Security optical data storage in Fourier holograms

Wei-Chia Su,[1] Yu-Wen Chen,[2,*] Yu-Jen Chen,[1] Shiuan-Huei Lin,[3] and Li-Karn Wang[2]

[1]Graduate Institute of Photonics, National Changhua University of Education, Changhua 500, Taiwan

[2]Institute of Photonics Technologies, National Tsing Hua University, Hsinchu 30013, Taiwan

[3]Department of electrophysics, National Chiao Tung University, Hsinchu 30050, Taiwan

*Corresponding author: d928101@oz.nthu.edu.tw

Received 7 November 2011; revised 9 January 2012; accepted 9 January 2012;
posted 17 January 2012 (Doc. ID 157738); published 15 March 2012

We have proposed and demonstrated a holographic security storage system that is implemented with a shift multiplexing technique. The security function of this storage system is achieved by using a microdiffuser (MD) for random phase encoding of the reference beams. The apparatus of random phase encoding in this system offers an additional and flexible function during the recording processes. The system can generate holographic security memory or nonsecurity holographic memory via using the MD or not. The storage capacity and the average signal-to-noise value of the security storage system are 16 bits/μm^2 and 3.5, respectively. Lateral shifting selectivity in this holographic security storage system is theoretically analyzed and experimentally investigated.

OCIS codes: 210.2860, 210.0210, 090.0090.

1. Introduction

Volume-holographic storage has received increasing attention owing to its potential high storage capacity and fast access rate [1–3]. A novel technique for holographic storage called collinear holography has been investigated in recent years [4]. This apparatus is implemented with a coaxial optical structure to record holograms. The signal and reference beams in this system can be generated by using a spatial light modulator (SLM), and they are usually distributed on the inner and outer surface region of the SLM. These two beams propagate along the optical axis of the system and pass through a Fourier lens, and then finally they interfere at the focal area of the Fourier lens. A recording material is located at the focal area of the Fourier lens for the holographic recording. It has been proven that the collinear holographic storage system performs high potential in miniaturization of the optical architecture and could be compatible with the existing disc storage systems. Shimura *et al.* have also shown that an additional random phase encoding in the reference pixels improves the imaging performance in a collinear holographic data storage system [5]. Meanwhile, random phase encoding in holographic storage is one attractive and important issue for security storage due to the growing demand for protection of information [6–13]. Random phase encoding generated by using a microdiffuser (MD) has shown great advantages for holographic security data storage owing to their difficulty in duplication [14].

The Fourier-architecture-based holographic storage system with random phase encoding has been studied for a long time [15–18]. In this paper, the traditional Fourier-architecture-based holographic storage system is modified to become a coaxial optical structure. Accordingly, a holographic security storage system based on random phase encoding is presented, and the system is implemented with a shifting multiplexing technique.

As shown in Fig. 1, the MD was placed in the reference arm in order to generate a random phase wavefront for encryption of the holographic storage. The stored image can be retrieved from the medium if the original MD is placed in the original spatial position to generate the same random phase wavefront for

1559-128X/12/091297-07$15.00/0

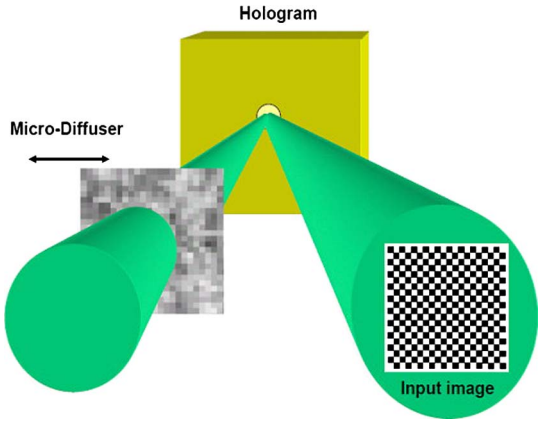


Fig. 1. (Color online) Security holographic storage implemented with a MD.

holographic reconstruction. However, the stored image can not be retrieved if users lack the original MD. Accordingly, security storage in this system is implemented by this MD. If the MD is moved away from the reference arm, the shift multiplexing mechanism for holographic storage can still be performed in this system, and the whole system becomes very similar to a system presented by Steckman *et al.* [19]. Consequently, the characteristic of the MD in this system offers an additional function during the recording process. We can generate a holographic security or nonsecurity memory optionally by moving the MD into the reference arm or moving it away in each holographic recording. As a result, a holographic security and nonsecurity memory both can be generated individually by using our proposed system.

In our previous study, we developed similar techniques to implement encryption-selectable holographic storage systems [20,21]. However, the study in this manuscript is different from our previous publications. In comparison with the system proposed in [20], the holographic security storage proposed in this paper can be accessed without using phase-conjugated readout algorithms. In [20], we have shown that the fidelity of the phase-conjugated reference beam is an important factor that significantly affects the signal-to-noise ratio (SNR) of the reconstructed holograms. In addition, a scheme of encryption-selectable holographic storage in $LiNbO_3$ using angular multiplexing based on 90° geometry is described in [21]. Currently, we find that the study of encryption-selectable holographic storage based on Fourier holograms is still less discussed. Therefore, not only is the holographic security storage system demonstrated in this paper, but the encryption-selectable function of the proposed system is also discussed. The effect of the MD on shifting selectivity in this holographic security storage system is analyzed theoretically and experimentally. The experimental results show that storage capacity with 16 bits/μm^2 in the security storage system can be obtained and that the average SNR of the retrieved data image is 3.5.

2. Security Holographic Storage System

The experimental apparatus of the holographic security storage system is shown in Fig. 2. We used a diode-pumped, solid-state laser at 532 nm as the light source. The laser beam was collimated and split into two parts, one being the signal beam and the other being the reference beam. The signal beam was incident upon the input image and was then passed through the beam splitter (BS) directly. The reference beam was also incident on the BS, but it reflected from the BS. These two beams propagated along the optical axis of the Fourier lens L2 and then passed through it. The focal length of lens L2 was 50 mm. In the reference arm, a MD was placed at 5 mm in front of the recording medium in order to generate random phase wavefronts, and the MD was fixed at the same position for all the following encryption processes. In this study, handmade ground glass was used as the required MD. The ground glass in the experiment was made by grounding a flat glass with Al_2O_3 powders. Therefore, a random phase distribution on the surface of the ground glass diffuser was obtained. The detailed specifications of the ground glass can be found in our previous work [6]. Based on the coaxial geometry, the signal beam would interfere with the random phase wavefronts of reference beam in the focal area of the lens L2. A PQ-PMMA material [22] with dimensions of 20 mm × 20 mm × 2 mm was used as the holographic recording medium, and it was located at the focal area of the lens L2. The recording material was mounted upon a two-dimensional translation stage (piezo-motor driven linear stage, Newport) for implementing shift multiplexing of holographic storage. Based on the shift multiplexing algorithm, holograms were recorded track by track in the horizontal and vertical directions of PQ-PMMA during the recording processes. These holograms between adjacent tracks should be stored by shifting the recording material with a distance larger than or at least equal to the shifting selectivity of this system. The analysis of the shifting selectivity will be presented in the next section. In the reading processes, a Fourier lens L3 located between recording medium and CCD plane performed an inverse Fourier transform of

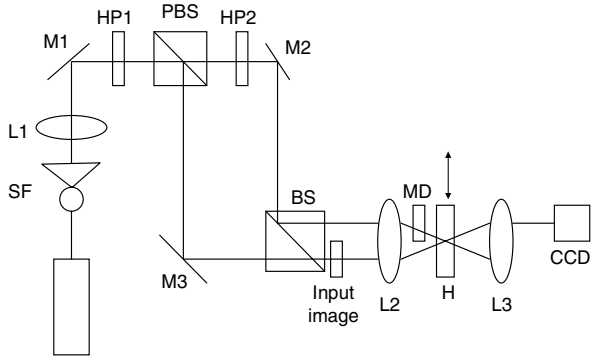


Fig. 2. Experiment setup for a security collinear holographic system: SF, spatial filter; L, lens; M, mirror; PBS, polarization beam splitter; HP, half-wave plate; MD, microdiffuser; H, hologram.

the diffraction beam. When the signal beam was blocked, the original reference beam was used as the reading beam and the medium was shifted to the corresponding recording position; the stored image could then be perfectly reconstructed on the CCD plane.

3. Lateral Selectivity

Shifting selectivity is an important parameter for affecting storage capacity. The lateral shifting selectivity can be analyzed theoretically by using the VOHIL model (the volume hologram being an integrator of the lights emitted from elementary light sources) [23]. As shown in Fig. 3, a convergent spherical wave was incident on the MD to generate the random phase wavefront. Thus, we can write the composite wavefront on the hologram plane as

$$R_w(x_3,y_3) = \int_{-d/2}^{d/2}\int_{-d/2}^{d/2} A_w \exp[j\phi(x_1,y_1)] \times \exp(jkr_1)\mathrm{d}x_1\mathrm{d}y_1, \quad (1)$$

where d is the dimension of the illumination region of the MD, A_w is the amplitude of each spherical wave, $\phi(x_1,y_1)$ is the initial random phase of each point source of MD, and $r_1 = [(x_3-x_1)^2+(y_3-y_1)^2+(z_3-z_1)^2]^{1/2}$ is the distance between the MD and the hologram. The object beam was a plane wave incident upon the input image, which was placed a Δx_o distance from optical axis to the image center and then passed through the Fourier lens L. Therefore, the interference fringes of the hologram records can be written as

$$H(x_3,y_3) = |R_w(x_3,y_3)|^2 + |\Im\{S(x_o+\Delta x_o,y_o)\}|^2 + R_w^*(x_3,y_3)\cdot\Im\{S(x_o+\Delta x_o,y_o)\} + R_w(x_3,y_3)\cdot\Im^*\{S(x_o+\Delta x_o,y_o)\}, \quad (2)$$

where $\Im\{\bullet\}$ represents the Fourier transform function and $S(x_o,y_o)$ is the input image function. During the reading process, we used a random phase wavefront to read the hologram. The reading wave on the hologram plane can be expressed as

$$R_r(x_3,y_3) = \int_{-d/2}^{d/2}\int_{-d/2}^{d/2} A_r \exp[j\phi(x_2,y_2)] \times \exp(jkr_2)\mathrm{d}x_2\mathrm{d}y_2, \quad (3)$$

where A_r is the amplitude of reading wave, $\phi(x_2,y_2)$ is the initial random phase of each point source of MD used for encoding the reading wave, and r_2 is the distance between the MD and the hologram, which can be expressed as $r_2 = [(x_3-x_2)^2+(y_3-y_2)^2+(z_3-z_2)^2]^{1/2}$. For the paraxial condition, $r_1 \approx z_0$ and $r_2 \approx z_0$, where z_0 is the distance between MD and the hologram. When the recording material is only laterally shifted and causes a relative displacement of speckle wave with a distance of $\Delta x = x_2 - x_1$, and $\Delta y = y_2 - y_1$, we can express the diffraction as

$$\begin{aligned} D &\propto \int_{-T/2}^{T/2} R_r\cdot H\cdot\exp\left[jk\left(\frac{T}{2}-r\right)\right]\mathrm{d}r \\ &\propto \int_{-T/2}^{T/2}\int_{-l_y/2}^{l_y/2}\int_{-l_x/2}^{l_x/2}\int_{-d_y/2}^{d_y/2}\int_{-d_x/2}^{d_x/2} \\ &\quad\times\Im\{S(x_o+\Delta x_o,y_o)\}|A_r||A_w| \\ &\quad\times\exp\left\{j\frac{k}{2z_0}[(x_3-x_1-\Delta x)^2+(y_3-y_1-\Delta y)^2 \right. \\ &\quad\left.+(x_3-x_1)^2+(y_3-y_1)^2]\right\} \\ &\quad\times\exp\left[jk\left(\frac{T}{2}-r\right)\right]\mathrm{d}x_1\mathrm{d}y_1\mathrm{d}x_3\mathrm{d}y_3\mathrm{d}r, \end{aligned} \quad (4)$$

where $r = z_3/\cos\alpha$, $T = t/\cos\alpha$, α is the propagation angle of the signal beam, and t is the thickness of hologram. Therefore, the diffraction intensity can be expressed as

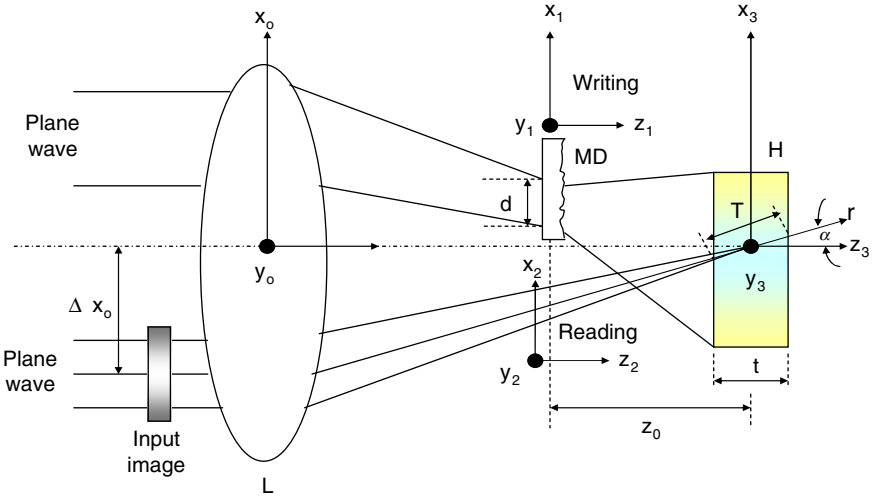


Fig. 3. (Color online) Theoretical model for analysis of shifting selectivity in security collinear holograms.

$$
\begin{aligned}
I &\propto |D|^2 \\
&\propto \left| \int_{-l_x/2}^{l_x/2} e^{-j2\pi\left(\frac{x_0}{\lambda f}+\frac{\Delta x}{\lambda z_0}\right)x_3} \mathrm{d}x_3 \int_{-d_x/2}^{d_x/2} e^{-j2\pi\left(-\frac{\Delta x}{\lambda z_0}\right)x_1} \mathrm{d}x_1 \int_{-l_y/2}^{l_y/2} e^{-j2\pi\left(\frac{y_0}{\lambda f}+\frac{\Delta y}{\lambda z_0}\right)x_3} \mathrm{d}y_3 \int_{-d_y/2}^{d_y/2} e^{-j2\pi\left(-\frac{\Delta y}{\lambda z_0}\right)y_1} \mathrm{d}y_1 \right. \\
&\quad \times \left. \int_{-w/2}^{w/2} \int S(x_0+\Delta x_0, y_0) \mathrm{d}x_0 \mathrm{d}y_0 \int_{\frac{-t}{2\cos\alpha}}^{\frac{t}{2\cos\alpha}} \frac{1}{\cos\alpha} e^{jk\left(\frac{t}{2\cos\alpha}\right)} e^{-j2\pi\left(\frac{1}{\lambda\cos\alpha}\right)z_3} \mathrm{d}z_3 \right|^2 \\
&\propto \mathrm{sinc}^2\left(\frac{d_x \Delta x}{\lambda z_0}\right) \mathrm{sinc}^2\left(\frac{d_y \Delta y}{\lambda z_0}\right) \mathrm{sinc}^2\left(\frac{t}{\lambda \cos^2\alpha}\right) \left| S\left(\Delta x_0 - \frac{f\Delta x}{z_0}, -\frac{f\Delta y}{z_0}\right)\right|^2, \qquad (5)
\end{aligned}
$$

where f is the focal length of lens L, and w is the dimension of the illumination region of the pattern. Here we can define the lateral selectivity as the shift deviation for the first zero diffraction obtained from the sinc functions in Eq. (5). The theoretical simulation and experimental results are shown in Fig. 4. The parameters used in the theoretical simulation are $\lambda = 532$ nm, $Z_0 = 5$ mm, $d_x = 2.5$ mm, $d_y = 2$ mm, $t = 2$ mm, and $f = 50$ mm. As shown in Fig. 5, a chessboard pattern with 20×20 pixels was used as the input pattern. From our experimental measurement results, the lateral selectivity of collinear holographic storage by shifting a single hologram was about only 1.3 and 1.5 μm in the horizontal (x) and vertical (y) directions, respectively.

4. Optical Implementation

In this section, a practical holographic security storage system using the shift multiplexing technique was demonstrated. In order to keep a higher SNR of the reconstructed data image, the shift distance for storing next adjacent hologram in this practical demonstration system was set as 5 μm in both lateral directions [24]. According to the [24], we chose more than the third Bragg null in order to make sure that the reconstructed data image could keep a higher SNR. In this demonstration, 100 image pages were recorded within this material with 10 rows. Each row contained 10 holograms, and these 10 holograms were partially spatially overlapped, but the shift separation of each adjacent hologram was 5 μm. After the recording in the first row was completed, the material was horizontally shifted to its original position and additionally shifted in a vertical direction with 5 μm. We repeated the row recording process described above until the whole 100 holograms were stored within these 10 rows. The dimension of each pixel of the chessboard pattern with 20×20 pixels was 500 μm $\times$ 500 μm. Therefore, the DC term dimension of the signal beam located at the focal plane was around 100 μm $\times$ 100 μm. We can find these 100 holograms were partially spatially overlapped. The spatial distributions of these 100 holograms are illustrated in Fig. 6. Figure 7(a) to (e) are the 1st, 45th, 50th, 55th, and 100th retrieved images obtained from this system, respectively. Figure 7(f) shows the retrieved images of encryption storage without using the correct MD. The storage capacity of our practical system can be expressed as

$$
N = \frac{M}{\Delta x \cdot \Delta y}, \qquad (6)
$$

where M is the pixel number of the data pages. According to Eq. (6), the security storage capacity of our experimental system will reach16 bits/μm^2.

The SNR of each retrieve image that was encrypted by MD based on the coaxial geometry was also calculated. In our experimental setup, the chessboard pattern with 20×20 pixels (500 μm in size) was used as a binary pattern. The magnification of

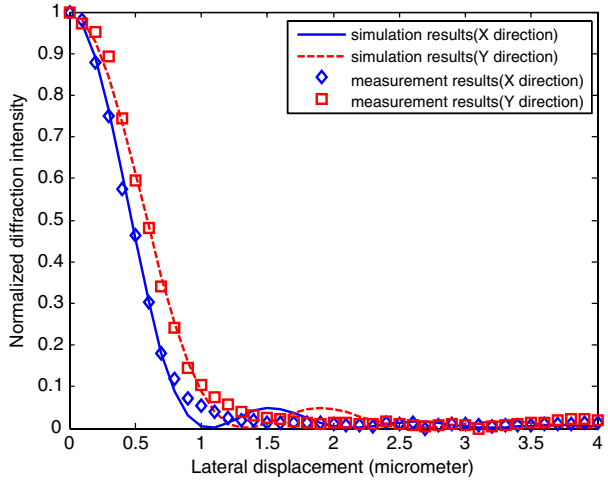


Fig. 4. (Color online) Theoretical and experimental results of lateral selectivity for security collinear holograms.

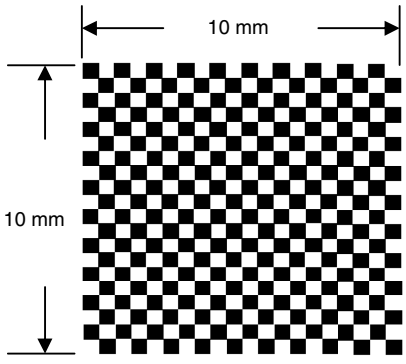


Fig. 5. Input image: chessboard pattern with 20×20 pixels.

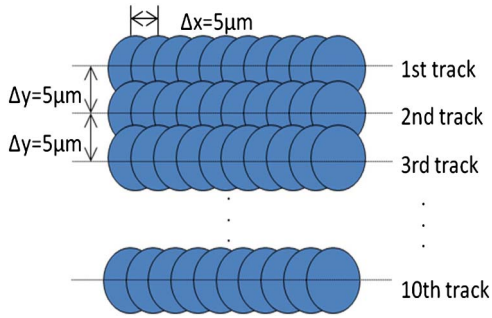


Fig. 6. (Color online) Spatial distribution of 100 stored holograms within the recording material. There are a total of 100 holograms in 10 tracks. Each track contains 10 shift-multiplexed holograms.

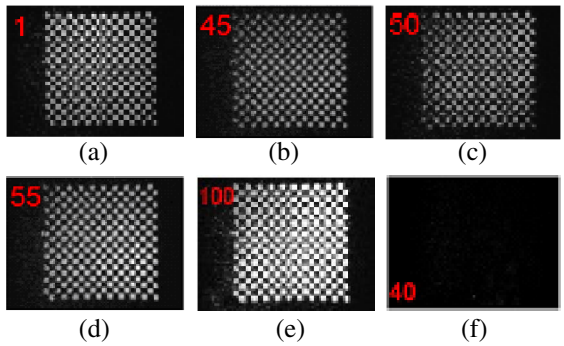


Fig. 7. (Color online) Retrieved images of the stored patterns in this collinear holographic storage system. (a)–(e) Retrieved images by using the same MD locating at the correct position. (f) Diffraction results of encryption storage without using the correct MD.

our retrieved image system was about 0.19. Therefore, the magnification of the retrieved image on the CCD plane was modulated such that one pixel on the retrieved image corresponded to one superpixel on the CCD image sensor. One superpixel was composed of 20×20 camera pixels. For each retrieved image, there were 20×20 superpixels used for SNR calculation. Although 20×20 camera pixels on the retrieved image represent 1 bit, the edges were left out, so only the central 10×10 pixels effectively within a superpixel was used for calculation of SNR. The SNR formula can be expressed as

$$\mathrm{SNR} = \frac{\mu_1 - \mu_0}{(\sigma_1^2 + \sigma_0^2)}, \tag{7}$$

where μ_1, μ_0 and σ_1, σ_0 are the mean value and deviation of the detected energy for one and zero bits, respectively [25]. As shown in Fig. 8, the average SNR value of 100 pages data of retrieved images was about 3.5.

5. Security-Selectable Storage

In this paper, we extend the concept mentioned above to configure a security-selectable holographic storage system. We can generate a holographic security or nonsecurity memory optionally by using the same system. A holographic security memory means that the whole stored images in the memory are encrypted during the recording processes, and a holographic nonsecurity memory means that whole stored images in the memory are not encrypted during the recording processes. If users choose nonencryption recording for all the stored images in this system, the MD should be moved away from the reference arm and the multiplexing storage mechanism in our storage system becomes similar to the conventional shift-multiplexed holographic storage system [19]. If users choose encryption recording for all the stored images in this system, we still perform shift multiplexing for recording, but the MD is moved into the reference arm for each exposure. Thus, a holographic security memory described in Section 4 can be generated.

In our system design, each security-selectable storage system of volume holography has a unique MD for encryption and decryption. The MD in each system only can be shifted in horizontal direction but it

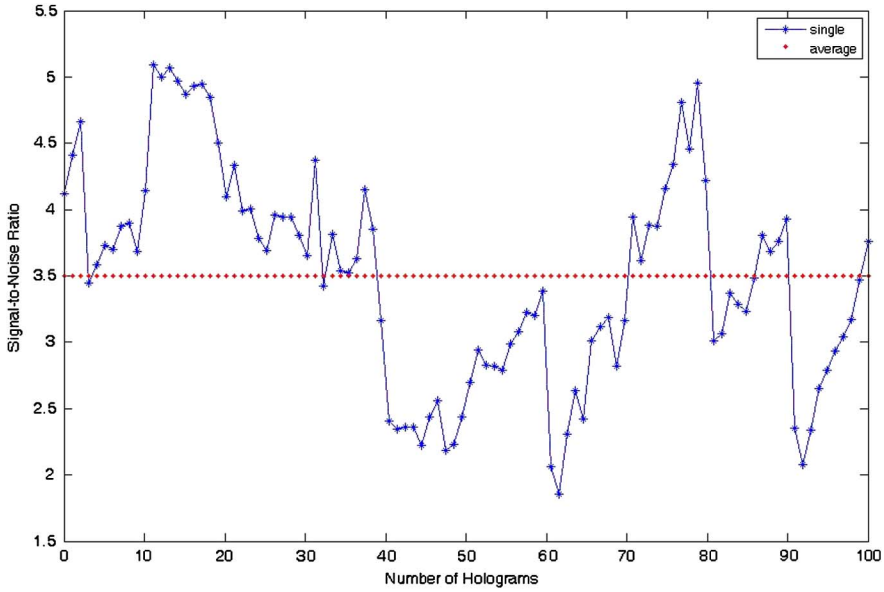
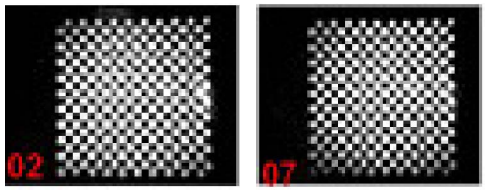


Fig. 8. (Color online) SNR of retrieved images for the security collinear holographic storage system.



(a) (b)

Fig. 9. (Color online) (a), (b) Retrieved images of nonencryption storage implemented with the same system.

cannot be removed from the system without destruction. Holographic nonsecurity memory generated in an arbitrarily recording system can be used as a removable memory. Stored data in holographic nonsecurity memory can be easily retrieved in another system because only spherical reference wave is required for the readout. Contrary to nonsecurity memory, the readout of holographic security memory generated by an arbitrary recording system in another system is impossible because lack of the original encryption key to decrypt the security information. Encrypted holographic memory only can be accessed in the original recording system. Accordingly, each system can generate its own encrypted memory and therefore offers high security for content protection.

In our demonstration of nonsecurity storage, the shift selectivity of shift-multiplexed holographic storage without using a MD in this system is 6 μm and 90 μm in x and y directions, respectively. However, we have noticed the shifting selectivity in horizontal and vertical directions for nonsecurity storage are quiet different for this conventional shift-multiplexed holograms owing to the Bragg degeneration in the vertical direction [6,21,26,27]. Accordingly, 15 image pages were recorded within this material with 3 rows. Each row contained 5 holograms, and these 5 holograms were partially spatially overlapped, but the shift separation of each adjacent hologram was 6 μm. In addition, the shift separation of each adjacent row was 90 μm. After the recording in the first row was completed, we repeated the row recording process described above until all 15 holograms were stored within these 3 rows. Figures 9(a) and (b) are the retrieved images of the nonencryption storage. The average SNR value of 15 pages data of retrieved images was about 4.2.

6. Conclusion

In this paper, we have proposed a holographic security storage system by using a shift multiplexing technique. A MD played an important role in encryption and decryption of holographic storage and reconstruction. Shift selectivity of the proposed security holographic storage system was analyzed. The experiments demonstrate a security holographic storage of 100 holograms within this system, and the storage capacity and the average SNR value of the presented security collinear holographic storage system were 16 bits/μm^2 and 3.5, respectively. Selective encryption storage also can be achieved by moving the MD into the reference arm or moving it away during the recording process. Nonsecurity holographic storage using the same system was also presented.

This work was supported by the National Science Council of Taiwan under contract no. NSC 97-2221-E-108-002-MY3

Reference

1. H. J. Caulfield, D. Psaltis, and G. Sincerbox, *Holographic Data Storage* (Springer-Verlag, 2000).
2. S. S. Orlov, W. Phillips, E. Bjornson, Y. Takashima, P. Sundaram, L. Hesselink, R. Okas, D. Kwan, and R. Snyder, "High-transfer-rate high-capacity holographic disk data-storage system," Appl. Opt. **43**, 4902–4914 (2004).
3. G. W. Burr, C. M. Jefferson, H. Coufal, M. Jurich, J. A. Hoffnagle, R. M. Macfarlane, and R. M. Shelby, "Volume holographic data storage at an areal density of 250 gigapixels/in.^{2}," Opt. Lett. **26**, 444–446 (2001).
4. H. Horimai, X. Tan, and J. Li, "Collinear holography," Appl. Opt. **44**, 2575–2579 (2005).
5. T. Shimura, S. Ichimura, R. Fujimura, K. Kuroda, X. D. Tan, and H. Horimai, "Analysis of a collinear holographic storage system: introduction of pixel spread function," Opt. Lett. **31**, 1208–1210 (2006).
6. C. C. Sun and W. C. Su, "Three-dimensional shifting selectively of random phase encoding in volume holograms," Appl. Opt. **40**, 1253–1260 (2001).
7. C. Denz, K.-O. Muller, F. Visinka, and T. Tschudi, "Digital volume holographic data storage using phase-coded holographic memory system," Proc. SPIE **3802**, 142–147 (1999).
8. J. F. Heanue, M. C. Bashaw, and L. Hesselink, "Encrypted holographic data storage based on orthogonal-phase-code multiplexing," Appl. Opt. **34**, 6012–6015 (1995).
9. W. C. Su and C. H. Lin, "Three-dimensional shifting selectivity of decryption phase mask in double random phase encoding holographic memory," Opt. Commun. **241**, 29–41 (2004).
10. O. Matoba and B. Javidi, "Encrypted optical memory system using three-dimentional keys in the Fresnel domain," Opt. Lett. **24**, 762–764 (1999).
11. O. Matoba and B. Javidi, "Encrypted optical storage with angular multiplexing," Appl. Opt. **38**, 7288–7293 (1999).
12. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption system that uses phase conjugation in a photorefractive crystal," Appl. Opt. **37**, 8181–8186 (1998).
13. O. Matoba, Y. Yokohama, M. Miura, K. Nitta, and T. Yoshimura, "Reflection-type holographic disk memory with random phase shift multiplexing," Appl. Opt. **45**, 3270–3274 (2006).
14. 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**, 1728–1733 (2004).
15. Y. Takeda, Y. Oshida, and Y. Miyamura, "Random phase shifters for Fourier transformed holograms," Appl. Opt. **11**, 818–822 (1972).
16. C. B. Burckhardt, "Use of a random phase mask for the recording of Fourier transform holograms of data masks," Appl. Opt. **9**, 695–700 (1970).
17. O. Matoba and B. Javidi, "Secure holographic memory by double-random polarization encryption," Appl. Opt. **43**, 2915–2919 (2004).
18. M. Yamazaki and J. Ohtsubo, "Optimization of encrypted holograms in optical security systems," Opt. Eng. **40**, 132–137 (2001).
19. G. J. Steckman, A. Pu, and D. Psaltis, "Storage density of shift-multiplexed holographic memory," Appl. Opt. **40**, 3387–3394 (2001).
20. C. C. Sun, W. C. Su, B. Wang, and A. E. T. Chiou, "Lateral shifting sensitivity of a ground glass for holographic encryption

and multiplexing using phase conjugate readout algorithm," Opt. Commun. **191**, 209–224 (2001).
21. W. C. Su and C. C. Sun, "Encryption-selectable holographic storage in $LiNbO_3$ with angle multiplexing," Microw. Opt. Technol. Lett. **42**, 227–230 (2004).
22. S. H. Lin, K. Y. Hsu, W. Z. Chen, and W. T. Whang, "Experimental characterization of phenanthrenequinone-doped poly (methyl methacrylate) photopolymer for volume holographic storage," Opt. Eng. **42**, 1390–1396 (2003).
23. C. C. Sun, "A simplified model for diffraction analysis of volume holograms," Opt. Eng. **42**, 1184–1185 (2003).
24. G. Barbastathis, M. Levene, and D. Psaltis, "Shift multiplexing with spherical reference waves," Appl. Opt. **35**, 2403–2417 (1996).
25. C. Moser and D. Psaltis, "Holographic memory with localized recording," Appl. Opt. **40**, 3909–3914 (2001).
26. C. C. Sun, M. S. Tsaur, W. C. Su, B. Wang, and E. T. Chiou, "Two-dimensional shifting tolerance of a volume-holographic correlator," Appl. Opt. **38**, 4316–4324 (1999).
27. C. C. Sun, W. C. Su, B. Wang, and Y. OuYang, "Diffraction selectivity of holograms with random phase encoding," Opt. Commun. **175**, 67–74 (2000).