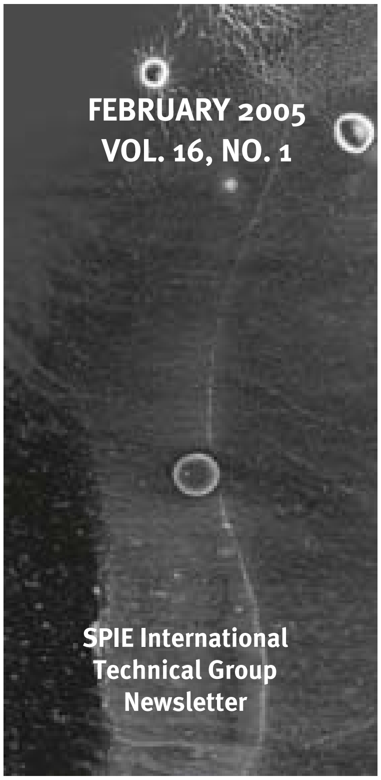
The International Society for Optical Engineering



FEBRUARY 2005
VOL. 16, NO. 1

SPIE International
Technical Group
Newsletter

Special Issue on:

Optical Encryption

Editors
Tom Naughton
National Univ. of Ireland
John Sheridan, Univ. College Dublin

Newsletter now available online

Technical Group members are being offered the option of receiving the Optics in Information Systems Newsletter electronically. An e-mail is being sent to all group members with the web location for this issue, and asking members to choose between the electronic and printed version for future issues. If you are a member and have not yet received this message, then SPIE does not have your correct e-mail address.

To receive future issues electronically, please send your e-mail address to:
spie-membership@spie.org
with the word **OIS** in the subject line of the message and the words **electronic version** in the body of the message.

If you prefer to receive the newsletter in the printed format, but want to send your correct e-mail address for our database, include the words **print version preferred** in the body of your message.

Optics in Information Systems

Micro-optics for phase-only cryptography

While most common implementations of cryptographic techniques are performed via electronic or computer-based algorithms, using parallel optical processing provides ciphered information with extremely-fast decryption speeds. To date, most of the proposed optical cryptographic methods have used classical macro-optical systems. Miniaturizing the optical components allows us to move towards systems that are more realistic for genuine application and potentially enables us to directly interface to microelectronic devices.

We have demonstrated the miniaturization of the generalized phase-contrast (GPC) method[1-3] in a planar-integrated micro-optics (PO) platform.[4-6] Implementing optical processes in this way allows coupled light to undergo free-space propagation between integrated micro-optical components. The GPC-PO device is therefore particularly robust and not prone to position tolerances and alignment problems: major issues when using discrete and macro-optical components.

In the miniaturized setup, the GPC-based visualization of the decrypted pattern is achieved in a folded optical path configuration using the device shown in Figure 1. The micro-lenses of the 4-f lens setup and the phase contrast filter (PCF) at the Fourier plane are integrated into a single optical flat. First, multiple-phase-level diffractive micro-optical elements are fabricated on the top side of a glass substrate using multi-mask lithography. The micro-lenses are then reflection-coated and fabricated using two binary lithographic steps that make up a four-phase-level diffractive optical element. The first micro-lens focuses the beam onto the Fourier plane where the reflection-coated circular PCF is positioned to introduce a π phase shift to the on-axis region of the focused light. The PCF is fabricated as a 7μm-diameter pit on the substrate. The reverse optical Fourier transform is performed in the succeeding half of the symmetric system.

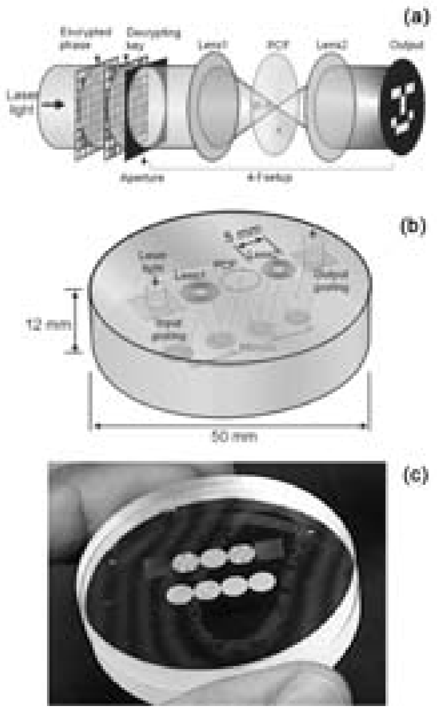


Figure 1. (a) Phase-only optical decryption using the generalized phase contrast (GPC) method. (b) Diagram and (c) photograph of the planar-integrated optical implementation.

We have carried out 'proof-of-principle' experiments with the GPC-PO device shown in Figure 1(c). The decryption-key information is encoded using a phase-only spatial light modulator (SLM), illuminated from an expanded laser beam. The encrypted phase mask is fabricated on an optical flat where the phase-shift-

Continues on page 10.

Editorial

Optical Encryption

Encryption involves turning data into a form that is unreadable by all except those with the appropriate, secret, decryption key. Sometimes, this key can be derived from that used to encrypt the data: as is the case with most optical encryption systems. A drawback of such systems when used for communication is that, at some point, this secret key must be transmitted and thus risks interception. (Usually, one key cannot be derived from the other: one makes the encryption key publicly available and never transmits the secret decryption key to others.)

However, there is a place for *symmetric* encryption systems, as they are called, and optical implementations of the same. Optical implementations have some very promising scalability advantages over their purely electronic counterparts as, in principle, the size of the key can be increased without increasing the encryption or decryption time. Furthermore, optics is perfectly suited to scenarios where one might like to dynamically trade off data integrity in the encryption/decryption process against efficiency. We welcome you to this special issue, which brings together some of the latest advances in symmetric optical encryption.

Encryption also provides an ideal application to showcase the power and flexibility of optics and the field of optical information processing. Throughout this special issue, optical encryption applications illustrate the inherent speed and parallelism of optics, complex-signal representation, three-dimensional object sensing, reduced power consumption, symbiosis with existing digital electronic technologies, as well as the mathematical operations of optical-Fourier and fractional-Fourier transformation, image multiplication and convolution, and optical logic. The systems presented here employ a range of state-of-the-art optoelectronic technologies including lasers, photorefractive materials, liquid-crystal spatial light modulators, digital cameras, and micro-optics.

Since there were more responses to the call for participation than a single issue could accommodate, we have had to hold back some contributions until the next issue. We greatly appreciate the opportunity afforded our community by this special topical issue and acknowledge the support of the Optics in Information Systems Technical Group chairs Bahram Javidi and Demetri Psaltis. We wish to thank all the contributors for their interesting articles. Sincere thanks are also due to Sunny Bains and Stuart Barr for making our job completely straightforward and enjoyable. This special issue will be a success if it promotes collaboration between contributors and readers, so please feel free to contact any authors with whom you feel you share an interest.

Thomas J. Naughton
National University of Ireland
Maynooth, Ireland
E-mail: tom.naughton@nuim.ie

John T. Sheridan
University College Dublin, Ireland
E-mail: john.sheridan@ucd.ie

CALENDAR

2005

SPIE Defense and Security Symposium
28 March - 1 April
Orlando, Florida USA
Program • Advance Registration Ends 15 March 2005
Exhibition
spie.org/conferences/programs/05/dss

SPIE Europe International Symposium Opto Ireland
4 - 6 April
Dublin, Ireland
Program • Advance Registration Ends 18 March 2005
Exhibition
spie.org/conferences/programs/05/ire

ICONO 2005: International Conference on Coherent and Nonlinear Optics
colocated with
LAT 2005: International Conference on Lasers, Applications, and Technologies
11 - 15 May
St. Petersburg, Russia
Sponsored by SPIE Russia Chapter. SPIE will publish proceedings. Program
congress.phys.msu.ru/ICONO-lat-2005

Holography 2005
International Conference on Holography, Optical Recording, and Processing of Information
21 - 25 May
Varna, Bulgaria
Sponsored by SPIE Bulgaria Chapter. SPIE will publish the proceedings. Program
optics.bas.bg/holo05.html

XVIth Conference on Photonics and Web Engineering
31 May - 5 June
Wilga Resort, Poland
Organized by SPIE Poland Chapter, SPIE Student Branch-WUT and IEEE Poland section.SPIE will publish proceedings. Program
nms.ise.pw.edu.pl/wilga/2005/pol/

Lasers for Measurement and Information Transfer 2005
8 - 10 June
St. Petersburg, Russia
Sponsored by SPIE Russia Chapter. SPIE will publish proceedings.

10th OptoElectronics and Communications Conference (OECC 2005)
5 - 8 July
Seoul, South Korea
SPIE is a technical cosponsor. Program
oecc2005.org/

Visual Communications and Image Processing (VCIP 2005)
12 - 15 July 2005
Beijing, China
SPIE is a cooperating organization. Program
research.microsoft.com/asia/VCIP2005/

Optics & Photonics 2005
co-located with the
SPIE 50th Annual Meeting
31 July - 4 August
San Diego, California USA
Call for Papers • Abstracts Due 17 January 2005
Exhibition
spie.org/conferences/calls/05/am/

International Congress on Optics and Optoelectronics
28 August - 2 September 2005
Warsaw, Poland
Sponsored by SPIE Europe and SPIE Polish Chapter
Call for Papers • Abstracts Due 14 February 2005
eurocongress.home.pl/Spie2005/

Tell us about your news, ideas, and events!

If you're interested in sending in an article for the newsletter, have ideas for future issues, or would like to publicize an event that is coming up, we'd like to hear from you. Contact our technical editor, Sunny Bains (sunny@spie.org) to let her know what you have in mind and she'll work with you to get something ready for publication.

Deadline for the next edition, 16.2, are:

25 February 2005: Suggestions for special issues and guest editors.

11 March 2005: Ideas for articles you'd like to write (or read).

13 May 2005: Calendar items for the twelve months starting August 2005.

Encryption of volume holograms using complementary input images and a binary key

The security of two-dimensional (2D) data has attracted much attention because it has become increasingly easy to counterfeit identity cards, credit cards, currency notes, and so on. Currently, 2D data such as fingerprints and faces are protected by using holograms bonded to them for security applications. However, these holograms can be read by intensity-sensitive detectors and then simply copied. To solve this problem, many authors have reported on the use of optical encryption to improve the security of 2D data and of their holograms.[1-4]

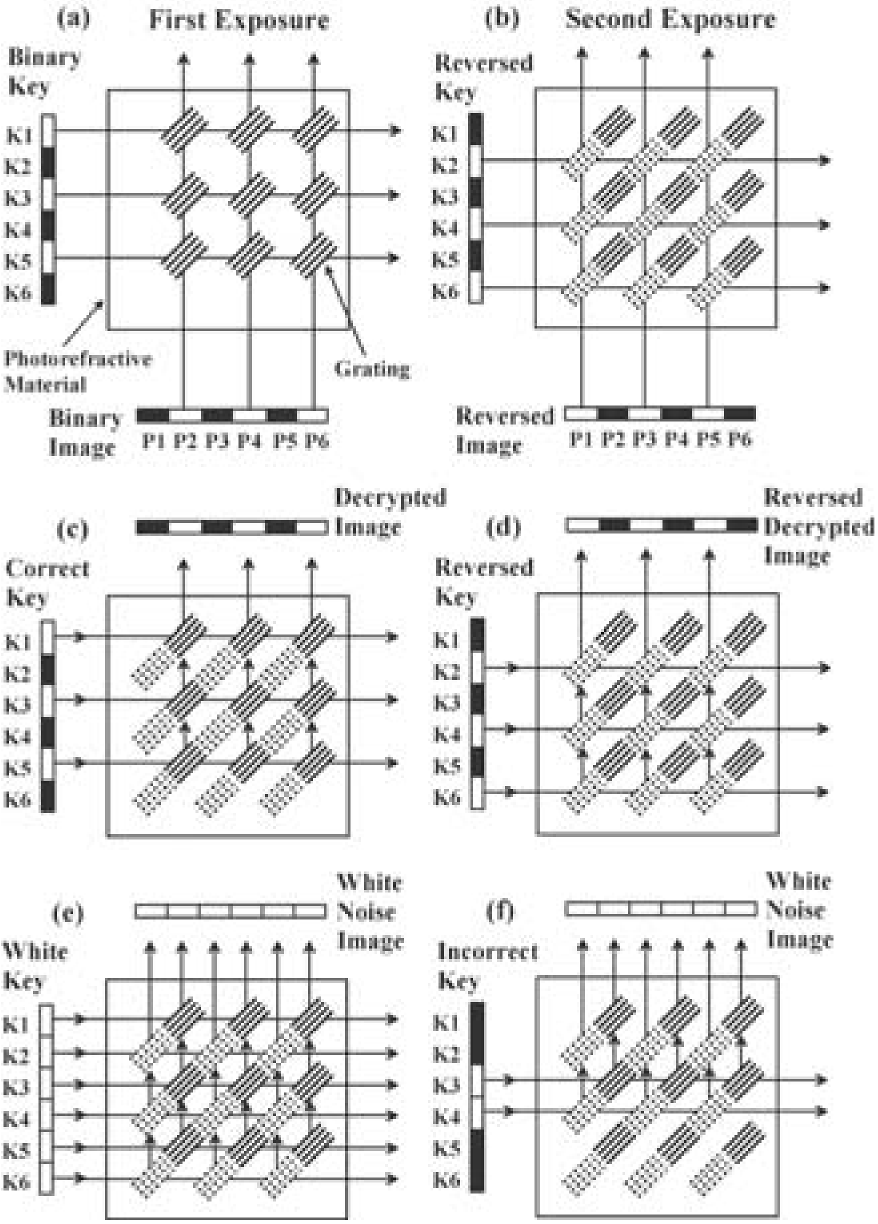


Figure 1. Schematic diagram of our encryption system. Holographic recordings of (a) the original image (solid lines) and (b) the reversed image (dotted lines). Hologram reconstructions are shown in parts (c)-(f).

Our new volume-hologram encryption system uses a complementary data page and binary key (or random amplitude mask), shown schematically in Figure 1.[5] In the proposed system, a binary image is first recorded as a volume hologram through interference with a binary key. Then the complementary (or reversed) image is recorded in the same volume as another volume hologram, interfering this time with the complementary key, (see parts (a) and (b) of Figure 1). The diagonal lines represent the gratings.

Parts (c) and (d) show that the original (or reversed) images can be recovered only when the hologram is read by the correct (or reverse) key. This is because beams from the correct key only diffract from the first hologram and those from the reversed key only diffract from the second hologram. Parts (e) and (f) show that only a white-noise-like image appears in the output when the hologram is read by white key or incorrect keys because, statistically, only half of the pixels will belong to the correct pattern and half to the reverse.

Figure 2(a) shows the experimental setup. The signal beam passes through the first spatial light modulator (SLM1) and is then focused into a BaTiO$_3$ crystal via lens L1 of focal length 260mm. Similarly, the reference beam passes through SLM2 and is then slightly focused into the crystal via lens L2 (same focal length) for better overlap with the signal. The SLMs are identical and have usable pixels of 400×600 at a pitch of 18mm×18mm. SLM2 pixels are grouped into 40×60 cells to display checkerboard-like patterns, as shown in Figure 2(a). The image displayed by the SLMs had an intensity contrast of 125, and the intensities of the reference and signal were measured at 20.4mW/cm^2 and 1.7 mW/cm^2, respectively. Exposure times for the first and second holograms were 4.5s and 2.5s, respectively, for equal-strength Bragg diffraction.

Figure 2(b) shows the experimental results for our encryption system. In this experiment, a United States Air Force (USAF) resolution chart was first recorded in the crystal using the binary key shown in Figure 2(a). Next, the reversed chart was recorded over the first hologram using binary key's complement. It is clear from Figure 2(b) that the stored holograms can only be read by either the correct key or the reverse keys.

Our system was also tested experimentally in more stringent conditions such as reading holograms with the correct key displaced by one cell horizontally or vertically and proved to be robust to this kind of decryption. Our system operation is simpler than many others because it uses binary-amplitude rather than phase SLMs. Also, not only the pattern of the binary key but also the exact size of a single cell can be used as encryption keys. Further, preliminary experi-

Continues on page 9.

Optical information security using Fourier- and fractional-Fourier-domain techniques

Optical techniques for encrypting data have generated considerable interest in the last decade.[1-10] For instance, the work of Refregier and Javidi,[1] which initiated the research work in this area, uses two random phase masks (RPM)—one in the input plane and the other in the Fourier plane—to convert the input image to a white stationary noise. This is optical encryption. Applications of these techniques include both volume holographic memory[2-6] and secure data transmission.[7-9]

Secure holographic memory

We have developed an encryption technique[2-6] that uses optical phase conjugation in a photorefractive crystal. Using two RPMs—one in the input and one in the frequency plane—the data to be encrypted is converted into a white stationary noise. The encrypted image is holographically recorded in a photorefractive crystal (see Figure 1), and we record multiple data in the same crystal using angular multiplexing. The result is a secure holographic memory. To decrypt the image, it's conjugate is generated using phase conjugation. This also corrects for phase distortions, such as aberrations from optical components. The key used for encryption can also be used for decryption, the key's conjugate is not needed. However, in this geometry, the RPM used in the frequency plane serves as the only key for decryption. Substituting the amplitude image in the input plane with the phase image requires both the RPMs for successful decryption: this further enhances security.

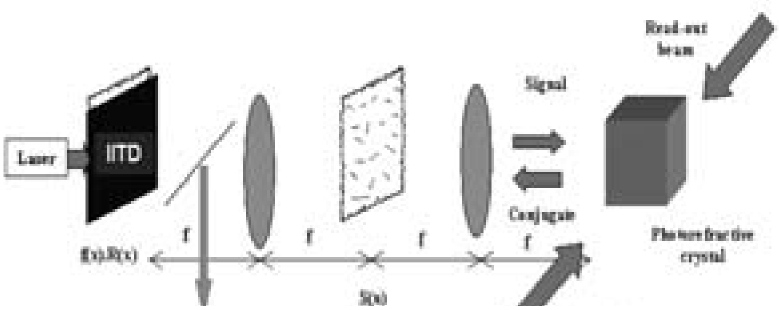


Figure 1. Schematic for encryption and decryption using optical phase conjugation in a photorefractive crystal.

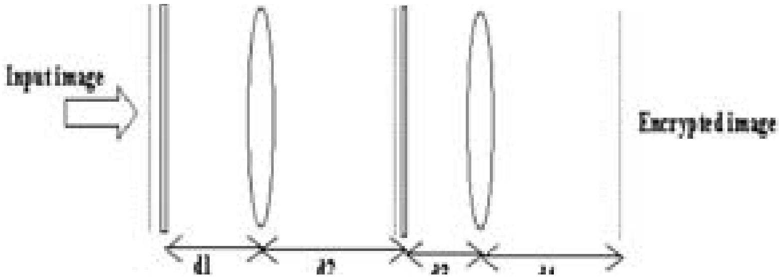


Figure 2. Schematic for encryption using a fractional Fourier transform.

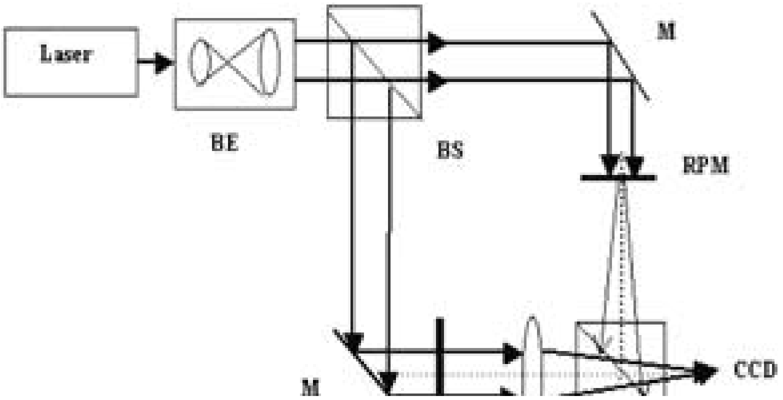


Figure 3. Experimental set-up for secure information transmission using digital holography.

If the original image is phase-encoded and encrypted, then it is impossible to acquire the information content of the encrypted phase image, even after decryption is done with the correct keys.[5,6,9] To convert the decrypted phase image into an amplitude image, a phase spatial light modulator (SLM) was used.[5,6] Use of a phase SLM means that no phase contrast filter (PCF) is necessary: the modulator can be used both to display the input image and to perform the function of the PCF. SLMs can also be used to display the RPMs also, and an all-SLM-based encryption system could potentially be used for practical applications.

The security of an encryption system depends on the size of the key used. An enlarged key space provides enhanced security. Techniques based on the fractional Fourier transform (FRT)[6,7,9,10] have this property. As the optical wavefront propagates through the quadratic phase system (QPS), the distributions in any two planes are replaced, in general, by an FRT of the appropriately-scaled distribution in the two planes (see Figure 2). Thus, a QPS offers a continuum of planes in which encoding can be done. Without significantly increasing hardware complexity, the encryption system can acquire multidimensional keys in addition to the RPMs. In the fore-mentioned geometry for encryption, the Fourier transform (FT) operation was extended to fractional-order Fourier transformation, which further enhances the security of the system.

Secure information transmission

Because the encrypted data is fully complex, it must be recorded and stored holographically. Information recorded in this way is difficult to transmit over digital communication channels. Digital holography involves recording the complex amplitude distribution of the Fourier or Fresnel diffraction pattern on a CCD camera, storage of the captured hologram in a computer, and numerical reconstruction of the hologram. It combines the high speed and security of encryption with the advantages of electronic transmission, storage, and decryption.[7-9] Here, an RPM is attached to the input image located in the Fourier or fractional plane of an optical processor in one arm of an off-axis Mach-Zehnder interferometer (see Fig-

Continues on page 8.

Hybrid optical encryption of a three-dimensional object

We propose a way to securely encrypt a three-dimensional (3D) object using phase modulation of the object beam. Encryption is accomplished via a combination of a real and virtual optical system, so we have called our method ‘hybrid optical encryption.’ The keys for an encryption step consist of both a phase distribution and a virtual optical phase mask position: if either is incorrect, the 3D object cannot be decrypted.

The hybrid encryption system[1] is shown schematically in Figure 1. The encryption step is denoted by solid arrows and the *U* variables, and decryption is denoted by dashed arrows and *V* variables. First, we shall describe the encryption step in detail. A digital Fresnel hologram of a 3D object (a die) is recorded in advance by using a phase-shifting technique.[2] Using the digital hologram, the wavefront of the object $U(x_o)$ is obtained and encrypted using a virtual optical system. Next, we compute the Fresnel diffraction integral. We have a wavefront $U(x_m)$ at a virtual phase mask (VPM) plane, and multiply the two to produce a uniformly-random phase distribution. Thus, we obtain the encrypted wavefront $U'(x_m)$. Finally, the wavefront is propagated to the charge-coupled device (CCD) camera where it is called $U'(x_c)$, the encrypted digital hologram. Because it is digital, this hologram is suitable for storage and transmission, and can also be compressed.[3]

To decrypt, the encrypted digital hologram is propagated from the CCD to the VPM placed at $z=z_m$. We obtain a wavefront at the VPM given by $V'(x_m)$ and then calculate the product of the wavefront $V'(x_m)$ and the complex conjugate of the phase distribution of the VPM. This allows the encrypted digital hologram to be decrypted correctly, producing the wavefront $U(x_m)$. Note that both the phase distribution and position of the VPM are needed in order to encrypt or decrypt hologram.

Encryption and decryption experiments

A He-Ne laser (with wavelength of 632.8nm) was used as a coherent light source. We used a CCD camera with 1280×960 pixels and 8bit grey levels. Each CCD pixel was 4.65µm×4.65µm. For 3D objects, we use two dice, each as large as 10×10×10mm each. The distances from the dice to the CCD were 180mm and 270mm, respectively, and the distance from the VPM to the CCD was 30mm.

Using the encryption step described above, we obtained an encrypted digital hologram of the two dice. Here, we show the results of decryption. Figure 2(a) shows the reconstructed object using a non-encrypted digital hologram. With the correct position and phase distribution of the VPM, the decrypted 3D objects are shown in Figure 2(b). Figures 2(c) and (d) show the decrypted 3D objects if either the position or phase distribution is wrong. In Figure 2(c), the distance from the CCD to the VPM is set to 31mm. In Figure 2(d), to decrypt we use a VPM that has a phase distribution independent of that used in the encryption process. From these experimental results, if both the information and phase distribution of the VPM are correct, the encrypted digital hologram can be decrypted.

Takanori Nomura
Department of Opto-Mechatronics
Faculty of Systems Engineering
Wakayama University, Wakayama, Japan
E-mail: nom@sys.wakayama-u.ac.jp

References

1. T. Nomura, K. Uota, and Y. Morimoto, *Hybrid optical encryption of a 3-D object using a digital holographic technique,* **Opt. Eng. 43** (10), p. 2228, 2004.
2. I. Yamaguchi and T. Zhang, *Phase-shifting digital holography,* **Opt. Lett. 22** (16), p. 1268, 1997.
3. T. Nomura, A. Okazaki, M. Kameda, Y. Morimoto, and B. Javidi, *Digital holographic data reconstruction with data compression,* **Proc. SPIE 4471,** p. 235, 2001.

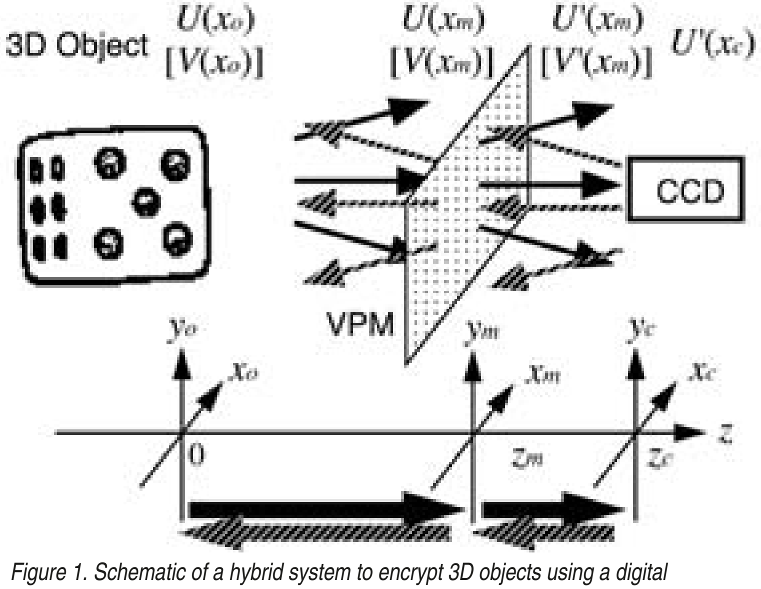


Figure 1. Schematic of a hybrid system to encrypt 3D objects using a digital holographic technique.

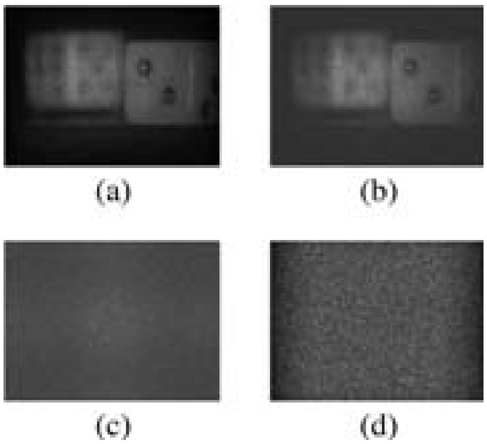


Figure 2. (a) The reconstructed 3D object from a non-encrypted digital hologram. Decrypted 3D objects using (b) both the correct position and phase distribution, (c) no information, and (d) the wrong position and correct phase distribution.

Secure three-dimensional object reconstruction based on digital holography

Optical communication channels have the potential to carry huge amounts of data for three-dimensional (3D) display applications. It is well known that holography is ideal for implementing such displays and, thanks to recent advances in image sensor technology,[1] digital holography is now available as an alternative to film. Figure 1 shows an example of a successfully reconstructed 3D object—a rotating die—made using phase-shifting digital holography. Information security is one of the most important issues in the use of remotely-driven 3D display systems, and encryption can be easily introduced using random phase modulation. Here, we present a secure 3D display using holographic information that is acquired and transmitted digitally.

There are two ways to use random phase modulation to encrypt digital holographic data:[2-4] encrypt the reference beam[2] or encrypt the object beam.[3,4] With both techniques, the recorded data can be securely transmitted to remote users via data communication channels. At the remote user's location, the original 3D object can then be reconstructed optically in real-time by decrypting the information. Here we present a secure display system where the *object itself* is encrypted by a random phase mask.

Figure 2 shows our secure 3D display. In this system, the object information is encrypted by a random phase mask that is located at the Fourier plane after the reflected light from the object has propagated in free space. The information is recorded by an image sensor as an encrypted digital hologram (EDH) by making an interference pattern between this encrypted object beam and a plane reference wave. A key hologram (KH) is recorded at the same time, also recorded as the interference pattern between the random phase mask and the reference beam. This is transmitted to the authorized user before the EDH.

In the reconstruction, both EDH and KH are used to decrypt the data and reconstruct the 3D object, as shown in Figure 2(b). In the decryption process, an optical correlator is used because this allows the phase modulation introduced at the Fourier plane to be cancelled completely: we use a joint transform correlator architecture. In this system, as shown in Figure 2(b), the joint power spectrum(JPS) is recorded by an intensity-sensitive spatial light modulator after the input has been Fourier transformed. By illuminating a readout beam, another Fourier transform is operated by a lens. After the appropriate propagation in free space, we obtain the conjugate of the original 3D object. The operation of the proposed system is described in Reference 4.

In the construction of the optical system, a critically-important device is the optically-addressed spatial light modulator (OA-SLM) that records the JPS. The crucial factors are the spatial and intensity resolutions. We have investigated the effect of the intensity resolution of the OA-SLM on the quality of the reconstructed image, where the JPS is quantized from 1-12 bits. In the numerical simulation we use 2D binary data with a random phase distribution. This random phase mask enables us to reconstruct the original data only at the appropriate propagation distance. Figure 3 shows the intensity distribution of original 2D binary data and numerically-reconstructed images. Figures 3(a) and (b) show that the reconstruction is successful in the case of no quantization.

However, by using a JPS with quantization reduced to six bits, the original data could not

Continues on page 9.

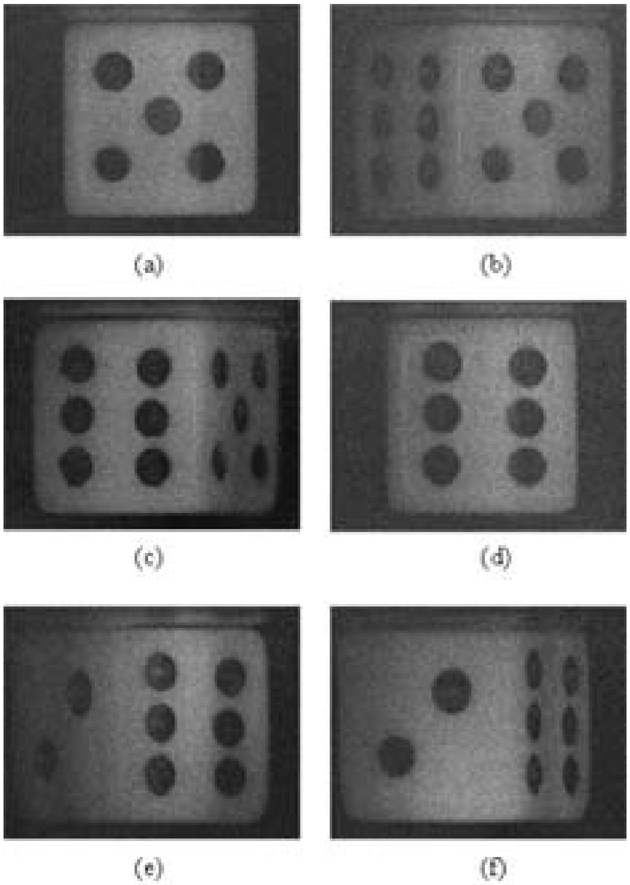


Figure 1. Reconstructed images obtained at different rotation angles: (a) 0°, (b) 30°, (c) 60°, (d) 90°, (e) 120°, and (f) 150°.

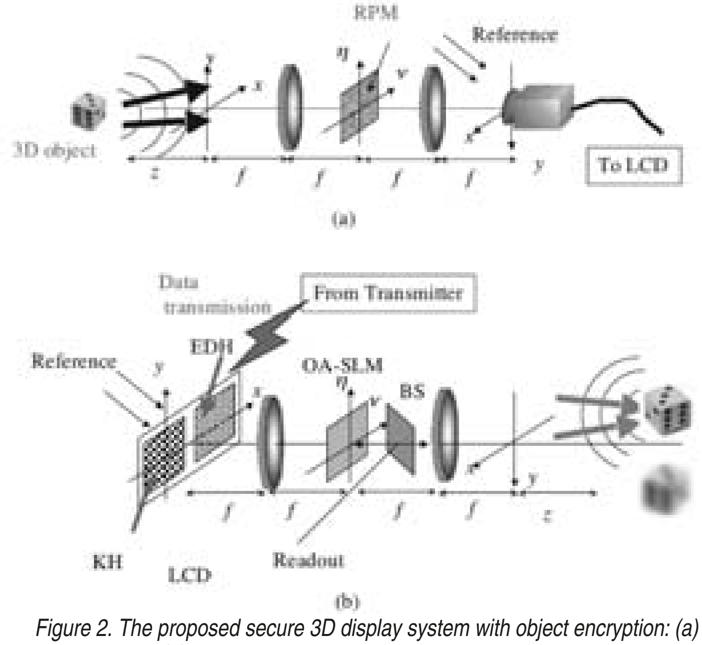


Figure 2. The proposed secure 3D display system with object encryption: (a) recording and (b) reconstruction systems.

Image encryption and watermarking by phase-only wave reconstruction and phase matching

It is well known that the phase of an optical field plays a much more important role than its amplitude for many applications. Based on this idea, we report here our recent studies on image encryption and watermarking using phase-only information and phase matching. These methods can considerably reduce transmission load and realize multiple-image encryption and watermarking with a single set of delivered data. It is particularly well suited to internet transmission.

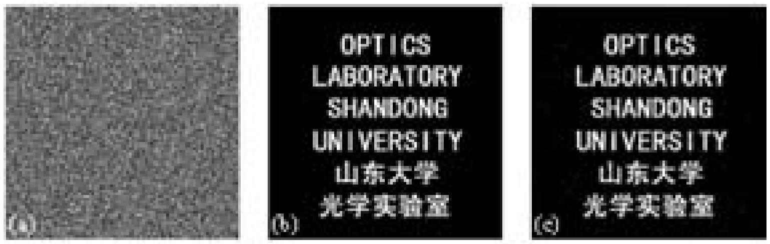


Figure 1. Simulation results of phase-only image encryption: (a) transmitted phase map; (b) retrieved binary image by using the correct G_2 at the right position; (c) retrieved binary image from a 400×400-pixel section of the image shown in (a).

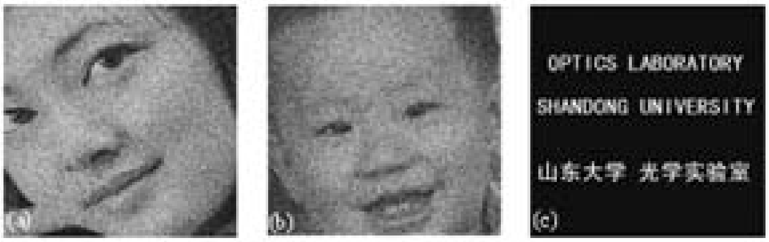


Figure 2. Results of phase-only image encryption and watermarking. (a) Watermarked phase map for an image of a baby's face; (b) retrieved image from (a); (c) retrieved image from a watermarked phase map for a binary image.

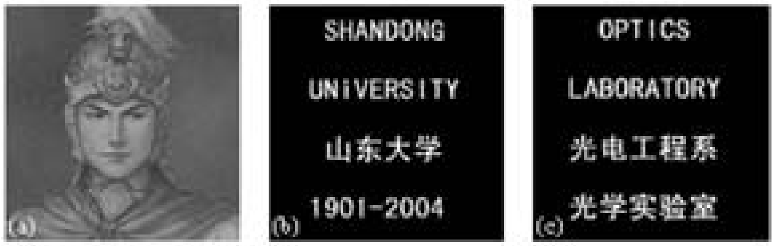


Figure 3. Double-image encryption and watermarking with one set of interferograms embedded in four different host images: (a) One of the four transmitted watermarked images; (b) and (c) retrieved binary images with different G_2.

Image encryption with phase-only information

Our method is based ondouble-random phase encoding[1,2] and phase-shifting interferometry (PSI).[3-5] An object image O is in close contact with a random phase mask (RPM), G_1. Another RPM, G_2, is placed between plane O and the recording (CCD) plane P. By introducing a phase-controllable plane reference wave, standard four-frame PSI can be implemented and then the complex object field in plane P can be calculated. The amplitude of object O can be further retrieved by performing two successive inverse Fresnel diffractions using RPM G_2.

We investigated the effects of wave reconstruction from only the real part, the imaginary part, and the phase information from the retrieved complex diffraction field for both the binary and grey-level input images. We found that the phase-only reconstruction was much better than that with the real or imaginary parts, and that the binary amplitude images yield much more satisfactory reconstruction results than the grey-level images. One of our simulation results, with a binary image, is shown in Figure 1. Here, (a) is the phase map (512×512 pixels), (b) is the retrieved binary image, and (c) is the retrieved result using part of the phase map (a) (400×400 pixels). We can see Figure that 1(b) is perfect and Figure 1(c) is also fairly clear. These results have convincingly shown the feasibility of this method for binary-image encryption and for the reconstruction of images from part of the transmitted image.

Image watermarking using phase-only information

We have also proposed a method of image watermarking using only one grey-level image—the phase map of the diffraction field embedded into a host image—for delivery. The authorized receiver can retrieve the hidden image through the aforementioned procedure without knowledge of the host image. This method has been verified using the simulation results shown in Figure 2. Here (a) shows the watermarked phase map for the input of a baby's face, and (b) is the retrieved image from (a). We can see some noise in both Figure 2(a) and (b) due to the addition of host image, but in Figure 2(b) the baby's face is still clearly recognizable. If we use a binary image as the hidden one, the retrieved image—shown in Figure 2(c)—appears almost perfect.

Multiple image encryption and watermarking by phase matching

We wanted to take a full advantage of the critical effect of phase information in wave reconstruction to increase the efficiency of transmitted data. For this reason, we proposed a novel method of multiple-image encryption and watermarking using phase-mask matching, which can encrypt and then decrypt more than one image with the same set of transmitted patterns.

This method is based on the idea of superposition of interferograms or, equivalently, the complex diffraction fields resulting from the different combinations of original images and certain RPMs. First we record four interferograms using input image O_1 and RPM G_2. Next we use another image, O_2, and another RPM, G_2', to get a new set interferograms. After that we add the two sets together and embed each resultant composite interferogram into a host image to obtain a single set of images for internet transmission. The authorized receiver can calculate the complex field in the recording plane and then reconstruct the original image via two inverse Fresnel diffraction steps. Here, if we use G_2 in its original position, we will obtain the original image O_1: if G_2' is used, the original image O_2 will be obtained.

The simulation results of this approach are given in Figure 3. The original images are two binary word patterns (not shown). Figure 3(a) shows one of the four watermarked composite interferograms embedded into four different host images (cartoon portraits). Figure 3(b) and

Continues on page 10.

Phase-key replication with three-step phase-shifting digital holography

In classic double-random phase-encoding techniques,[1-3] the encrypted information is complex and has to be stored holographically.[4-6] Generally, random scattering media—such as ground glass screens—are used in practical encryption systems as the phase keys.[7] These are necessary to retrieve the stored, encrypted information. Thus, the ability to replicate phase keys becomes of important when the holographic memory is to be distributed to, and accessed by, another legal user. Recently, Su et al.[7] proposed a method for replication that involves holographically recording the key wavefront using a Fe:LiNbO$_3$ crystal plate.

Here, we describe an alternative method based on digital holography. That is, the phase-key wavefront is recorded digitally and is therefore easy to distribute. A legal user with these digital holograms can reconstruct the correct phase key easily using the appropriate reconstruction algorithm, and then access the encrypted information by loading the phase key into a spatial light modulator. The method of recording the phase key as a digital hologram was previously used by Tajahuerce et al.,[8] with the general four-step phase-shifting algorithm. However, here we introduce a simpler algorithm—first proposed, to the best of our knowledge, by Frantz et al.[9]—that only requires the recording of three holograms. The three-step phase-shifting algorithm was also recently used by Cai et al.[10] for image encryption and watermarking.

A Mach-Zehnder interferometer can be used for this task. A collimated beam is divided into two using a beamsplitter to obtain a reference wave and another to illuminate the phase key plate (yielding the key wave). The reference beam is stepwise phase-shifted, introducing phase retardations of ϕ_1, ϕ_2 and ϕ_3. The phase-shifted references each interfere with the key wave, yielding three interference patterns: I_1, I_2 and I_3, respectively. These holograms contain the phase key information and are recorded using a charge-coupled device (CCD) camera. They are then distributed to the legal user to access the encryption system.

With these three holograms, the user can easily reconstruct the phase key distribution by employing the algorithm described below. For the sake of simplicity, the reference is supposed to be a plane wave with unity amplitude and zero phase, and the phase retardations ϕ_1, ϕ_2, and ϕ_3 are 0, $\pi/2$, and π, respectively. The holograms I_1, I_2 and I_3 can be expressed as:

$$I_1 = |K(x, y)+1|^2,$$

$$I_2 = |K(x, y)+i|^2, \text{ and}$$

$$I_3 = |K(x, y)-1|^2,$$

where $K(x, y)$ is the key wavefront at the CCD plane, which is essentially the Fresnel transform of the phase-key function. $K(x, y)$ can then be calculated from the recorded holograms with the following formula:

$$K(x, y) = [(I_1 - I_3) - i(I_1 + I_3-I_2)]/4.$$

Finally, the phase key is obtained by inverse Fresnel transforming $K(x, y)$ from the CCD plane backward to the key plane.

Theoretically, the phase key—and therefore the encrypted information—can be reconstructed with high fidelity if the recoding system is free of issues like phase-shifting inaccuracy in the reference wave, CCD camera noise, high-frequency spatial noise from dirt in the optical path, and the inhomogeneity in the beam. Unfortunately, it is difficult to avoid all these completely in a practical system and they would influence the quality of the decrypted information. For example, if there is a phase-shifting error, a twin image would be superimposed on the reconstructed phase-key distribution, resulting in an incorrect key. The analysis of the effects of such errors to decryption performance is therefore of great importance. However, detailed discussion of this topic is beyond the scope of this article.

Guohai Situ and Jingjuan Zhang
College of Physical Sciences
Graduate School of the Chinese Academy of Sciences, Beijing, China
E-mail: ghsitu@mail.china.com

References

1. P. Refregier and B. Javidi, *Optical image encryption based on input plane and Fourier plane random encoding*, **Opt. Lett. 20**, p. 464, 1995.
2. B. M. Hennelly and J. B. Sheridan, *Image encryption and the fractional Fourier transform,* **Optik 114,** p. 251, 2003.
3. G. Situ and J. Zhang, *Double random-phase encoding in the Fresnel domain*, **Opt. Lett. 29,** p. 1584, 2004.
4. O. Matoba and B. Javidi, *Encrypted optical memory system using three-dimensional keys in the Fresnel domain*, **Opt. Lett. 24,** p. 762, 1999.
5. O. Matoba and B. Javidi, *Encrypted optical storage with wavelength-key and random phase codes*, **Appl. Opt. 38**, p. 6785, 1999.
6. X. Tan, O. Matoba, T. Shimura, K, Kuroda, and B. Jaivid, *Secure optical storage that uses fully phase encoding*, **Appl. Opt. 39,** p. 6689, 2000.
7. W. -C. Su, C. -C. Sun, Y.-C. Chen, and Y. Ouyang, *Duplication of phase key for random-phase-encrypted volume holograms*, **Appl. Opt. 43,** p.1728, 2004.
8. E. Tajahuerce, O. Matoba, S. C. Verrall, and B. Javidi, *Optoelectronic information encryption with phase-shifting interferometry*, **Appl. Opt. 39,** p. 2313, 2000.
9. L. M. Frantz, A. A.Sawchuk, and W. von der Ohe, *Optical phase measurement in real time*, **Appl. Opt. 18,** p. 3301, 1979
10. L. -Z. Cai, M. -Z. He, Q. Liu, and X. -L. Yang, *Digital image encryption and watermarking by phase-shifting interferometry*, **Appl. Opt. 43,** p. 3078, 2004.

Optical information security

Continued from page 4.

ure 3). The encrypted information, interfered with an RPM in second arm of the system, is recorded in a CCD camera. An electronic key is generated and the encrypted hologram is multiplied with this key, and a digital FT or FRT is obtained. Digital information about the reference arm RPM (key hologram) is obtained in the same way by removing the input object—the first RPM—and the FT lens. Decryption is then performed digitally in the computer using the fast FT algorithm. The input amplitude image can be replaced with a phase image to further enhance the security of the system.[9]

Naveen K. Nishchal, G. Unnikrishnan*, Joby Joseph*, and Kehar Singh†
Photonics Division
Instruments Research and Development Establishment
Dehradun, India
E-mail: kehars@physics.iitd.ernet.in
*Photonics Group, Department of Physics
Indian Institute of Technology Delhi
New Delhi, India

References

1. P. Refregier and B. Javidi, *Optical image encryption using input and Fourier plane random phase encoding,* **Opt. Lett. 20** (7), p. 767, 1995.
2. G. Unnikrishnan, J. Joseph, and K. Singh, *Optical encryption system that uses phase conjugation in a photorefractive crystal,* **Appl. Opt. 37,** p. 8181, 1998.
3. G. Unnikrishnan, J. Joseph, and K. Singh, *Optical encryption using double random phase encoding in the fractional Fourier domain,* **Opt. Lett. 25** (12), p. 887, 2000.
4. G. Unnikrishnan, J. Joseph, and K. Singh, *Fractional Fourier domain encrypted holographic memory by use of an anamorphic optical system,* **Appl. Opt. 40** (2), p. 299, 2001.
5. N. K. Nishchal, J. Joseph, and K. Singh, *Optical phase encryption by phase contrast using electrically addressed spatial light modulator,* **Opt. Commun. 217** (1-6), p. 117, 2003.
6. N. K. Nishchal, J. Joseph, and K. Singh, *Fully phase encryption using fractional Fourier transform,* **Opt. Eng. 42** (6), p. 1583, 2003.
7. N. K. Nishchal, J. Joseph, and K. Singh, *Securing information using fractional Fourier transform in digital holography,* **Opt. Commun. 235,** p. 253, 2004.
8. T. J. Naughton and B. Javidi, *Compression of encrypted three-dimensional objects using digital holography,* **Opt. Eng. 43** (10), p. 2233, 2004.
9. N. K. Nishchal, J. Joseph, and K. Singh, *Fully phase encryption using digital holography,* **Opt. Eng. 43** (12), 2004.
10. B. Hennelly and J. T. Sheridan, *Fractional Fourier transform-based image encryption: phase retrieval algorithm,* **Opt. Commun. 226** (1-6), p. 61, 2003.

Secure three-dimensional object reconstruction based on digital holography

Continued from page 6.

be reconstructed, as shown in Figure 3(d). We calculated the mean squared error between the reconstructed images, both with and without the reduced quantization. Figure 4 shows the mean squared error as a function of quantization reduction. We can see that 10bit intensity resolution is required for successful reconstruction. This encourages us to continue to develop a remote, real-time 3D display system.

Osamu Matoba and Bahram Javidi*
Dept. Computer and Systems Engineering
Kobe University, Japan
E-mail: matoba@kobe-u.ac.jp
*Dept. Computer and Electrical Engineering
University of Connecticut, Storrs
E-mail: bahram@engr.uconn.edu

References

1. O. Matoba, T. Naughton, Y. Frauel, N. Bertaux, and B. Javidi, *Real-time three-dimensional object reconstruction by use of a phase-encoded digital hologram,* **Appl. Opt. 41** (29), pp. 6187-6192, 2002.
2. E. Tajahuerce and B. Javidi, *Encrypting three-dimensional information with digital holography,* **Appl. Opt. 39** (35), pp. 6595-6601, 2000.
3. O. Matoba and B. Javidi, *Optical retrieval of encrypted digital holograms for secure real-time display,* **Opt. Lett. 27** (5), pp. 321-323, 2002.
4. O. Matoba and B. Javidi, *Secure Three-Dimensional Data Transmission and Display,* **Appl. Opt. 43** (11), pp. 2285-2291, 2004.

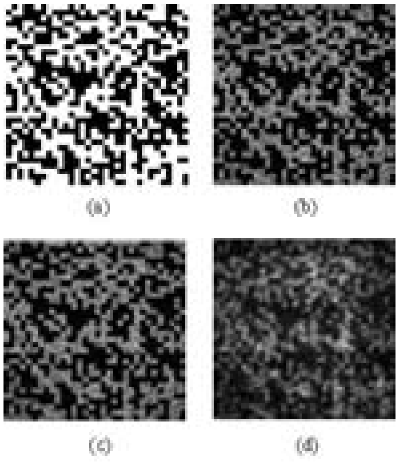


Figure 3. Numerical results: (a) input data; (b) reconstructed data without quantization; and reconstructed data with quantization reductions to (c) 8bit and (d) 6bit, respectively.

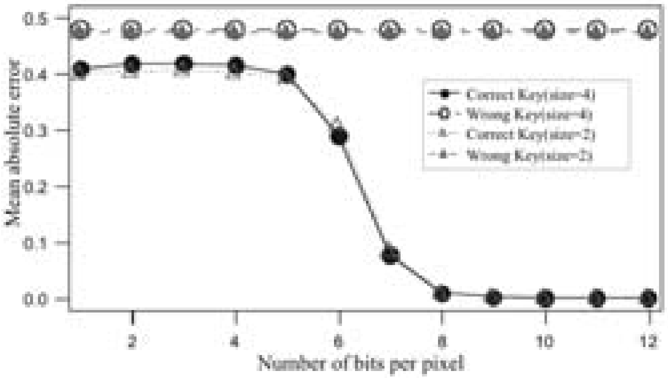


Figure 4. Mean squared error as a function of a number of bits in the intensity resolution in the optically-addressed spatial light modulator.

Encryption of volume holograms

Continued from page 3.

ments show that gray scale images could be also encrypted using our technique.

Hyun Kim and Yeon H. Lee
School of Information and Communication Engineering,
Sungkyunkwan University
South Korea
E-mail: yeonlee@ece.skku.ac.kr

References

1. P. Refregier and B. Javidi, *Optical image encryption based on input plane and Fourier plane random encoding*, **Opt. Lett. 20,** pp. 767-769, 1995.
2. S. Liu, Q. Mi, and B. Zhu, *Optical image encryption with multistage and multichannel fractional Fourier-domain filtering*, **Opt. Lett. 26,** pp. 1242-1244, 2001.
3. 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,** pp. 1508-1514, 2003.
4. J. F. Heanue, M. C. Bashaw, and L. Hesselink, *Encrypted holographic data storage based on orthogonal-phase-code multiplexing*, **Appl. Opt. 34,** pp. 6012-6015, 1995.
5. H. Kim and Yeon H. Lee, *Encryption of volume holograms by complementary binary input image and key*, submitted to **Opt. Lett.**

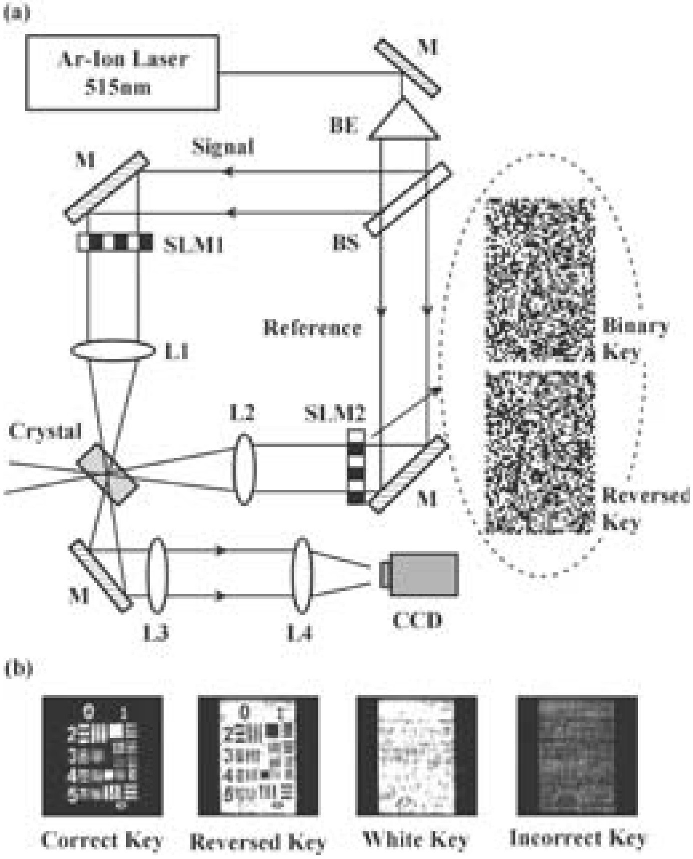


Figure 2. (a) The experimental setup: SLMs are spatial light modulators, CCD is a charge-coupled device. (b) Restored images.

Micro-optics for phase-only cryptography

Continued from cover.

ing pixels of 0 and π constitute a 17×9-pixel phase key where the size of each pixel is approximately 176×333μm. In the current experiment, shown in Figure 2, an external macro-optical setup is needed to scale both the encrypted and key patterns to the appropriate sizes for imaging using the GPC-PO device.

The prospect, however, is to miniaturize the entire optical setup into a fully-integrated micro-optical system. Figure 3 shows the intended implementation of the whole optical system in planar-integrated optics using a two-stage 4-f lens setup. An image of a phase-encrypted pattern is projected on the decrypting phase key pattern using the first 4-f system. An encrypted phase-only pattern recorded on a bank card, a passport, a currency note, etc., can be instantly verified for authenticity using this system. The phase-only key can be dynamically encoded on a compact, electronically-controlled liquid-crystal-on-silicon (LCOS) SLM. Non-mechanical alignment of the two phase patterns can be achieved by automated electronic scrolling of the encoded pattern. The decrypted phase data is then converted into an intensity pattern using the GPC method via the second 4-f filter. The intensity pattern at the output can subsequently be recorded using a detector array and transformed into another medium for transmission.

Jesper Glückstad, Vincent R. Daria, Peter J. Rodrigo and Stefan Sinzinger*
Optics and Plasma Research Department
RISÖ National Laboratory
Roskilde, Denmark
E-mail: jesper.gluckstad@risoe.dk,
http://www.ppo.dk
*Faculty of Mechanical Engineering
Technical University of Ilmenau, Denmark

References

1. J. Glückstad, *Phase contrast scrambling,* **Int'l PCT patent WO 002339A1,** 3 July 1998.
2. P. C. Mogensen and J. Glückstad, *Phase-only optical encryption,* **Opt. Lett. 25,** pp. 566-568, 2000.
3. P. C. Mogensen and J. Glückstad, *Phase-only optical decryption of a fixed mask,* **Appl. Opt 40,** pp. 1226-1235, 2001.
4. V. Daria, J. Glückstad, P. C. Mogensen, R. L. Eriksen, and S. Sinzinger, *Implementing the generalized phase-contrast method in a planar-integrated micro-optics platform,* **Opt. Lett. 27,** pp. 945-947, 2002.
5. J. Glückstad, V. Daria, and P. J. Rodrigo, *Decrypting binary phase patterns by amplitude,* **Opt. Eng. 43,** pp. 2250-2258, 2004.
6. V. Daria, P. J. Rodrigo, S. Sinzinger, and J. Glückstad, *Phase-only optical decryption in a planar integrated micro-optics system,* **Opt. Eng. 43,** pp. 2223-2227, 2004.

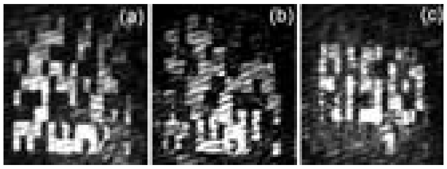


Figure 2. Visualization of the millimetre-sized 17×9-pixellated phase-images corresponding to: (a) the decrypting key, (b) the encrypted phase pattern, and (c) the decrypted phase pattern using the planar optical implementation of the GPC.

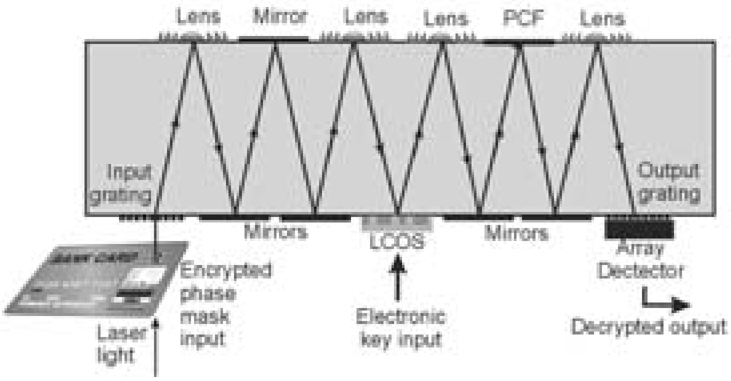


Figure 3. The proposed integration of the whole phase-only decryption setup using a two-stage 4-f lens planar optical system. The phase-encrypted pattern is read-out from a credit card and the phase-only decryption key is dynamically reconfigured and spatially aligned on an electronically-addressed liquid-crystal-on-silicon (LCOS) spatial light modulator.

Image encryption and watermarking

Continued from page 9.

(c) are retrieved binary images using their corresponding phase masks, which are clear enough for easy subject recognition.

This work is partly supported by the National Natural Science Foundation (Grant 60177002) and the Ph.D. Training Foundation of the Education Ministry of China.

L. Z. Cai, Q. Liu, M. Z. He, and X. F. Meng
Department of Optics
Shandong University, Jinan, China
E-mail: lzcai@sdu.edu.cn

References

1. P. Refregier and B. Javidi, *Optical image encryption based on input plane and Fourier plane random encoding,* **Opt. Lett. 20,** pp. 767-769, 1995.
2. S. Kishk and B. Javidi, *Information Hiding Technique with Double Phase Encoding,* **Appl. Opt. 41,** pp. 5462-5470, 2002.
3. N. Takai and Y. Mifune, *Digital Watermarking by a Holographic Technique,* **Appl. Opt. 41,** pp. 865-873, 2002.
4. S. Kishk and B. Javidi, *Watermarking of three-dimensional objects by digital holography,* **Opt. Lett. 28,** pp. 167-169, 2003.
5. L. Z. Cai, M. Z. He, Q. Liu, and X. L. Yang, *Digital image encryption and watermarking by phase-shifting interferometry,* **Appl. Opt. 43,** pp. 3078-3084, 2004.

Secure display with limited viewing

Continued from page 12.

Hirotsugu Yamamoto, Yoshio Hayasaki, and Nobuo Nishida
Dept. of Optical Science and Technology
The University of Tokushima, Japan.
E-mail: yamamoto@opt.tokushima-u.ac.jp

References

1. H. Yamamoto, Y. Hayasaki, and N. Nishida, *Securing information display by use of visual cryptography,* **Opt. Lett. 28,** pp. 1564-1566, 2003.
2. H. Yamamoto, Y. Hayasaki, and N. Nishida, *Secure information display with limited viewing zone by use of multi-color visual cryptography,* **Optics Express 12,** pp. 1258-1270, 2004.
3. M. Naor and A. Shamir, *Visual Cryptography, in Advances in Cryptography - EUROCRYPT'94,* **Vol. 950 of Lecture Notes in Computer Science**, Springer-Verlag, Berlin, pp. 1-12, 1994.
4. J. Tanida and Y. Ichioka, *Optical logic array processor using shadowgrams,* **J. Opt. Soc. Am. 73,** pp. 800-809, 1983.

Join the Technical Group

...and receive this newsletter

Membership Application

Please Print □ **Prof.** □ **Dr.** □ **Mr.** □ **Miss** □ **Mrs.** □ **Ms.**

First Name, Middle Initial, Last Name ______________________________

Position ____________________ SPIE Member Number ____________________

Business Affiliation ______________________________

Dept./Bldg./Mail Stop/etc. ______________________________

Street Address or P.O. Box ______________________________

City/State ____________________ Zip/Postal Code __________ Country __________

Telephone ____________________ Telefax ____________________

E-mail Address/Network ______________________________

Technical Group Membership fee is $30/year, or $15/year for full SPIE members.

□ Optics in Information Systems
Total amount enclosed for Technical Group membership $ __________

□ **Check enclosed.** Payment in U.S. dollars (by draft on a U.S. bank, or international money order) is required. Do not send currency. Transfers from banks must include a copy of the transfer order.

□ **Charge to my:** □ VISA □ MasterCard □ American Express □ Diners Club □ Discover

Account # ____________________ Expiration date ____________________

Signature ______________________________
(required for credit card orders)

This newsletter is printed as a benefit of the **Optics in Information Systems Technical Group.** Membership allows you to communicate and network with colleagues worldwide.

As well as a semi-annual copy of the *Optics in Information Systems* newsletter, benefits include SPIE's monthly publication, **oe***magazine,* and a membership directory.

SPIE members are invited to join for the reduced fee of $15. If you are not a member of SPIE, the annual membership fee of $30 will cover all technical group membership services. For complete information about SPIE membership and an application form, please contact us.

Send this form (or photocopy) to:
SPIE • P.O. Box 10
Bellingham, WA 98227-0010 USA
Tel: +1 360 676 3290
Fax: +1 360 647 1445
E-mail: spie@spie.org

http://www.spie.org/info/ois

Please send me
□ Information about full SPIE membership
□ Information about other SPIE technical groups
□ FREE technical publications catalog

Reference Code: 4646

OPTICSONLINE

Optics Web Discussion Forum

You are invited to participate in SPIE's online discussion forum on Optics in Information Systems. To post a message, log in to create a user account. For options see **"subscribe to this forum."**

You'll find our forums well-designed and easy to use, with many helpful features such as automated email notifications, easy-to-follow 'threads,' and searchability. There is a full FAQ for more details on how to use the forums.

Main link to the new Optics in Information Systems forum: **http://spie.org/app/forums/tech/**

Related questions or suggestions can be sent to forums **@spie.org.**

SPIE The International Society for Optical Engineering

Optics in Information Systems

This newsletter is published semi-annually by SPIE—The International Society for Optical Engineering, for its International Technical Group on Optics in Information Systems.

Technical Group Chairs	Bahram Javidi Demetri Psaltis	*Technical Editor*	Sunny Bains
		Editorial Assistant	Stuart Barr
		Managing Editor	Linda DeLano

Articles in this newsletter do not necessarily constitute endorsement or the opinions of the editors or SPIE. Advertising and copy are subject to acceptance by the editors.

SPIE is an international technical society dedicated to advancing engineering, scientific, and commercial applications of optical, photonic, imaging, electronic, and optoelectronic technologies. Its members are engineers, scientists, and users interested in the development and reduction to practice of these technologies. SPIE provides the means for communicating new developments and applications information to the engineering, scientific, and user communities through its publications, symposia, education programs, and online electronic information services.

SPIE—The International Society for Optical Engineering, P.O. Box 10, Bellingham, WA 98227-0010 USA. Tel: +1 360 676 3290. Fax: +1 360 647 1445.

European Office: Karin Burger, Manager, karin@spieeurope.org, Tel: +44 7974 214542. Fax: +44 29 2040 4873.

In Russia/FSU: 12, Mokhovaja str., 119019, Moscow, Russia • Tel/Fax: +7 095 202 1079
E-mail: edmund.spierus@relcom.ru

Secure display with limited viewing zone using visual cryptography

Many types of encryption technique have been developed to ensure data security against unauthorized access to confidential information: these include theft and code-breaking of recorded media, wire-tapping of communication links, and counterfeiting of valuable documents. In practice, however, the security of confidential information is also limited by the fact that security risks arise from the very act of displaying the decrypted information. These include the possibilities of eavesdropping on the electrical video signal and peeping at the screen. To counter this, we propose a display technique that ensures the security of visual information through the use of visual cryptography.

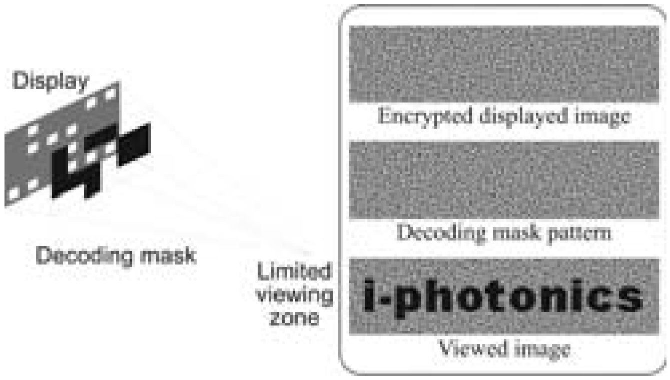


Figure 1. Schematic diagram of a secure display using visual cryptography.

We have reported secure information display techniques for monochromatic and multi-colored images using a decoding mask to view the display.[1,2] The decoding mask has two functions: as a key for decryption of the image and as a means of limiting its viewing zone. The encryption is based on visual cryptography, which was originally proposed by Naor and Shamir.[3] An example of encryption of a monochromatic image is shown in Figure 1. The information for the secret image is shared between two random patterns. One of them is shown on the display panel, and the other is the decoding mask, which contains black (opaque) and white (transparent) pixels. The decryption process requires no special computing device and is implemented using only human vision. Decryption is based on optical logic.[4]

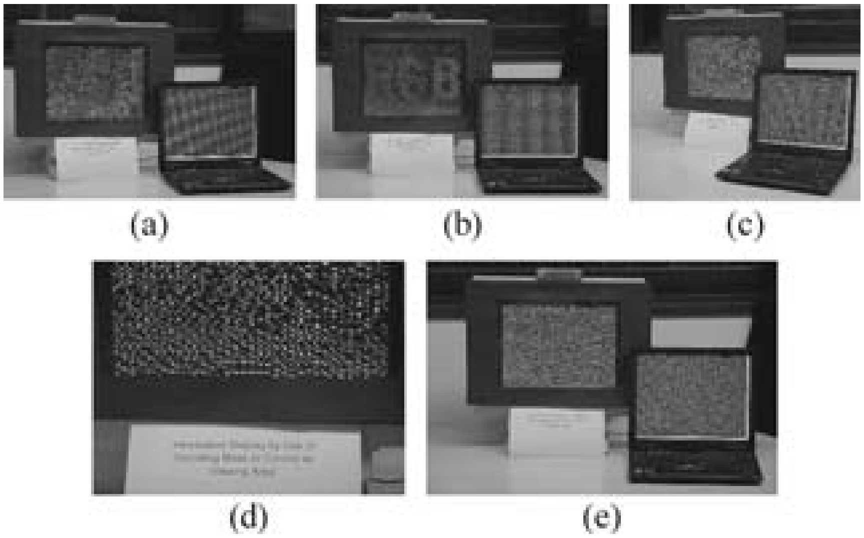


Figure 2. Images seen from at different viewing positions: (a), (c), (d), and (e) are taken from outside the viewing zone; (b) is from inside.

In our system, to limit the viewing zone of the secret image, the decoding mask has a reduced pitch and is placed some distance away from the displayed image. Each subpixel of the displayed image has a corresponding subpixel in the decoding mask. There is a limited viewing zone where this one-to-one relationship is preserved. The displayed image appears as a totally random pattern to anyone looking at it unless that person views it through the decoding mask from the correct distance. When the decoding mask is placed in front of the display panel, the secret image becomes visible within the limited viewing zone.

For the purpose of experimentally demonstrating secure display technique, we have developed a prototype multi-color display system with a decoding mask.[2] Images viewed at different points are shown in Figure 2. When seen from relatively close to the ideal position, the secret image *RGB* was visible, as shown in Figure 2(b). When viewed from the left and right sides (2(a) and (c), respectivley), the secret image was not perceived. When viewed at a close and long range (2(d) and (e), respectively), the secret image was not perceived. Thus, the proposed display technique is secure against theft of the decrypted data and eavesdropping of the display signals, and provides a limited viewing zone. We are now investigating improvements into both the security of the decoding mask and the image quality.

Continues on page 10.

SPIE Society of Photo-Optical Instrumentation Engineers
P.O. Box 10 • Bellingham, WA 98227-0010 USA