Research Article | Vol. 27, No. 16 | 5 Aug 2019 | OPTICS EXPRESS 22147
Optics EXPRESS

Secure storage and retrieval schemes for multiple encrypted digital holograms with orthogonal phase encoding multiplexing

YOUHYUN KIM, MINWOO SIM, AND INKYU MOON*

Department of Robotics Engineering, Daegu Gyeongbuk Institute of Science & Technology, Dalseong-gun, Daegu, 42988, South Korea
**inkyu.moon@dgist.ac.kr*

Abstract: Recent developments in 3D computational optical imaging such as digital holographic microscopy has ushered in a new era for biological research. Therefore, efficient and secure storage and retrieval of digital holograms is a challenging task for future cloud computing services. In this study, we propose a novel scheme to securely store and retrieve multiple encrypted digital holograms by using phase encoding multiplexing. In the proposed schemes, an encrypted hologram can only be accessed using a binary phase mask, which is the key to retrieve the image. In addition, it is possible to independently store, retrieve, and manage the encrypted digital holograms without affecting other groups of the encrypted holograms multiplexed using different sets of binary phase masks, due to the orthogonality properties of the Hadamard matrices with high autocorrelation and low cross-correlation. The desired encrypted holograms may also be searched for, removed, and added independently of other groups of the encrypted holograms. More and more 3D images or digital holograms can be securely and efficiently stored, retrieved, and managed.

1. Introduction

Cloud computing has emerged as a new computing paradigm for hosting and delivering various types of applications services over the Internet. Specifically, the cloud-based outsourced data storage and retrieval service is one of the most cloud computing applications [1–3]. Therefore, to protect clouds, providers must securely and efficiently store and retrieve cloud data. Over the past decades, optical image encryption techniques have played an important role in the area of the information security due to the advantage of their multiple parameters and high-speed parallel processing [4–6]. One of the most well-known encryption techniques is double random phase encoding (DRPE), which was introduced by Réfrégier and Javidi [7]. The technique allows one to encode an image into stationary white noise using two random phase-only masks (RPMs) in the input and Fourier planes of an optical 4-*f* system. Various encryption schemes and applications have been proposed, which are based on the fractional Fourier transform (FRT), Fresnel transform (FrT), phase-truncated Fourier transforms (PTFT), digital holography, interference, gyrator transform (GT), and other methods [8–18].

The amplitude and phase information of an object can be computed numerically in the form of a complex image using digital holographic techniques [19,20]. Digital holography techniques can be used to realize objects in three dimensions in virtual reality. Many fields, including biomedicine and public health care, deal with important personal information such as three-dimensional (3D) images (or holograms) of samples, such as red blood cells. Vast amounts of 3D images must be securely and efficiently protected as personal information. Therefore, it is necessary to develop a security system that can be used to store and retrieve the encrypted 3D images.

Situ and Zhang introduced multiple-image encryption using wavelength multiplexing [21]. Since then, optical multiple-image cryptosystems have attracted more and more

#367595 https://doi.org/10.1364/OE.27.022147
Journal © 2019 Received 16 May 2019; revised 30 Jun 2019; accepted 10 Jul 2019; published 22 Jul 2019

Optics EXPRESS

attention due to the improvement of encryption capacity, the facilitation of transmission, and efficient storage of mass information [22–29]. Several multiple-image encryption systems have a disadvantage in that there is crosstalk noise between images, or a time-consuming iterative process is required due to the use of the phase-retrieval algorithm. However, the phase encoding multiplexing technique [30–33] can efficiently multiplex multiple images by using Hadamard codes, which have the property of high autocorrelation and low cross-correlation.

We present a new scheme to securely store and retrieve multiple encrypted digital holograms by using orthogonal phase encoding multiplexing. Multiple digital holograms are filtered by applying digitally defined filter masks in the spatial spectrum domain to enhance the image quality and then encrypted by using DRPE. They are phase encoded and superimposed using sets of binary phase masks (BPMs), which are generated from Hadamard matrices. Many groups of encrypted digital holograms may be independently phase encoded and multiplexed by using many different sets of BPMs. More and more digital hologram or 3D images can be securely and efficiently stored, retrieved, and managed. The validity of the proposed scheme is verified by numerical simulations.

2. Storage and retrieval schemes for multiple encrypted 3D images

Off-axis digital holography (DH), which is based on a Mach-Zehnder interferometer as shown in Fig. 1, is used to acquire digital holograms for 3D image reconstruction. In the off-axis configuration, the coherent laser source is divided into an object (***O***) and a reference waves (***R***) using the beam splitter. The object wave illuminates the sample such as red blood cells and creates object wave front. The microscope objective (MO) collects and magnifies the object wave front. A detector such as a CCD camera records the hologram generated by the interference of the object wave and the reference wave, which is incident at a small angle (θ) with respect to the object wave, as shown in the inset of Fig. 1. The recorded holograms are sent to the PC for filtering, encrypting and multiplexing, and reconstruction of the phase contrast image.

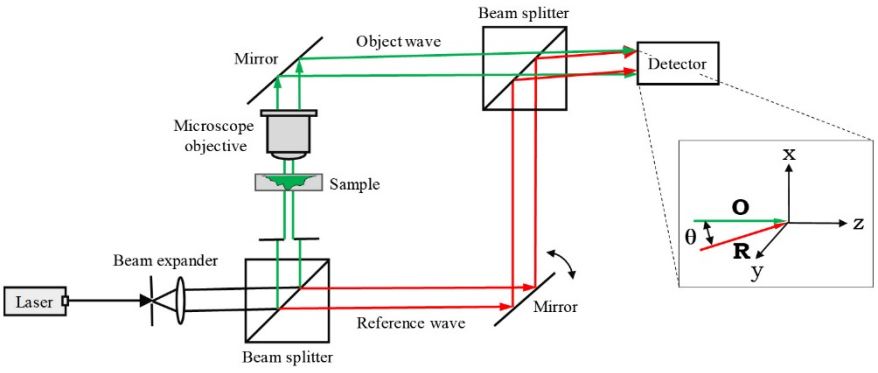

Fig. 1. Off-axis configuration in digital holography microscopy.

Figure 2(a) shows a hologram of 3D objects that are recorded using the off-axis DH, which is given by

$$I_H(x,y) = |\mathbf{R}|^2 + |\mathbf{O}|^2 + \mathbf{R}^*\mathbf{O} + \mathbf{R}\mathbf{O}^*. \quad (1)$$

When the 3D image is reconstructed numerically on computer from the recorded digital hologram, the reconstructed image includes zero-order noise of diffraction (the first two terms in Eq. (1)) and the virtual image (or twin image) and the real image, which correspond to the third and fourth terms in Eq. (1), respectively [19,34].

Optics EXPRESS

We need to suppress the undesired data, i.e. zero-order noise and virtual image, by applying a digitally defined filter mask to a Fourier transform of the hologram in the spatial spectrum domain. This is shown in Fig. 2(c) and results in the filtered hologram, which is shown in Fig. 2(d) and represented by

$$I_R^F(x,y) = FT^{-1}\left\{SF \cdot FT\left[I_H(x,y)\right]\right\} = \mathbf{RO}^*, \tag{2}$$

where FT and FT^{-1} are the Fourier and inverse Fourier transforms, respectively, and SF denotes spatial filtering in the Fourier domain. A non-circular shaped SF, as shown in Fig. 2(c), is used to filter only the first-order spatial spectral component of a hologram while removing the second-order spectral component at the top right corner of Fig. 2(b). The center of the SF is not intentionally centered on the $\boldsymbol{RO}^*$ in order to filter the first-order spectrum as much as possible while minimizing the overlap of the first-order spectrum with the second-order spectrum and the zero-order noise.

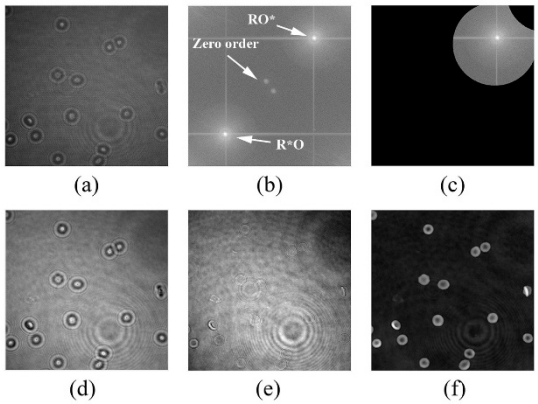

Fig. 2. Reconstruction of an off-axis hologram. (a) original hologram, (b) spatial spectrum of the hologram, (c) filtered spectrum of the hologram, (d) filtered hologram, (e) amplitude image, (f) phase contrast image.

The reconstruction of a hologram in the hologram plane is achieved by illuminating the hologram with a replica of the reference wave. The wave front of the reconstructed image is propagated toward the observation plane, in which the 3D image of the object can be observed. The digitally reconstructed image in the observation plane is computed by a numerical calculation of scalar diffraction in the Fresnel approximation, which is expressed as [19,34]

$$\begin{aligned}\boldsymbol{\Psi}(m,n) = A\,exp\left[\frac{i\pi}{\lambda d}\left(m^2\Delta\xi^2 + n^2\Delta\eta^2\right)\right] \\ \times FT\left\{\mathbf{R}_D(k,l)\,I_R^F(k,l)\,exp\left[\frac{i\pi}{\lambda d}\left(k^2\Delta x^2 + l^2\Delta y^2\right)\right]\right\},\end{aligned} \tag{3}$$

where $A = exp(i2\pi d/\lambda)/(i\lambda d)$ is a constant, d is the distance between both planes, λ is the wavelength of illumination light, m, n, k, and l are integers ($-N/2 \le m, n, k, l \le N/2$), and $N \times N$ is the number of pixels on the CCD camera. Δx and Δy are the sampling intervals in the hologram plane, $\Delta\xi = \lambda d/(N\Delta x)$ and $\Delta\eta = \lambda d/(N\Delta y)$ are the sampling intervals in the observation plane, and $\boldsymbol{R}_D$ is the digital reference wave:

$$\mathbf{R}_D(k,l) = A_R\,exp\left[i(2\pi/\lambda)\left(k_x k\Delta x + k_y l\Delta y\right)\right], \tag{4}$$

where k_x and k_y are two components of the wave vector, and A_R is the amplitude of the reference wave.

The intensity of the amplitude image can be computed by

$$I(m,n) = \mathrm{Im}\left[\Psi(m,n)\right]^2 + \mathrm{Re}\left[\Psi(m,n)\right]^2. \tag{5}$$

The phase contrast image is obtained by the argument of

$$\phi(m,n) = \tan^{-1}\left\{\frac{\mathrm{Im}\left[\Psi(m,n)\right]}{\mathrm{Re}\left[\Psi(m,n)\right]}\right\}. \tag{6}$$

The phase contrast image from the numerical reconstruction of the hologram, as shown in Fig. 2(f), can be used to calculate morphological properties such as thickness, surface area, and volume of samples such as red blood cells.

Figure 3 shows the schematics for encrypting and storing n digital holograms, which is based on DRPE and phase encoding multiplexing. In Fig. 3, the two-dimensional digital holograms are obtained by spatially filtering holograms from the DH, for example, Fig. 2(d). The digital holograms are phase modulated by the RPM[1]s, which are placed at the input plane and expressed by $exp[j\varphi^1(x, y)]$. x and y are space coordinates of a given pixel in the RPM[1]. The digital hologram is then Fourier transformed, which is expressed as

$$F_i(\xi,\eta) = FT\left[O_i(x,y)e^{j\varphi_i^1(x,y)}\right] \quad \text{for } i = 1, 2, \cdots, n, \tag{7}$$

where ξ and η are coordinates of a given pixel in the Fourier-transformed image and $O_i(x, y)$ is the amplitude information of the (x, y)th pixel in the ith hologram. $\varphi_i^1(x, y)$ is the random phase of the (x, y)th pixel in the RPM[1] applied to the ith hologram, which is in the range of $-\pi$ to π.

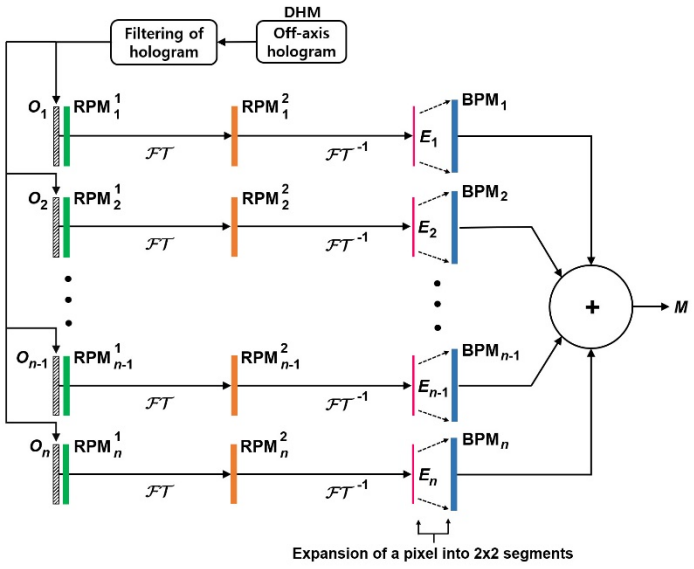

Fig. 3. Schematics for encrypting and multiplexing digital holograms using DRPE and phase encoding multiplexing. O is the filtered hologram, RPM denotes the random phase-only mask, BPM denotes the binary phase mask, FT and FT^{-1} are the Fourier and inverse Fourier transform operators, E is the encrypted hologram, and M is the multiplexed image.

Optics EXPRESS

The Fourier transformed image is phase modulated by the RPM^{2}s and then inverse Fourier transformed to obtain the encrypted hologram, which is expressed as

$$E_i(x,y) = FT^{-1}\left\{F_i(\xi,\eta)e^{j\varphi_i^2(\xi,\eta)}\right\} \quad \text{for } i = 1, 2, \cdots, n, \tag{8}$$

where $\varphi_i^2(\xi, \eta)$ denotes the random phase of the (ξ, η)th pixel in the ith RPM^2.

It is possible to superimpose multiple images using Hadamard codes, which have the property of high autocorrelation and low cross-correlation, to obtain a single multiplexed image. In general, an n-order Hadamard matrix is expressed as an $n \times n$ square matrix and its elements are either + 1 or −1, which can be generated by the Sylvester's construction such as

$$H_{1\times1} = 1,\ H_{2\times2} = \begin{bmatrix} H_{1\times1} & H_{1\times1} \\ H_{1\times1} & -H_{1\times1} \end{bmatrix},\ \cdots,\ H_{n\times n} = \begin{bmatrix} H_{(n/2)\times(n/2)} & H_{(n/2)\times(n/2)} \\ H_{(n/2)\times(n/2)} & -H_{(n/2)\times(n/2)} \end{bmatrix}, \tag{9}$$

where n is 2^k and k is the integer. Its rows, which correspond to Hadamard codes, are mutually orthogonal:

$$H^T H = nI, \tag{10}$$

where H^T is the transpose of the Hadamard matrix H, and I is the $n \times n$ identity matrix. The n-order Hadamard matrix must satisfy the orthogonality condition:

$$\sum_{j=1}^{n} h_{ij} h_{kj} = n\delta_{ik}, \tag{11}$$

where h_{ij} is the (i, j)th element of the Hadamard matrix H, and δ is the Kronecker delta function:

$$\delta_{ik} = \begin{cases} 1, & i = k \\ 0, & i \neq k. \end{cases} \tag{12}$$

We can multiplex encrypted holograms by using the phase encoding multiplexing, which utilize the orthogonality condition of Eq. (11). To do this, we first need to expand each pixel in the image into n (= $p \times q$) identical segments, where n is the number of bits in the Hadamard codes and p and q are integers. As an example, in the case of a 4-order Hadamard matrix, a Hadamard code have 4 bits. We expand each pixel in the first encrypted hologram, $E_1(x, y)$ into 2 × 2 identical segments for simplicity, as shown in Figs. 4(a) and 4(b), with the (x, y)th pixel in the hologram. Note that in Fig. 4, only the phase information of the (x, y)th pixel in the encrypted holograms is displayed. All four segments in the (x, y)th pixel have the same phase information as the (x, y)th original pixel, as shown in Fig. 4(b). The four elements in the first row of the Hadamard matrix, $H(x, y)$, map to 2 × 2 segments in the (x, y)th pixel of the mask, which is referred to as a 'binary phase mask (BPM)' [35].

The element 1 is expressed as $exp(j0)$ and corresponds to shifting the phase by 0 radians. Meanwhile, the element −1 is expressed as $exp(j\pi)$ and corresponds to shifting the phase by π radians. Thus, BPMs are binary phase representations of the Hadamard matrices. The four segments are separately phase shifted according to the four elements in the first row of the Hadamard matrix, $H(x, y)$, as shown in Fig. 4(c). Similarly, the other pixels in the first encrypted hologram are expanded and phase encoded but with the first rows of another Hadamard matrices, which are generated randomly by exchanging or negating rows and/or columns of the Hadamard matrix [35]. As a result, we can get the 1st phase-encoded image.

Optics EXPRESS

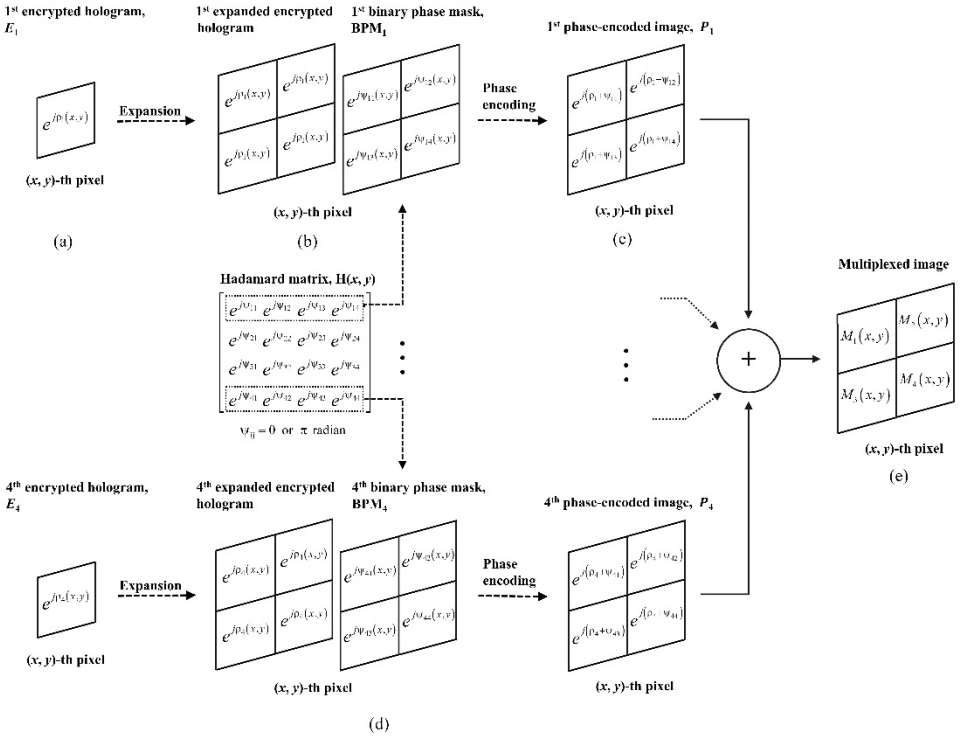

Fig. 4. Phase encoding and multiplexing of the (x, y)th pixel in encrypted holograms using phase-encoding multiplexing. (a)-(c) Phase encoding of the first encrypted hologram with the first row of the Hadamard matrix. (d) Phase encoding of the fourth encrypted hologram with the fourth row of the Hadamard matrix. (e) Multiplexing of four phase encoded images. ρ_i is the phase of a pixel in the ith encrypted hologram and ψ_{ij} denotes the phase (0 or π radian) of the (i, j)th element of the Hadamard matrix.

The filtered hologram (O_i) can be securely encoded because the phase distribution of Fourier-transformed image (F_i) is subjected to phase modulation by applying RPM in the Fourier domain using the DRPE. We can finally obtain four phase-encoded images by applying this procedure to the other holograms. The pixel in the 2nd, 3rd, and 4th phase-encoded images that is coincident with a pixel in the 1st phase-encoded image is expanded and then phase encoded with the 2nd, 3rd, and 4th rows of the same Hadamard matrix, respectively. The four holograms are phase encoded by applying the four BPMs, which are generated from four rows of the 4-order Hadamard matrices, respectively, and are called 'a set of four BPMs'. These four phase-encoded images are superimposed to get a single complex multiplexed image, as shown in Fig. 4(e).

As described above, similarly to the process of storing four encrypted holograms as a single multiplexed image, the n encrypted holograms can be stored as a single multiplexed image by using 'a set of n BPMs', which is generated from n-order Hadamard matrices. The multiplexed image can be expressed as

$$M(x,y) = H_{n\times n}^{T}\begin{bmatrix} e_1(x,y)e^{j\rho_1(x,y)} \\ e_2(x,y)e^{j\rho_2(x,y)} \\ e_3(x,y)e^{j\rho_3(x,y)} \\ \vdots \\ e_n(x,y)e^{j\rho_n(x,y)} \end{bmatrix}, \tag{13}$$

Optics EXPRESS

where (x, y) are coordinates of the (x, y)th pixel in the phase-encoded image, H^T is the transpose of the Hadamard matrix H, $e_i(x, y)$ and $\rho_i(x, y)$ are the amplitude and phase information of the (x, y)th pixel in the ith encrypted hologram, n is 2^k, and k is the integer.

The restoration is the reverse of the encryption and multiplexing process, as shown in Fig. 5. The BPM used for phase encoding an expanded encrypted hologram in the multiplexing process is applied to the multiplexed image to obtain the expanded encrypted hologram. Then, we convert n segments in the expanded hologram into one pixel to recover the original encrypted hologram. According to Eq. (10), the recovered encrypted hologram is expressed as

$$E(x,y)=\frac{1}{n}H_{n\times n}H_{n\times n}^{T}\begin{bmatrix} e_1(x,y)e^{j\rho_1(x,y)} \\ e_2(x,y)e^{j\rho_2(x,y)} \\ e_3(x,y)e^{j\rho_3(x,y)} \\ \vdots \\ e_n(x,y)e^{j\rho_n(x,y)} \end{bmatrix}. \quad (14)$$

The recovered encrypted hologram is phase modulated by applying the complex conjugate of the RPM^2 in the Fourier domain, inverse Fourier transformed, and then phase modulated by applying the complex conjugate of the RPM^1 to retrieve finally the desired hologram, which can be represented by

$$D_i'(x,y)=\left[e^{j\varphi_i^1(x,y)}\right]^{*} FT^{-1}\left\{\left[e^{j\varphi_i^2(\xi,\eta)}\right]^{*} FT\left[E(x,y)\right]\right\} \quad \text{for } i=1,2,\cdots,n, \quad (15)$$

where * is the complex conjugate operator.

When storing n digitally encrypted holograms as a single multiplexed image on a page basis, 'a set of n BPMs' can be used as a multiplexing code. By doing so, it is possible not only to efficiently store and manage many encrypted holograms but also to search for.

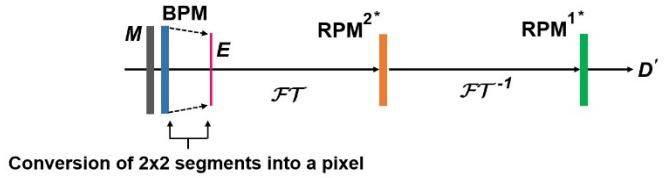

Fig. 5. Schematics for the restoration of digital holograms. M is the multiplexed image, FT and FT^{-1} are the Fourier and the inverse Fourier transform operators, E is the recovered encrypted hologram, D' is the decrypted hologram, and * is the complex conjugate operator.

3. Numerical simulations

Figure 6 shows the filtered holograms obtained by filtering four holograms, which are recorded using the off-axis DHM in Fig. 1. In our configuration, the wavelength of the coherent laser source is 666 nm. The magnification factor for microscope is 40 × /0.75NA. The angle θ between the object wave and the reference wave that are incident on the detector is about 3.26 degrees. We use these filtered holograms with the size of 1024 × 1024 pixels for numerical simulations to verify the feasibility of the proposed scheme. A set of four BPMs is applied to four encrypted holograms to obtain a single multiplexed image, which are shown in Fig. 7.

Optics EXPRESS

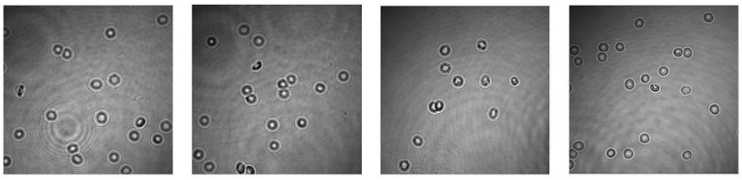

Fig. 6. Four digital holograms used in numerical simulations for the proposed scheme.

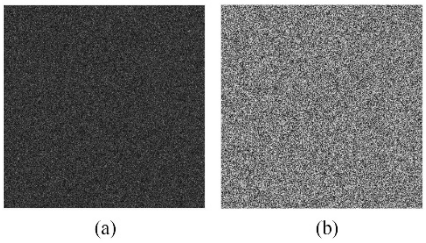

Fig. 7. (a) Amplitude and (b) phase distributions of the multiplexed image.

We calculate the correlation coefficient (CC) between the decrypted hologram and the original hologram to objectively evaluate the correlation between two holograms, which is defined as

$$CC = \frac{cov(D, O)}{\sigma(D)\sigma(O)}, \tag{16}$$

where $cov(D, O)$ is the cross covariance between the decrypted hologram and the original hologram, and $\sigma(D)$ and $\sigma(O)$ are the standard deviations for both holograms.

In the decryption process, we first extract the four encrypted holograms from the multiplexed image by applying the same BPMs that were used in the phase encoding and multiplexing process. Then, we can restore four original holograms by applying the RPM^2s to those encrypted holograms in Fourier domain and then inverse Fourier transforming those images, respectively. In our simulations, we can successfully restore four holograms using correct BPMs and correct RPMs, as shown in Figs. 8(a)-8(d), where the CC values are 1. Figures 8(e)-8(h) shows four holograms decrypted using the correct RPMs but the wrong BPMs. Their CC values were 0.001645, 0.001097, –0.0008185, and 0.0005702, respectively. These values are so small that there is no way to find out any information about the holograms.

Next, we first encrypt 16 holograms, which are shown in Fig. 9, separately by using DRPE and divide them into four groups of four encrypted holograms. We can phase encode and superimpose them by separately applying different four sets of four BPMs, and then obtain four multiplexed images, as shown in Fig. 10. For example, Figs. 10(a) and 10(e) are the amplitude and phase distributions of the multiplexed image from group I, which is shown in Figs. 9(a)-9(d). This multiplexed image is obtained by phase encoding and superimposing four encrypted holograms of group I by applying the first set of four BPMs.

Optics EXPRESS

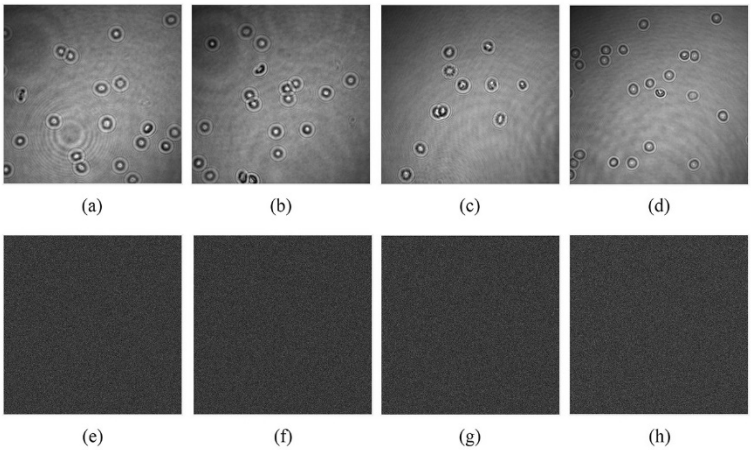

Fig. 8. (a)-(d) Four holograms decrypted by using the correct BPMs and the correct RPMs. (e)-(h) Four holograms decrypted by using the correct RPMs but wrong BPMs.

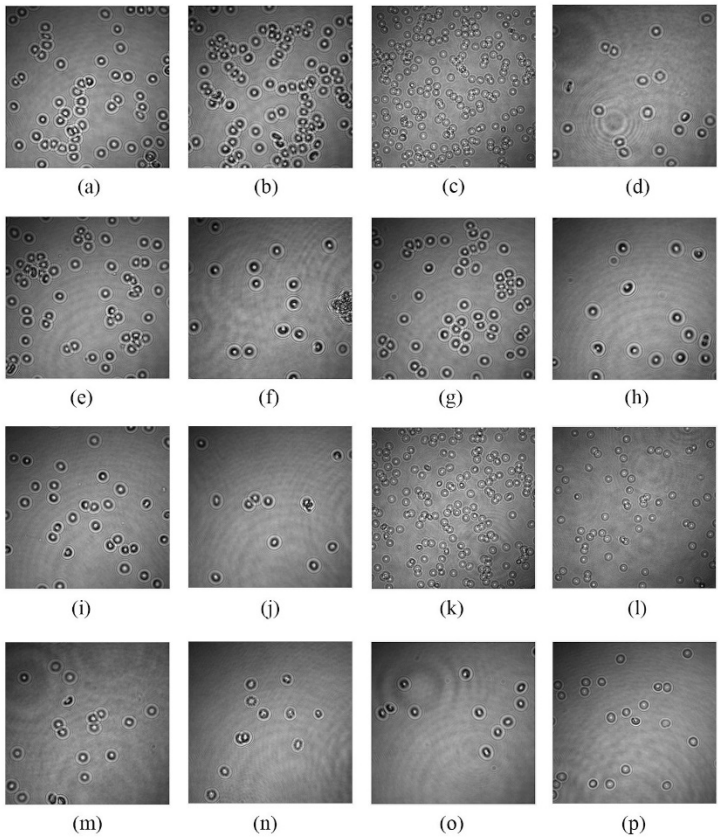

Fig. 9. 16 digital holograms (four groups of four holograms) used in numerical simulations. (a)-(d) Group I, (e)-(h) group II, (i)-(l) group III, (m)-(p) group IV.

Optics EXPRESS

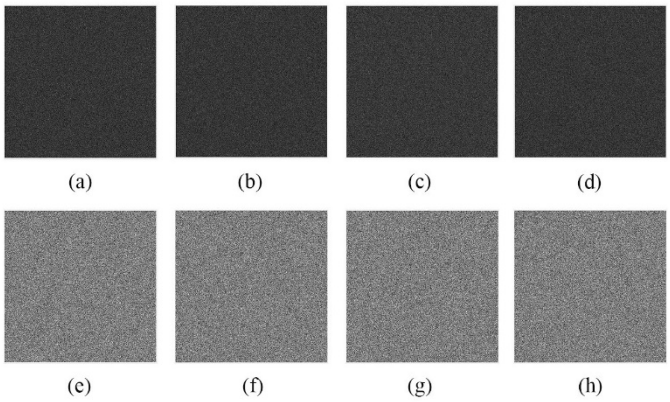

Fig. 10. Four multiplexed images obtained from four groups of four encrypted holograms. (a)-(d) Amplitude distributions, (e)-(h) phase distributions; (a) and (e) the multiplexed image from group I, (b) and (f) the multiplexed image from group II, (c) and (g) the multiplexed image from group III, (d) and (h) the multiplexed image from group IV.

Figures 11(a)-11(d) show four holograms restored by applying the 2nd BPM to the four multiplexed images in Fig. 10. Similarly, when applying the 8th, 9th, and 15th BPM to the four multiplexed images, we can obtain the decrypted holograms, which are shown in Figs. 11(e)-11(h), Figs. 11(i)-11(l), and Figs. 11(m)-11(p), respectively. The calculated CCs are given in Table 1. The amplitude and phase contrast images of the 2nd, 8th, 9th, and 15th decrypted holograms are shown in Fig. 12. When the BPM used for phase encoding a hologram in the multiplexing process is applied to the multiplexed image, containing the hologram, the desired hologram is retrieved successfully according to the orthogonality condition. However, when applied to other multiplexed images, the desired holograms are not restored, and the absolute values of their CCs are very small (less than 0.05). These results confirm that there is very low probability of the orthogonality condition between different sets of four BPMs being satisfied. This means that different sets of BPMs can be used and managed independently of each other.

The results of numerical simulations confirm that when encrypting many groups of 3D images or digital holograms, they can be multiplexed independently using many different sets of BPMs without affecting other groups of 3D images. These simulation results show that a hologram or a 3D image can be removed or added, independently of the other groups of four images on a cloud system or database. When an image is desired to be deleted, the multiplexed image containing the image is first unwound, the image is removed, and the remaining images are multiplexed and stored again using the same set of four BPMs. When adding a new 3D image, it is inserted into the multiplexed image that contains three or fewer images or it is multiplexed and stored using a new set of four BPMs, which are generated independently of other sets of four BPMs. Of course, the orthogonality condition must always be satisfied between different sets of four BPMs. More and more 3D images or digital holograms can be efficiently stored, retrieved, and managed by using larger order Hadamard matrices.

Table 1. The correlation coefficients between original holograms and decrypted holograms.

	Multiplexed image I	Multiplexed image II	Multiplexed image III	Multiplexed image IV
2nd BPM	1.0000	–0.0009255	–0.001300	–0.0005477
8th BPM	0.0009955	1.0000	0.0008860	–0.001170
9th BPM	0.0007401	–0.002232	1.0000	–0.001916
15th BPM	0.0003019	–0.00008838	0.0001371	1.0000

Optics EXPRESS

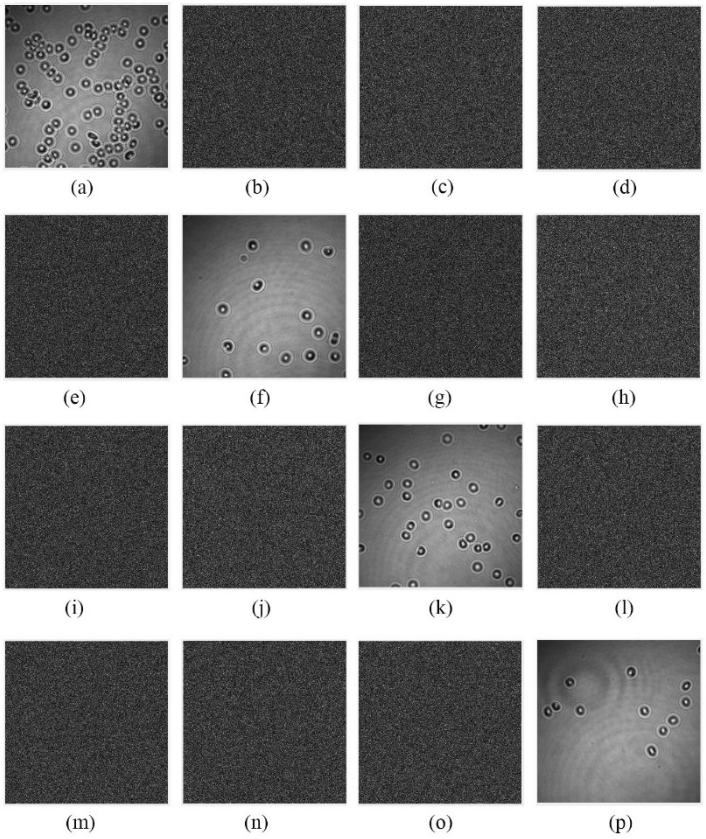

Fig. 11. Decrypted holograms obtained from four multiplexed images in Fig. 10. (a)-(d) Holograms decrypted by the 2nd BPM, (e)-(h) holograms decrypted by the 8th BPM, (i)-(l) holograms decrypted by the 9th BPM, (m)-(p) holograms decrypted by the 15th BPM.

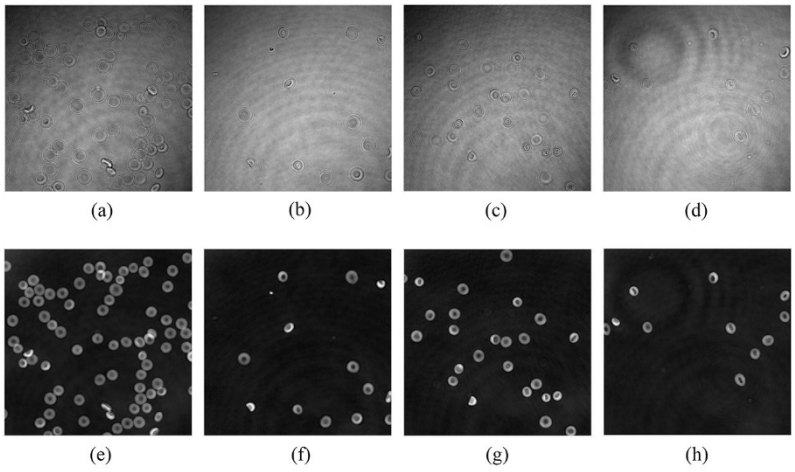

Fig. 12. Amplitude and phase contrast images of correct decrypted holograms in Fig. 11. (a)-(d) Amplitude images, (e)-(h) phase contrast images; (a) and (e) for the 2nd decrypted hologram, (b) and (f) for the 8th decrypted hologram, (c) and (g) for the 9th decrypted hologram, (d) and (h) for the 15th decrypted hologram.

Optics EXPRESS

Figure 13 shows the CCs for decrypted holograms according to the ratio of correct Hadamard matrices in the BPMs. When the hologram is restored using the BPM with 50% correct Hadamard matrices, the CC value for the decrypted hologram is approximately 0.12, as shown in Fig. 13. This result means that it would be difficult for an attacker to obtain the desired hologram completely from the multiplexed image, even after correctly finding out the phase information of 50% of the pixels in the BPMs.

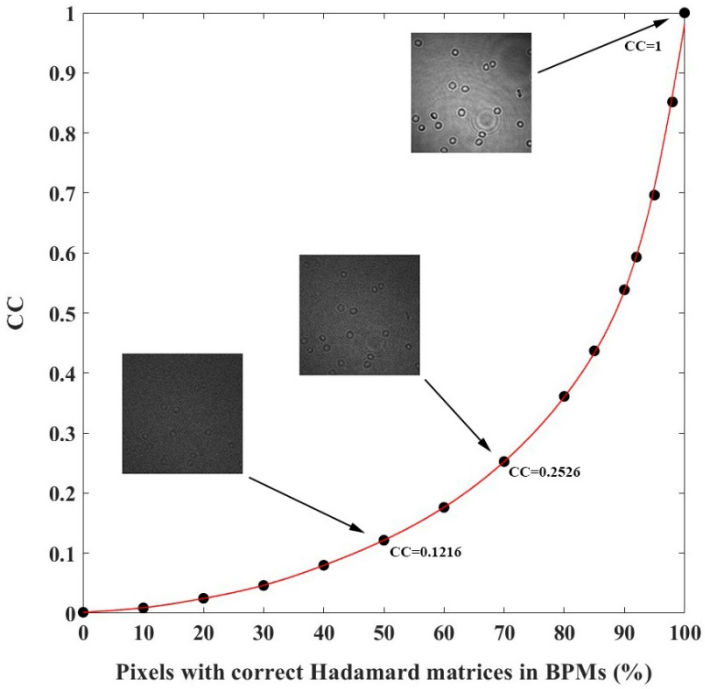

Fig. 13. Correction coefficients of the decrypted hologram according to the ratio of correct Hadamard matrices in BPMs.

4. Conclusion

We have presented a new scheme to store and retrieve multiple digital holograms or 3D images securely and effectively using DRPE and phase encoding multiplexing. The zero-order noise and virtual image of the off-axis hologram of 3D objects are suppressed by applying a digitally defined filter mask in spatial spectrum domain to enhance the image quality. Four digital holograms are encrypted separately by using DRPE, and then phase encoded and multiplexed using a set of four BPMs. When the holograms are restored using incorrect BPMs or incorrect RPMs, the absolute values of their CCs are very small (less than 0.05), which indicates that there is no way to find out any information about the original holograms.

When the digital hologram is restored by applying the BPMs with less than 50% of the correct phases of pixels, the absolute CC value of the decrypted digital hologram is less than 0.15. When encrypting many groups of 3D images or digital holograms, they are multiplexed independently using many different sets of BPMs without affecting other groups of 3D images. It is possible to efficiently store, retrieve, and manage more and more 3D images using larger order Hadamard matrices. It can be also possible to search for, remove, and add desired images on a cloud system or database.

Funding

Research Foundation of Korea (NRF) (NRF-2019R1F1A1055568).

Optics EXPRESS

References

1. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security **11**(11), 2594–2608 (2016).
2. Z. Xia, Y. Zhu, X. Sun, Z. Qin, and K. Ren, "Towards privacy-preserving content-based image retrieval in cloud computing," IEEE Trans. Cloud Comput. **6**(1), 276–286 (2018).
3. N. Wang, J. Fu, B. K. Bhargava, and J. Zeng, "Efficient retrieval over documents encrypted by attributes in cloud computing," IEEE Trans. Inf. Forensics Security **13**(10), 2653–2667 (2018).
4. B. Javidi and J. L. Horner, "Optical pattern recognition for validation and security verification," Opt. Eng. **33**(6), 1752–1756 (1994).
5. O. Matoba, T. Nomura, E. Pérez-Cabré, M. S. Millan, and B. Javidi, "Optical techniques for information security," Proc. IEEE **97**(6), 1128–1148 (2009).
6. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photonics **6**(2), 120–155 (2014).
7. P. Réfrégier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**(7), 767–769 (1995).
8. G. Unnikrishnan, J. Joseph, and K. Singh, "Optical encryption by double-random phase encoding in the fractional Fourier domain," Opt. Lett. **25**(12), 887–889 (2000).
9. B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," Opt. Lett. **28**(4), 269–271 (2003).
10. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**(14), 1584–1586 (2004).
11. I. Moon, F. Yi, Y. H. Lee, and B. Javidi, "Avalanche and bit independence characteristics of double random phase encoding in the Fourier and Fresnel domains," J. Opt. Soc. Am. A **31**(5), 1104–1111 (2014).
12. W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," Opt. Lett. **35**(2), 118–120 (2010).
13. B. Javidi and T. Nomura, "Securing information by use of digital holography," Opt. Lett. **25**(1), 28–30 (2000).
14. I. Mehra, K. Singh, A. K. Agarwal, U. Gopinathan, and N. K. Nishchal, "Encrypting digital hologram of three-dimensional object using diffractive imaging," J. Opt. **17**(3), 035707 (2015).
15. N. K. Nishchal and T. J. Naughton, "Flexible optical encryption with multiple users and multiple security levels," Opt. Commun. **284**(3), 735–739 (2011).
16. Y. Zhang and B. Wang, "Optical image encryption based on interference," Opt. Lett. **33**(21), 2443–2445 (2008).
17. X. Wang and D. Zhao, "Image encoding based on coherent superposition and basic vector operations," Opt. Commun. **284**(4), 945–951 (2011).
18. J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Applications of gyrator transform for image processing," Opt. Commun. **278**(2), 279–284 (2007).
19. E. Cuche, F. Bevilacqua, and C. Depeursinge, "Digital holography for quantitative phase-contrast imaging," Opt. Lett. **24**(5), 291–293 (1999).
20. U. Schnars and W. P. O. Jüptner, "Digital recording and numerical reconstruction of holograms," Meas. Sci. Technol. **13**(9), R85–R101 (2002).
21. G. Situ and J. Zhang, "Multiple-image encryption by wavelength multiplexing," Opt. Lett. **30**(11), 1306–1308 (2005).
22. G. Situ and J. Zhang, "Position multiplexing for multiple-image encryption," J. Opt. A, Pure Appl. Opt. **8**(5), 391–397 (2006).
23. M. Z. He, L. Z. Cai, Q. Liu, X. C. Wang, and X. F. Meng, "Multiple image encryption and watermarking by random phase matching," Opt. Commun. **247**(1-3), 29–37 (2005).
24. A. Alfalou and A. Mansour, "Double random phase encryption scheme to multiplex and simultaneous encode multiple images," Appl. Opt. **48**(31), 5933–5947 (2009).
25. H. E. Hwang, H. T. Chang, and W. N. Lie, "Multiple-image encryption and multiplexing using a modified Gerchberg-Saxton algorithm and phase modulation in Fresnel-transform domain," Opt. Lett. **34**(24), 3917–3919 (2009).
26. Y. Shi, G. Situ, and J. Zhang, "Multiple-image hiding in the Fresnel domain," Opt. Lett. **32**(13), 1914–1916 (2007).
27. X. Wang and D. Zhao, "Fully phase multiple-image encryption based on superposition principle and the digital holographic technique," Opt. Commun. **285**(21-22), 4280–4284 (2012).
28. Q. Wang, Q. Guo, L. Lei, and J. Zhou, "Multiple-image encryption based on interference principle and phase-only mask multiplexing in Fresnel transform domain," Appl. Opt. **52**(28), 6849–6857 (2013).
29. M. R. Abuturab, "Optical interference-based multiple-image encryption using spherical wave illumination and gyrator transform," Appl. Opt. **53**(29), 6719–6728 (2014).
30. C. Denz, G. Pauliat, G. Roosen, and T. Tschudi, "Volume hologram multiplexing using a deterministic phase encoding method," Opt. Commun. **85**(2-3), 171–176 (1991).
31. J. Lembcke, C. Denz, and T. Tschudi, "General formalism for angular and phase-encoding multiplexing in holographic image storage," Opt. Mater. **4**(2-3), 428–432 (1995).

Optics EXPRESS

32. C. Denz, K.-O. Müller, T. Heimann, and T. Tschudi, "Volume holographic storage demonstrator based on phase-coded multiplexing," IEEE J. Sel. Top. Quantum Electron. **4**(5), 832–839 (1998).
33. H. Kim and Y. H. Lee, "Cross talk between holograms of finite contrast in a phase-code multiplexing system," Opt. Lett. **29**(1), 113–115 (2004).
34. E. Cuche, P. Marquet, and C. Depeursinge, "Spatial filtering for zero-order and twin-image elimination in digital off-axis holography," Appl. Opt. **39**(23), 4070–4075 (2000).
35. Y. Kim, J. Song, I. Moon, and Y. Lee, "Interference-based multiple-image encryption using binary phase masks," Opt. Lasers Eng. **107**, 281–287 (2018).