2\pi n(x)\right]\}\}. \tag{29}$$

This complex data is collected using interofemetric methods and a second Jigsaw transform with permutation b_2 is now applied. The result of this is given by

$$J_{b2}\{F_{a1}\{J_{b1}\{f(x)\,\exp\left[\mathrm{i}2\pi n(x)\right]\}\}\}. \tag{30}$$

Again this complex data can be represented using SLMs. A second FRT, this time of order a_2 is now applied to give

$$F_{a2}\{J_{b2}\{F_{a1}\{J_{b1}\{f(x)\,\exp\left[\mathrm{i}2\pi n(x)\right]\}\}\}\}. \tag{31}$$

Once again, the data can be collected using holographic methods. Applying a third Jigsaw transform, display the result on the SLM and apply a third and final FRT, this time of order a_3, to give us the encrypted image

$$g(x) = F_{a3}\{J_{b3}\{F_{a2}\{J_{b2}\{F_{a1}\{J_{b1}\{f(x)\,\exp\left[\mathrm{i}2\pi n(x)\right]\}\}\}\}\}\}. \tag{32}$$

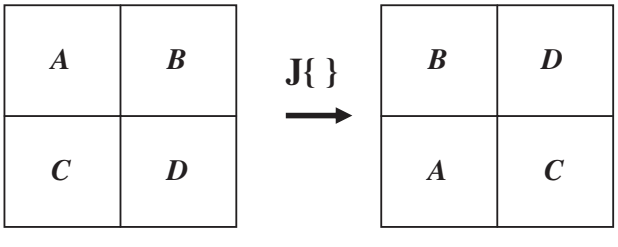

Fig. 24. Simple illustration of the Jigsaw transform used in method 8.

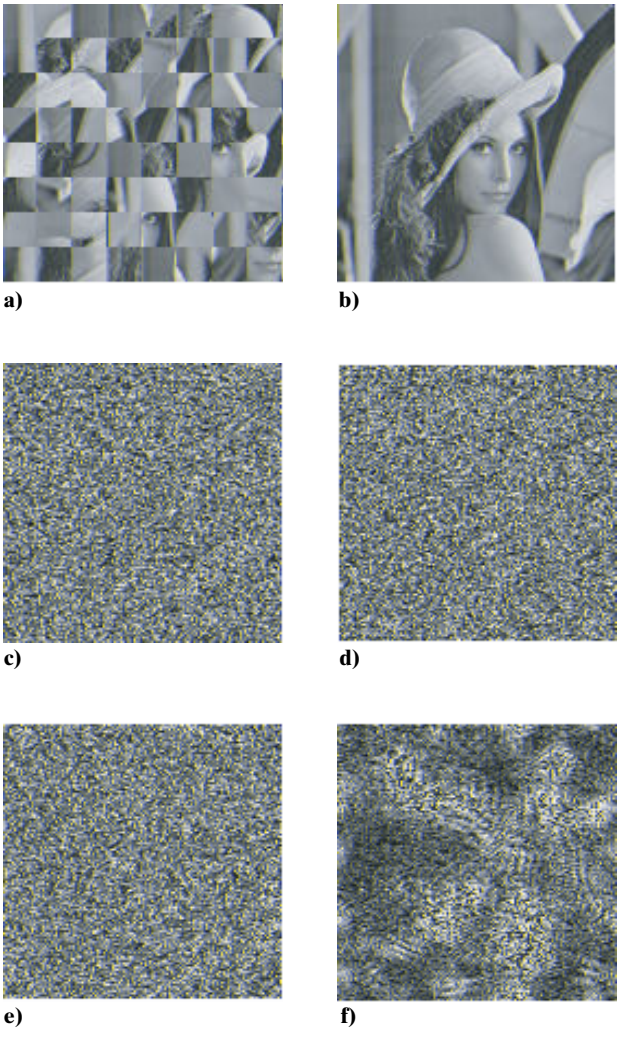

Fig. 25. Method 8: a) The input image after the first 16×16 Jigsaw transform; b) correctly decrypted (0.5, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 0.00; c) incorrectly decrypted (0.55, 0.5, 0.5, 0.5, 0.5, 0.5) with MSE = 3943.14; d) incorrectly decrypted (0.5, 0.5, 0.55, 0.5, 0.5, 0.5) with MSE = 5441.89; e) incorrectly decrypted (0.5, 0.5, 0.5, 0.5, 0.55, 0.5) with MSE = 5690.98; f) decrypted using incorrect phase key with MSE = 5937.99.

We could of course continue this procedure of FRT and Jigsaw to further encrypt our image but practical limitations, in terms of time taken and susceptibility to noise and error, would increase.

The intensity of the encrypted image is shown in fig. 25c for the case when ($a_{1x} = a_{1y} = 0.5$, $a_{2x} = a_{2y} = 0.5$, and $a_{3x} = a_{3y} = 0.5$).

Decryption is given by the operation

$$f(x) = J_{-b1}\{F_{-a1}\{J_{-b2}\{F_{-a2}\{J_{-b3}\{F_{-a3}\{g(x)\}\}\}\}\}\} \tag{33}$$

and is simply the inverse of the encryption process. At the final stage we need only capture the intensity information since this represents our original image.

The phase of the decrypted signal should be equal to the random phase we added to our image originally. It can be discarded since it no longer serves any purpose. Without this initial phase, the Jigsaw scheme would not be an advisable encryption method because it might be possible to recognize high frequency discontinuities and thus break the Jigsaw encryption process. However, the inclusion of the random phase at the beginning serves to whiten the image. Therefore no obvious sharp discontinuities will occur in the image because of the juxtaposition of the image pieces. In fig. 25f we show the result of encrypting the image without the random phase at the input and with the same orders. The encrypted image shows unwanted patterns, which are a result of the random shifting in the FRT domains. The patterns become more pronounced as we decrypt with fractional order keys close to the correct values.

The decryption process described requires the knowledge of 9 keys in total. These nine keys are made up of 6 FRT order keys (3 in x and 3 in y) and 3 Jigsaw transform permutations. We examine the sensitivities of the keys a_{1x}, a_{2x}, and a_{3x} in fig. 26. The thickest line corresponds to varying the value of a_{1x} in the decryption process while all other keys are correct. The thinnest line corresponds to varying the value of a_{3x} and the middle line shows variation of a_{2x}. In fig. 25e we show the decrypted image when a_{x3} is in error by 0.05. In this case, the image remains totally encrypted. The permutation keys are also robust to blind decryption. Even if the dimensions of the blocks involved are known, there are a vast number of possible permutations. In the case shown here, there are $64! = 1.27 \times 10^{89}$ possible permutations for each Jigsaw transform. The result of using a randomly incorrect permutation for b_3 in the decryption process is shown in fig. 25d. Again the image remains totally encrypted.

A schematic for a possible optical implementation of this system is shown in fig. 13. As described, the Jigsaw transforms are applied digitally. SLMs are used to display the signal after each step in the encryption/decryption process a single lens configuration is used to implement the FRT. A reference beam is employed to record the complex data after each FRT operation. We note that in the final stage of the decryption process we do not need the reference beam.

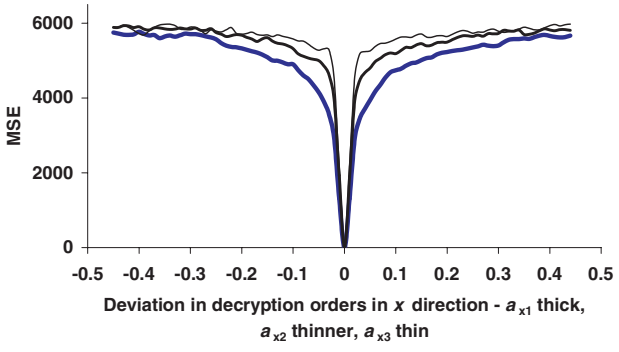

Fig. 26. Graph of deviation in decryption order keys for method 8 from the correct values against the resultant MSE.

4.9. Method 9

One possible definition of the DFRT [12] has a correlation property which has been used to derive a recursive algorithm for the phase retrieval of a signal provided we have available the intensities of two fractional Fourier transforms of the original signal [7]. However, this 1-D algorithm cannot be simply extended to include a second dimension, as significant non-trivial differences occur in going from 1-D to 2-D. In [31] a method is outlined which allows the algorithm to be extended to more than one dimension and can be used to encrypt images.

First our input image is multiplied by some random phase function and then an FRT of some arbitrary order a_1 is applied. Only the intensity of the resultant image is stored. We then take the same input image and multiply by a second (and different) random phase function. This time we apply another FRT operation of order a_2 and again we only store the intensity of this. These two intensities make up our encrypted image.

In order to decryption the encoded image we use of the following definition

$$\begin{aligned}
&f_{p_x,p_y}(m_x\,\Delta x_{p_x},\, m_y\,\Delta y_{p_y}) \\
&= F^{p_x,p_y}\{f_{0,0}(l_x\,\Delta x_0,\, l_y\,\Delta y_0)\}\;(m_x\,\Delta x_{p_x},\, m_y\,\Delta y_{p_y}) \\
&= A_{p_x}A_{p_y}\,\Delta x_0\,\Delta y_0 \times \sum_{l_y=\frac{-N_y}{2}}^{\frac{N_y}{2}-1}\sum_{l_x=\frac{-N_x}{2}}^{\frac{N_x}{2}-1}\Bigg[f_{0,0}(l_x\,\Delta x_0,\, l_y\,\Delta y_0) \\
&\quad\times \exp\left\{\mathrm{i}\pi\cot\left(\frac{p_x\pi}{2}\right)[(l_x\,\Delta x_0)^2 + (l_x\,\Delta x_{p_x})^2] - \mathrm{i}2\pi\,\frac{l_x m_x}{N_x}\right\} \\
&\quad\times \exp\left\{\mathrm{i}\pi\cot\left(\frac{p_y\pi}{2}\right)[(l_y\,\Delta y_0)^2 + (m_y\,\Delta y_{p_y})^2] - \mathrm{i}2\pi\,\frac{l_y m_y}{N_y}\right\}\Bigg]
\end{aligned} \tag{34}$$

and its correlation property

$$\sum_{l_y=-\frac{N}{2}}^{\frac{N_y}{2}-1}\sum_{l_x=-\frac{N}{2}}^{\frac{N_y}{2}-1}\Big[f^{*}_{0,0}(l_x\,\Delta x_0,\,l_y\,\Delta y_0)\,f_{0,0}[(l_x+k_x)\,\Delta x_0,\,(l_y+k_y)\,\Delta y_0]$$
$$\times\exp\left\{\mathrm{i}2\pi\cot\left(\frac{p_x\pi}{2}\right)l_xk_x(\Delta x_0)^2\right\}$$
$$\times\exp\left\{\mathrm{i}2\pi\cot\left(\frac{p_y\pi}{2}\right)l_yk_y(\Delta y_0)^2\right\}\Big]$$
$$=\frac{\left|\sin\left(\frac{p_x\pi}{2}\right)\right|}{N_x\,\Delta x_0^2}\,\frac{\left|\sin\left(\frac{p_y\pi}{2}\right)\right|}{N_y\,\Delta y_0^2}$$
$$\times\exp\left\{\mathrm{i}\pi\cot\left(\frac{p_x\pi}{2}\right)k_x^2(\Delta x_0)^2\right\}$$
$$\times\exp\left\{\mathrm{i}\pi\cot\left(\frac{p_y\pi}{2}\right)k_y^2(\Delta y_0)^2\right\}$$
$$\times\sum_{m_y=\frac{-N_y}{2}}^{\frac{N_y}{2}-1}\sum_{m_x=\frac{-N_x}{2}}^{\frac{N_x}{2}-1}\Big[|f_{p_x,p_y}(m_x\,\Delta x_{p_x},m_y\,\Delta y_{p_y})|^2$$
$$\times\exp\left\{\mathrm{i}2\pi\,\frac{k_xm_x}{N_x}\right\}\exp\left\{\mathrm{i}2\pi\,\frac{k_xm_x}{N_x}\right\}\Big], \tag{35}$$

where $f_{0,0}(l_x\,\Delta x_0,\,l_y\,\Delta y_0)$ is the discrete function which we transform, and the integers l_x and l_y have the following ranges

$$-\frac{N_x}{2}\le l_x\le\frac{N_x}{2}-1\quad\text{and}\quad-\frac{N_y}{2}\le l_y\le\frac{N_y}{2}-1\,. \tag{36}$$

Δx_0 and Δy_0 are the sampling intervals of our input function in the x and y directions respectively, and Δx_{p_x} and Δy_{p_y} are the sampling intervals in the new FRT domain. Both m_x and m_y have the same range of values as l_x and l_y.

In order to decrypt out data we need to know the fractional orders (a_{x1}, a_{y1}, a_{x2}, a_{y2},) used to encrypt the data and the two phase keys used in the encryption process. The authors propose implementation of the encryption using optical FRT and SLMs. Decryption being carried out digitally. Numerical simulations revealed that the decryption scheme is extremely sensitive to errors in any of the fractional keys. This makes the algorithm difficult to implement using conventional bulk and GRIN optical methods since on needs to know the physical parameters of the system to an extremely high degree and even low-level noise generated within the system would be critical [32]. Nevertheless the algorithm is shown to be a very effective method of digital encryption. The results of numerical simulations on a 32×32 lena image are shown below.

It was not possible to run the error simulations (MSE) for the 256×256 image case, because the pixel values of incorrectly decrypted images could not be processed by the software used. This meant that in this case the robustness of the various fractional keys could not be measured and graphed. However ideal encryption and decryption could still be carried out for 256×256 images. For these reasons a 32×32 pixel image was chosen for demonstration purposes.

The input image is shown in fig. 27a. The encrypted image is shown in fig. 27b, which displays the amplitude of a signal, whose real and imaginary parts are given by the two intensities obtained from the encryption procedure. A correctly decrypted image is shown in fig. 27c. In fig. 27d we show the result of decrypting with $a_{x1}=0.50001$, i.e. an error of 1×10^{-5} in the FRT order in the x direction, and in fig. 27e we show the result of decrypting with $a_{x2}=0.50001$. The resulting image has a MSE of $1.37\times10^{+43}$. In fig. 27f we show the result of decrypting the signal using all the correct fractional order keys but a completely incorrect phase key.

Fig. 28 and fig. 29 correspond to the 32×32 image case. Both show how deviations from the correct values for a_{x1} and a_{x2} effect the MSE of the resulting de-

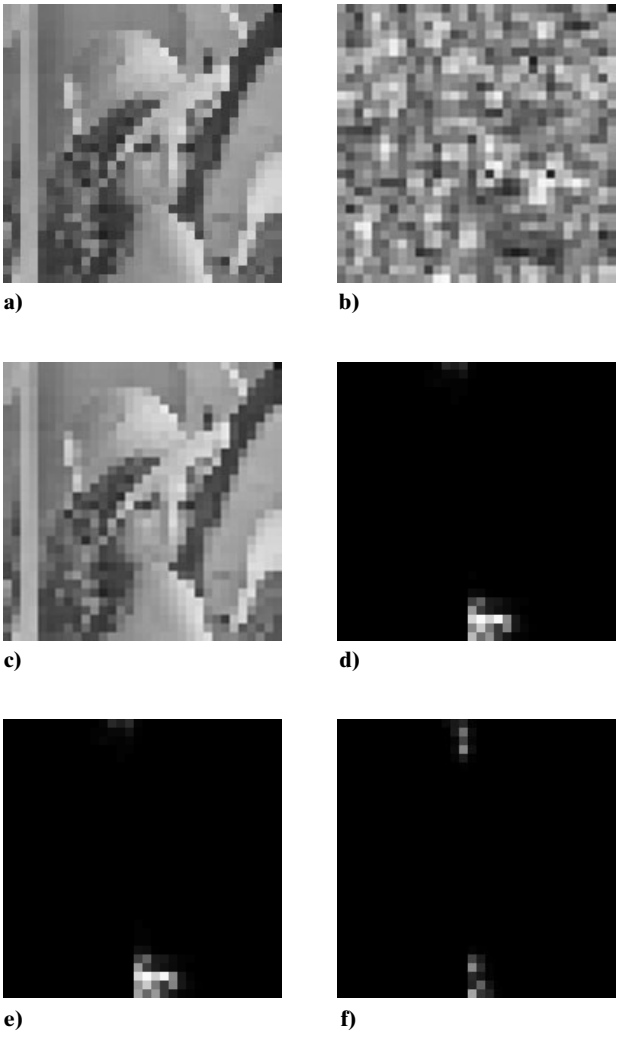

Fig. 27. Method 9: a) input image; b) encrypted image MSE = 17394.68; c) decrypted image with MSE = 0.40; d) decrypted using an incorrect value of a_{x1}, out by 1×10^{-5} with MSE = 1.46×10^{39}; e) decrypted using an incorrect value of a_{x2}, out by 1×10^{-5} with MSE = 1.37×10^{34}; f) decrypted using an incorrect phase key with MSE = 1.51×10^{75}.

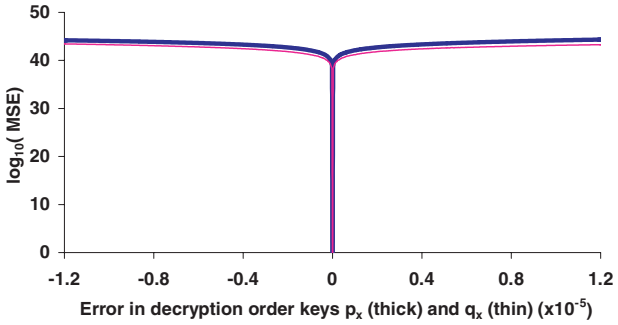

Fig. 28. Small error in decryption order keys used versus the resultant MSE of the decrypted 32 × 32 image in method 9.

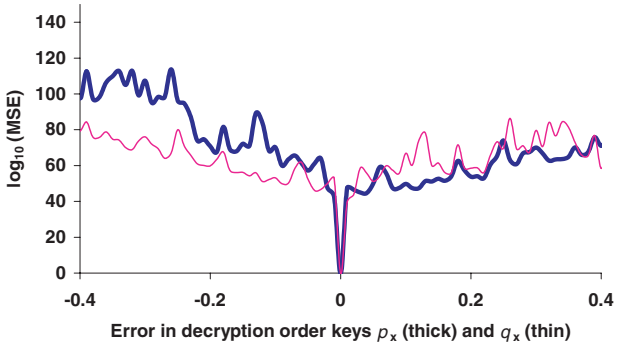

Fig. 29. Error in decryption order keys used versus the resultant MSE of the decrypted 32 × 32 image in method 9.

crypted image. Fig. 28 shows this variation for very small deviations in the orders, in step sizes of 1.0×10^{-6} while fig. 29 is the same case for a wider range of deviations. It can be seen that symmetry exists in the curves for increases in a_{x1} and decreases in a_{x2} and vice versa.

It should also be noted that as we increase the size of the image we are dealing with, the sensitivity of the fractional orders increases considerably and the MSE of incorrectly decrypted images also increases considerably.

5. Conclusions

In this paper we have compared and contrasted nine recently proposed optical encryption algorithms involving the use of the fractional Fourier transform. We have measured the robustness of the various keys in these systems and provided simulation results for almost all of these methods under conditions of ideal encryption and decryption and incorrect decryption based on the use of incorrect keys.

Acknowledgements. The authors would like to acknowledge the support of Enterprise Ireland through the Research Innovation Fund.

References

[1] Namias V: The fractional order Fourier transform and its applications to quantum mechanics. J. Inst. Math. Appl. **25** (1980) 241–265
[2] McBride AC, Kerr FH: On Namias fractional Fourier transform. IMA J. Appl. Math **39** (1987) 159–179
[3] Mendolovic D, Ozaktas HM: Fractional Fourier transforms and their optical implementation: I. J. Opt. Soc. Am. A **10** (1993) 1875–1880
[4] Ozaktas HM, Mendolovic D: Fractional Fourier transforms and their optical implementation: II. J. Opt. Soc. Am. A **10** (1993) 2522–2531
[5] Lohmann AW: Image rotation, Wigner rotation and the fractional Fourier transform. J. Opt. Soc. Am. A **10** (1993) 2181–2186
[6] Zalevsky Z, Mendolovic D, Dorsch RG: Gerchberg-Saxton algorithm applied in the fractional Fourier or Fresnel domain. Opt. Lett. **21** (1996) 842–844
[7] Cong W-X, Chen N-X, Gu B-Y: Recursive algorithm for phase retrieval in the fractional Fourier transform domain. Appl. Opt. **37** (1998) 6906–6910
[8] Zhang Y, Dong B, Gu B, Yang G: Beam shaping in the fractional Fourier transform domain. J. Opt. Soc. Am. A **15** (1998) 1114–1120
[9] Ozaktas HM, Barshan B, Mendolovic D, Onural L: Convolution, filtering, and multiplexing in fractional Fourier domains and their relation to chirp and wavelet transforms. J. Opt. Soc. Am. A **11** (1994) 547–559
[10] Refregier P, Javidi B: Optical image encryption based on input plane and Fourier plane random encoding. Opt. Lett. **20** (1995) 767–769
[11] Bitran Y, Mendolovic D, Dorsch R, Lohmann A, Ozaktas HM: Fractional Fourier Transform: simulations and experimental results. Appl. Opt. **34** (1995) 1329–1332
[12] Ozaktas HM, Arikan O, Kutay MA, Bozdagi G: Digital computation of the fractional Fourier transform. IEEE Trans. Signal Proc. **44** (1996) 2141–2150
[13] Garcia J, Mas D, Dorsch R: Fractional Fourier transform calculation through the fast Fourier transform algorithm. Appl. Opt. **35** (1996) 7013–7018
[14] Marinho FJ, Francisco J, Bernardo L: Numerical calculation of fractional fourier transforms with a single fast Fourier transform algorithm. J. Opt. Soc. Am. A **15** (1998) 2111–2116
[15] Candan C, Kutay MA, Ozaktas HM: The discrete fractional Fourier transform. IEEE Trans. Signal Proc. **48** (2000) 1329–1337
[16] Wang B, Sun CC, Su WC, Chiou AET: Shift tolerance property of an optical double random phase encoding encryption system. Appl. Opt. **39** (2000) 4788–4793
[17] Goudail F, Bollaro F, Javidi B, Refregier P: Influence of a perturbation in a double random phase encoding system. J. Opt. Soc. Am. A **15** (1998) 2629–2638
[18] Javidi B, Towghi N, Maghzi N, Verrall SC: Error reduction techniques and error analysis for fully phase and amplitude based encryption. Appl. Opt. **39** (2000) 4117–4130
[19] Towghi N, Javidi B, Lou Z: Fully phase encrypted image processor. J. Opt. Soc. Am. **16** (1999) 1915–1927
[20] Unnikrishnan G, Singh K: Double random fractional Fourier domain encoding for optical security. Opt. Eng. **39** (2000) 2853–2859
[21] Unnikrishnan G, Joseph J, Singh K: Optical encryption by double random phase encoding in the fractional Fourier domain. Opt. Lett. **25** (2000) 887–889
[22] Abe S, Sheridan JT: Optical operations on wave functions as the Abelian subgroups of the special affine Fourier transformation. Opt. Lett. **9** (1994) 1801–1803
[23] Unnikrishnan G, Singh K: Optical encryption using quadratic phase systems. Opt. Commun. **193** (2001) 51–67
[24] Liu S, Yu L, Zhu B: Optical image encryption by cascaded fractional Fourier transforms with random phase filtering. Opt. Commun. **187** (2001) 57–63

[25] Zhang Y, Zheng CH, Tanno N: Optical encryption based on iterative fractional Fourier transform. Opt. Commun. **202** (2002) 277–285
[26] Zhu B, Liu S: Optical Image encryption based on the the generalized fractional convolution operation. Opt. Commun. **195** (2001) 371–381
[27] Zhu B, Liu S: Optical image encryption with multistage and multichannel fractional Fourier-domain filtering. Opt. Lett. **26** (2001) 1242–1244
[28] Shih CC: Fractionalization of Fourier transform. Opt. Commun. **118** (1995) 495–498
[29] Zhu B, Liu S, Ran Q: Optical image encryption based on multifractional Fourier transforms. Opt. Lett. **25** (2000) 1159–1161
[30] Hennelly B, Sheridan JT: Optical image encryption by random shifting in fractional Fourier domains. Opt. Lett. **28** (2003) 269–271
[31] Hennelly B, Sheridan JT: Fractional Fourier transform based image encryption: Phase retrieval algorithm. Opt. Commun. accepted for publication (2003)
[32] Abe S, Sheridan JT: Random fractional Fourier transform: Stochastic perturbations along the axis of propagation. J. Opt. Soc. Am. A **16** (1999) 1986–1991