Optical image encryption by random shifting in fractional Fourier domains

B. Hennelly and J. T. Sheridan*

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

Received September 24, 2002

A number of methods have recently been proposed in the literature for the encryption of two-dimensional information by use of optical systems based on the fractional Fourier transform. Typically, these methods require random phase screen keys for decrypting the data, which must be stored at the receiver and must be carefully aligned with the received encrypted data. A new technique based on a random shifting, or jigsaw, algorithm is proposed. This method does not require the use of phase keys. The image is encrypted by juxtaposition of sections of the image in fractional Fourier domains. The new method has been compared with existing methods and shows comparable or superior robustness to blind decryption. Optical implementation is discussed, and the sensitivity of the various encryption keys to blind decryption is examined.

OCIS codes: 070.6020, 070.2590, 200.3050.

Information security and data encryption techniques have received increasing attention recently. Optical systems have the distinct advantage of processing complex two-dimensional data in parallel and carrying out otherwise slow operations at great speeds. In Ref. 1 an optical encryption scheme called double random phase encoding, which involves multiplying by random phase screens, one in the input plane and then a second in the Fourier domain, was presented. It can be shown that if the phases in these screens can be accurately described as statistically independent white noise, then the resulting encrypted image is also a white-noise distribution.[2] The first random phase plane serves to make the input image white but nonstationary and not encrypted. The second serves to make the image stationary and encoded. Thus, the random phase key located at the Fourier plane of this system serves as the only key in this encryption scheme.

The fractional Fourier transform (FRT) was introduced to the optical community by Ozaktas and Mendolovic.[3,4] The transform was used to describe wave propagation in graded index media. Lohmann described the relationship between the FRT and the Wigner distribution function[5] and gave two possible optical implementations, one of which, like the optical implementation of the Fourier transform, uses a single lens and free space. The FRT has an order associated with it, indicating the domain into which it transforms; i.e., the FRT of order $a = 1$ is simply the Fourier transform. The FRT is a linear transformation that is separable in both the x and y directions, and optical systems have been proposed that allow for implementation with different continuously variable orders in both the x and y directions.[6]

A number of algorithms have been proposed to compute the FRT numerically[7–9] with order $N\log(N)$ calculations that make use of the fast Fourier transform algorithm. We have implemented and compared these algorithms, and the algorithm outlined in Ref. 7 is used to produce the results presented here.

Several techniques have been proposed in the literature to optically encrypt images by use of the FRT.[2,10–14] We have examined all these encryption methods numerically, using all three of the fast algorithms[7–9] discussed above, and tested and compared their robustness to blind decryption. In Ref. 2 the method first presented in Ref. 1 is modified, with the two Fourier transform operations being replaced with two FRT operations; the phase key is therefore applied in some fractional domain. In this way, four new FRT order keys have been introduced, i.e., two in each direction. This work was developed in Refs. 10 and 11, in which the number of FRT operations and phase keys was increased. A fractional convolution operation was used for encryption in the study reported in Ref. 12 by making use of one phase key and three two-dimensional FRT operations. A method based on a multichannel approach was given in Ref. 13, in which the number of FRT operations is related to the number of channels used in the encryption scheme. Also, a method based on a more generalized FRT operation was developed in Ref. 14.

We now propose a new encryption scheme that uses jigsaw transforms that shift randomly in position to encrypt and decrypt the data.

We define the FRT operation on our input image $f(x)$ as follows:

$$f_a(x_a) = F_a\{f(x)\}(x_a) = \int_{-\infty}^{+\infty} A_\phi \exp[\, j\pi(x^2\cot\phi - 2xx_a + x_a{}^2\cot\phi)]f(x)\mathrm{d}x\,. \quad (1)$$

For the sake of brevity we describe only the one-dimensional case, where x_a represents the ath fractional domain, $\phi = a\pi/2$, and A_ϕ is a constant phase factor that is dependent on only the order of the transform. This definition is valid for values of a not equal to 0 or ± 2. We begin with the image to be encrypted.

0146-9592/03/040269-03$15.00/0

In our numerical simulations, a 256×256 image was used [see Fig. 1(a)]. First, we multiply our image to be encrypted by a random phase function, giving us

$$f(x)\exp[\,j2\pi n(x)], \tag{2}$$

where $n(x)$ is a white sequence uniformly distributed in $[0, 1]$. We now define the jigsaw transform, $J\{\}$, which juxtaposes different sections of the complex image. An example is shown in Fig. 1(b). In this case the image was broken up into 64 subsections of 8×8 pixels, which were repositioned relative to one another according to some random permutation. The jigsaw transform is unitary; its energy is conserved through the transform, and it also has an inverse. In the case shown in Fig. 1(b), there are 64! possible permutations. We denote any particular jigsaw transform by some index b, e.g., $J_b\{\}$, and its inverse by $J_{-b}\{\}$. We note that it is not necessary for the jigsaw transform to operate with square pieces, adding a further possible generalization that is not considered here. The jigsaw transform is applied to Eq. (2):

$$J_{b1}\{f(x)\exp[\,j2\pi n(x)]\}. \tag{3}$$

Optically, the resulting complex information can be displayed by use of spatial light modulators, which have the capability of modulating both the phase and the intensity of a waveform. Now we apply a FRT operation of order a_1. This gives us

$$F_{a1}\{J_{b1}\{f(x)\exp[\,j2\pi n(x)]\}\}. \tag{4}$$

We collect these complex data by use of holographic methods and apply another jigsaw transform with permutation b_2. The result of this is given by

$$J_{b2}\{F_{a1}\{J_{b1}\{f(x)\exp[\,j2\pi n(x)]\}\}\}. \tag{5}$$

We continue this procedure, applying in sequence the operators F_{a2}, J_{b3}, and F_{a3}. We could of course further continue this procedure of repeated FRT and jigsaw transform application to more deeply encrypt our image, but the time taken, complexity, and susceptibility to noise of the method would increase. Our encrypted image is now given by

$$g(x) = F_{a3}\{J_{b3}\{F_{a2}\{J_{b2}\{F_{a1}\{J_{b1}\{f(x)\exp[\,j2\pi n(x)]\}\}\}\}\}\}. \tag{6}$$

The intensity of the encrypted image is shown in Fig. 1(c) for the case when $a_{1x} = a_{1y} = a_{2x} = a_{2y} = a_{3x} = a_{3y} = 0.5$. By a_{1x} we mean the order in the x direction of the first FRT operation.

Decryption is then given by

$$f(x) = J_{-b1}\{F_{-a1}\{J_{-b2}\{F_{-a2}\{J_{-b3}\{F_{-a3}\{g(x)\}\}\}\}\}\}. \tag{7}$$

Decryption is simply the exact inverse of the encryption process. At the final stage we need capture only the intensity information, since this represents our original image. The phase of the decrypted signal should be equal to the random phase that we added to our image originally and 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 crack the jigsaw encryption. However, the inclusion of the random phase at the beginning serves to whiten the image. In Fig. 1(f) we show the result of encrypting the image without the random phase at the input and with the same orders. The encrypted image shows undesirable patterns, which are a result of the random shifting in the FRT domains. These patterns become more pronounced as we decrypt with fractional-order keys close to the correct values.

The decryption process described above requires knowledge of nine keys in total. These nine keys are made up of six FRT order keys (3 in x and 3 in y) and three jigsaw transform permutations. We examine the sensitivities of keys a_{1x}, a_{2x}, and a_{3x} in Fig. 2. The thin solid curve corresponds to varying the value of a_{1x} in the decryption process while all other keys are correct. Similarly, the thick solid curve corresponds to varying a_{3x}; the dashed curve, to varying a_{2x}. Analogous results occur for a_{1y}, a_{2y}, and a_{3y}. We use the mean-square error[11] between our original image and the incorrectly decrypted image as a measure of how encrypted the image remains. The sensitivities to the a_2 and a_3 fractional-order keys are qualitatively very similar to results for the analogous keys in previous methods[2,10–12] and

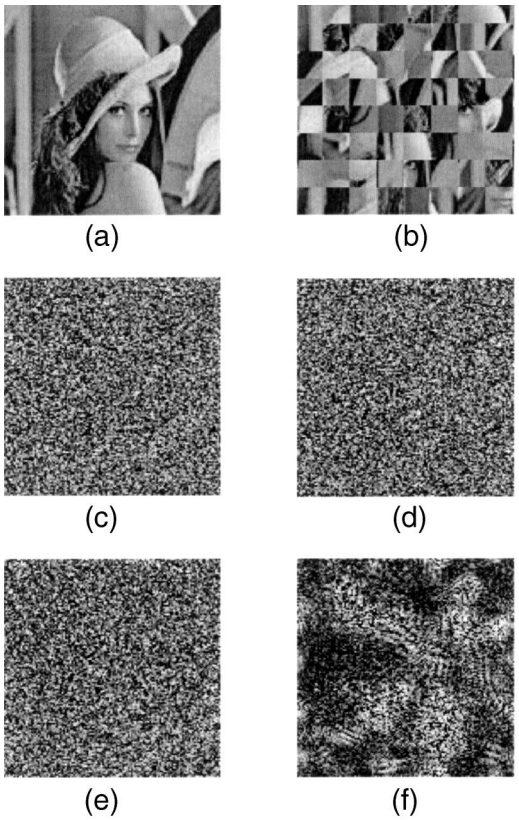

Fig. 1. Results of certain cases of encryption and decryption.

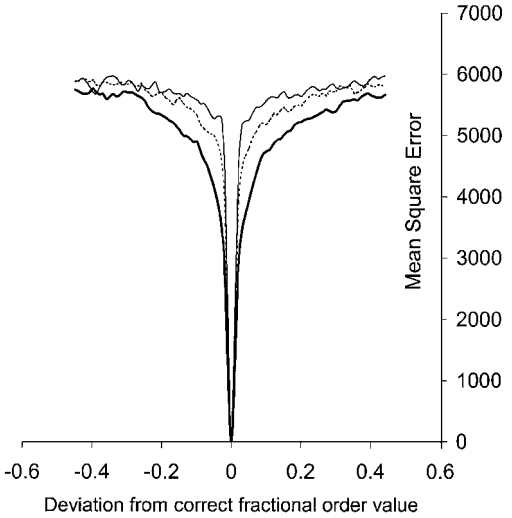

Fig. 2. Mean-square error plotted as a function of error in the decryption fractional-order key.

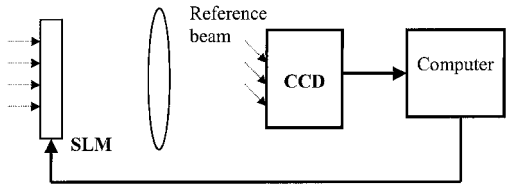

Fig. 3. Optical implementation of the encryption–decryption algorithm. SLM, spatial light modulator.

show an improvement in key sensitivity in other methods.[13,14] However, the sensitivity of the first fractional-order key appears better than the equivalent key in all analogous methods.[2,10–12] In Fig. 1(e) we show the decrypted image when a_{x3} deviates from its correct value 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. 1(d). Again, the image remains totally encrypted. Transmitting the permutation keys to the receiver is simple. A program can be written at the encryption–transmission end and at the decryption–receiving end, such that some number will generate the same permutation at both ends. All that needs to be conveyed to decrypt the image is nine numbers, six FRT orders and three permutation number keys.

A schematic for a possible optical implementation of this system is shown in Fig. 3. As described, the jigsaw transforms are applied digitally. Spatial light modulator modes are used to display the signal after each step in the encryption–decryption process, and a single-lens configuration is used to implement the FRT. A reference beam allows the complex data to be recorded after each FRT operation. We note that in the final stage of the decryption process the reference beam is not necessary.

We acknowledge the support of Enterprise Ireland through the Research Innovation Fund. J. T. Sheridan's e-mail address is john.sheridan@ucd.ie.

*Corresponding author, John.Sheridan@ucd.ie, http://www.ucd.ie/eleceng.

References

1. P. Réfrégier and B. Javidi, Opt. Lett. **20,** 767 (1995).
2. G. Unnikrishnan and K. Singh, Opt. Eng. **39,** 2853 (2000).
3. D. Mendolovic and H. M. Ozaktas, J. Opt. Soc. Am. A **10,** 1875 (1993).
4. H. M. Ozaktas and D. Mendolovic, J. Opt. Soc. Am. A **10,** 2522 (1993).
5. A. W. Lohmann, J. Opt. Soc. Am. **10,** 2181 (1993).
6. M. F. Erden, H. M. Ozaktas, A. Sahin, and D. Mendolovic, Opt. Commun. **136,** 52 (1996).
7. J. Garcia, D. Mas, and R. Dorsch, Appl. Opt. **35,** 7013 (1996).
8. H. M. Ozaktas, O. Arikan, M. A. Kutay, and G. Bozdagi, IEEE Trans. Signal Process. **44,** 2141 (1996).
9. F. J. Marinho and L. Bernardo, J. Opt. Soc. Am. A **15,** 2111 (1998).
10. S. Liu, L. Yu, and B. Zhu, Opt. Commun. **187,** 57 (2001).
11. Y. Zhang, C. H. Zheng, and N. Tannom, Opt. Commun. **202,** 277 (2002).
12. B. Zhu and S. Liu, Opt. Commun. **195,** 371 (2001).
13. B. Zhu and S. Liu, Opt. Lett. **26,** 1242 (2001).
14. B. Zhu, S. Liu, and Q. Ran, Opt. Lett. **25,** 1159 (2000).