Computer-generated hologram marked by correlated photon imaging

WEN CHEN[1,2,*]

[1]The Hong Kong Polytechnic University Shenzhen Research Institute, Shenzhen 518057, China
[2]Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong, China
*Corresponding author: owen.chen@polyu.edu.hk

Received XX Month XXXX; revised XX Month, XXXX; accepted XX Month XXXX; posted XX Month XXXX (Doc. ID XXXXX); published XX Month XXXX

Computer-generated hologram (CGH) has been studied for many applications. In this paper, CGH is watermarked by correlated photon imaging. An input image is encoded into two cascaded phase-only masks by using CGH principle. Subsequently, two different marks are independently encoded into one-dimensional (1D) intensity points by using correlated photon imaging (or ghost imaging), and the recorded 1D intensity points are embedded into the extracted phase masks for optical watermarking. During the decoding, the input is recovered by using two watermarked phase masks. To verify copyright of the recovered input image, information embedded in two phase-only masks is retrieved, and is used to decode the hidden marks. The decoded marks do not visually render clear information due to only a few measurements, and instead are authenticated. It is illustrated that quality of the recovered input image is high, and a different imaging approach can be applied in CGH system for optical watermarking. The proposed approach provides a promising strategy for optical information security. © 2018 Optical Society of America

OCIS codes: *(200.4560) Optical data processing; (200.4740) Optical processing.*

http://dx.doi.org/10.1364/AO.99.099999

1. INTRODUCTION

Optical technologies [1–8], such as ghost imaging and integral imaging, have been studied for various applications, such as security and display. To facilitate optical implementation, computer-generated hologram (CGH) [9–12], has been applied as a promising alternative. There are several approaches [9–12] to generate CGH. In addition, Gerchberg-Saxton algorithm [13] is also applied or modified to generate phase-only masks, and Fienup [14] proposed several iterative algorithms using finite support and non-negativity constraint to extract phase patterns.

The CGH principles have also been applied to generate phase patterns as ciphertexts for optical information security. Wang et al. [15] and Li et al. [16] studied CGH encryption. Chang et al. [17] presented an algorithm based on CGH to encode an input into several phase masks. Although CGH is used as a promising alternative for optical security, previous work focused on purely encoding algorithms. It is always desirable to achieve the higher security for CGH-secured system. To address the existing concern, Chen et al. [18] proposed a CGH system using sparse representation for securing information. However, the same CGH setup is applied to generate the watermark, and system flexibility is limited. In addition, quality of the recovered input image is highly influenced by watermark information, and the method [18] is more suitable for securing binary images.

In this paper, CGH is watermarked by correlated photon imaging. An input is encoded into phase masks by using CGH principle. Subsequently, two different marks are independently encoded into one-dimensional (1D) intensity points by using correlated photon imaging, and the recorded 1D intensity points are embedded into the extracted phase masks for optical watermarking. During the decoding, the input is recovered by using two watermarked phase masks. To verify copyright of the recovered input image, information embedded in two phase-only masks is retrieved, and is used to recover the hidden marks. The decoded marks do not visually render clear information, and instead are authenticated. It is computationally illustrated that quality of the recovered input image is high, and a different imaging approach can be flexibly applied in the CGH system for optical watermarking.

2. PRINCIPLES

Figure 1 shows a schematic for CGH-secured system. The light source can be collimated for the illumination, and an input is encoded into cascaded phase masks M1 and M2. Here, fractional Fourier transform (*FrFT*) [19] is employed as a typical example, and other transform domains [5] can also be applicable in the proposed method.

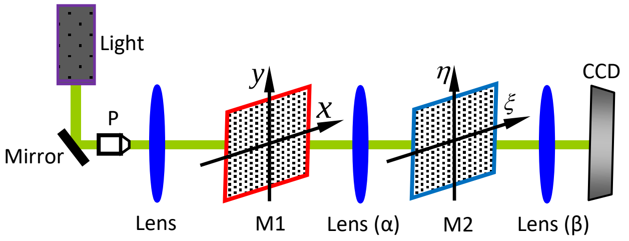

Fig. 1. A schematic for CGH-secured system [18]: M, phase mask; P, pinhole; CCD, charge-coupled device. Symbols α and β are *FrFT* function orders. In practice, the fractional order could be related to lens position and focal length [19]. Phase masks can be embedded into spatial light modulator (SLM) for optical decoding. Image "Peppers" (1024×1024 pixels) is employed as an input. The normalized input image is used, and all pixels' values of input image are divided by the maximum value of the input image.

The plane wave can be generated by using a pinhole and a lens for illumination in Fig. 1. Retrieval of M1 and M2 has been studied [5,13–18], and here the retrieval process is briefly described as follows:

(1) M1 and M2 are initialized in a range of $[0, 2\pi]$. Let $M_1^{(n)}(x,y)$ and $M_2^{(n)}(\xi,\eta)$ (integer *n*=1,2,3,...) respectively denote phase masks M1 and M2.

(2) Wave propagate to the input image plane:

$$O^{(n)}(\mu,\nu)=FrFT_{\beta,\beta}\left(\left\{FrFT_{\alpha,\alpha}\left[M_1^{(n)}(x,y)\right]\right\}M_2^{(n)}(\xi,\eta)\right). \qquad (1)$$

(3) Update M1 and M2 [5,13–18]:

$$\hat{O}^{(n)}(\mu,\nu)=\left[IP(\mu,\nu)\right]^{1/2}O^{(n)}(\mu,\nu)\Big/\left|O^{(n)}(\mu,\nu)\right|, \qquad (2)$$

$$\hat{M}_2^{(n)}(\xi,\eta)=\left\{\frac{FrFT_{-\beta,-\beta}\left[\hat{O}^{(n)}(\mu,\nu)\right]}{FrFT_{\alpha,\alpha}\left[M_1^{(n)}(x,y)\right]}\right\}\Bigg/\left|\frac{FrFT_{-\beta,-\beta}\left[\hat{O}^{(n)}(\mu,\nu)\right]}{FrFT_{\alpha,\alpha}\left[M_1^{(n)}(x,y)\right]}\right|, \qquad (3)$$

$$\hat{M}_1^{(n)}(x,y)=\frac{FrFT_{-\alpha,-\alpha}\left(\left\{FrFT_{-\beta,-\beta}\left[\hat{O}^{(n)}(\mu,\nu)\right]\right\}\left[\hat{M}_2^{(n)}(\xi,\eta)\right]^*\right)}{\left|FrFT_{-\alpha,-\alpha}\left(\left\{FrFT_{-\beta,-\beta}\left[\hat{O}^{(n)}(\mu,\nu)\right]\right\}\left[\hat{M}_2^{(n)}(\xi,\eta)\right]^*\right)\right|}, \qquad (4)$$

where asterisk denotes complex conjugate, $FrFT_{-\alpha,-\alpha}$ and $FrFT_{-\beta,-\beta}$ denote inverse *FrFT* [19], and $IP(\mu,\nu)$ denotes an input image. In this study, *FrFT* can be described by [19]

$$FrFT_{\alpha}\left[M_1(x)\right]=\int_{-\infty}^{+\infty}M_1(x)\rho_{\alpha}(\xi,x)\,dx, \qquad (5)$$

where

$$\rho_{\alpha}(\xi,x)=\begin{cases}\Re\exp\left\{j\pi\left[\xi^2\cot\left(\alpha\pi/2\right)+x^2\cot\left(\alpha\pi/2\right)\right.\right. & \\ \qquad\left.\left.-2\xi x\csc\left(\alpha\pi/2\right)\right]\right\} & \text{if } \alpha\neq 2m \\ \delta(\xi-x) & \text{if } \alpha=4m \\ \delta(\xi+x) & \text{if } \alpha=4m\pm 2\end{cases},$$

$j=\sqrt{-1}$, m denotes an integer, and $\Re=\sqrt{1-j\cot\left(\alpha\pi/2\right)}$.

The updated masks $\hat{M}_1^{(n)}(x,y)$ and $\hat{M}_2^{(n)}(\xi,\eta)$ are used to respectively replace $M_1^{(n)}(x,y)$ and $M_2^{(n)}(\xi,\eta)$ in Eq. (1), i.e., *n*=*n*+1. When a preset threshold is satisfied, phase-only masks M1 and M2 can be correspondingly determined and denoted as $M_1(x,y)$ and $M_2(\xi,\eta)$, respectively. In essence, the extracted masks M1 and M2 can be used as CGHs.

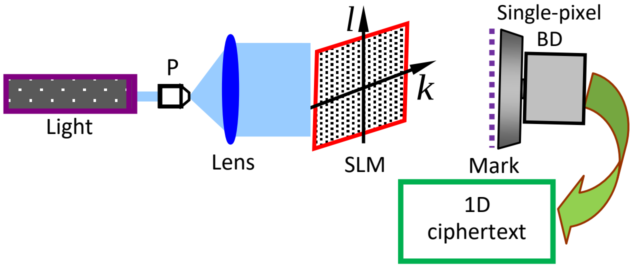

Fig. 2. A schematic for correlated photon imaging [7,20–22]: P, pinhole; BD, bucket detector. Images "Lena" and "Baboon" (64×64 pixels) are employed as watermarks. In practice, a collecting lens can be used. The normalized images are used.

In this study, two watermarks generated by using correlated photon imaging (or called ghost imaging [7,20–22]) are respectively embedded into the two extracted phase-only masks for copyright protection. When random phase masks $R_i(k,l)$ $(i=1,2,3...)$ are sequentially embedded into the SLM (see Fig. 2), 1D intensity points $\{B_i\}$ recorded by bucket detector can be described by

$$B_i=\iint\left|\left\{FrT_{d,\lambda}[R_i(k,l)]\right\}H(\mu,\nu)\right|^2d\mu d\nu, \qquad (6)$$

where $H(\mu,\nu)$ denotes a mark, *d* denotes the distance between the SLM and bucket detector, λ denotes the wavelength, and FrT denotes Fresnel transform [23]. Two different marks are sequentially encoded by using the setup in Fig. 2, and the same series of random phase masks $R_i(k,l)$ $(i=1,2,3...)$ is repeatedly applied. The recordings B_i are further converted into binary signals $\hat{B}_i$ (i.e., containing only 0 and 1) via the compression [7], and two series of 1D binary intensity points $\hat{B}_i^{(1)}$ and $\hat{B}_i^{(2)}$ can be correspondingly generated. Subsequently, new series of 1D intensity points $\hat{C}_i^{(1)}$ and $\hat{C}_i^{(2)}$ are respectively generated by

$$\hat{C}_i^{(1)}=\hat{A}_i^{(1)}+\hat{B}_i^{(1)}, \qquad (7)$$

$$\hat{C}_i^{(2)}=\hat{A}_i^{(2)}+\hat{B}_i^{(2)}, \qquad (8)$$

where $\hat{A}_i^{(1)}$ and $\hat{A}_i^{(2)}$ denote 1D maps randomly distributed within $[0,\ \pi]$. Finally, each point in the series $\hat{C}_i^{(1)}$, i.e., $\exp(j\hat{C}_i^{(1)})$, randomly replaces a pixel in the extracted phase mask $M_1(x,y)$, and the final phase mask M1 [i.e., $\bar{M}_1(x,y)$] can be correspondingly determined. Similarly, each point in the series $\hat{C}_i^{(2)}$, i.e., $\exp(j\hat{C}_i^{(2)})$, randomly replaces a pixel in $M_2(\xi,\eta)$, and the final phase mask M2 [i.e., $\bar{M}_2(\xi,\eta)$] can be correspondingly determined. In practice, two random-position replacement maps, i.e., binary maps $p_1(x,y)$ and $p_2(\xi,\eta)$, can be pre-generated as additional security keys to guide the pixel replacement process. A flow chart is given in Fig. 3.

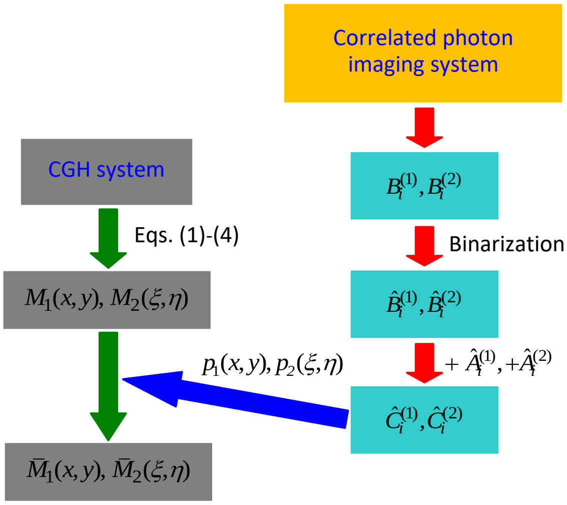
Correlated photon imaging system
CGH system
$B_i^{(1)}, B_i^{(2)}$
Eqs. (1)-(4)
Binarization
$M_1(x,y),\ M_2(\xi,\eta)$
$\hat{B}_i^{(1)}, \hat{B}_i^{(2)}$
$p_1(x,y),\ p_2(\xi,\eta)$
$+\ \hat{A}_i^{(1)}, +\hat{A}_i^{(2)}$
$\hat{C}_i^{(1)}, \hat{C}_i^{(2)}$
$\bar{M}_1(x,y),\ \bar{M}_2(\xi,\eta)$

Fig. 3. Flow chart for the optical encoding.

During optical decoding, input image is recovered by

$$IP'(\mu,\nu)=\left|FrFT_{\beta,\beta}\left(\left\{FrFT_{\alpha,\alpha}\left[\bar{M}_1(x,y)\right]\right\}\bar{M}_2(\xi,\eta)\right)\right|^2, \qquad (9)$$

where $IP'(\mu,\nu)$ denotes a recovered input.

To verify copyright of the recovered input image, information hidden in $\bar{M}_1(x,y)$ and $\bar{M}_2(\xi,\eta)$ is further extracted. When 1D random maps [i.e., $\hat{A}_i^{(1)}$ and $\hat{A}_i^{(2)}$] and random-position replacement maps [i.e., $p_1(x,y)$ and $p_2(\xi,\eta)$] are available to the authorized persons, two series of 1D binary intensity points $\hat{B}_i^{(1)}$ and $\hat{B}_i^{(2)}$ can be respectively extracted from M1 and M2 for mark decoding. Subsequently, when random phase masks $R_i(k,l)$ $(i=1,2,3...)$ are also available (such as by authorized persons), two marks can be recovered by using the correlation which is respectively described by [7,20,21]

$$H_1'(\mu,\nu)=\left\langle \hat{B}^{(1)}\,\mathrm{X}(\mu,\nu)\right\rangle-\left\langle \hat{B}^{(1)}\right\rangle\left\langle \mathrm{X}(\mu,\nu)\right\rangle, \qquad (10)$$

$$H_2'(\mu,\nu)=\left\langle \hat{B}^{(2)}\,\mathrm{X}(\mu,\nu)\right\rangle-\left\langle \hat{B}^{(2)}\right\rangle\left\langle \mathrm{X}(\mu,\nu)\right\rangle, \qquad (11)$$

where $H_1'(\mu,\nu)$ and $H_2'(\mu,\nu)$ denote the decoded marks, $\langle\ \rangle$ denotes ensemble average, and $X_i(\mu,\nu)$ denotes reference intensity patterns calculated by $\left|FrT_{d,\lambda}[R_i(k,l)]\right|^2$. Since only a few 1D binary intensity points are available for mark recovery in this study, the decoded marks do not render clear information. Here, information authentication is conducted by using nonlinear correlation [4,5,7,24–26] between the original mark and the recovered mark.

3. RESULTS AND DISCUSSION

Optical setups in Figs. 1 and 2 are numerically conducted to show validity of the proposed approach. In Figs. 1 and 2, wavelength of the plane wave is 600 nm. In practice, other wavelengths can also be applied for the proposed method. In CGH-secured system, an input "Peppers" with 1024×1024 pixels is encoded, and α and β are 0.35 and 0.75, respectively. In correlated photon imaging setup, the distance between the SLM and bucket detector is 13.0 cm, and the series of phase masks $R_i(k,l)$ $(i=1,2,3...)$ is randomly distributed in a range of $[0,\ 2\pi]$ which is sequentially embedded into a phase-only SLM (64×64 pixels and pixel size of 15 μm) for the encoding. In practice, other axial distances can also be applicable, and free-space wave propagation algorithm should be correspondingly applied [23]. Two marks "Lena" and "Baboon" with 64×64 pixels are encoded by using the correlated photon imaging setup in Fig. 2, and 1500 and 2000 measurements are respectively conducted to record 1D intensity points by using bucket detector. More measurements can be obtained to suppress speckle, however the retrieved watermarks may become visible. In this study, authentication of the retrieved watermarks is conducted instead of directly viewing their information. To recover the input image, CCD camera (pixel size of 15μm and 1024×1024 pixels) can be applied. In the designed setups, the parameters given here are used as a typical example, which can be flexibly designed and modified in practice. Due to the shortage of some experimental devices, virtual-optics concept and theoretical analyses are used and conducted to show feasibility and effectiveness of the proposed method.

In CGH-secured system, M1 and M2 [i.e., $M_1(x,y)$ and $M_2(\xi,\eta)$] are first extracted as shown in Figs. 4(a) and 4(b), respectively. The iterative process is shown in Fig. 4(c). A rapid convergence rate is achieved, and only 10 iterations are requested. In correlated photon imaging setup, the two marks are respectively encrypted by using the same series of random phase masks $R_i(k,l)$ $(i=1,2,3...)$. Two series of 1D intensity points $B_i^{(1)}$ and $B_i^{(2)}$ are respectively generated in Figs. 5(a) and 5(b), and subsequently the two series of 1D binary intensity points $\hat{B}_i^{(1)}$ and $\hat{B}_i^{(2)}$ can be correspondingly obtained in Figs. 5(c) and 5(d), respectively. To clearly show the binary maps, enlarged parts in Figs. 5(c) and 5(d) are given in Figs. 5(e) and 5(f), respectively. Finally, new series of 1D intensity points $\hat{C}_i^{(1)}$ and $\hat{C}_i^{(2)}$ are generated [see Eqs. (7) and (8)], and using random-position replacement maps the masks $\bar{M}_1(x,y)$ and $\bar{M}_2(\xi,\eta)$ are obtained in Figs. 6(a) and 6(b), respectively.

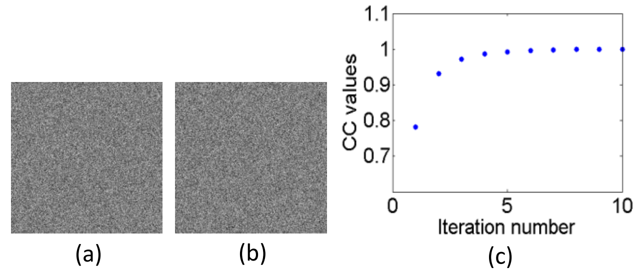

Fig. 4. (a) M1 [i.e., $M_1(x,y)$] and (b) M2 [i.e., $M_2(\xi,\eta)$], and (c) the iterative process.

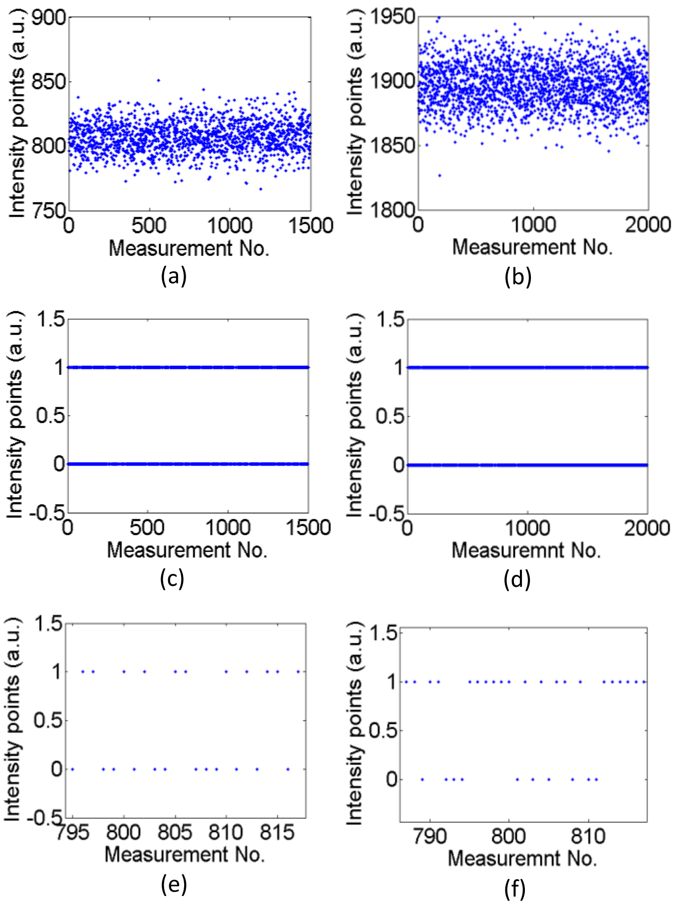

Fig. 5. (a) $B_i^{(1)}$ and (b) $B_i^{(2)}$, and (c) $\hat{B}_i^{(1)}$ and (d) $\hat{B}_i^{(2)}$. To clearly show binary points, enlarged parts of (c) and (d) are illustrated in (e) and (f), respectively.

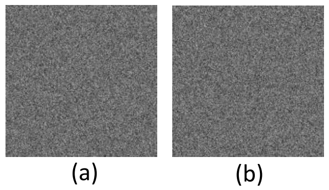

Fig. 6. (a) $\bar{M}_1(x,y)$ and (b) $\bar{M}_2(\xi,\eta)$.

During optical decoding, the input is recovered as shown in Fig. 7(a) by using the final phase-only masks $\bar{M}_1(x,y)$ and $\bar{M}_2(\xi,\eta)$. Correlation coefficient (CC) and mean square error (MSE) for Fig. 7(a) are 0.9779 and 0.3995, respectively. It is seen in Fig. 7(a) that high-quality input image is still recovered. To verify copyright of the recovered input image, two marks are further decoded as shown in Figs. 7(b) and 7(d), respectively. The CC and MSE for Fig. 7(b) are 0.4140 and 0.1946, respectively. The CC and MSE values for Fig. 7(d) are 0.4791 and 0.4607, respectively. Since clear information is not directly rendered due to only a few measurements, information authentication is conducted to verify the decoded marks [i.e., in Figs. 7(b) and 7(d)] and the corresponding authentication distributions are respectively generated in Figs. 7(c) and 7(e). It is seen in Figs. 7(c) and 7(e) that only one remarkable peak is generated. This means that the recovered input image is owned by the person who holds these correct keys for mark decoding and authentication.

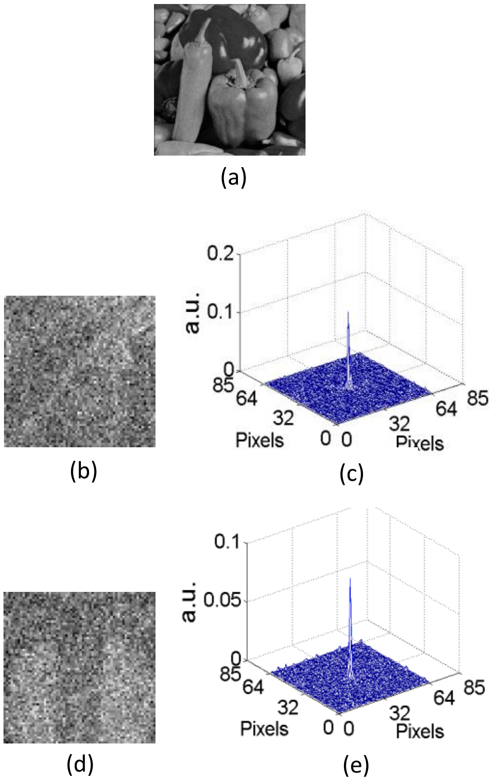

Fig. 7. (a) A recovered input using $\bar{M}_1(x,y)$ and $\bar{M}_2(\xi,\eta)$, (b) and (d) the decoded marks, and (c) and (e) authentication maps respectively corresponding to (b) and (d). Peak values in (c) and (e) are 0.1289 and 0.0843, respectively.

The two hidden marks should be simultaneously decoded and authenticated to verify copyright of the recovered input image. When security keys are incorrect (such as by unauthorized persons), it is impossible to generate correct authentication outputs. Figure 8(a) shows a decoded mark $H_1^{'}(\mu,\nu)$, when $R_i(k,l)$ $(i=1,2,3...)$ are incorrect during the decoding. The corresponding authentication distribution is generated in Fig. 8(b). Figure 8(c) shows a decoded mark $H_1^{'}(\mu,\nu)$, when random-position replacement map $p_1(x,y)$ is wrong. The corresponding authentication distribution is generated in Fig. 8(d). Figure 8(e) shows a decoded mark $H_1^{'}(\mu,\nu)$, when wavelength (λ) contains an error of 2.0 nm and axial distance (*d*) contains an error of 0.5 cm during mark decoding. The corresponding authentication distribution is generated in Fig. 8(f). It is shown in Figs. 8(b), 8(d) and 8(f) that only noisy distributions are generated. The same performance is also observed for the second mark, and for the sake of brevity the results are not presented here.

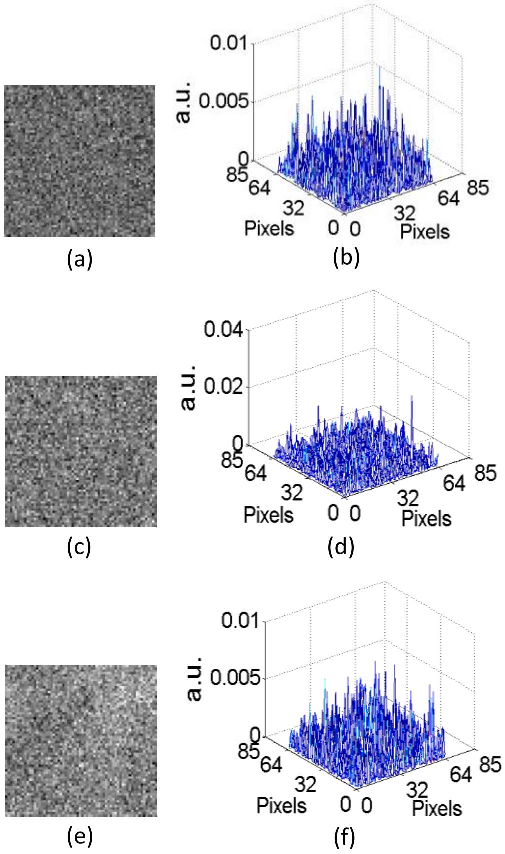

Fig. 8. (a) A decoded mark $H_1^{'}(\mu,\nu)$ obtained when $R_i(k,l)$ $(i=1,2,3...)$ are incorrect, (b) the corresponding authentication distribution. (c) A decoded mark $H_1^{'}(\mu,\nu)$ obtained when random-position replacement map $p_1(x,y)$ is wrong, (d) the corresponding authentication distribution. (e) A decoded mark $H_1^{'}(\mu,\nu)$ obtained when wavelength contains an error of 2.0 nm and axial distance contains an error of 0.5 cm, (f) the corresponding authentication distribution.

Since contaminations, such as occlusion, may happen during the storage or transmission, system robustness is also analyzed. Figure 9(a) shows a recovered input image, when 128×128 pixels of $\bar{M}_1(x,y)$ are occluded (i.e., as zeros). Figure 9(b) shows a decoded mark $H_1^{'}(\mu,\nu)$, and the corresponding authentication distribution is generated in Fig. 9(c). In this case, performance of the second mark is not affected. Figure 9(d) shows a recovered input image, when 128×128 pixels of $\bar{M}_2(\xi,\eta)$ are occluded (i.e., as zeros). Figure 9(e) shows a decoded mark $H_2^{'}(\mu,\nu)$, and the corresponding authentication distribution is generated in Fig. 9(f). In this case, performance of the first mark is not affected. It can be seen in Figs. 9(a)–9(f) that high robustness against contamination is achieved.

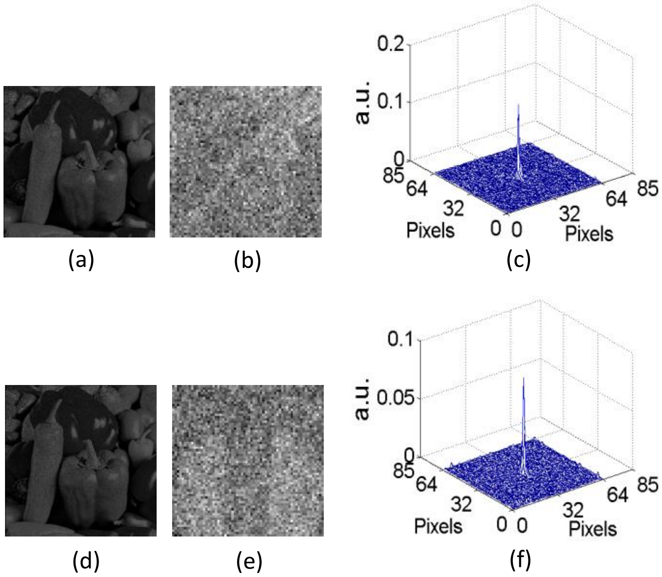

Fig. 9. (a) A recovered input image obtained when 128×128 pixels of $\bar{M}_1(x,y)$ are occluded, (b) a decoded mark $H_1^{'}(\mu,\nu)$, and (c) the corresponding authentication distribution. (d) A recovered input image obtained when 128×128 pixels of $\bar{M}_2(\xi,\eta)$ are occluded, (e) a decoded mark $H_2^{'}(\mu,\nu)$, and (f) the corresponding authentication distribution. Peak values in (c) and (f) are 0.1258 and 0.0826, respectively.

Noise contamination may also happen during the storage or transmission, and the system performance is further analyzed. Figure 10(a) shows a recovered input image, when $\bar{M}_1(x,y)$ is contaminated by additive white noise (zero mean noise with 0.01π variance). Figure 10(b) shows a decoded mark $H_1^{'}(\mu,\nu)$, and the corresponding authentication distribution is generated in Fig. 10(c). Figure 10(d) shows a recovered input image, when $\bar{M}_2(\xi,\eta)$ is contaminated by additive white noise (zero mean noise with 0.01π variance). Figure 10(e) shows a decoded mark $H_2^{'}(\mu,\nu)$, and the corresponding authentication distribution is generated in Fig. 10(f). It can be seen in Figs. 10(a)–10(f) that high robustness against noise contamination is also achieved in the proposed method.

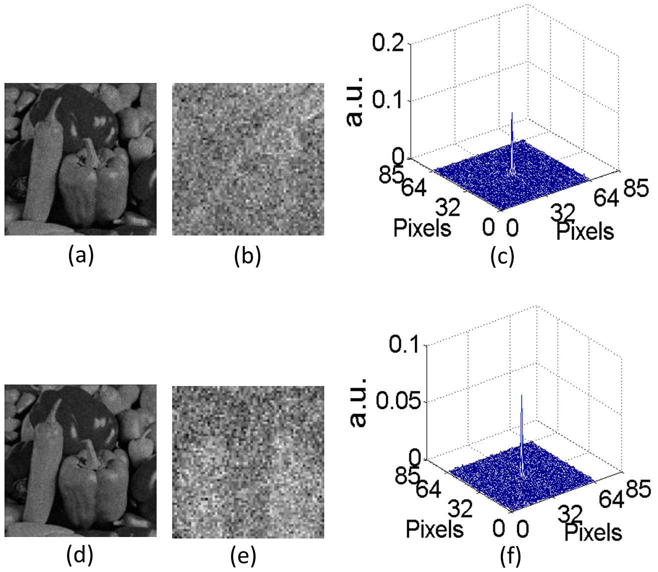

Fig. 10. (a) A recovered input image obtained when $\bar{M}_1(x,y)$ is contaminated by white noise (zero mean noise with 0.01π variance), (b) a decoded mark $H_1^{'}(\mu,\nu)$, and (c) the corresponding authentication distribution. (d) A recovered input image obtained when $\bar{M}_2(\xi,\eta)$ is contaminated by white noise (zero mean noise with 0.01π variance), (e) a decoded mark $H_2^{'}(\mu,\nu)$, and (f) the corresponding authentication distribution.

The major difference between the proposed method and previous works is briefly described as follows: For the first time, information generated by using a different optical imaging approach has been successfully embedded as a watermark in computer-generated hologram system, and authentication of the decoded watermarks is conducted instead of directly viewing the watermarks [27–30]. Here, correlated photon imaging has been used as a typical example to generate a series of one-dimensional data which are converted and embedded. The proposed method can open up a different research perspective for the optical watermarking field. The significant advantages are briefly summarized as follows: (1) quality of the recovered input image is high, and is not highly affected by watermark information. (2) A different imaging approach has been successfully applied in CGH system for optical watermarking. (3) A simple authentication operation is applicable to verify the decoded image in the developed optical system, and design of relatively complicated conditions using compressed sensing [31] is not necessary.

4. CONCLUSIONS

Watermarked CGH has been developed and assisted by correlated photon imaging. The input image is encoded into phase-only masks based on CGH, and the watermarks are generated by using correlated photon imaging. The 1D intensity points generated by correlated photon imaging are hidden into phase-only masks for optical watermarking. The proposed approach provides a promising strategy for optical information security [32–39].

Funding. National Natural Science Foundation of China (NSFC) (61605165); Hong Kong Research Grants Council Early Career Scheme (25201416); Shenzhen Science and Technology Innovation Commission through Basic Research Program (JCYJ20160531184426473); The Hong Kong Polytechnic University (1-ZE5F, 4-BCDY, G-YBVU and 4-ZZHM).

References

1. O. Matoba, T. Nomura, E. P. Cabré, M. S. Millán, and B. Javidi, “Optical techniques for information security,” *Proc. IEEE* **97**, 1128–1148 (2009).
2. B. Javidi, “Securing information with optical technologies,” *Phys. Today* **50**, 27–32 (1997).
3. P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.* **20**, 767–769 (1995).
4. E. Pérez-Cabré, M. Cho, and B. Javidi, “Information authentication using photon-counting double-random-phase encrypted images,” *Opt. Lett.* **36**, 22–24 (2011).
5. W. Chen, B. Javidi, and X. Chen, “Advances in optical security systems,” *Adv. Opt. Photon.* **6**, 120–155 (2014).
6. W. Chen and X. Chen, “Ghost imaging for three-dimensional optical security,” *Appl. Phys. Lett.* **103**, 221106 (2013).
7. W. Chen and X. Chen, “Grayscale object authentication based on ghost imaging using binary signals,” *EPL* **110**, 44002 (2015).
8. A. Markman, J. Wang, and B. Javidi, “Three-dimensional integral imaging displays using a quick-response encoded elemental image array,” *Optica* **1**, 332–335 (2014).
9. A. W. Lohmann and D. P. Paris, “Binary Fraunhofer holograms, generated by computer," *Appl. Opt.* **6**, 1739–1748 (1967).
10. T. C. Poon, *Digital Holography and Three-dimensional Display*. Springer-Verlag, 2007.
11. P. W. M. Tsang, J. P. Liu, K. W. K. Cheung, and T. C. Poon, “Modern Methods for fast generation of digital holograms," *3D Research* **1**, 11–18 (2010).
12. Y. Pan, X. Xu, S. Solanki, X. Liang, R. B. A. Tanjung, C. Tan, and T. C. Chong, “Fast CGH computation using S-LUT on GPU," *Opt. Express* **17**, 18543–18555 (2009).
13. R. W. Gerchberg and W. O. Saxton, “A practical algorithm for the determination of phase from image and diffraction plane pictures,” *Optik (Stuttgart)* **35**, 237–246 (1972).
14. J. R. Fienup, “Phase retrieval algorithms: a comparison,” *Appl. Opt.* **21**, 2758–2769 (1982).
15. R. K. Wang, I. A. Watson, and C. Chatwin, “Random phase encoding for optical security,” *Opt. Eng.* **35**, 2464–2469 (1996).
16. Y. Li, K. Kreske, and J. Rosen, “Security and encryption optical systems based on a correlator with significant output images,” *Appl. Opt.* **39**, 5295–5301 (2000).
17. H. T. Chang, W. C. Lu, and C. J. Kuo, “Multiple-phase retrieval for optical security systems by use of random-phase encoding,” *Appl. Opt.* **41**, 4825–4834 (2002).
18. W. Chen, X. Chen, A. Stern, and B. Javidi, “Phase-modulated optical system with sparse representation for information encoding and authentication,” *IEEE Photon. J.* **5**, 6900113 (2013).
19. H. M. Ozaktas, Z. Zalevsky, and M. A. Kutay, *The Fractional Fourier Transform with Applications in Optics and Signal Processing*. New York: Wiley, 2001.

20. J. H. Shapiro, "Computational ghost imaging," *Phys. Rev. A* 78, 061802 (2008).
21. B. I. Erkmen and J. H. Shapiro, "Ghost imaging: from quantum to classical to computational," *Adv. Opt. Photon.* **2**, 405–450 (2010).
22. F. Ferri, D. Magatti, L. A. Lugiato, and A. Gatti, "Differential ghost imaging," *Phys. Rev. Lett.* **104**, 253603 (2010).
23. J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. New York: McGraw-Hill, 1996.
24. F. Sadjadi and B. Javidi, *Physics of the Automatic Target Recognition*. Berlin: Springer, 2007.
25. W. Chen, X. Wang, and X. Chen, "Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase," *J. Opt.* **17**, 035702 (2015).
26. W. Chen and X. Chen, "Object authentication in computational ghost imaging with the realizations less than 5% of Nyquist limit," *Opt. Lett.* **38**, 546–548 (2013).
27. B. Javidi, *Optical and Digital Techniques for Information Security*, New York: Springer, 2005.
28. N. K. Nishchal, "Optical image watermarking using fractional Fourier transform," *J. Opt.* **38**, 22–28 (2009).
29. A. Patino, H. Altamar, and J. C. Martinez-Santos, "Speckle free optical watermarking based on pseudo-random phase encoding," pp. 1–6, XXI Symposium on Signal Processing, Images and Artificial Vision (STSIVA), 2016.
30. T. Y. Lee and S. D. Lin, "Dual watermark for image tamper detection and recovery," *Pattern Recogn.* **41**, 3497–3506 (2008).
31. M. F. Duarte, M. A. Davenport, D. Takhar, J. N. Laska, T. Sun, K. F. Kelly, and R. G. Baraniuk, "Single-pixel imaging via compressive sampling", *IEEE Signal Process. Mag.* **25**, 83–91 (2008).
32. X. Wang, W. Chen, and X. Chen, "Optical information authentication using compressed double-random-phase-encoded images and quick-response codes," Opt. Express **23**, 6239–6253 (2015).
33. D. Fan, X. F. Meng, Y. Wang, X. Yang, X. Pan, X. Peng, W. He, G. Dong, and H. Chen, "Multiple-image authentication with a cascaded multilevel architecture based on amplitude field random sampling and phase information multiplexing," *Appl. Opt.* **54**, 3204–3215 (2015).
34. X. Y. Shi, Z. Chen, D. Zhao, H. Mao, and L.F. Chen, "Phase retrieval encryption in an enhanced optical interference by key phase constraint," *Appl. Opt.* **54**, 3197–3203 (2015).
35. B. Javidi, A. Carnicer, M. Yamaguchi, T. Nomura, E. Pérez-Cabré, M. S Millán, N. K Nishchal, R. Torroba, J. F. Barrera, W. He, X. Peng, A. Stern, Y. Rivenson, A Alfalou, C Brosseau, C. Guo, J. T Sheridan, G. Situ, M. Naruse, T. Matsumoto, I. Juvells, E. Tajahuerce, J. Lancis, W. Chen, X. Chen, P. W H Pinkse, A. P Mosk, and A. Markman, "Roadmap on optical security," J. Opt. **18**, 083001 (2016).
36. L. Gong, X. Liu, F. Zheng, and N. Zhou, "Flexible multiple-image encryption algorithm based on log-polar transform and double random phase encoding technique," J. Mod. Opt. **13**, 1074–1082 (2013).
37. N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," Opt. Laser Technol. **82**, 121–133 (2016).
38. W. Chen, "Computer-generated hologram using binary phase with an aperture," Appl. Opt. **56**, 9126–9131 (2017).
39. W. Chen, "Ghost identification based on single-pixel imaging in big data environment," Opt. Express **25**, 16509–16516 (2017).