SCIENTIFIC REPORTS

OPEN

Received: 16 June 2015
Accepted: 28 September 2015
Published: 23 October 2015

Optically secured information retrieval using two authenticated phase-only masks

Xiaogang Wang[1], Wen Chen[2,3], Shengtao Mei[3] & Xudong Chen[3]

We propose an algorithm for jointly designing two phase-only masks (POMs) that allow for the encryption and noise-free retrieval of triple images. The images required for optical retrieval are first stored in quick-response (QR) codes for noise-free retrieval and flexible readout. Two sparse POMs are respectively calculated from two different images used as references for authentication based on modified Gerchberg-Saxton algorithm (GSA) and pixel extraction, and are then used as support constraints in a modified double-phase retrieval algorithm (MPRA), together with the above-mentioned QR codes. No visible information about the target images or the reference images can be obtained from each of these authenticated POMs. This approach allows users to authenticate the two POMs used for image reconstruction without visual observation of the reference images. It also allows user to friendly access and readout with mobile devices.

When designing diffractive optical elements that allow for the encryption of data for security applications, phase retrieval algorithms (PRAs) such as the Gerchberg-Saxton algorithm (GSA)[1], Fienup method[2] and their derivative[3] can be used. In 1996, Johnson and Brasher encrypted a biometric image in two phase-only masks (POMs) that together reconstruct an image although neither diffractive element by itself gives any hints as to what is in the image[4]. Under the framework of linear double-random-phase encoding (DRPE) scheme[5], many modified algorithms in Fourier domain[6,7], Fresnel domain[8–14] and gyrator domain[15] have been proposed to generate POMs for data retrieval. Recently, we have also proposed several methods to produce two POMs for single-image retrieval using iterative nonlinear DRPE[16,17]. Degrees of freedom to manipulate the physical parameters of optical waves can be used in those algorithms where an image can be encoded into two or more POMs[4–17]. Optical information hiding with POMs has now been one of the most popular application areas for PRAs[18–20]. However, the identifying and the capacity of those computer-generated POMs and the deteriorated original inputs reconstructed optically are still the major concerns in regards to the PRA-based data security protocols.

In this paper, a method for jointly designing two diffractive optical elements having quasi-random phases that allow for the authentication of the elements themselves, the encryption and noise-free retrieval of triple images is proposed based on modified PRAs. No visible information can be obtained from each of the POMs. The target images are inserted into QR codes via hyperlinks that allow for flexible readout with mobile devices. This approach allows users to authenticate the two POMs without visual observation of those images used as references for authentication. The target images can be revealed without visible loss of information due to the property of high damage tolerance capability of QR codes.

Results

Optical image reconstruction scheme. The proposed reconstruction procedure of target images is demonstrates in Fig. 1. When the authenticated POM P_1 is illuminated with incident plane wave and then modified by another authenticated POM P_2, the approximates of the input QR codes $\left(q_i', \; i = 1, 2, 3\right)$ can be detected in three different object planes. Thus, we have

[1]School of Sciences, Zhejiang A&F University, Linan 311300, China. [2]Department of Electronic and Information Engineering, The Hong Kong Polytechnic University, Hong Kong China. [3]Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583, Singapore. Correspondence and requests for materials should be addressed to X.W. (email: wxg1201@163.com)

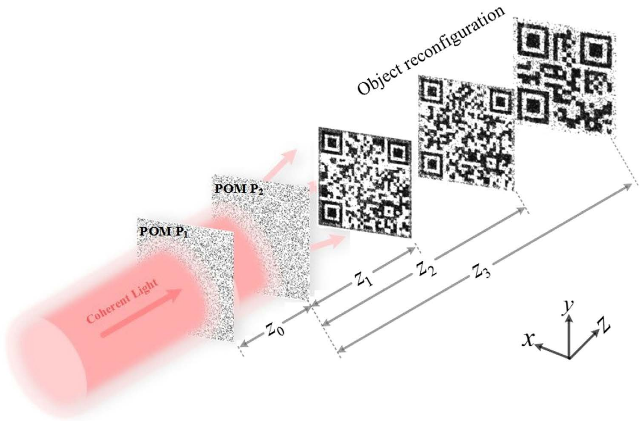

Figure 1. Optical image reconstruction procedure with two authenticated POMs.

$$q_i'(x_{i+1}, y_{i+1}) = \left|\mathrm{FrT}_{z_i,\lambda}\left\{P_2(x_1, y_1) \times \mathrm{FrT}_{z_0,\lambda}\left[P_1(x_0, y_0)\right]\right\}\right|, \tag{1}$$

where the operator || denotes a modulus operation and FrT[•] represents Fresnel transform[17].

Image hiding algorithm with sparsity constrains. The procedure of designing two POMs P_1 and P_2 that together reconstruct triple images consists of the following steps: 1. Storing three target images (f_1, f_2, f_3) in QR codes (q_1, q_2, q_3). 2. Generating two sparse POMs (p_{1s}, p_{2s}) from two images (g_1, g_2), which are used as reference for authentication and differ from the target images. 3. Numerical calculation of the two POMs P_1 and P_2 using the sparse POMs and the QR codes.

To generate two sparse POMs, two secret images g_1 and g_2 need to be respectively encoded in two different POMs by using a modified Fresnel domain GSA[11,12] with the two intensity constraints, i.e., a unit amplitude in the input plane and the image to be encoded in the output plane at a certain distance. Note that the two images used as references are not QR codes used for image encoding. The images g_1 and g_2 are independently encoded into POMs p_m and $p'_{m'}$ in two iterative processes where the propagation distances are d_1 and d_2. Note that the subscripts m and m' represent the number of iterations in iterative processes. When p_m is illuminated with incident plane wave, an approximation of g_1 can be observed in the object plane at distance d_1, which can be written by

$$g_1'(x_1, y_1) = \left|\mathrm{FrT}_{d_1,\lambda}\left[p_m(x_0, y_0)\right]\right|. \tag{2}$$

Likewise, we can obtain an approximation of g_2 in the output domain at the distance d_2, which can be given by $g_1'(x_2, y_2) = |\mathrm{FrT}_{d_2,\lambda}[p'_{m'}(x_0, y_0)]|$.

Sparse representation of the encrypted data can be successfully used for information authentication in some DRPE-based security systems[14,21–25]. In this step, two sparse phase functions p_{1s} and p_{2s} that used for the calculation of P_1 and P_2 can be randomly extracted from the outcomes of the iterative processes, i.e., p_m, $p'_{m'}$. Then the following step is numerical calculation of the two authenticated POMs P_1 and P_2 by using the obtained sparse POMs together with the QR codes. A modified double-phase retrieval algorithm (MDPRA) is proposed to achieve this purpose, where the sparse POMs and the QR codes are used as support constraints. In the MDPRA, let functions $P_1^{(n)}$ and $P_2^{(n)}$ respectively denote the two estimates for P_1 and P_2, where the superscript n represents the nth iteration of the algorithm. In the initial stage, two random POMs can be used as $P_1^{(1)}$ and $P_2^{(1)}$, respectively. The QR codes, i.e., q_1, q_2 and q_3, are the three amplitude constraints in the output planes with respect to different distances from the second POM $P_2^{(n)}$, i.e., z_1, z_2 and z_3.

Note that the final solutions for P_1 and P_2 are $P_1^{(N+1)}$ and $P_2^{(N+1)}$ if the iterative stops after N iterations. The obtained two POMs P_1 and P_2 require authentication before being applied for optical image retrieval. For brevity, only the identifying of P_1 is explained. The reconstructed signal from P_1 given by $g_{1s}(x_1, y_1) = |\mathrm{FrT}_{d_1,\lambda}[P_1(x_0, y_0)]|$ will be compared with the original image g_1, by nonlinear correlation in our proposal, where the two parameters d_1 and λ can be used as keys for authentication. The authentication method is described as follows[25,26]:

$$NC(x, y) = |\mathrm{IFT}[c(\mu, \nu)\,|c(\mu, \nu)|^{\omega-1}]|^2, \tag{3}$$

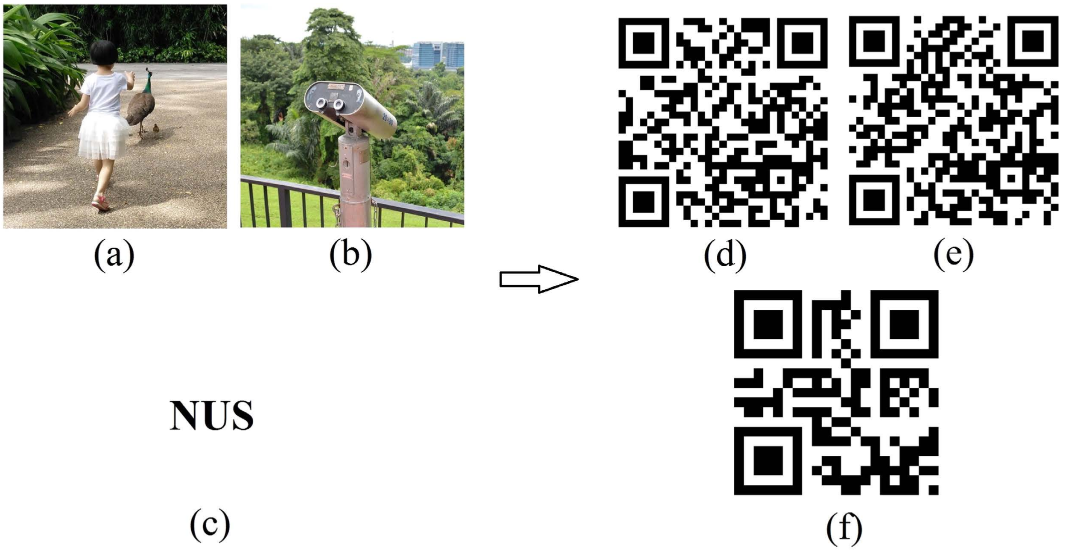

Figure 2. Storing three target images in QR codes. (**a**) Girl, (**b**) Telescope, (**c**) input text information. (**d–f**) their respective QR codes. Photographs taken by author.

where IFT[•] denotes inverse Fourier transform and ω defines the strength of the applied nonlinearity. Function $c(\mu, v)$ is given by $c(\mu, v) = \mathrm{FT}\left[g_{1s}(x, y)\right] \cdot \left\{\mathrm{FT}\left[g_1(x, y)\right]\right\}^*$, where FT[•] denotes Fourier transform.

Experimental Simulations and performance analyses. Figure 2(a,b) are two 500 × 500 color images, which can be respectively inserted into the QR codes shown in Fig. 2(d,e) via hyperlinks. When a user scans the QR code containing the hyperlink which automatically redirects the user to the image. Figure 2(c) shows input the input text information (NUS stands for National University of Singapore) and its respective QR code is presented in Fig. 2(f). All of the QR Codes have the size of 500 × 500. Due to its fast readability, great storage capacity and high damage tolerance capability, storing data in QR codes during the processes of optical encryption[27–29] and authentication[21–23] holds many practical advantages. Once the reconstructed QR codes are scanned by smartphones or tablets, the target images can be successfully revealed.

In our simulations, the pixel dimensions and the illumination wavelength are set as $8\mu m \times 8\mu m$ and $\lambda = 633\,nm$, respectively. Figure 3(a,c) show two 500 × 500 pixels binary images used as references for authentication. The propagation distances are given by $d_1 = 6\,cm$ and $d_2 = 8\,cm$, respectively. Figure 3(b,d) demonstrate two sparse phase functions p_{1s} and p_{2s} that are randomly extracted from the outcomes of the iterative processes, p_{50} and p'_{50}, for which both the percentages of the extracted pixels with respect to the pixel size of their originally recovered phase images are 28%.

The two sparse POMs are used as two constraints in the proposed MDPRA, together with the three QR codes. The correlation coefficient (CC) is applied to evaluate the similarity between the recovered images q_i' and their original images q_i, which is defined by

$$\mathrm{CC} = \frac{E\left\{\left[q_i - E\left[q_i\right]\right]\left[q_i' - E\left[q_i'\right]\right]\right\}}{\sqrt{E\left\{\left[q_i - E\left[q_i\right]\right]^2\right\} E\left\{\left[q_i' - E\left[q_i'\right]\right]^2\right\}}}, \tag{4}$$

where $E[]$ denotes the expected value operator. The CC values get the maximum value of 1 if q_i' are perfectly correlated with q_i. Figure 4(a) shows the relation between number of iterations and CC values (between q_i and q_i'), where we set the parameters as $z_0 = 8\,cm$, $z_1 = 12\,cm$, $z_2 = 20\,cm$ and $z_3 = 30\,cm$. It can be seen from Fig. 4(a) that the CC value increases as the number of iterations increases. At the beginning iterations, the three curves shown in Fig. 4(a) overlap almost completely, which implies that the three recovered QR codes have almost identical CC values at the first several iterations. After 100 iterations, the CC values increase very slightly. As expected, two authenticated POMs $P_1^{(n+1)}$ and $P_2^{(n+1)}$ can be generated after the nth iteration, which require authentication before being used for image reconstruction. Evaluation of the correlation outputs can be implemented by using peak-to-correlation (PCE)[23], which is defined as the ratio between the maximum intensity peak value and the total energy of the output plane, usually indicates the sharpness and height of the output correlation peak. Figure 4 shows

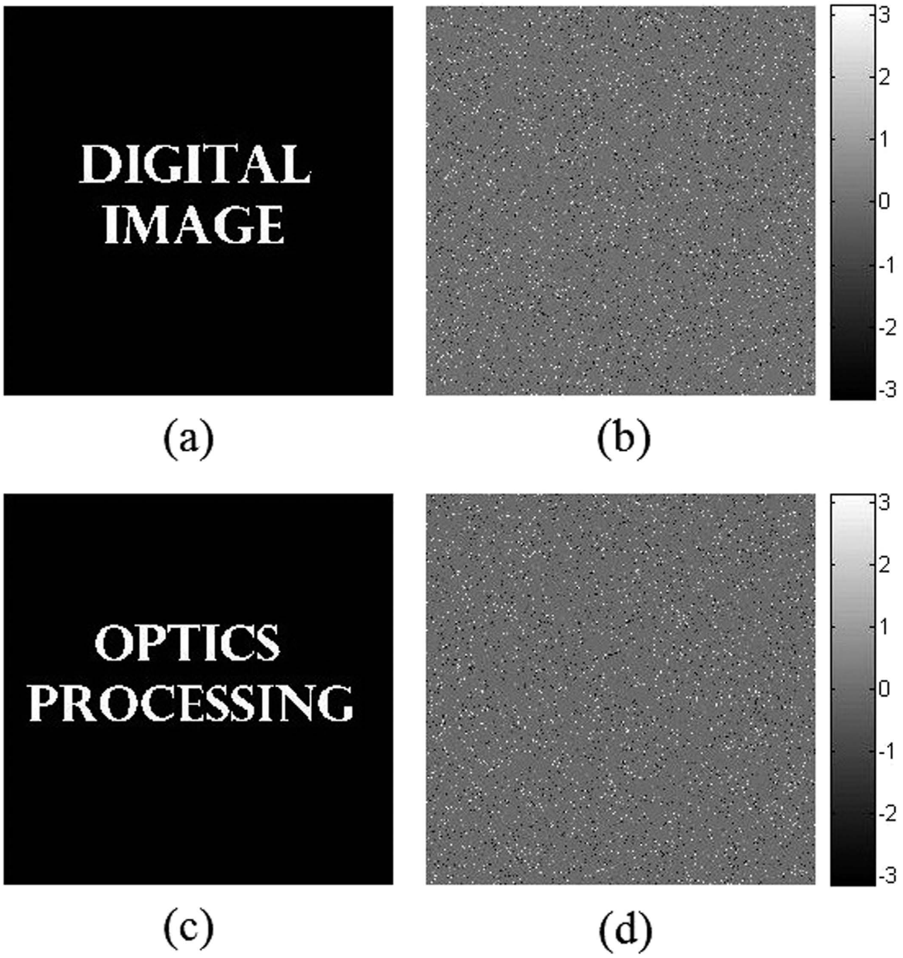

Figure 3. Secret images used as references for authentication and their respective sparse POMs. (**a**) g_1; (**b**) phase distribution of p_{1s}; (**c**) g_2; (**d**) phase distribution of p'_{1s}.

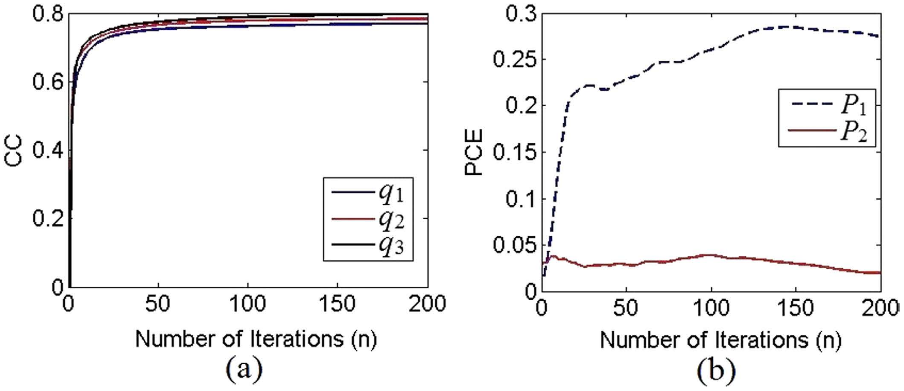

Figure 4. Performance of the proposed iterative algorithm. (**a**) Relation between CC and number of iterations and (**b**) the PCE curves versus the number of iterations.

the two PCE curves obtained by using all correct authentic keys and the nonlinearity strength $\omega = 0.4$. Different from the PCE curve corresponding to P_2, the curve with respect to P_1 rises rapidly during the first twenty iterations. After that, the PCE values increased slowly and then reaches a plateau (0.2846) at 145 iteration. However, the PCE values obtained with the second POM P_2 moves up and down in a limited range. It reaches its maximum (0.0390) at 99 iterations. In order to obtain high-quality correlation peak intensity in authentication, the POMs generated after 99 iterations are chosen as the two POMs

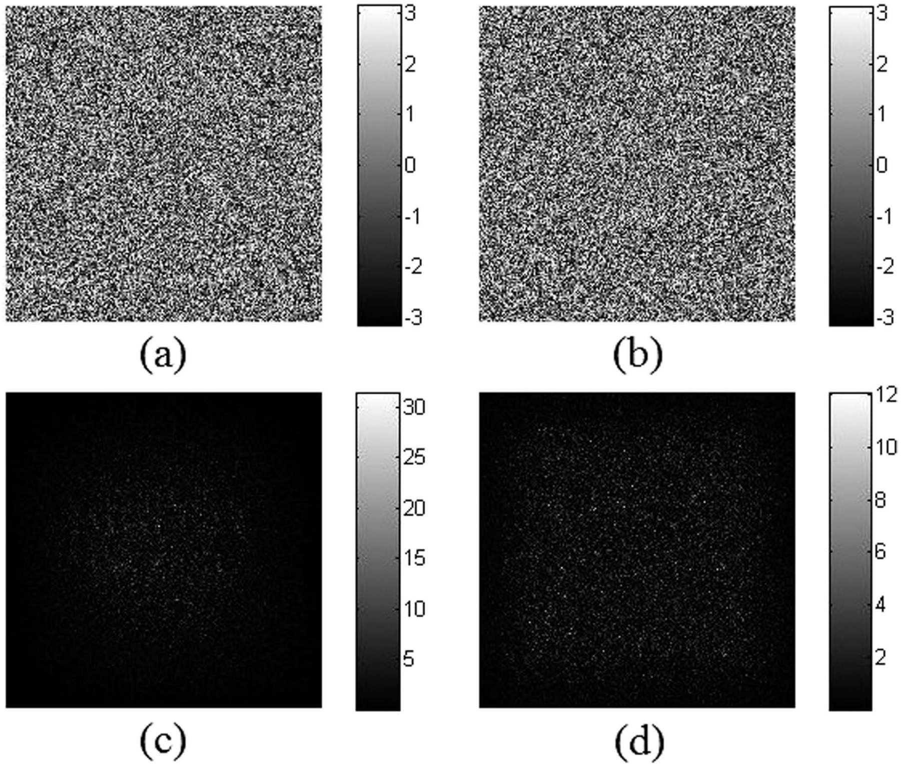

Figure 5. Two obtained POMs and their respective diffractive patterns. Phase distributions (**a**) P_1 and (**b**) P_2, and their respective Fresnel diffraction intensity patterns (**c**) at distance d_1; (**d**) at distance d_2.

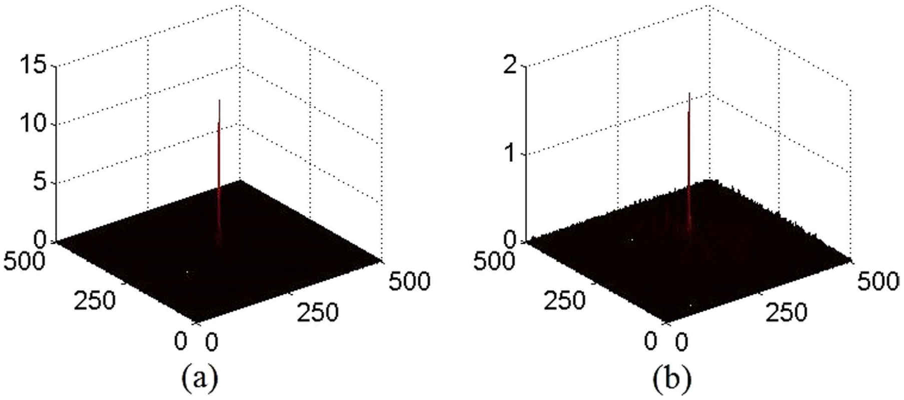

Figure 6. Authentication of the POMs based on nonlinear correlation. (**a**) Correlation outputs corresponding to P_1 and (**b**) P_2.

used for authentication and image retrieval since the CC values increase very slowly after 100 iterations.

The two POMs P_1 and P_2 designed for triple-image reconstruction and obtained after iteration number of 99 are respectively shown in Fig. 5(a,b). They are required for authentication before being used for image reconstruction. The diffraction patterns of P_1 and P_2 are shown in Fig. 5(c,d), at the distances of d_1 and d_2 respectively, from which no information about the two secret binary images can be observed.

When those two visually unrecognizable images [Fig. 5(c,d)] are respectively compared with the references, i.e., Fig. 3(a,c), by nonlinear correlation, sharp correlation peaks could be obtained as shown in Fig. 6(a,b), which implies that the two POMs are successfully authenticated with correct parameters.

The security performance of the two POMs is further investigated. When only one of the POMs is placed in the optical scheme shown in Fig. 1, the diffraction patterns in the three object planes are shown in Fig. 7, from which no valuable information about the QR codes could be observed. Note that Fig. 7 only shows the intensity distributions within the area of $4\,mm \times 4\,mm$ on the output display. The results

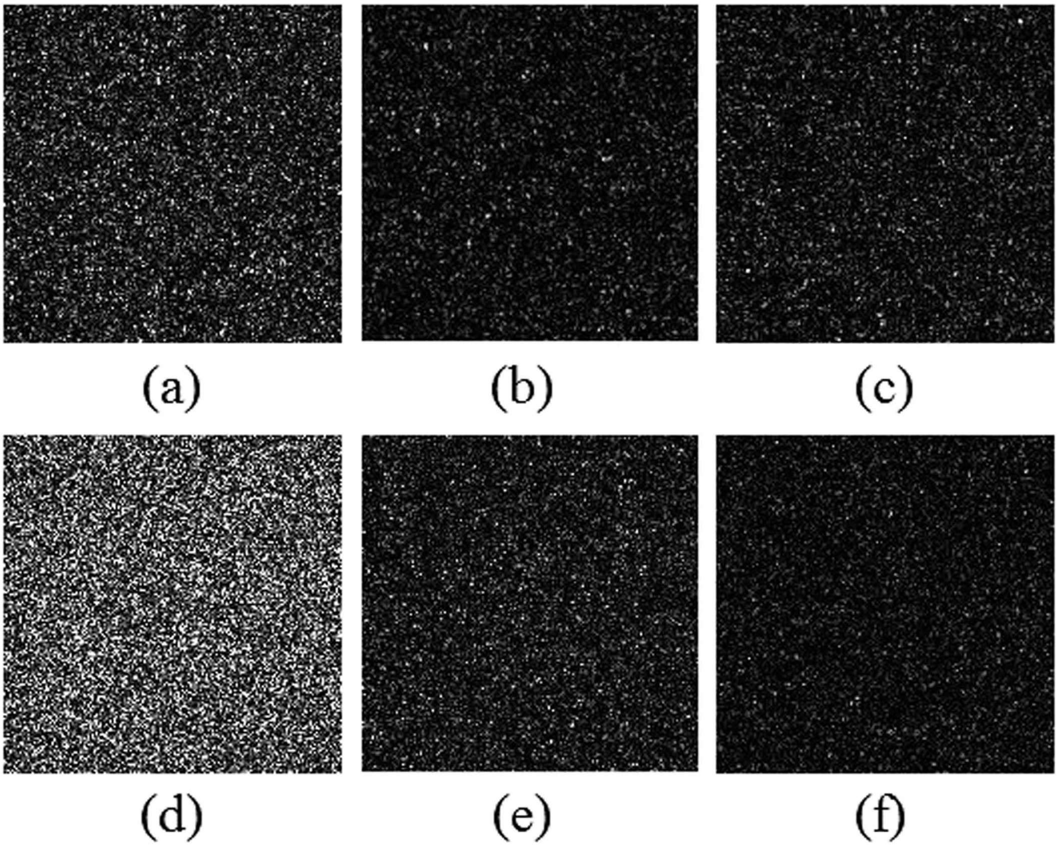

Figure 7. Images reconstructed from only one of the POMs. (**a**–**c**) are the three images reconstructed from P_1 in the different object planes (located from near to far from P_1); (**d**–**f**) are the three images reconstructed from P_2 in the three different object planes.

shown that neither of the two POMs has the problem of untended information disclosure. The proposed security system can be regard as an information sharing system. Each POM will be sent to different receivers through communication channels. Only when a matched pair of POMs are used for decryption, the primary images can be retrieved by scanning the decrypted QR codes.

Results for the reconstructed images from the two POMs P_1 and P_2 in different object planes using all the correct physical and geometric parameters are shown in Fig. 8(a–c), which have worse quality than the original images due to the effect of energy loss. The energy of the above three recovered images respectively account for about 85%, 84% and 79% of the total energy in their corresponding object planes. Smartphone was used to display the decrypted images by scanning the reconstructed QR codes. As demonstrated in Fig. 8(d–f), the two target color images and the text information can be retrieved without visible loss of information.

Discussions

We developed an algorithm for jointly designing two POMs that allow for the encryption and noise-free retrieval of triple images. Compared with previous works, the proposed algorithm based on sparsity constraints and QR codes has the following features:

- This approach allows users to authenticate the two POMs without visual observation of those images used as references for authentication. Since a huge number of differently encoded POMs can be sent out through communication channels[14], the identifying and matching of the POMs in a simple and direct manner can help increase efficiency. The MPRA with sparsity constraints may expect to be used in the computation of digital holograms and meta-holograms[30–32] for image display and information authentication.
- There is no problem of information disclosure in the proposed method. No information can be visually observed from the two POMs and their respective diffraction patterns. Our method can also be used for encryption of three-dimensional objects.
- It allows user to friendly access and readout with mobile devices. The target images can be revealed without visible loss of information due to the property of high damage tolerance capability of QR codes. Optically secured information retrieval can be realized when the two designed POMs manufactured by a number of techniques including embossing on plastic films and encoding on photopolymer are placed in the proposed scheme shown in Fig. 1.

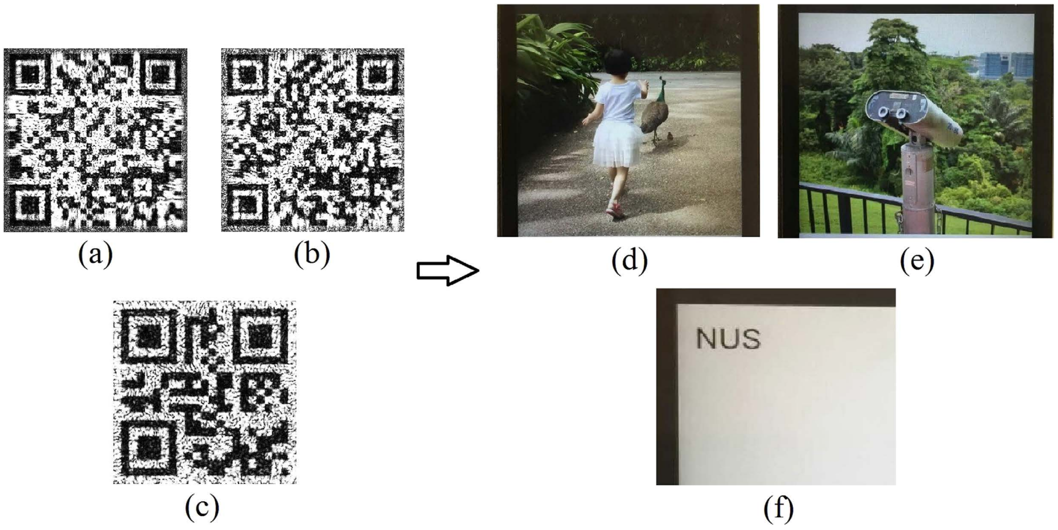

Figure 8. The reconstructed QR codes from P_1 and P_2 at different object planes and their respective retrieved images using a smartphone.

Methods

Double-phase retrieval algorithm with sparsity constraints. Let functions $P_1^{(n)}$ and $P_2^{(n)}$ respectively denote the two solutions for P_1 and P_2, where the superscript n represents the nth iteration of the algorithm. In the initial stage, two random POMs can be used as $P_1^{(1)}$ and $P_2^{(1)}$, respectively. The QR codes, i.e., q_1, q_2 and q_3, are the three amplitude constraints in the output planes with respect to different distances from the second POM $P_2^{(n)}$, i.e., z_1, z_2 and z_3. The process proceeds as follows:

(i) The first POM $P_1^{(n)}$ illuminated with incident plane wave is first Fresnel-transformed at the propagation distance z_0. The resultant wave function can be written as

$$U_0^{(n)} = \mathrm{FrT}_{z_0,\lambda}[P_1^{(n)}] \tag{5}$$

which is then multiplied by the second POM $P_2^{(n)}$ and propagates forward to the output plane through distances $z_i\,(i=1,2,3)$ to obtain new wave functions

$$U_i^{(n)} = \mathrm{FrT}_{z_i,\lambda}[P_2^{(n)} \times U_0^{(n)}], \tag{6}$$

where the coordinates are omitted for simplicity.

(ii) Replace amplitude parts of the diffraction space wave functions $U_i^{(n)}$ with amplitude constraints q_i. Then the modified functions in the three output planes simultaneously transform back to the plane where the second POM $P_2^{(n)}$ locates to get a new wave function $U_4^{(n)}$.

$$U_4^{(n)} = \sum_{i=1}^{3} \mathrm{IFrT}_{z_i,\lambda}\left\{q_i \times \mathrm{PR}\left[U_i^{(n)}\right]\right\}, \tag{7}$$

where IFrT[•] represent inverse Fresnel transform and PR[•] denotes phase reservation, retaining the phase of a complex function but truncating its amplitude part.

(iii) Update the two input POMs $P_1^{(n)}$ and $P_2^{(n)}$ with $P_1^{(n+1)}$ and $P_2^{(n+1)}$. First, we obtain a POM function $r_1^{(n)}$ and then update the input POM $P_1^{(n)}$ with $P_1^{(n+1)}$ using $r_1^{(n)}$, which can be written as

$$r_1^{(n)} = \mathrm{PR}\left\{\mathrm{IFrT}_{z_0,\lambda}\{|U_4^{(n)}| \times \mathrm{PR}[U_0^{(n)}]\}\right\}, \tag{8}$$

$$P_1^{(n+1)} = r_1^{(n)} \oplus p_{1s}, \tag{9}$$

where the symbol $\bigoplus$ denotes a particular way of data embedding. For clarity, the calculation of $P_1^{(n+1)}$ described by Eq. (9) is explained. We first extract the non-zero pixels of POM p_{1s} as the data background for POM $P_1^{(n+1)}$, and then embed the pixel values of $r_1^{(n)}$ into $P_1^{(n+1)}$ pixel by pixel but keep the background unchanged.

To generate another POM used for next iteration, we first compute a POM function $r_2^{(n)}$ by using $r_2^{(n)} = \mathrm{PR}\{\mathrm{FrT}_{z_0,\lambda}[P_1^{(n+1)}]\}$ and then obtain POM $P_2^{(n+1)}$ by

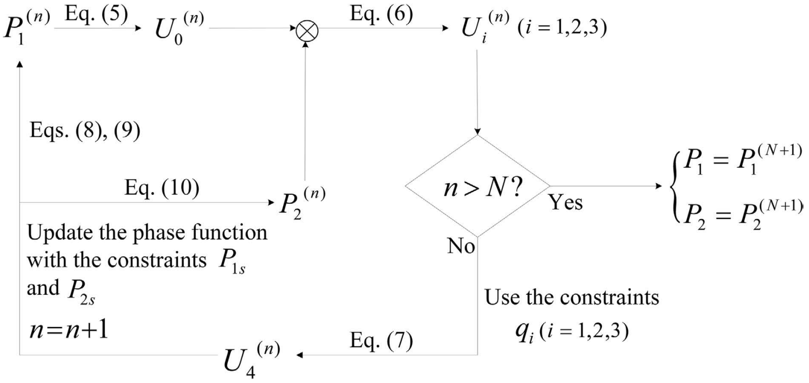

Figure 9. Flowchart of the proposed double-phase retrieval algorithm.

$$P_2^{(n+1)} = \mathrm{PR}\{U_4^{(n)} \times [r_2^{(n)}]^*\} \oplus p_{2s}, \tag{10}$$

where the superscript * denotes conjugation.

(iv) Repeat steps (i)–(iii) until the preset threshold value is satisfied. Suppose the iteration process stop at the Nth iteration. The convergence of the algorithm is demonstrated by the relation between the CC values [between q_i and their approximates q_i' obtained by substituting the two POMs computed with Eqs. (9) and (10) into Eq. (1)] and the iteration numbers.

To sum up, a flowchart of the iterative phase retrieval algorithm is depicted in Fig. 9. So far, we have obtained the two POMs P_1 and P_2, which require authentication before being applied for optical image retrieval and can be respectively represented by function $P_1^{(N+1)}$ and $P_2^{(N+1)}$. In general, the amplitude parts of function $U_i^{(n)}$ would be closer to the constraints q_i with the increasing of iterations until stagnation. After N iterations, the estimates of q_i are denoted by $|U_i^{(N+1)}|$. From Eqs. (1), (5) and (6), we can readily obtain $q_i' = |U_i^{(N+1)}|$, which implies that the finally recovered images q_i' could be expected to be closer to their original images q_i by increasing the number of iterations before reaching plateau values. It should be pointed out that the MDPRA is designed under the framework of nonlinear double random phase encoding. Different from previously proposed methods of single image encoding[16,17], here we encode three QR codes into two POMs in Fresnel domain. Two sparse POMs calculated from two reference images for authentication are used as constraints in the iteration process.

References

1. Gerchberg, R. W. & Saxton, W. O. A practical algorithm for the determination of phase from image and diffraction plane pictures. *Optik* **35,** 237–246 (1972).
2. Fienup, J. R. Phase retrieval algorithms: a comparison, *Appl. Opt.* **21,** 2758–2769 (1982).
3. Faulkner, H. M. L. & Rodenburg, J. M. Movable aperture lensless transmission microscopy: a novel phase retrieval algorithm. *Phys. Rev. Lett.* **93,** 023903 (2004).
4. Johnson, E. G. & Brasher, J. D. Phase encryption of biometrics in diffractive optical elements. *Opt. Lett.* **21,** 1271–1273 (1996).
5. Refregier, P. & Javidi, B. Optical image encryption based on input plane and Fourier plane random encoding. *Opt. Lett.* **20,** 767–769 (1995).
6. Situ, G & Zhang, J. A cascaded iterative Fourier transform algorithm for optical security applications. *Optik* **114,** 473–477 (2003).
7. Alfalou, A. & Mansour, A. Double random phase encryption scheme to multiplex and simultaneous encode multiple images. *Appl. Opt.* **48,** 5933–5947 (2009).
8. Situ, G & Zhang, J. A lensless optical security system based on computer-generated phase only masks. *Opt. Commun.* **232,** 115–122 (2004).
9. Shi, Y., Situ, G. & Zhang, J. Multiple-image hiding in the Fresnel domain. *Opt. Lett.* **32,** 1914–1916 (2007).
10. Shi, Y., Situ, G. & Zhang, J. Multiple-image hiding by information prechoosing. *Opt. Lett.* **33,** 542–544 (2008).
11. Hwang, H., Chang, H. & Lie, W. Fast double-phase retrieval in Fresnel domain using modified Gerchberg-Saxton algorithm for lensless optical security systems. *Opt. Express* **17,** 13700–13710 (2009).
12. Huang, J., Hwang. H., Chen, C. & Chen, C. Optical multiple-image encryption based on phase encoding algorithm in the Fresnel transform domain. *Opt & Laser Technol* **44,** 2238–2244 (2012).
13. Rajput, S. K. & Nishchal, N. K. Fresnel domain nonlinear optical image encryption scheme based on Gerchberg–Saxton phase-retrieval algorithm. *Appl. Opt.* **53,** 418–425 (2014).
14. Chen, W., Wang, X. & Chen, X. Security-enhanced phase encryption assisted by nonlinear optical correlation via sparse phase. *J. Opt.* **17,** 035702 (2015).
15. Liu, Z., Xu, L., Gou, Q., Lin, C. & Liu, S. Image watermarking by using phase retrieval algorithm in gyrator transform domain. *Opt. Commun.* **283,** 4923–4927.
16. Wang, X., Chen, W. & Chen, X. Fractional Fourier domain optical image hiding using phase retrieval algorithm based on iterative nonlinear double random phase encoding. *Opt. Express* **22,** 22981–22995 (2014).
17. Wang, X., Chen, W. & Chen, X. Optical image hiding using double-phase retrieval algorithm based on nonlinear cryptosystem under vortex beam illumination. *J. Opt.* **17,** 035704 (2015).
18. Alfalou, A. & Brosseau, C. Optical image compression and encryption methods. *Adv. Opt. Photon.* **1,** 589–636 (2009).
19. Chen, W., Javidi, B. & Chen, X. Advances in optical security systems. *Adv. Opt. Photon.* **6,** 120–155 (2014).

20. Fienup, J. R. Phase retrieval algorithms: a personal tour [Invited]. *Appl. Opt.* **52,** 45–56 (2013).
21. Markman, A., Javidi, B. & Tehranipoor, M. Photon-counting security tagging and verification using optically encoded QR codes. *IEEE Photon. J.* **6,** 6800609 (2014).
22. Markman, A., Wang, J. & Javidi, B. Three-dimensional integral imaging displays using a quick-response encoded elemental image array. *Optica* **1,** 332–335 (2014).
23. Wang, X., Chen, W. & Chen, X. Optical information authentication using compressed double-random-phase-encoded images and quick-response codes. *Opt. Express* **23,** 6239–6253 (2015).
24. Wang, X., Chen, W. & Chen, X. Optical Encryption and Authentication Based on Phase Retrieval and Sparse Constraints. *IEEE Photon. J.* **7,** 7800310 (2015).
25. Pérez-Cabré, E., Cho, M. & Javidi, B. Information authentication using photon-counting double-random-phase encrypted images. *Opt. Lett.* **36,** 22–24 (2011).
26. Sadjadi, F. & Javidi, B. *Physics of Automatic Target Recognition* (Springer, New York, 2007).
27. Barrera, J. F., Mira, A. & Torroba, R. Optical encryption and QR codes: Secure and noise-free information retrieval. *Opt. Express* **21** 5373–5378 (2013).
28. Barrera, J. F., Mira, A. & Torroba, R. Experimental scrambling and noise reduction applied to the optical encryption of QR codes. *Opt. Express* **22,** 20268–20277 (2014).
29. Barrera, J. F., Mira, A. & Torroba, R. Experimental QR code optical encryption: noise-free data recovering. *Opt. Lett.* **39,** 3074–3077 (2014).
30. Yifat, Y. J. *et al.* Highly efficient and broadband wide-angle Holography Using Patch-Dipole Nano-antenna Reflectarrays, *Nano Lett.* **14,** 2485–2490 (2014).
31. Huang, L. *et al.* Three-dimensional optical holography using a plasmonic metasurface, *Nat. Commu* **4,** 2808 (2013).
32. Huang, Y. D. *et al.* Aluminum plasmonic multicolor meta-hologram, *Nano Lett.* **15,** 3122–3127 (2015).

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61575178 and 61205006), Singapore MINDEF-NUS Joint Applied R&D Cooperation Programme (JPP) Project: MINDEF/NUS/JPP/14/01/02.

Author Contributions

W.X.G. proposed the method and wrote the main manuscript text. W.X.G. and M.S.T. made the numerical simulations. C.W. and C.X.D. helped revise the manuscript and got involved in the discussions.

Additional Information

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Wang, X. *et al.* Optically secured information retrieval using two authenticated phase-only masks. *Sci. Rep.* **5**, 15668; doi: 10.1038/srep15668 (2015).