

Hybrid encryption and decryption technique using microfabricated diffractive optical elements

X.-C. Yuan, MEMBER SPIE

S. H. Tao

W. C. Cheong

Y. W. Chen

M. S. Lim

K. J. Moh

A. T. S. Ho

Nanyang Technological University
School of Electrical & Electronic
Engineering

Photonics Research Centre

Nanyang Avenue, Singapore 639798

E-mail: excyuan@ntu.edu.sg

Abstract. A hybrid encryption and decryption technique for optical information security is proposed. In this method, the iterative Fourier transform algorithm is employed to optimize the encrypted hologram and the decryption key as binary phase-only diffractive optical elements, which were fabricated by electron-beam lithography. In a simple optical setup, the optical decryption is implemented by superimposing the encrypted hologram and the decryption key. Numerical simulation and optical experiment confirm the proposed technique as a simple and easy implementation for optical decryption. © 2004 Society of Photo-Optical Instrumentation Engineers. [DOI: 10.1117/1.1802272]

Subject terms: image reconstruction; joint transforms; holograms; Fourier transforms.

Paper 04040 received Apr. 20, 2004; revised manuscript received Jul. 16, 2004; accepted for publication Jul. 16, 2004; appeared online Jul. 16, 2004.

The drive to protect intellectual property and confidential information has given rise to various encryption/decryption techniques; among them, optical security techniques such as the joint transform correlator (JTC), the 4- f system, double-random phase encoding, XOR, and others¹⁻⁸ have gained great interest because of their high level of security. Practical implementation of the optical security techniques is a challenge, as all of them require stringent alignment between an encrypted element and the corresponding decoding key. For the JTC system, the input and the reference signals are located at the same plane but shifted laterally. When the distance between the input and the reference signals is changed laterally, the only effect is to shift the correlation peaks at the output plane. The 4- f system has very high security level, but it requires a rigid alignment between the input and the reference in different planes simultaneously. In this letter, we propose a hybrid technique, with a combination of the advantages of the JTC system and the 4- f system, to completely eliminate the need for optical alignment in the spatial domain. The decryption process is implemented by superimposing the encrypted element and the decryption key in the Fourier

plane. The light that passes through the two superimposed elements, i.e., the encrypted hologram and the decryption key, are then employed to reconstruct the original image in a Fourier transform. Note that the proposed method could help reduce the stringent alignment requirement in spatial domain when the key is used in the 4- f system. Furthermore, since the encryption is implemented numerically and the requirement of optical alignment and beam propagation in free space is reduced for the decryption, this technique and the microfabricated optical elements could be employed in a miniaturized optical system for information security.

Assume that $f(x,y)$ and $g(x,y)$ denote the original image to be encrypted and the reference image, respectively. In the rear focal plane of the lens, the Fourier transform of this field is obtained, and then the encryption is performed. The intensity pattern at the recording plane can be mathematically described as

$$\begin{aligned} H(u,v) &= |\text{FT}[f(x-x_0,y)] + \text{FT}[g(x+x_0,y)]|^2 \\ &= |F(u,v)|^2 + |G(u,v)|^2 \\ &\quad + F^*(u,v)G(u,v)\exp(i4\pi ux_0) \\ &\quad + F(u,v)G^*(u,v)\exp(-i4\pi ux_0), \end{aligned} \quad (1)$$

where x_0 is the shift distance of the image center along the x axis, $*$ represents the conjugate, FT represents a Fourier transform, $H(u,v)$ stands for the encrypted hologram, and the third and fourth terms are the main terms of interest. Note that $F(u,v)$ and $G(u,v)$ are determined by Fourier transforms of $f(x,y)$ and $g(x,y)$, respectively. Here $G(u,v)$ is used as a key in the decryption process. In our case, the Gerchberg-Saxton algorithm⁹ is employed to design $F(u,v)$ and $G(u,v)$ as phase-only binary elements. For simplicity, we ignore the constant phase shifts in Eq. (1). Thus, $H(u,v)$ can be simplified as

$$H(u,v) = F^*(u,v)G(u,v) + F(u,v)G^*(u,v). \quad (2)$$

Note that if the phases of $G(u,v)$ and $F(u,v)$ are binary quantized, $H(u,v)$ will be a binary real distribution. Encryption of the key and the original image can be performed with aid of a computer running iterative algorithms to obtain the binary holograms.

The two holograms are superimposed directly pixel by

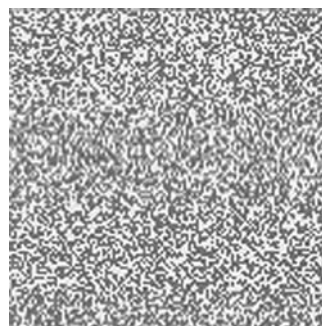


Fig. 1 Encrypted hologram $H(u,v)$.



Fig. 2 Decrypted image in the simulation.

pixel for a decryption. When the superimposed holograms are Fourier transformed by a lens, the procedure can be written as

$$d(x,y) = \text{FT}[H(u,v)G(u,v)] = f^*(x,y) + f(-x,-y). \quad (3)$$

The second item is the fully recovered original image, and the first item is related to the conjugate of the original image.

The preceding system is verified by use of a simulation with 128×128 sampling points. The original image $f(x,y)$ to be encrypted is set as an amplitude-only image of a character E. The decryption key $G(u,v)$ is a randomly selected phase-only binary phase distribution, which is inversely Fourier transformed to determine $g(x,y)$ in the JTC. Next $f(x,y)$ and $g(x,y)$ are employed digitally to generate an encrypted hologram, and $G(u,v)$ is used to verify the encrypted information optically. The encoded hologram and the decoded image are shown in Figs. 1 and 2, respectively. We can see from Fig. 2 that the encrypted image can be clearly recovered with a decryption key.

For the experiment, the optical setup is shown schematically in Fig. 3. A He-Ne laser is used as a coherent light source. The decryption key hologram is closely superimposed with the encrypted hologram. A CCD beam profiler is employed to capture the decrypted image.

Each hologram is placed on a precision adjustment stage so that fine-tuning of the alignment between the two holograms is enabled. The decryption key and the encrypted hologram are of the same size; therefore, the alignment problem is reduced, as it is easier to align two holograms of the same size as compared to a $4-f$ system, where the sizes of the encrypted hologram and the decryption key are dif-

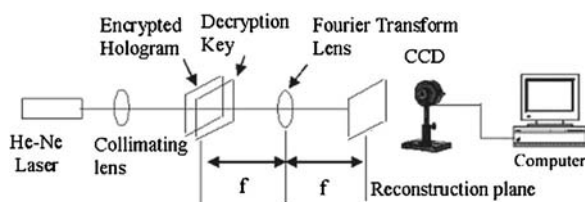


Fig. 3 Schematic setup of the optical decryption.



Fig. 4 Decrypted image in the experiment.

ferent. For the fabrication, the same number of sampling points of 128×128 is selected. The size of each pixel is $8 \times 8 \mu\text{m}$ for both holograms. The hologram patterns are transferred onto pieces of quartz with a coating of MMA (methyl methacrylate) by electron-beam lithography.

The decoded image is shown in Fig. 4. We can see that the original image is clearly recovered with an optical decryption key. In the figure, the bright on-axis spot corresponds to the zeroth-order diffraction component.

In summary, we proposed a hybrid encryption and decryption system that incorporates a JTC system for the encryption and only requires a $2-f$ system rather than a $4-f$ setup for the decryption. The decoding key hologram has the same size as the encrypted hologram, which makes the decryption (superimposing of the two holograms) easier. Computer simulations and experiments demonstrated the effectiveness of this technique. Furthermore, with the advent of the low-cost materials such as sol-gel glass and other polymers as well as the low-cost and high-volume replication lithographic techniques (for example, soft-lithography), the diffractive optical elements can be fabricated in an inexpensive way. Consequently, with the compact nature of the proposed technique, it facilitates the application of microfabricated optical elements as a low-cost solution to implement optical encryption and decryption for potential applications such as information verification and anticounterfeit in a miniaturized optical system.

References

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.* **20**, 767–769 (1995).
2. P. C. Mogensen and J. Glückstad, "Phase-only optical encryption," *Opt. Lett.* **25**, 566–568 (2000).
3. S. Kishk and B. Javidi, "Information hiding technique with double phase encoding," *Appl. Opt.* **41**, 5462–5470 (2002).
4. R. K. Wang, I. A. Watson, and C. Chatwin, "Random phase encoding for optical security," *Opt. Eng.* **35**, 2464–2460 (1996).
5. B. Javidi, L. Bernard, and N. Towghi, "Noise performance of double-phase encryption compared to XOR encryption," *Opt. Eng.* **38**, 9–19 (1999).
6. T. Nomura, S. Mikan, Y. Morimoto, and B. Javidi, "Secure optical data storage with random phase key codes by use of a configuration of a joint transform correlator," *Appl. Opt.* **42**, 1508–1514 (2003).
7. B. Wang, C. Sun, W. Su, and A. E. T. Chiou, "Shift-tolerance property of an optical double-random phase-encoding encryption system," *Appl. Opt.* **39**, 4788–4793 (2000).
8. S.-J. Park, J.-Y. Kim, J.-K. Bae, and S.-J. Kim, "Fourier-plane encryption technique based on removing the effect of phase terms in a joint transform correlator," *Opt. Rev.* **8**, 413–415 (2001).
9. R. W. Gerchberg and W. O. Saxton, "A practical algorithm for the determination of phase from image and diffraction plane pictures," *Optik (Stuttgart)* **35**, 237–246 (1972).