Research Article Vol. 35, No. 1 / January 2018 / Journal of the Optical Society of America A A23

Journal of the Optical Society of America A

OPTICS, IMAGE SCIENCE, AND VISION

Is QR code an optimal data container in optical encryption systems from an error-correction coding perspective?

Shuming Jiao, Zhi Jin, Changyuan Zhou, Wenbin Zou,* and Xia Li

Shenzhen Key Laboratory of Advanced Telecommunication and Information Processing, College of Information Engineering, Shenzhen University, Shenzhen, Guangdong, China
**Corresponding author: wzouszu@sina.com*

Received 3 July 2017; revised 14 September 2017; accepted 2 October 2017; posted 3 October 2017 (Doc. ID 300555); published 25 October 2017

Quick response (QR) code has been employed as a data carrier for optical cryptosystems in many recent research works, and the error-correction coding mechanism allows the decrypted result to be noise free. However, in this paper, we point out for the first time that the Reed-Solomon coding algorithm in QR code is not a very suitable option for the nonlocally distributed speckle noise in optical cryptosystems from an information coding perspective. The average channel capacity is proposed to measure the data storage capacity and noise-resistant capability of different encoding schemes. We design an alternative 2D barcode scheme based on Bose–Chaudhuri–Hocquenghem (BCH) coding, which demonstrates substantially better average channel capacity than QR code in numerical simulated optical cryptosystems.

OCIS codes: (100.4998) Pattern recognition, optical security and encryption; (060.4785) Optical security and encryption; (070.4560) Data processing by optical means.

https://doi.org/10.1364/JOSAA.35.000A23

1. INTRODUCTION

In the digital age, massive amounts of data are stored, processed, and transmitted in computer systems and the Internet at every moment. Much of these data contain private, sensitive, or confidential information for individuals, companies, and governments that needs to be protected from unauthorized access. Data encryption techniques are developed to encode the original data into cyphertexts that are only readable by authorized parties to prevent illegal access. In addition to commonly used digital encryption techniques, various optical encryption techniques [1–4] have been proposed as alternative solutions in recent years. Optical encryption techniques generally have the advantages of parallel processing and multidimensional capabilities. The research of optical encryption can be dated back to the double random phase encoding (DRPE) scheme [1] proposed by Philippe and Javidi in 1995. Since then, numerous research works on optical encryption have been conducted, and comprehensive reviews on these works can be found in [2–4].

Many of the proposed optical encryption methods in the past two decades gained moderate success from different perspectives, but some challenges still remain to be addressed. For example, due to the general use of random phase masks, the final decrypted image from an optical encryption system is usually contaminated with heavy speckle noise, and the image quality is significantly reduced. The speckle noise problem can be alleviated by methods such as multiple captures and averaging [2], fully phased encryption [5], and thresholding of encrypted images [6]. However, the speckle noise can only be suppressed to a certain extent instead of being fully removed.

In recent years, the application of quick response (QR) code in optical information security systems has been very extensively investigated [7–28] and QR coding is employed to achieve noise-free decrypted results. The basic idea of these works is illustrated in Fig. 1. The original plain text is first transformed into QR code pattern(s), which serves as "data containers." If the data format of the plain text is not originally supported by the standard QR coding protocol [29] (e.g., the plain text is a gray-scale image), the conversion between plain text and QR code(s) can be implemented with appropriate additional processing [24]. The QR code pattern image undergoes optical encryption and decryption procedures through one certain optical cryptosystem. The decrypted QR code pattern image will suffer from speckle noise contamination, but the noise can be eliminated by the inherent error-correction mechanism of QR coding [29]. Finally, noise-free decrypted data can be retrieved from the noise-free QR code(s). It should be noted that the feasibility of employing QR code for noise-free optical encryption was verified not only by computer simulation but also by some optical experimental results in past

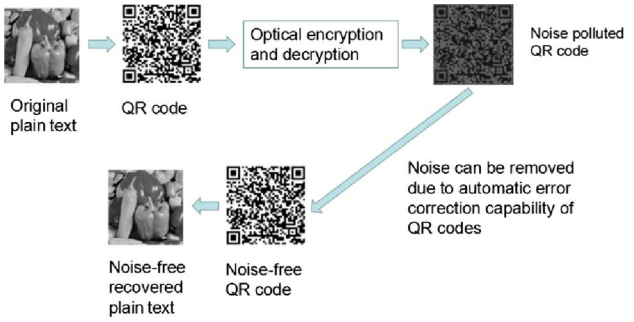


Fig. 1. Application of QR codes in noise-free optical cryptosystems.

works, including joint transform correlator systems [11,12], computational ghost imaging systems [15], digital holography [18], and spatially incoherent illumination systems [28]. Some optodigital techniques [12,18] such as scrambling, nonlinear normalization, and multiplexing were proposed to reinforce QR code-based optical encryption systems in real optical experiments.

Despite the fact that QR code is widely employed in many optical security research works [7–28] and moderate success is gained, the question "Is QR code really a feasible option in optical encryption systems?" remains to be answered. Some previous works discuss the deficiency of QR coding for optical encryption in certain conditions. As pointed out in [2], the QR coding standard [29] was originally designed for automatic identification purposes in manufacturing industries and consumer products. QR codes are mainly employed for storing simple types of data such as characters, words, and short expressions. It is possible to represent a large amount of data such as a gray-scale image by QR codes [24], but the number of code patterns can be rather huge. The data storage capacity of QR code is yet to be improved. In addition, when the number of pixels inside each individual square is reduced, a QR code pattern becomes denser and much less resistant to speckle noise [2].

Recently, a customized data container with spatially separated square dots has been proposed [30] that shows certain advantages over QR code in optical encryption systems. However, the analysis of error-correction coding is not involved in the customized data container scheme proposed in the previous work [30]. The error-correction coding mechanism is a crucial factor affecting the noise resistance capability of a 2D barcode data container in a noisy environment. The data container can be improved from both the aspect of error-correction coding algorithms and the aspect of spatial allocation of square dots [30]. In other words, the proposed scheme in this work can be jointly employed with previous schemes [30] at the same time to achieve better performance.

In this work, we will analyze the feasibility of QR coding in optical encryption systems from the error-correction coding perspective. We propose to replace the Reed–Solomon (RS) coding with Bose–Chaudhuri–Hocquenghem (BCH) coding for a 2D barcode. BCH code can outperform QR code in terms of data storage capacity and noise-resistant capability in optical cryptosystems.

2. ERROR-CORRECTION CODING: QR CODE VERSUS BCH CODE

As stated above, QR code is employed in optical encryption systems because it has an automatic noise-resistant (or error-correction) capability. In this section, we will point out that the RS error-correction mechanism in QR code is not optimally suitable for the nonlocally distributed speckle noise in optical cryptosystems. An alternative error-correction coding scheme, BCH code, is more suitable for this kind of noise distribution from the information coding perspective.

A. QR Code and RS Algorithm

The QR code, defined by the International Organization for Standardization IEC18004 international standard [29], is a 2D barcode pattern widely applied in manufacturing, sales, logistics, storage, transportation, and consumer product industries. A QR code pattern is composed of black and white square dots, representing "0"and "1" binary values, respectively. These binary bits can further represent various forms of information stored in the QR code pattern. The number of square dots in a QR code varies for different versions and examples, as shown in Fig. 2.

The error-correction capability of QR coding is built from two aspects. First, one individual binary square dot in a QR code pattern usually contains multiple pixels (e.g., 3 pixels × 3 pixels) and an averaging and binarization operation of pixel intensities in the same square dot can reduce noise contamination during decoding. Second, the binary values of different square dots are designed based on the RS error-correction algorithm [31], and a certain number of wrong dots can be automatically corrected when the QR code pattern is decoded. Error-correction coding [31] is a technique to enable reliable transmission, storage, or processing of data over noisy communication channels or environments by automatic detecting and correcting errors to reconstruct the original data. Error correction is generally achieved by adding extra data bits to a message before data transmission or processing, and the receiver or reader can check the consistency of delivered message to recover corrupted data. There are various categories of error-correction coding schemes [31], and the RS algorithm is a well-known one.

Since this paper is focused on the application of RS coding, we shall not go deeply into the mathematical principles of RS coding; a comprehensive explanation on the coding principles can be found in [31]. In RS coding, first all the data to be stored (including message bits and error check bits) are divided into symbols. For example, in a QR code, every eight neighboring binary square dots are grouped as one symbol by the RS

Fig. 2. (a) Version 1 QR code with 21 × 21 square dots; (b) Version 3 QR code with 29 × 29 square dots; (c) Version 5 QR code with 37 × 37 square dots.

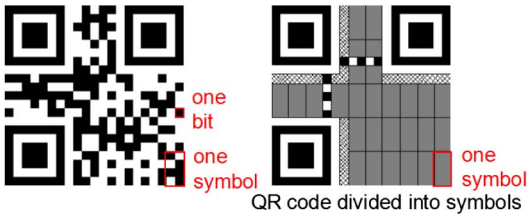


Fig. 3. Grouping bits (square dots) into bytes in RS coding of QR code.

algorithm (shown in Fig. 3). Then for every n symbols, k symbols actually carry a message; $(n-k)$ symbols are error check symbols and at maximum t ($t=(n-k)/2$), wrong symbols can be corrected during decoding (n, k, and t are under certain constraints and are predefined by users). When the number of wrong symbols (within a group of n symbols) is beyond t, the errors cannot be completely corrected, and the decoding will fail. It should be noted that one entire symbol is considered as wrong as long as any single square dot (or bit) inside the symbol is wrong. This feature of RS coding is favorable for restoring locally continuous damage and noise in the code pattern for daily life use (e.g., some part in the QR code pattern is occluded by a logo), but is not favorable for eliminating the nonlocally distributed speckle noise in optical systems.

In optical encryption systems, the speckle noise is usually uniformly and randomly distributed across the entire decrypted image (e.g., Fig. 7). The RS algorithm is not an optimal choice for this type of noise contamination situation, because it will group neighboring bits into symbols during encoding and decoding. The RS algorithm can correct wrong symbols up to a certain percentage in the code pattern (related to the t parameter) depending on the predefined error-correction level (L, 7%; M, 15%; Q, 25%; H, 30%). If one QR code is contaminated with locally continuously distributed noise, damage, or occlusion, the defective square dots are concentrated within a few symbols, shown in Fig. 4(a), and the RS algorithm can usually work successfully. On the other hand, if one QR code is contaminated with uniformly and randomly distributed noise (like the speckle noise in optical encryption systems), the wrong square dots are distributed across the entire pattern and a large number of symbols become wrong, as shown in Fig. 4(b), which can often exceed the upper limit of correctable erroneous symbols and possibly result in decoding failure.

In addition to RS error-correction code, there are many other commonly used error-correction codes such as BCH code, convolutional code, Turbo Code, low density parity check code (LDPC), etc. The above-mentioned problem can be solved by replacing RS code with other error-correction coding schemes. In this paper, BCH code, rather than RS code, is employed for error correction in the binary 2D barcode pattern.

B. BCH Code

In this paper, we design an alternative 2D barcode scheme for noise-free optical encryption systems. Like QR code, the black and white square dots in our proposed barcode represent binary bits. But the error-correction coding mechanism in our code is a BCH algorithm instead of an RS algorithm.

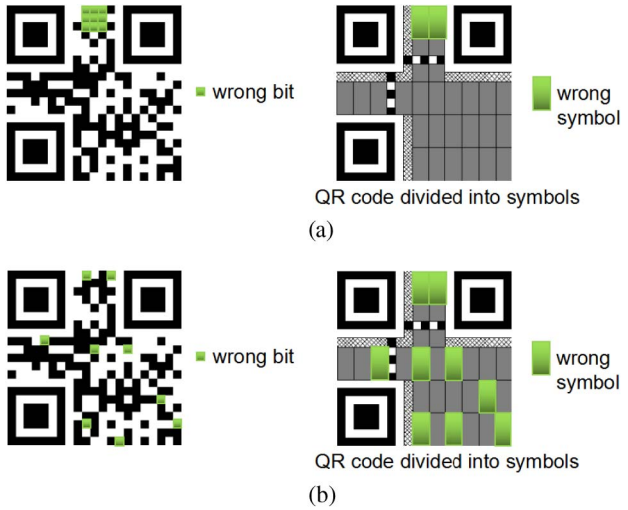


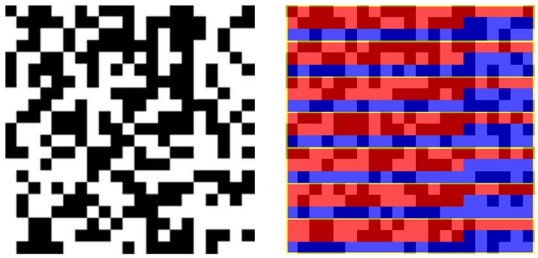
Fig. 4. Relationship between error bits and error symbols in RS coding of QR code when the error bits are distributed (a) in locally continuous regions; (b) evenly and randomly across the entire code pattern.

BCH coding is similar to QR code in that for every n bits, k bits actually carry a message; $(n-k)$ bits are error check bits, and at a maximum t (here $t \neq (n-k)/2$), wrong bits can be corrected during decoding (n, k, and t satisfy certain relationships and are predefined by users). The major difference between BCH code and RS code is that BCH code works on the basis of individual binary square dots (binary bits), but RS code works on the basis of each group of square dots (a symbol). This difference in error-correction mechanism allows BCH code better resistance to nonlocally distributed noise and errors in a 2D barcode pattern. As an example, previous work demonstrates that BCH code can effectively enhance the noise-resistant capability of embedded watermark information in hologram watermarking applications [32].

In BCH coding, it is assumed that originally k binary bits of data are to be encrypted and decrypted optically. After encoding, $(n-k)$ check bits will be added to the original data so a total of n bits will be employed for encryption. In the n bits of data after noise contamination, if the number of error bits is fewer than the number of t bits, all the incorrect bits can be detected and corrected. The k bits of the message can be reconstructed in an error-free manner. The number of check bits $(n-k)$ can be adjusted according to the expected error-correction level and data size requirement. The trade-off of correcting more bit errors in the noisy data is that a smaller amount of a message can be initially stored in the code, and more check bits need to be employed if n is to be fixed. An example of our proposed BCH code is shown in Fig. 5, where the code contains 21×21 square dots; these binary dots are divided into seven subregions. The number of bits in each subregion is 63, with $n=63$ and $k=36$.

3. NUMERICAL SIMULATION RESULTS

In this paper, a Fresnel domain double random phase encoding (DRPE) optical encryption system [33] is employed (shown in



(a) (b)

Fig. 5. (a) One example of our proposed BCH code with 21 × 21 square dots; (b) structure of the BCH code in (a) (red, message bits with $k = 36$; blue, error check bits with $(n - k) = 27$; yellow box, each subregion with $n = 63$ bits).

Fig. 6). In the system, the two propagation distances z_1 and z_2 are set to be both 0.1 m. The optical wavelength is 650 nm and the pixel size is 7 μm.

The encryption and decryption process can be illustrated by Eqs. (1) and (2), respectively,

$$g(x,y) = \mathrm{FrT}\{\mathrm{FrT}[f(x,y)\exp(j\varphi_1(x,y)), z_1]\exp(j\varphi_2(x,y)), z_2\}, \quad (1)$$

$$u(x,y) = |\mathrm{FrT}[\mathrm{FrT}(g^*(x,y), z_2)\exp(j\varphi_2(x,y)), z_1]|, \quad (2)$$

where FrT refers to a Fresnel transform, $\varphi_1(x,y)$ and $\varphi_2(x,y)$ are the two random phase masks, $f(x,y)$ is the original plain text image or QR code pattern image generated from plain text, $g(x,y)$ is the cipher text ($g^*(x,y)$ is the conjugate), and $u(x,y)$ is the decrypted image. It should be noted that the same optical setup (shown in Fig. 6) is employed for both encryption and decryption stages. In practical numerical simulation of the Fresnel light field propagation in Eqs. (1) and (2), either the convolution method or the angular spectrum method [34] can be employed. However, the effect of speckle noise contamination can only be produced by the convolution method (used in this paper), whereas the decrypted image is noiseless and identical to the plain text image by the angular spectrum method.

An example of original plain text image and noise contaminated decrypted result is shown in Figs. 7(a) and 7(b), respectively. Without using error-correction coding, the image quality of the decrypted result is heavily degraded compared with the original plain text image.

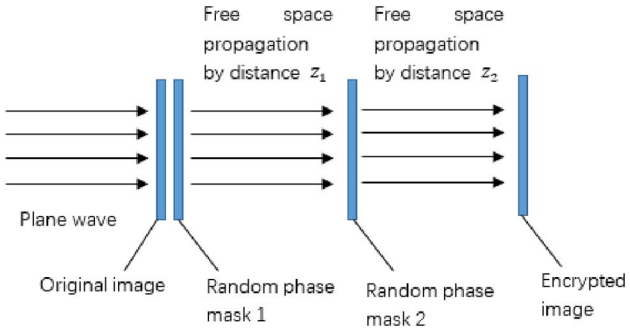


Fig. 6. Fresnel domain DRPE optical encryption system.

(a) (b)

Fig. 7. Example of (a) original input image (plain text) image; and (b) noise-contaminated decrypted image for the Fresnel domain DRPE system in Fig. 5.

QR codes and BCH codes are employed as data containers (or data carriers) in this system, and their performances are compared under the condition that the number of square dots in the patterns is the same. The size of 2D barcode are set to be 21 × 21 (corresponding to Version 1 QR code), 29 × 29 (corresponding to Version 3 QR code) and 37 × 37 (corresponding to Version 5 QR code). In QR code, two different modes of the RS error-correction algorithm, i.e., the L level and the H level, are evaluated.

In either QR code or BCH code, each pixel in the code pattern image is the basic unit for carrying information, despite the fact that multiple pixels jointly constitute a square dot. We define the average channel capacity (ACC) to measure the noise-free information capacity of a given coding scheme in an optical encryption system. The ACC is calculated by the total number of data bits that can be stored noise-free in the 2D barcode, divided by the total number of image pixels in the 2D barcode pattern, in the unit of bits/pixel. On one hand, the ACC is a measure of information storage capacity when the same amount of noise is eliminated. On the other hand, the ACC is a measure of noise-resistant capability when the information storage capacity is the same in the barcode.

It is assumed that the number of square dots in the 2D barcode pattern is X ($X = 21 \times 21$, 29×29 or 37×37 in this work). The number of pixels in each square dot is Y (for example, $Y = 1 \times 1$, 2×2, or 3×3). In numerical simulation, when the QR code or BCH code with certain parameters is employed, the value of Y is gradually adjusted from high value to low value (e.g., from 5×5 to 4×4 to 3×3…) until the entire original message stored in the QR code or BCH code can be recovered noise-free. The minimum Y value, $Y_{\min}$, is closely related to the noise-free data storage capacity of a 2D barcode pattern under a certain noisy environment. The maximum number of message bits stored in the 2D barcode is assumed to be M, and the channel capacity (CC) can be defined as follows:

$$\mathrm{CC} = \frac{M}{X \cdot Y_{\min}}. \quad (3)$$

For an optical encryption system like the Fresnel domain DRPE system, the random phase masks can vary in each time of simulation, and $Y_{\min}$ may vary accordingly due to change of

noise distribution each time in the decrypted result. As a consequence, the CC value is not absolutely fixed. The numerical simulation can be repetitively performed for N times and the ACC can be obtained from the average value of CC at each time of simulation, given by the following:

$$\mathrm{ACC} = \frac{1}{N}\sum_{n=1}^{N} \mathrm{CC}_n. \tag{4}$$

In this work, the encoding of QR code follows the QR code standard rules [29], and the decoding is performed by "ZXing Decoder Online" [35]. The encoding and decoding of BCH code simply follows the BCH coding principles [31]. When the number of square dots is 21×21, the parameters are set to be $n = 63$ and $k = 36$ for BCH coding. When the number of square dots is 29×29 and 37×37, the parameters are set to be $n = 255$ and $k = 131$ for BCH coding. In addition, since a QR code pattern consists of some square dots as functional patterns that do not carry information (such as the three location markers at top left, top right, and bottom left corners), we test pure RS barcodes in the simulation as well. The pure RS barcode employs RS error-correction coding algorithm like QR code, but every square dot in the pure RS code is an information carrier without functional patterns (like our proposed BCH code in Fig. 5). The comparison between pure RS code and BCH code can more faithfully reflect the advantage of BCH coding over RS coding in resisting nonlocally distributed speckle noise. When the number of square dots is 21×21, the parameters are set to be ($n = 26$, $k = 19$) for pure RS coding. When it is 29×29, the parameters are set to be ($n = 70$, $k = 55$) and ($n = 26$, $k = 19$) for different subregions. When it is 37×37, the parameters are set to be ($n = 134$, $k = 108$) and ($n = 26$, $k = 19$). The ACC values for three different-sized 2D barcode patterns with QR coding, pure RS coding, and BCH coding are presented in Table 1.

From the results, it can be observed that the ACC values for pure RS code are higher than for QR code (with different error-correction levels), because the elimination of functional patterns increases the storage capacity of the barcode. It is obvious that our proposed BCH code can achieve a significantly higher ACC value than both QR code and pure RS code when the barcodes are different sizes. This indicates that BCH code possesses a larger data storage capacity or a stronger noise-resistant capability than QR code. BCH code is a more suitable option of "data container" than a barcode based on the RS algorithm for noise-free optical encryption systems.

Table 1. ACC Values for Three Different-Sized 2D Barcode Patterns with QR Coding, Pure RS Coding, and BCH Coding (in the Unit of Bits/Pixel) When the Cipher Text Is Intact

No. of square dots in the 2D barcode pattern	21×21	29×29	37×37
ACC for QR code with L level error correction	0.0447	0.0556	0.0671
ACC for QR code with H level error correction	0.034	0.0492	0.0311
ACC for pure RS code	0.0626	0.0697	0.071
ACC for BCH code	0.1058	0.1103	0.1063

Table 2. ACC Values for Three Different-Sized 2D Barcode Patterns with QR Coding, Pure RS Coding, and BCH Coding (in the Unit of Bits/Pixel) When the Cipher Text Is Partially Occluded

No. of square dots in the 2D barcode pattern	21×21	29×29	37×37
ACC for QR code with L level error correction	0.0355	0.0523	0.0614
ACC for QR code with H level error correction	0.0326	0.0373	0.0299
ACC for pure RS code	0.0601	0.0585	0.0579
ACC for BCH code	0.1032	0.1080	0.0928

Furthermore, we compare the performance of different barcodes when the cipher text is partially occluded. It is assumed that 75% of the cipher text is missing; the ACC values for different coding are presented in Table 2. It can be observed that all the ACC values in different schemes decrease correspondingly compared with Table 1, since the occlusion in the cipher text introduces more noise in the decrypted result. However, our proposed BCH coding still performs better than QR code and pure RS code. The results indicate that our proposed BCH coding is robust to occlusion in the cipher text.

One specific example is given below to further demonstrate the outperformance of BCH code over QR code in terms of data storage capacity. A QR code (L level) and a BCH code with a size of 21×21 square dots [Figs. 8(a) and 8(b)] are tested in the optical encryption system. The number of pixels in each square dot can be reduced to 3×3 at most for both cases to ensure a stable noise-free decrypted result. In BCH code, the parameters are set to be ($n = 63$, $k = 36$) to obtain sufficient error-correction capability and maximum data storage capacity at the same time. The noise-contaminated decrypted results for both codes are shown in Figs. 8(b) and 8(f), respectively. Then the noisy gray-scale images in Figs. 8(b) and 8(f) are binarized into binary square code images by calculating the average pixel values inside each square dot and thresholding the

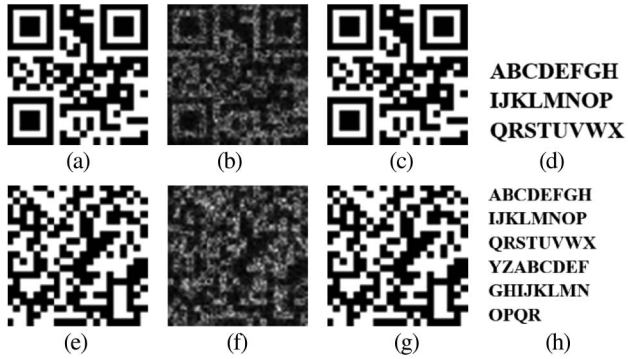


Fig. 8. (a) QR code (L level) with 21×21 square dots; (b) noise-corrupted decrypted result for (a); (c) restored result with error-correction code for (a); (d) amount of information stored in the QR code (24 alphanumeric letters); (e) BCH code with 21×21 square dots ($n = 63$, $k = 36$); (f) noise-corrupted decrypted result for (e); (g) restored result with error-correction code for (e); (h) amount of information stored in the BCH code (44 alphanumeric letters).

average value to 0 or 1 regarding the average intensity of the entire code image (like the approach used in [36,26]). The obtained binary code images may contain a number of wrong dots and can be recovered by QR code decoding or BCH error-correction decoding in each case. The final recovered results after decoding are shown in Figs. 8(c) and 8(f), respectively; they are noise-free compared with Figs. 8(a) and 8(e). Even though both codes exhibit similar noise-resistant capability, the amount of information that can be stored in the QR code is only 24 alphanumeric letters (up to 152 bits), but it is 44 alphanumeric letters in BCH code, shown in Figs. 8(d) and 8(h). The data storage capacity for BCH code is evidently higher than for QR code under similar conditions.

Another specific example is given below to demonstrate the outperformance of BCH code over QR code in noise-resistance capability. A QR code (L level) and a BCH code with a size of 21×21 square dots are compared. In both the QR code and BCH code, the number of pixels in each square dot is 3 pixels × 3 pixels. The parameters in BCH coding are set to be $n = 63$ and $k = 24$ to ensure the storage capacity of both codes are very close (152 bits and 168 bits). The noise-free QR code and BCH code are shown in Figs. 9(a) and 9(e), respectively. When the cipher text is intact, the noise-contaminated decrypted code images are shown in Figs. 9(b) and 9(f), respectively. In both cases, after error-correction coding, noise-free results can be recovered from Figs. 9(b) and 9(f), which are identical to Figs. 9(a) and 9(e). When the cipher text is cropped to 10% of the original area, the decrypted code images [Figs. 9(c) and 9(g), respectively], exhibit stronger noise contamination compared with Figs. 9(b) and 9(f). For Fig. 9(g), after binarization and BCH error-correction decoding, the recovered result is shown in Fig. 9(h), which does not contain any wrong square dots compared with Fig. 9(e). However, after Fig. 9(c) is binarized, the binary code shown in Fig. 9(d) contains a number of wrong dots compared with Fig. 9(a), which is beyond the upper limit of RS error-correction coding in a QR code reader and cannot be further restored. The overall results in Fig. 9 indicate that the BCH code in this example demonstrates stronger noise-resistant capability than the QR code, while the BCH code stores slightly more data than the QR code (168 bits versus 152 bits).

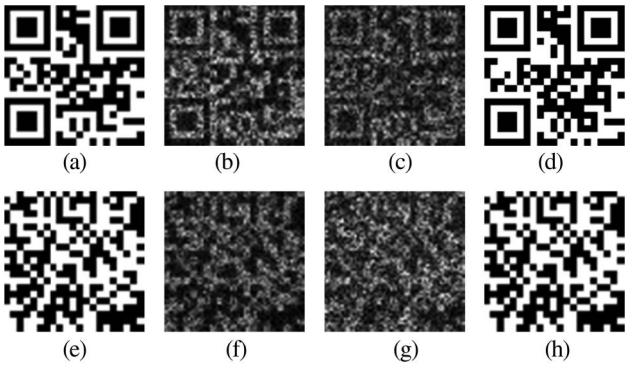


Fig. 9. (a) QR code (L level) with 21 × 21 square dots (data storage capacity: 152 bits); (b) noise-corrupted decrypted result for Fig. 8(a) when the cipher text is intact; (c) noise-corrupted decrypted result for Fig. 8(a) when the cipher text is cropped to 10% of original area; (d) binarization result of Fig. 8(c) (beyond the error-correction capability of QR code); (e) BCH code with 21×21 square dots ($n = 63$, $k = 24$; data storage capacity, 168 bits); (f) noise-corrupted decrypted result for Fig. 8(e) when the cipher text is intact; (g) noise-corrupted decrypted result for Fig. 8(e) when the cipher text is cropped to 10% of original area; (h) recovered noise-free result after binarization and BCH error-correction decoding is performed on Fig. 8(g).

In this work, all analysis and evaluation above are performed based on a simulated Fresnel domain DRPE optical encryption system. The real implementation of a DRPE system in optical experiments still remains a challenging issue in state-of-the-art works due to practical difficulties such as precise alignment of random phase masks. As a consequence, numerical simulation is commonly employed in research works related to DRPE and other optical encryption systems. Certain discrepancies between simulation results and experimental results can be inevitable. For example, the speckle noise intensity in real experiments may be stronger than simulation results. However, as long as the speckle noise in real experiments is still nonlocally spread over the entire code pattern, BCH coding will have an evident advantage over QR coding. In fact, from previous works [11,12,15,18,28], the speckle noise in the experimental results from different optical encryption systems generally demonstrates an appearance of nonlocally spread distribution (similar to simulation results).

4. CONCLUSION

In recent years, numerous research works have investigated employing QR codes to achieve noise-free optical encryption. In this paper, we point out that the RS error-correction coding mechanism in QR code is not a very suitable option for the nonlocally distributed speckle noise in optical encryption systems. We propose an alternative 2D barcode scheme based on BCH coding, rather than RS coding, for optical cryptosystems. In numerical simulation, our proposed BCH code demonstrates better data storage capacity and noise-resistant capability than QR codes in terms of ACC. Furthermore, in addition to RS coding and BCH coding, there are many other error-correction coding schemes in telecommunication and information engineering such as convolutional coding, LDPC coding, and Turbo coding [37]. These more advanced coding schemes can be attempted for noise-free optical cryptosystems, and better results can possibly be achieved.

Funding. National Natural Science Foundation of China (NSFC) (61401287); Natural Science Foundation of Shenzhen (JCYJ20160307154003475, JCYJ2016050617265125).

REFERENCES

1. P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," Opt. Lett. **20**, 767–769 (1995).
2. 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).

3. S. Liu, C. Guo, and J. T. Sheridan, "A review of optical image encryption techniques," Opt. Laser Technol. **57**, 327–342 (2014).
4. W. Chen, B. Javidi, and X. Chen, "Advances in optical security systems," Adv. Opt. Photon. **6**, 120–155 (2014).
5. N. Towghi, B. Javidi, and Z. Luo, "Fully phase encrypted image processor," J. Opt. Soc. Am. A **16**, 1915–1927 (1999).
6. B. Javidi, N. Towghi, N. Maghzi, and S. C. Verrall, "Error-reduction techniques and error analysis for fully phase-and amplitude-based encryption," Appl. Opt. **39**, 4117–4130 (2000).
7. J. F. Barrera, A. Mira, and R. Torroba, "Optical encryption and QR codes: secure and noise-free information retrieval," Opt. Express **21**, 5373–5378 (2013).
8. A. Markman, B. Javidi, and M. Tehranipoor, "Photon-counting security tagging and verification using optically encoded QR codes," IEEE Photon. J. **6**, 1–9 (2014).
9. C. Lin, X. Shen, and B. Li, "Four-dimensional key design in amplitude, phase, polarization and distance for optical encryption based on polarization digital holography and QR code," Opt. Express **22**, 20727–20739 (2014).
10. Y. Qin and Q. Gong, "Optical information encryption based on incoherent superposition with the help of the QR code," Opt. Commun. **310**, 69–74 (2014).
11. J. F. Barrera, A. Mira-Agudelo, and R. Torroba, "Experimental QR code optical encryption: noise-free data recovering," Opt. Lett. **39**, 3074–3077 (2014).
12. J. F. Barrera, A. Vélez, and R. Torroba, "Experimental scrambling and noise reduction applied to the optical encryption of QR codes," Opt. Express **22**, 20268–20277 (2014).
13. Z. Ren, P. Su, J. Ma, and G. Jin, "Secure and noise-free holographic encryption with a quick-response code," Chin. Opt. Lett. **12**, 010601 (2014).
14. Z. Wang, S. Zhang, H. Liu, and Y. Qin, "Single-intensity-recording optical encryption technique based on phase retrieval algorithm and QR code," Opt. Commun. **332**, 36–41 (2014).
15. S. Zhao, L. Wang, W. Liang, W. Cheng, and L. Gong, "High performance optical encryption based on computational ghost imaging with QR code and compressive sensing technique," Opt. Commun. **353**, 90–95 (2015).
16. X. Deng, "Optical image encryption based on real-valued coding and subtracting with the help of QR code," Opt. Commun. **349**, 48–53 (2015).
17. C. Lin, X. Shen, B. Hua, and Z. Wang, "Three-dimensional polarization marked multiple-QR code encryption by optimizing a single vectorial beam," Opt. Commun. **352**, 25–32 (2015).
18. S. Trejos, J. F. Barrera, and R. Torroba, "Optimized and secure technique for multiplexing QR code images of single characters: application to noiseless messages retrieval," J. Opt. **17**, 085702 (2015).
19. 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).
20. X. Wang, W. Chen, S. Mei, and X. Chen, "Optically secured information retrieval using two authenticated phase-only masks," Sci. Rep. **5**, 15668 (2015).
21. Y. Qin, H. Wang, Z. Wang, Q. Gong, and D. Wang, "Encryption of QR code and grayscale image in interference-based scheme with high quality retrieval and silhouette problem removal," Opt. Lasers Eng. **84**, 62–73 (2016).
22. P. Tsang, "Enhanced single random phase holographic encryption," in *Digital Holography and Three-Dimensional Imaging* (OSA, 2016), paper DT2E.2.
23. T. Sanpei, T. Shimobaba, T. Kakue, Y. Endo, R. Hirayama, D. Hiyama, S. Hasegawa, Y. Nagahama, M. Sano, M. Oikawa, T. Sugie, and T. Ito, "Optical encryption for large-sized images," Opt. Commun. **361**, 138–142 (2016).
24. S. Jiao, W. Zou, and X. Li, "QR code based noise-free optical encryption and decryption of a gray scale image," Opt. Commun. **387**, 235–240 (2017).
25. P. W. M. Tsang, "Single-random-phase holographic encryption of images," Opt. Lasers Eng. **89**, 22–28 (2017).
26. T. Shimobaba, Y. Endo, R. Hirayama, Y. Nagahama, T. Takahashi, T. Nishitsuji, T. Kakue, A. Shiraki, N. Takada, N. Masuda, and T. Ito, "Autoencoder-based holographic image restoration," Appl. Opt. **56**, F27–F30 (2017).
27. H. Li, C. Guo, I. Muniraj, B. C. Schroeder, J. T. Sheridan, and S. Jia, "Volumetric light-field encryption at the microscopic scale," Sci. Rep. **7**, 40113 (2017).
28. P. A. Cheremkhin, V. V. Krasnov, V. G. Rodin, and R. S. Starikov, "QR code optical encryption using spatially incoherent illumination," Laser Phys. Lett. **14**, 026202 (2017).
29. International Organization for Standardization, *Information Technology: Automatic Identification and Data Capture Techniques-QR Code 2005 Bar Code Symbology Specification*, 2nd ed., IEC18004 (ISO, 2006).
30. A. V. Zea, J. F. Barrera, and R. Torroba, "Customized data container for improved performance in optical cryptosystems," J. Opt. **18**, 125702 (2016).
31. S. Lin and D. J. Costello, *Error Control Coding* (Pearson Education, 2004).
32. Z. Zhuang, S. Jiao, W. Zou, and X. Li, "Embedding intensity image into a binary hologram with strong noise resistant capability," Opt. Commun. **403**, 245–251 (2017).
33. G. Situ and J. Zhang, "Double random-phase encoding in the Fresnel domain," Opt. Lett. **29**, 1584–1586 (2004).
34. T. C. Poon, *Digital Holography and Three-Dimensional Display: Principles and Applications* (Springer, 2006).
35. ZXing Decoder Online, https://zxing.org/w/decode.jspx.
36. J. Shuming and P. W. M. Tsang, "An iterative algorithm for holographic-QR (H-QR) code damage restoration," in *IEEE 13th International Conference on Industrial Informatics* (IEEE, 2015), pp. 682–685.
37. S. Jiao, W. Zou, and X. Li, "Noise removal for optical holographic encryption from telecommunication engineering perspective," in *Digital Holography and Three-Dimensional Imaging* (OSA, 2017), paper Th2A.5.