Secure and noise-free holographic encryption with a quick-response code

Zhenbo Ren (任振波)[1], Ping Su (苏 萍)[2], Jianshe Ma (马建设)[2], and Guofan Jin (金国藩)[1]

[1]*Department of Precision Instruments, Tsinghua University, Beijing 100084, China*

[2]*Graduate School at Shenzhen, Tsinghua University, Shenzhen 518055, China*

[*]*Corresponding author: su.ping@mail.sz.tsinghua.edu.cn*

Received September 24, 2013; accepted November 28, 2013; posted online December 25, 2013

In holographic encryption, double random-phase encoding in the Fresnel domain (DRPEiFD) is a prevalent encryption method because it is lensless and secure. However, noises bring adverse effects during decryption. In this letter, we introduce quick-response (QR) coding during encryption to resist noises. We transform the original information into a QR code and then encrypt the code as a hologram through DRPEiFD. To retrieve the input, we decrypt the hologram in the opposite manner to the encryption and subsequently obtain a QR code with noises. By scanning this code with proper applications in smartphones, we can obtain a noise-free retrieval. Numerical experiments and images scanned by a smartphone are shown to validate our proposed method.

OCIS codes: 060.4785, 070.4560, 090.1760, 100.4998.

doi: 10.3788/COL201412.010601.

In optical communication systems, optical encryption and data security are critical issues in preventing data storage and transmission from unauthorized access and attack. The optical image encryption method based on double random-phase encoding (DRPE) was proposed by Refregier *et al.*[1]. Since then, optical encryption technique is attracting increased research attention. Numerous proposals and improvements in optical encryption based on multiple-parameter fractional Fourier transform[2], Fresnel transform[3], joint transform correlator[4], digital holography[5], and phase-shift interference[6] have also been made presented. In particular, the introduction of holography[7] greatly broadens the flexibility, applicability, and variety of optical encryption. Holography can improve the security and can simplify the optical system by cancelling the lens[8−11]. Aside from digital holography[12], increasing interest is given to computer-generated holography (CGH)[13−15] because of its flexibility; this type of holography is invented in 1965 by Lohmann. Using a computer, we can simulate the whole process of generating a hologram without optical exposure and development. Hence, many researchers implemented CGH into optical encryption, and proposed many useful methods[16−20]. Among those methods, double random-phase encryption in Fresnel domain (DRPEiFD) is one of the most commonly used methods. For traditional DRPE, lenses make the optical system difficult in alignment in space. However, DRPEiFD does not need any lens during encryption and decryption. This encryption method is completely lensless, which reduces the requirements in hardware. Therefore, DRPEiFD is more applicable and easier to implement.

For these methods, noise is merely an incidental improvement along with new setups or algorithms. However, for the encryption and decryption technology, noise is always a vital problem. If tremendous noise contaminates the decryption result from which people cannot recognize the original information, then the encryption method is not successful. More seriously, a lack of the original quality precisely may make potential users unwilling to use such encryption. Thus, we have to construct a new method to change the present circumstance in holographic encryption.

Quick-response (QR) code[21,22], which is a kind of two-dimensional (2D) barcodes, is widely used in security, cyber application, management system, etc. A QR code can conceal specific information in its special geometric pattern, which is composed of black and white dots in a square. QR code has become popular in our daily life because of its fast readability and great storage capacity. Since QR code has strong fault tolerance and error correction capability, even when nearly half of a QR code is broken, we can still recover the original information.

Barrera *et al.* introduced a QR code in a standard optical encryption system[23]. They used QR code to avoid speckle noise from polluting the outcomes of normal optical encryption and achieved attractive results. This new concept was reviewed as one of the research highlights in cryptography[24]. In this letter, we are making an effort to further improve the combination of QR code and optical encryption technology. We introduce QR code into DRPEiFD to eliminate noise during encryption and decryption. Firstly, we transform the original information (such as texts) to a QR code using available software on the internet. We then encrypt this QR code by DRPEiFD, and thus we can acquire a CGH. This makes the QR code as a container in the temporary storage of information. In the decryption procedure, which is opposite to the encryption, we obtain a contaminated QR code with noise. The distinctive error correction capability of this method provided the retrieval of clean and noise-free input information with appropriate applications in a smartphone[23−27]. The numerical results demonstrate the obvious advantages of our proposal because the final user is apparently satisfied with the retrieval information.

DRPEiFD realizes lensless encryption with two Fresnel diffraction transforms and two white-noise phase plates within statistic independence. Figure 1(a) shows the optical setup of encryption. Supposing that λ is the incident

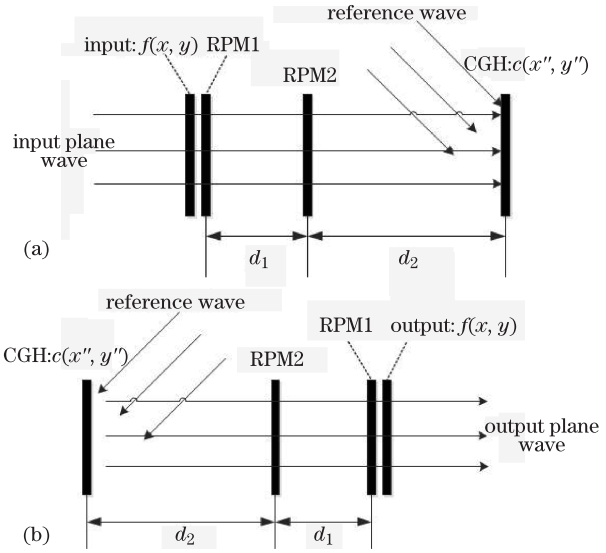


Fig. 1. Optical setup of DRPEiFD. (a) Encryption and (b) decryption.

wavelength; $f(x, y)$ is the input information to be encrypted; two random-phase plates RPM_1 and $\mathrm{RPM}_2$are $\delta(x, y) = \exp[\mathrm{j}n(x, y)]$ and $\phi(x', y') = \exp[\mathrm{j}m(x', y')]$, respectively, wherein $n(x, y)$ and $m(x', y')$ are evenly distributed white noises between $[0, 2\pi]$ within statistic independence; then the encryption procedure is described below.

Two random-phase plates are placed parallel at planes where $f(x, y)$ is located; and where $f(x, y)$ diffracts a distance of d_1. The reference wave is $R(x'', y'')$, which has the same wavelength as the input plane wave. Afterwards, we set a detector at the distance of $d_1 + d_2$ from the object plane to collect the encryption. The encryption $c(x'', y'')$ is

$$c(x'', y'') = |FrT_{d_2}\{FrT_{d_1}[f(x, y) \cdot \delta(x, y)] \cdot \phi(x', y')\} + R(x'', y'')|^2, \quad (1)$$

where FrT_d denotes the Fresnel transform with a distance of d. $c(x'', y'')$, which is actually a CGH, is the coherent superposition of input plane wave and reference wave.

The decryption, which is shown in Fig. 1(b), is the opposite procedure of encryption. A reference wave, which is the conjugation of $R(x'', y'')$, is needed to illuminate the CGH. Afterwards, the reconstructed beam propagates in Fresnel domain with a distance of d_2. After multiplying by the complex conjugation of $\phi(x', y')$, we transform the result in Fresnel domain with a distance of d_1 again. This process can be mathematically described as

$$f(x, y) = FrT_{d_1}\{FrT_{d_2}[c(x'', y'') \cdot R^*(x'', y'')] \cdot \phi(x', y')\}. \quad (2)$$

We conduct numerical experiments of the encryption and decryption in computer, and the results are shown in Fig. 2.

Figure 2(a) shows the input information "computer-generated hologram", and Fig. 2(b) is the encryption CGH by DRPEiFD. When one of the keys is incorrect, such as d_1 during decryption ($d_1 = 40$), the result is highly obscure to obtain any useful information, as shown in Fig. 2(c). The correct decryption result is shown in Fig. 2(d), which fades greatly because of the noise. To recognize the original input from the decryption is practically difficult. When the input information is more complicated, the decryption result definitely becomes more difficult to recognize.

The QR code[23] may be the most popular 2D barcodes for its fast readability and large storage capacity. With specific geometric patterns of black and white dots distributing in a square, a QR code can indicate the information of text, visiting card, email address, etc. Figure 3 shows a typical procedure of generating and retrieving a QR code. Black and white pixels in the matrix are similar to "0" and "1" in a computer. With appropriate applications in smartphones, which are massively used in our daily life, we can retrieve the original input easily.

Figure 3(a) shows a QR code which represents a character string in capital form "COMPUTER-GENERATED HOLOGRAM". A QR code is designed in a 2D plane. Three bigger squares are located at three corners, and a smaller square is located near the fourth corner to normalize the position, orientation, and angle of viewing. Due to the error correction, information can be accurately retrieved even the QR code is partly damaged or contaminated. By appropriate applications in smartphones with a semiconductor image sensor, we can easily obtain the input information that a QR code represents. Figure 3(b) shows an example. In this letter, we use a smartphone with some application on Android platform to scan the QR code in Fig. 3(a). Afterwards, we can read the text "COMPUTER-GENERATED HOLOGRAM" on the phone as shown in Fig. 3(c).

Subsequently, we combined DRPEiFD and QR code together to eliminate noise in encryption and decryption. Free, available software on the Internet is used to generate the QR image with an H-level error correction;

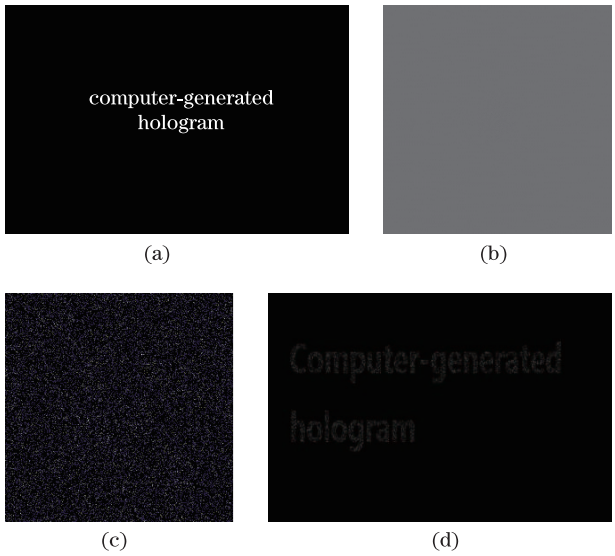
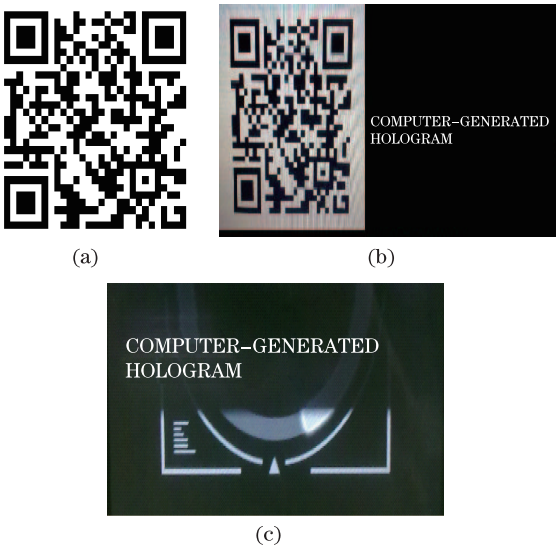
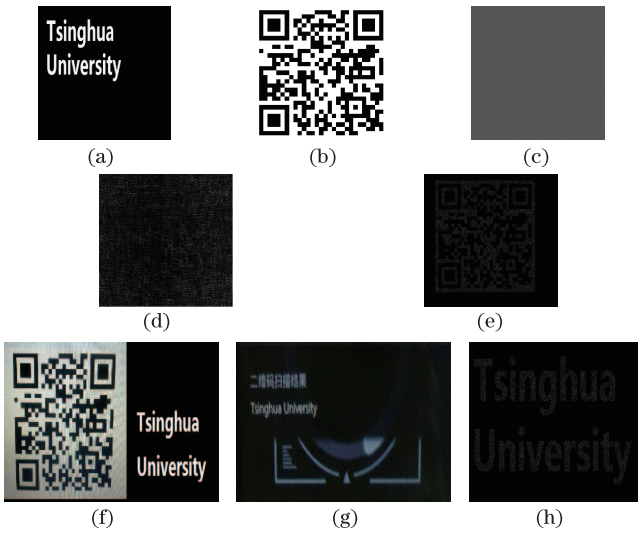


Fig. 2. (a) Input information, (b) corresponding encryption, (c) decryption with incorrect key d_1, and (d) decryption with correct keys, along with noise (we adjust the sizes of images to have the best appearance).



(a) (b) (c)

Fig. 3. (a) QR code of text "COMPUTER-GENERATED HOLOGRAM", (b) retrieval when reading the QR code with a smartphone, and (c) reading result on the smartphone.



(a) (b) (c) (d) (e) (f) (g) (h)

Fig. 4. (a) Original input, (b) corresponding QR image, (c) encryption hologram, (d) decryption with incorrect key $d1$, (e) decryption with correct keys, along with noise, (f) retrieval when reading the QR code with a smartphone, (g) reading result on the smartphone, and (h) retrieval by previous method.

therefore, the input can be retrieved correctly when 30% of the QR image is occluded or contaminated.

Figure 4 shows the numerical results. As shown in Fig. 4(a), the image of interest is a 256×256 pixel image of a character string "Tsinghua University", and Fig. 4(b) is its QR image. The QR code acts as a box to store the input temporarily. In our numerical experiments, d_1 and d_2 are 20 and 30 mm, respectively. Wavelengths λ of the input wave and reference wave are both 650 nm. All computational experiments are executed using a PC with a CPU of Intel T5750 (2 cores, both 2.0 GHz) processor and a memory of 2.0 Gb. We use conventional DRPEiFD to generate the CGH shown in Fig. 4(c). Figures 4(d) and 4(e) are decryption results with incorrect and correct keys, respectively. When one of the keys (d_1) is incorrect ($d_1 = 40$), the decryption result shown in Fig. 4(d) is very vague to distinguish any useful information. While decrypting the CGH with correct keys, we can obtain a contaminated QR code with serious noise shown in Fig. 4(e), which is for the next step of retrieval using a smartphone.

Scanning Fig. 4(e) with a smartphone directly reveals the result shown in Figs. 4(f) and (g) because of the error correction. This code is noise-free and completely similar to the original input. Figure 4(h) presents the noisy decryption result without using QR code. Serious noise decreases the image quality, and we can hardly recognize the characters. In our proposal, the QR code acts as a box to bear and resist all the damage and noisy contamination. Using QR encoding, the decryption result is guaranteed clean. Therefore, our proposal is proven to be effective, and have a potential in optical encryption systems.

In conclusion, we combine DRPEiFD and QR code together to resist noise and damage in optical encryption and decryption. DRPEiFD is a commonly used optical encryption system, which can improve the security and facility of holographic encryption. However, noise is always an inevitable problem. By encoding the input information to a QR code, we can make the QR code act as a box to store the information temporarily. Numerical experiments show that although the QR code is contaminated by serious noise after decryption, the retrieval outcome with a smartphone is absolutely noise-free. The computational simulations prove the effectiveness and potential of our proposal.

This work was supported by Shenzhen Key Laboratory of LED Packaging (No. ZDSY20120619141243215) and the National "973" Program of China (No. 2013CB328801).

References

1. P. Refregier and B. Javidi, Opt. Lett. **20,** 767 (1995).
2. R. Tao, J. Lang, and Y. Wang, Opt. Lett. **33,** 581 (2008).
3. G. Situ and J. Zhang, Opt. Lett. **29,** 1584 (2004).
4. T. Nomura and B. Javidi, Opt. Eng. **39,** 2031 (2000).
5. A. Nelleri, J. Joseph, and K. Singh, Opt. Eng. **47,** 115801 (2008).
6. N. K. Nishchal, J. Joseph, and K. Singh, Opt. Eng. **43,** 2959 (2004).
7. D. Gabor, Nature **161,** 777 (1948).
8. X. F. Meng, L. Z. Cai, Z, Y. R. Wang, X. L. Yang, X. F. Xu, G. Y. Dong, and X. X. Shen, Optics and Lasers in Engineering **47,** 96 (2009).
9. J. Ji, F. Huang, L. Wang, S. T. Feng, and S. P. Nie, Chinese J. Lasers (in Chinese) **34,** 1408 (2007).
10. A. Alfalou and C. Brosseau, Advances in Optics and Photonics **1,** 589 (2009).
11. X. G. Wang, D. M. Zhao, F. Jing, and X. F. Wei, Opt. Express **14,** 1476 (2006).
12. J. W. Goodman and R. W. Lawrence, Appl. Phys. Lett. **11,** 77 (1967).
13. A. W. Lohmann and D. P. Paris, Appl. Opt. **6,** 1739 (1967).
14. B. R. Brown and A. W. Lohmann, Appl. Opt. **5,** 967 (1966).
15. Z. L. Yu and G. F. Jin, *Computer Generated Hologram* (in Chinese)(Publishing House of Tsinghua University,

Beijing, 1984).

16. P. Tsang, K. W. K. Cheung, and T. C. Poon, Chin. Opt. Lett. **11,** 020901 (2013).
17. Q. Z. Huang, J. L. Du, Y. X. Zhang, F. H. Gao, and Y. K. Guo, Chinese J. Lasers (in Chinese) **10,** 90 (2000).
18. Y. Y. Wang, Y. R. Wang, Y. Wang, H. J. Li, and W. H. Sun, Optics and Lasers in Engineering **45,** 76 (2007).
19. J. Rosen, G. Brooker, G. Indebetouw, and N. T. Shaked, J. Holography Speckle **5,** 124 (2009).
20. Y. Rivenson, A. Stern, and B. Javidi, J. Display Techno. **6,** 506 (2010).
21. S. Dey, in *Proceedings of International Conference on Emerging Trends of Computers and Information Technology* **3,** 11 (2012).
22. ISO, IEC 18004: 2006, "Information technology-Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification," International Organization for Standardization, Geneva, Switzerland (2006).
23. J. F. Barrera, A. Mira, and R. Torroba, Opt. Express **21,** 5373 (2013).
24. O. Graydon, Nature Photon. **7,** 343 (2013).
25. E. Ohbuchi, H. Hanaizumi, and L. A. Hock, in *Proceedings of IEEE International Conference on Cyberworlds* 260 (2004).
26. K. C. Liao and W. H. Lee, J. Networks. **5,** 937 (2010).
27. Y. Qin and Q. Gong, Opt. Commun. **310,** 69 (2014).