Spread-space spread-spectrum technique for secure multiplexing

B. M. Hennelly, T. J. Naughton, and J. McDonald

Department of Computer Science, National University of Ireland, Maynooth, Ireland

J. T. Sheridan and G. Unnikrishnan

School of Electrical, Electronic and Mechanical Engineering, University College Dublin, Belfield, Dublin 4, Ireland

D. P. Kelly

Institut fur Photonik and Zentrum fur Mikro- und Nanostrukturen, Technische Universitt Wien, A-1040 Wien, Austria

B. Javidi

Electrical and Computer Engineering Department, University of Connecticut, 371 Fairfield Road, Unit 2157, Storrs, Connecticut 06269-2157, USA

Received November 1, 2006; revised January 11, 2007; accepted January 30, 2007; posted February 9, 2007 (Doc. ID 76691); published April 3, 2007

A novel technique for multiplexing complex images is proposed in which each image may be demultiplexed only if a set of random encryption keys is known. The technique utilizes the ability of the double random phase encoding method to spread a signals' energy in both the space and the spatial frequency domains in a controlled manner. To multiplex, images are independently encrypted with different phase keys and then superimposed by recording sequentially on the same material. Each image is extracted by using the particular key associated with it. During decryption the energy from the other images is further spread, making it possible to minimize its effects by using suitable filters. Wigner analysis is applied to the technique, and numerical results are presented. © 2007 Optical Society of America

OCIS codes: 070.6020, 090.4220, 070.2580.

A number of methods have been recently proposed in the literature for the encryption of 2D information using linear optical systems.[1–3] In particular, the double random phase encoding (DRPE) system[1] has received much attention. In this Letter we outline how such a system, with a slight adjustment, may be used for securely multiplexing and demultiplexing data for holographic data storage and threshold security. Holographic data storage[4,5] offers terabyte capacity with high transfer rates. Recently optical encryption systems have been applied during the multiplexing process[6–8] to improve the performance of these systems. The DRPE method has been applied with angular multiplexing,[6–9] and it has been observed that it offers an improved performance over traditional angular multiplexing in terms of storage capacity[8] and angular selectivity.[9] This improvement is attributed to the suppression of cross talk between adjacent images. While the original binary data is recovered with the correct random phase key, the overlapping reconstructed images from neighboring orders remain white-noise-like images because an incorrect random phase key has been used. In this Letter we both qualify and quantity these effects based on a discussion of energy spreading in phase space using the Wigner distribution function (WDF).

Various multiplexing schemes exist in holographic data storage including spatial, angular, spherical reference shift and speckle reference multiplexing. There are also various multiplexing schemes using phase keys in the reference beam.[10–14] All of these methods can be analyzed by using the WDF-based approach introduced here. Our results demonstrate that the DRPE may be used not only to improve upon existing angular multiplexing schemes but also as a multiplexing scheme in and of itself.

The standard DRPE method is well known. An input image wave field passes through a random diffuser (D1), an optical Fourier transform (OFT), a second diffuser (D2), and finally a second OFT. If the diffusers may be described as two statistically independent random phase functions, then the encrypted image may be described as a white process. Decryption involves passing the encrypted wave field back through the encryption system in which D2 is replaced by its conjugate $D2^*$ and D1 is simply removed. The effect of D2 is canceled, and $D1^*$ is not employed, since we are interested only in the intensity of the decrypted signal. Our multiplexing scheme comprises a DPRE and a recording material. A number of images are encoded and recorded sequentially on the same material by using the same reference beam but different diffusers. The effects of the diffusers on the spatial extent of an input signal and its spatial frequency extent as it evolves through these systems are well known.[15] The WDF allows us to elegantly explain these effects for the purposes of this paper. The WDF of a 1D signal $u(x)$ is given as

$$\psi\{u(x)\}(x,k_x) = \int u\left(x-\frac{\epsilon}{2}\right)u^*\left(x+\frac{\epsilon}{2}\right)e^{-i2\pi k_x \epsilon}\mathrm{d}\epsilon, \qquad (1)$$

where x denotes the spatial coordinate and k_x denotes spatial frequency. In the case of a 2D signal the

0146-9592/07/091060-3/$15.00

WDF is four dimensional. Much of our analysis is limited to the 1D case, the extension to 2D being trivial. The WDF has many properties, only a few of which are critical in the present context. The first property is that of localization; in many practical problems it we assume that a signal is bounded within some finite region in the spatial and spatial frequency domains. The spatial extent, W, and frequency extent, B, are the minimum values such that

$$u(x) \approx 0, \quad |x| > W, \qquad \int u(x) e^{-i2\pi k_x x} \mathrm{d}x \approx 0, \quad |k_x| > B. \tag{2}$$

The second property relates to Parseval's theorem; the total energy of the signal, E, is

$$E = \int \psi\{u(x)\}(x,k_x)\mathrm{d}x\mathrm{d}k_x. \tag{3}$$

Applying Eqs. (2) and (3), the average energy density of the signal in phase space is given by E/WB. The third property of interest is the product theorem of the WDF. When two signals are multiplied in space, their WDFs are convolved along the k_x axis:

$$\psi\{u(x)v(x)\}(x,k_x) = \int \psi\{u(x)\}(x,k_x - k')\psi\{v(x)\}(x,k_x)\mathrm{d}k'. \tag{4}$$

From Eqs. (2) and (4), the signal $u(x)h(x)$ will have a spatial width equal to the overlapping spatial distributions of the individual signals. Furthermore, the resulting spatial frequency distribution will have a bandwidth equal to the sum of the bandwidths of the product signals, $B_u + B_h$. The final property of interest is the relationship of the WDF to the Fourier transform (FT). If a FT is applied to a signal, the corresponding WDF rotates by $\pi/2$ rad: $\psi\{u(x)\}(x,k_x) \rightarrow \psi\{u(x)\}(-k_x,x)$. In the case of an OFT with focal length f and wavelength λ, we have the following relationship: $\psi\{u(x)\}(x,k_x) \rightarrow \psi\{u(x)\}(-\sqrt{\lambda f}k_x, x/\sqrt{\lambda f})$. If Eq. (2) holds, then the output OFT bandwidth is $B\sqrt{\lambda f}$; i.e., the OFT does not simply rotate the WDF but also stretches it.

Turning to the DRPE system, and with the aid of Fig. 1 and Table 1, we describe the evolution of a signal's spatial and spatial frequency distributions as it propagates through the system. The input signal has the Wigner volume chart shown in Fig. 1(i), where the signal is depicted having a width and bandwidth as defined in Table 1. The average energy density can be calculated at any plane as $E/(\text{Width } x)\ (\text{Width } k_x)$. If our image signal has been coded for efficient storage, then it will seem random in nature, and we may assume that it fully occupies the volume shown in Fig. 1(i). D1 and D2 are assumed to be lossless and are designed to have the well-specified widths and bandwidths[15] listed in Table 1. When the signal passes through D1, the product signal has an increased bandwidth, but the total energy must remain the same. Therefore the average energy density is reduced by a factor proportional to the spread. The resulting Wigner volume chart is shown in Fig. 1(ii), and the relevant values are given in Table 1. The first FT rotates the chart by $\pi/2$ rad, see Fig. 1(iii), and the resultant signal passes through D2. The spatial frequency domain is again stretched (we note that this is actually the spatial domain of the input signal), and, since the total energy again remains the same, the average energy density in phase space is further reduced; see Fig. 1(iv). The final FT rotates the chart once again as shown in Fig. 1(v). This 1D signal, with known extents in x and k_x, is now captured. We see that it is important to match W_{IN_x} and W_{D1_x} and also $\sqrt{\lambda f}(B_{\mathrm{IN}_x} + B_{\mathrm{D1}_x})$ and W_{D1_x}. Correct decryption of the signal follows a very similar pattern, in the exact reverse. Figures 1(ii)–1(v) in reverse order describe the evolution of a correctly decrypted signal. $\mathrm{D2}^*$ now acts to despread the signal in the space domain, while $\mathrm{D1}^*$ is not needed, since despreading in the frequency domain does not affect the intensity of a decrypted signal.

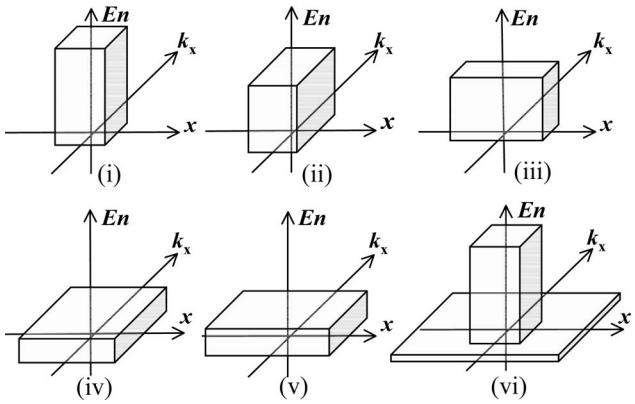

Fig. 1. Wigner volumes at different planes in the multiplexing and demultiplexing process. E_n, energy density.

Table 1. Quantifying the Spreading

Stage	Width x	Width k_x
D1	$W_{\mathrm{D1}x}$	$B_{\mathrm{D1}x}$
D2	$W_{\mathrm{D2}x}$	$B_{\mathrm{D2}x}$
Input	$W_{\mathrm{IN}x}$	$B_{\mathrm{IN}x}$
After D1	$W_{\mathrm{IN}x}$	$B_{\mathrm{IN}x} + B_{\mathrm{D1}_x}$
After 1st FT	$\sqrt{\lambda f}(B_{\mathrm{IN}x} + B_{\mathrm{D1}x})$	$W_{\mathrm{IN}x} / \sqrt{\lambda f}$
After D2	$\sqrt{\lambda f}(B_{\mathrm{IN}x} + B_{\mathrm{D1}x})$	$W_{\mathrm{IN}x} / \sqrt{\lambda f} + B_{\mathrm{D2}x}$
After 2nd FT	$W_{INk} + \sqrt{\lambda f} B_{\mathrm{D2}x}$	$B_{\mathrm{IN}x} + B_{\mathrm{D1}x}$
Incorrectly decrypted	$W_{INk} + 2\sqrt{\lambda f} B_{\mathrm{D2}x}$	$B_{\mathrm{IN}x} + 2B_{\mathrm{D1}x}$

Multiplexing is implemented by using a standard DRPE encryption system with different keys for each input image. Our demultiplexing system is shown in Fig. 2, made up of a standard DRPE decryption system except that we also use $\mathrm{D1}^*$ to despread in k_x. We also apply apertures in the decryption plane and its Fourier plane to remove all the energy of incorrectly decrypted signals except that part that lies inside the low-pass regions in the four dimensions. Figures 1(i)–1(v) in reverse describe the total evolution of demultiplexing. When decryption is performed by using an incorrect set of diffusers, the signal will not be de-

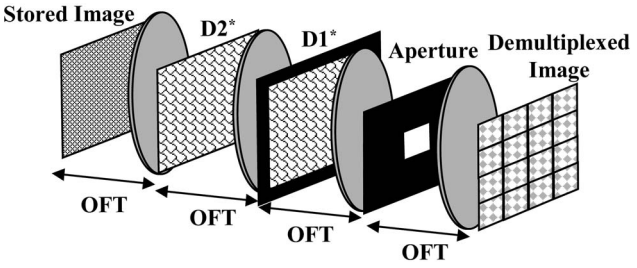

Fig. 2. Decryption–demultiplexing scheme.

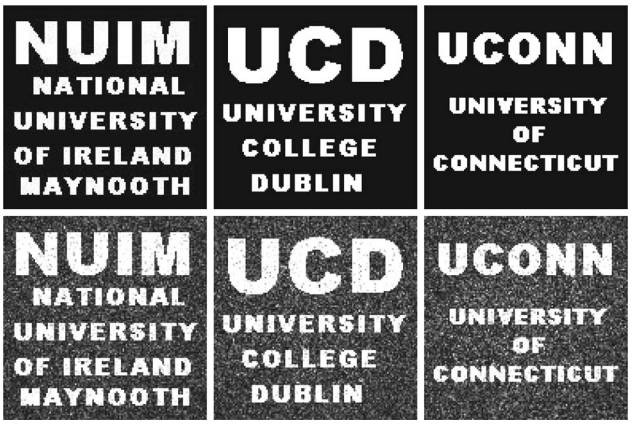

Fig. 3. Images before and after we multiplex and demultiplex.

spread in x and k_x but rather will be even further spread in these domains, and the average energy density will be further reduced. In Fig. 1(iv) we show Wigner volume charts of a correctly and incorrectly decrypted signal. The extents of an incorrectly decrypted signal are given in Table 1.

A 2D encrypted signal will also have extents in y and k_y that may be determined by replacing the subscript x with y in Table 1. For 2D signals, the average energy density at any plane is given by

$$E/(\text{Width } x)(\text{Width } y)(\text{Width } k_x)(\text{Width } k_y). \quad (5)$$

We consider the case where we encrypt multiple images, each with different diffusers, and add the encrypted images together. To demultiplex we decrypt using the correct phase keys. The incorrectly decrypted signals will have been spread out in x, y, k_x, and k_y, and their average energy densities will be given by Eq. (5) and Table 1. The number of images that can be multiplexed together and recovered with and without loss is proportional to the phase space signal spreading. The total energy of each incorrectly decrypted signal present in the final output image Wigner volume is determined by multiplying the average energy density, ρ, by the volume of interest, giving $\rho(B_{\mathrm{IN}_x}W_{\mathrm{IN}_x}B_{\mathrm{IN}_y}W_{\mathrm{IN}_y})$. Thus the average energy present due to incorrect decryption is given by $\rho(B_{\mathrm{IN}_x}B_{\mathrm{IN}_y})$. From this latter value the average error energy per bit can be determined.

Furthermore, each individual encryption is more robust than the traditional DPRE, since decryption requires knowledge of both the phase keys and filters used to despread and decrypt. If N signals are multiplexed together, to decode one we can expect an average error per bit of $\mathrm{AVE}_{\mathrm{IN}}(N-1)\rho(B_{\mathrm{IN}_x}B_{\mathrm{IN}_y})$ where $\mathrm{AVE}_{\mathrm{IN}}$ represents the average energy of an input signal. Taking the latter value and the dynamic range of the input signals into account, one may determine the sufficient parameters for the diffusers (B_{D1} and B_{D1}) such that each image may be recovered with minimal error. We also note that a further limit is imposed on the number of images by the dynamic range of the recording medium. We believe that this limit may also be represented efficiently by using Wigner analysis, but that is beyond the scope of this Letter. In Fig. 3 we show the results of a simulation to multiplex and demultiplex three 128×128 binary images. This case is clearly not optimal, since the input images have not been coded to evenly distribute the energy in the frequency domain. We chose $B_{\mathrm{IN}_x}=B_{\mathrm{D1}_x}$, $W_{\mathrm{IN}_x}=\sqrt{\lambda f}B_{\mathrm{D2}_x}$, $B_{\mathrm{IN}_y}=B_{\mathrm{D1}_y}$, $W_{\mathrm{IN}_y}=\sqrt{\lambda f}B_{\mathrm{D2}_y}$ so that the encrypted image had twice the width and bandwidth of the input, and therefore an incorrectly decrypted image had three times the width and bandwidth of the input. Thresholding was not applied to the results shown in Fig. 3. After thresholding the bit error rate for this case is $<1\%$. The performance of the technique is currently being investigated for large numbers of inputs and different spreads. We acknowledge that a practical implementation will differ from the ideal simulation, and we are also pursuing experimental validation. Similar analyses may be applied to optimize the performance of architectures outlined in Refs. 6–14.

We acknowledge the support of the Irish Research Council for Science Engineering and Technology. B. Hennelly's e-mail address is bryanh@cs.nuim.ie.

References

1. P. Refregier and B. Javidi, Opt. Lett. **20**, 767 (1995).
2. B. Hennelly and J. T. Sheridan, Opt. Lett. **28**, 269 (2003).
3. B. M. Hennelly and J. T. Sheridan, Optik (Stuttgart) **114**, 251 (2003).
4. H. J. Caulfield, D. Psaltis, and G. Sincerbox, *Holographic Data Storage* (Springer-Verlag, 2000).
5. L. Hesselink, S. S. Orlov, and M. C. Bashaw, Proc. IEEE **92**, 1231 (2004).
6. B. Javidi, G. Zhang, and J. Li, Appl. Opt. **36**, 1054 (1997).
7. O. Matoba and B. Javidi, Appl. Opt. **38**, 7288 (1999).
8. X. Tan, O. Matoba, T. Shimura, and K. Kuroda, Appl. Opt. **40**, 4721 (2001).
9. W. C. Su and C. H. Lin, Appl. Opt. **43**, 2298 (2004).
10. T. F. Krile, R. J. Marks II, J. F. Walkup, and M. O. Hagler, Appl. Opt. **16**, 3131 (1977).
11. E. L. Kral, J. F. Walkup, and M. O. Hagler, Appl. Opt. **21**, 1281 (1982).
12. J. F. Heanue, M. C. Bashaw, and L. Hesselink, Appl. Opt. **34**, 6021 (1995).
13. O. Matoba, Y. Yokohama, M. Miura, K. Nitta, and T. Yoshimura, Appl. Opt. **45**, 3270 (2006).
14. G. Situ and J. J. Zhang, J. Opt. A, Pure Appl. Opt. **8**, 391 (2006).
15. T. Nomura, E. Nitanai, T. Numata, and B. Javidi, Opt. Eng. **45**, 1 (2006).