scientific reports

OPEN

A QR code-based user-friendly visual cryptography scheme

Lijing Ren[1,2] & Denghui Zhang[1]✉

Benefiting from the development of the Internet and smart devices, it is now convenient to transmit images anywhere and anytime, which poses a new challenge for image security. The Visual Cryptography Scheme (VCS) is a secret sharing method for protecting an image without a key, the merit of VCS is the human visual system (HVS) can restore the secret image by simply superimposing qualified shares, without any computation. To eliminate noise-like shares in traditional VCS, this paper presents a novel QR code-based expansion-free and meaningful visual cryptography scheme (QEVCS), which generates visually appealing QR codes for transmitting meaningful shares. When distributing on public networks, this scheme does not attract the attention of potential attackers. By limiting the gray-level of a halftoned image, QEVCS both keep the computation-free of visual cryptography and the size of recovery image same as the secret images. The experimental results show the effectiveness of QEVCS when preserving the privacy of images.

In recent years, the rapid development of smart devices and 5G technologies have had a great impact on all walks of life, now people are enjoying conveniences brought by Internet services. As an important information carrier, digital images are widely used in fields including pattern recognition, virtual reality, and medical imaging[1]. The universality poses new challenges for personal privacy. With information leakage accidents emerging, it is urgent to protect important information in digital images[2,3]. Although the traditional cryptography, watermarking, and steganography techniques can protect sensitive information by encryption[4,5], the encryption and decryption processes are computationally intensive and require a lot of effort to the keys in these schemes.

Secret sharing is a scheme to split a secret into multiple shares, and each share is managed by different participants. Only qualified participants can collaborate to recover the secret message, while a single participant reveals nothing about the secret message. VCS is one of the secret-sharing methods for image security, which was first proposed by Naor and Shamir[6]. Since then, it has received widespread attention from researchers. The merit of VC lies in that HVS can restore the secret image by simply superimposing qualified shares, without any digital devices. VCS solves the problems of key management in traditional cryptography and provides a simple and effective method for distributed storage of images. However, VCS has suffered two drawbacks: (1) *pixel-expansion*: due to the use of subpixels with multiple pixels to encrypt a single secret pixel, the size of shared images is larger than the original image; (2) *meaningless*, VC protects a secret image by sharing it into noise-like shares. The shares prevent information leakage. However, it is difficult to distinguish each other and brings a burden for the management of noise-like shares.

Quick Response (QR) code is a kind of popular two-dimensional barcode[7], which is a machine-readable optical label with the advantages of speed reading, error correction ability, rich data formats[8]. Benefitting from the development of the mobile Internet, QR code is widely used to transmit complex digital information in the physical world, such as payment information, contact cards, and advertisements.

The appearance of the QR code is similar to the share of VCS, which both are black-and-white images (binary image). QR codes provide a suitable carrier for the transmission of shares. Researchers have put forward many contributions to aggregate the advantages of VCS and QR codes. Pan et al.[9] use four or more color QR codes to generate meaningful shares based on the color XOR scheme. Although the proposed scheme can fully restore a secret image, it still needs a meaningless share to meet the XOR operation constraint. Wan et al.[10] presented a scheme to alter the bits corresponding in the range of the error correction mechanism. HVS can reveal the secret image by stacking. When the computation is available, it can reveal a better visual quality image based on the XOR operation. To meet the error correction conditions, the larger the secret image, the more share images are generated. Tan et al.[11] proposed an XOR-based VCS applying to grayscale QR codes. The scheme substitutes a bit of a share for the second significant bit of the QR code cover image, which can resist common image attacks. Cheng et al.[12] designed an innovative two-level QR code that takes advantage of the concentric feature in the

[1]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, People's Republic of China. [2]School of Traffic and Transportation, Shijiazhuang Tiedao University, Shijiazhuang 050043, People's Republic of China. ✉email: zhang.denghui@foxmail.com

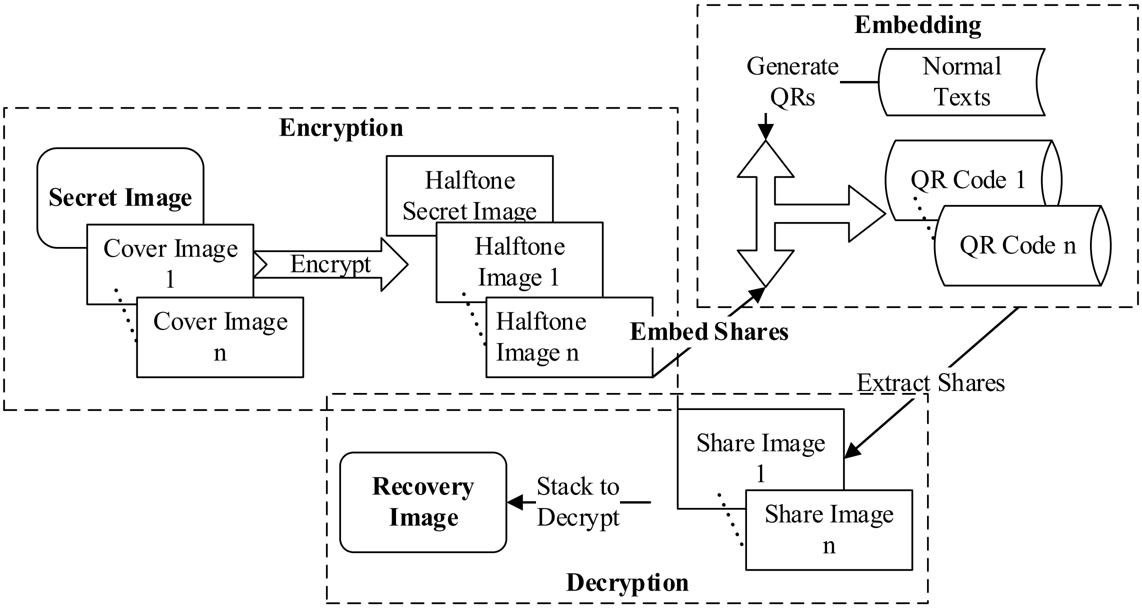


Figure 1. The encryption and decryption architecture of the proposed QEVCS.

QR code and replaces a module with a cell with 3 × 3 sub-modules. The concentric sub-module contains the public message while the remaining store secret messages. The scheme can recover secret messages with XOR and threshold operations. Cheng et al.[13] presented a novel scheme for $(n, n)(n \geq 3)$ threshold to improve the security of QR codes with XOR-based VCS. The proposed scheme further extended the access structure from (n, n) to (k, n) by the error correction mechanism of QR codes.

The aforementioned schemes cannot restore the secret image by simply superimposing images like the original VCS due to the XOR operation. However, it is still expected to reveal images directly through HVS in many scenarios including medical images and paper maps[14]. Our scheme can be applied to these scenes without cryptographic computation.

In this paper, we propose a QR code-based VCS to address the pixel-expansion and meaningless issues in VCS. First, we design a block-by-block extended VCS (EVCS, also called user-friendly VCS) to archive meaningful shares on the premise of keeping the size-invariant of secret images, thereby avoiding suspicion in potential attackers. With the OR operation, HVS can directly reveal the secret image by simply overlapping received shares. Then, we use the rich data capacity of QR codes to transmit shares. The encoded QR codes do not destroy the error correction codewords and can be scanned and decoded by a normal QR code reader. QECVS realizes the secure transmission of secret images without destroying the advantages of QR codes and VCS.

QEVCS: a QR code-based expansion-free extended visual cryptography scheme

The ideas behind QEVCS are (1) keeping the size-invariant when archiving meaningful shares of an image; (2) transmitting shares using QR codes. As shown in Fig. 1, QEVCS divides the encryption process of images into two parts. Firstly, we propose a gray-level limited EVCS, which splits a secret image into two equal-sized and meaningful cover images, and then embed cover images into coressponding QR codes images by using the gray decoding and concentric decoding characteristics of QR codes, so as to realize the QR codes transmission of a secret image. We will first introduce the proposed expansion-free EVCS.

In the original EVCS, to encrypt a single pixel, it needs a sub-pixel composed of multiple pixels for secret sharing. A common method is block-wise encryption[14,15] for eliminating pixel expansion. The basic idea of block encryption is to encrypt by sharing blocks whose size is equal to that of the secret block. To eliminate the same pixel expansion problem in the traditional EVCS model, we use a block-based halftoning operation instead of pixel-by-pixel encryption to maintain sizes in the secret block and share blocks.

The proposed QEVCS has to ensure that the generated pixel blocks meet the requirement of EVCS encryption during halftoning. Grayscale images have 256 levels, while images generated by VCS only have two grayscale levels of black and white. Therefore, halftone is indispensable to transmit images using EVCS. Algorithm 1 shows the flow of the proposed limited gray-level halftoning algorithm. The whole encoding flow of QEVCS is described in detail in Algorithm 2.

The size of the block s_b is the same as the pixel expansion value in the (k, n)-EVCS. When binarizing a grayscale image, the gray-level $\mathrm{b_{Bs}}$ of the secret block and the gray-levels $\mathrm{b_{B1}}, \mathrm{b_{B2}}$ of cover blocks have to satisfy the following relationship:

$$\mathrm{b_{Bs}} \in [\max(0, \mathrm{b_{B1}} + \mathrm{b_{B2}} - \mathrm{s_b}), \min(\mathrm{b_{B1}}, \mathrm{b_{B2}})] \tag{1}$$

The constraint enables it to reuse the existing EVCS when addressing pixel expansion in original methods. To reduce the loss of image quality, we can adjust the combination of sharing blocks. The algorithm is no longer constrained to produce a binary output with a single threshold but determines the closest allowed visual grayscale to generate an output image of more than two levels.

Algorithm 1: limited gray-level halftoning algorithm ($gray\_level$)

```
Data: Pixel block $B$, a collection of candidate black level $g_s$, block size $s_b$
Result: halftoning equal-sized block $B_h$
$s_l$ ←the size of $g_s$
$m \leftarrow \lfloor s_l/(s_b+1) \times (s_l - \sum Bi/255) \rfloor$
for each pixel $p$ in $B_h$ do
  | $p = 1$
end
$P$←randomly sample $g_{sm}$ elements from $[0, 1, \ldots, n], n <= s_b$
for each pixel $p$ in $P$ do
  | $B_{hp} = 0$
end
```

Algorithm 2: QEVCS: A QR code-based Expansion-free Extended Visual Cryptography Scheme

```
Data: A secret image $S$, Cover Images $H_1$, $H_2$, public message $M_1$, and $M_2$
Result: Share images $share_1$ and $share_2$ dispatched to participants $P_1$, and $P_2$
$s_s$ ←the size of the secret image $S$ and two cover images
$g_s$ ←a collection of the number of black pixel in recovery secret black
$g_{hi}$ ←a collection of the number of black pixel in basis matrix, $i \in \{1, 2\}$
for $i$ in range(0, $s_s - 1$, $s_b$) do
    $B_{si} = S[(i \times s_b) : ((i+1) \times s_b)]$
    funcall($gray\_level, B_{si}, g_s, s_b$)
    $B_{hij} = H_i[(j \times s_b) : ((j+1) \times s_b)]$
    funcall($gray\_level, B_{hij}, g_{hi}, s_b$)
end
for $j$ in range(0, $s_s - 1$, $s_b$) do
    $c_s$ ←the color block of $B_{sj}$, $c_s$ is interpreted as white or black pixels
    $c_{hi}$ ←the color block of $B_{hij}$, $i \in \{1, 2\}$, $c_{hi}$ is interpreted as white or black
      pixels
    $C \leftarrow$ all the matrics obtained by permuting the columns of $S^{c_s}_{c_{h1}c_{h2}}$
    $p$ ←a random, $0 <= p <= k$
    for each row $r_m$ in $C_p$ do
      | $share_m[(i \times s_b) : ((i+1) \times s_b)] = r_m$
    end
end
for $i$ in 1,2 do
    $Q_i$ ←the QR codes image for $M_i$
    Expand $Q_i$ to be larger than $share_i$, while the size of $Q_i$ is a multiple of 3
    $M_{mask}$ ←a image consists of reserved positions in a spefcific version of QR
      codes
    $share_i$ ←funcall(mix, $share_i$, $Q_i$)
    for $x, y$ in $M_{mask}$ do
      | $share_i(x, y)$+=funcall(sign, 128-$share_i(x, y)$)×$M_{mask}(x, y)$/255
    end
end
```

In the encoding process, a grayscale image is first divided into *n* non-overlapping black-and-white pixel blocks B_i, $B_i \cap B_j = \varnothing$, for$1 \leq i \neq j \leq n$. The B_i before halftoning and the block B_h after halftoning are both of the same size. The number of black pixels in B_i and B_h has to satisfy the following condition:

$$b_{Bi} = \left\lfloor s_l/(s_b+1) \times \left(s_l - \sum B_i/255\right) \right\rfloor \qquad (2)$$

where s_l denotes the number of candidate black blocks. For a secret block with the size $s_b = 2 \times 2$, the gray level is ranged from $b_{Bi} \in [0, 1, 2, 3, 4]$ after halftoning. Before converting the original gray image into a black-and-white image, it is necessary to determine the block criterion of the image. In the error diffusion algorithm, all five gray levels may appear, thus producing a halftone image similar to the original image. To ensure the gray-levels of cover blocks after halftoning can meet the requirement for the gray-level of the secret block, we use only a limited number of gray-levels in the chunked halftone set while fixing the ratio of black and white pixels in each block. Taking the (2,2)-EVCS for example, after splitting a secret image into (2,2) blocks, the number of black pixels can only be 3 or 4, that is, $g_s = [3, 4]$. While the number of black pixels in cover images only be 2 and 3, that is, $g_s = [2, 3]$. After completing the limited halftone of the secret image and cover images, we can combine the existing EVCS to rearrange the pixels of the halftoned block according to the secret color block.

Note that we do not use error-effusion technology in the *gray_level* method. Limiting gray levels is equivalent to reducing gray values artificially. Using the error-diffusion technology will quickly accumulate the white error of current pixels to adjacent pixels. It will result in the subsequent pixels becoming all-white blocks and generating images with lower quality.

The original purpose of a QR code is to transmit text information. Although the capacity increases with the increasing version, its capacity is still limited relative to the image. It can be seen that the size of the largest QR codes is only 177×177, and the size of an image is much larger than this size. If an image is directly embedded into a QR code, it will destroy the encoding rules of the QR code, which will make it difficult to identify.

$$M = \begin{bmatrix} p_{1,1} & p_{1,2} & p_{1,3} \\ p_{2,1} & p_{2,2} & p_{2,3} \\ p_{3,1} & p_{3,2} & p_{3,3} \end{bmatrix}_{\cdots} \tag{3}$$

$$p_{scan} = \tau(M_c) \tag{4}$$

The above operation shows the real value read by a reader when denoting a module in QR codes with a block M, where τ is a threshold function, M_c is the centric pixel in M and p_{scan} is the fetched pixel. Based on the centric property of QR codes, we first expand the size of QR codes so that its size is a multiple of the minimum 3 of the secret image. Then we overlay the pixels in the QR code to the position of M_c in the image pixel-by-pixel, while keeping the other pixels like $p_{1,1}, p_{n,n}$ in the cover image unchanged. HVS can still identify the image mixed with QR code and meaningful shares. However, because QR codes will overlay part of the share pixels, we further utilize the gray property of QR codes to embed shared pixels into the least significant bit of QR codes at the corresponding position of cover images:

$$P_Q(x,y) = P_Q(x,y) + sign\left(128 - P_Q(x,y)\right) \times p_e/255 \tag{5}$$

where p_e is the embedded pixel in the cover images, and $P_Q(x,y)$ is the corresponding pixel in the QR codes image. If p_e is a black pixel, $P_Q(x,y)$ will be unchanged. While if p_e and $P_Q(x,y)$ are both white pixel (255), the gray-level of $P_Q(x,y)$ will be 254. If p_e is a white pixel while $P_Q(x,y)$ is a black pixel, its gray level will be 1. It can be inferred that no matter which the gray-level of a pixel is, the influence on the gray value of the original pixel after the embedding operation does not exceed 1, thus archiving the minimum disturbance to QR codes.

Experiments and analyses

In this section, we will evaluate the effectiveness of the proposed QEVCS. Figure 2 shows the experimental result processed with the limited halftone (*gray_level*). The selected test images are the classic Barbara (Fig. 2a), Butterfly (Fig. 2e), and Peppers (Fig. 2i). The first column is original gray-scale images, the second column (Fig. 2b,f,j) is halftone images generated by the ER method, the third (Fig. 2c,g,k) and fourth (Fig. 2d,h,l) columns are halftone images generated by *gray_level* with two thresholds. The difference is that the third column represents black and white pixels with subpixels with 2/4 and 3/4 black pixels respectively, while the fourth column represents black and white pixels with 3/4 and 4/4 black pixels.

The limited halftone scheme reinterprets the color blocks with different proportions of black pixels (or white) into black (or white) pixels, thus matching the underlying EVCS schemes. By comparing images in the third and fourth columns, we can see that the contrast of images varies with the proportion of black and white blocks. There are different levels of image degradation. Because images in the second column adopt ER, the visual effect of the generated image is close to that of the original image. While the proportion of black pixels in the color block is constrained in the fourth column. The removal of the block arrangement with 4, 3, and 2 white pixels leads to a degradation of the quality of the recovered image, it can be seen that the recovered image is darker. However, we can still see the features of the original images.

Figure 3 shows the encrypted cover images and images mixed with meaningful shares and QR codes. Figure 3a–h is cover images mixed with QR codes and images embedded with overlayed pixels, and parsed information, respectively. Because QR codes are superimposed on the share shares, Fig. 3b(f) becomes darker compared with Fig. 3a(e). But Fig. 3c is visually unchanged. When the images of shares and QR codes are mixed, the black position in Fig. 3i will be overlapped by the pixels in QR codes, while the white areas will remain as the pixel in share images. Figure 3j is the difference image between Fig. 3f and g. Because we embed the overlapped pixels into the least significant bit of the pixels in QR codes, there is no difference between them. Figure 3k is the recovery image, which is the same as Fig. 2d.

We further evaluate the effectiveness of QEVCS on a plain text image. Figure 4a,b are QR code images that can be scanned and read normally. Parsed information is shown in Fig. 4c,d. Figure 4e,f are the secret and recovery image. As shown in Fig. 4, we can achieve good results on text images than normal images. This is because white pixels constitute the background, so its loss has little influence on image restoration. Benefiting from the property of perfect black of QEVCS, we can completely recover the black blocks that form secret characters.

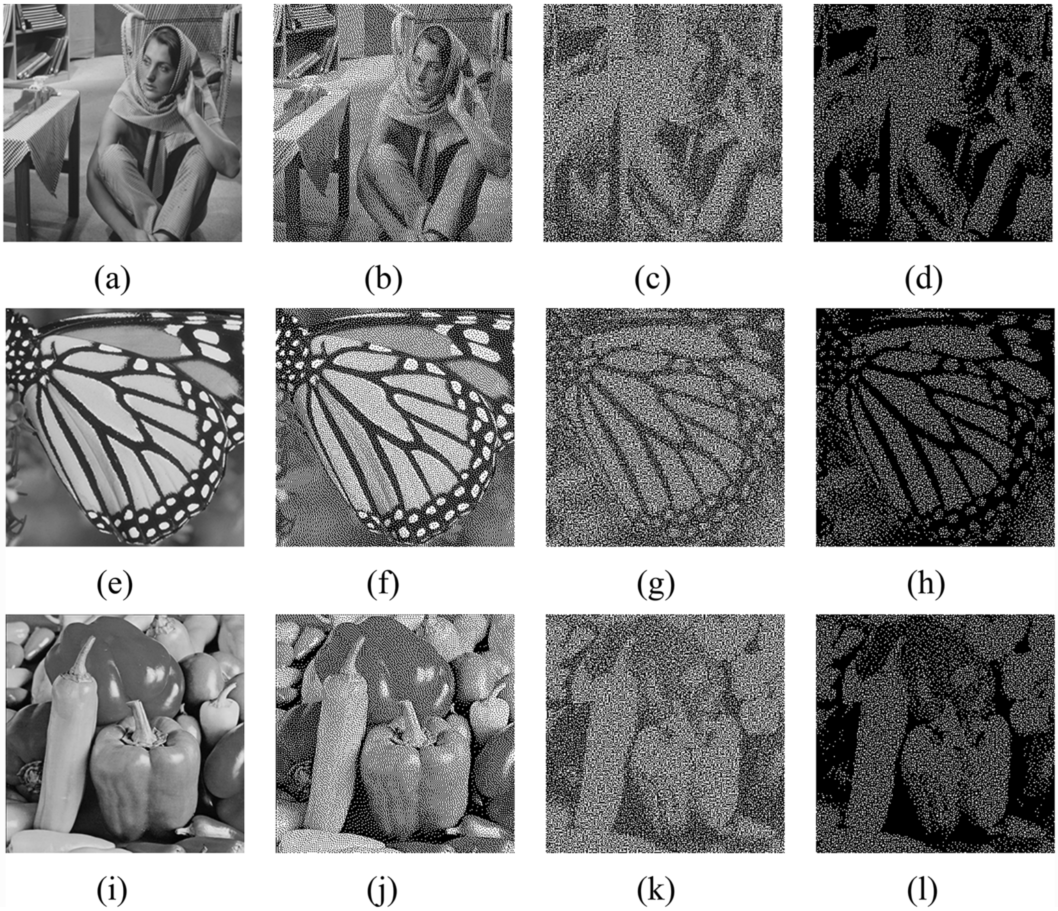


Figure 2. Experimental results of halftone images. Columns are original gray-scale images, halftone images generated by the ER method, halftone images generated by two thresholds, respectively. All the size is 512 × 512.

We evaluate the metrics[17] include SSIM (Structural Similarity Index Metric), PSNR (Peak Signal-to-Noise Ratio), and MSE (Mean Squared Error) for images recovery from the proposed scheme. The following table shows the performance of the proposed scheme for three secret images. The metric values for different QR codes versions are shown in Table 1. When one image is selected as the secret image, the other two images are used as cover images. The second column in Table 1 is the metrics values for the Barbara secret image, where Peppers and Butterfly are used for cover images. Since we have extended the QR codes size to fit the secret image size, the version of QR codes does not affect the image quality. All PSNR values are around 21, while the PSNR values are about 27 for the normal halftone images. To meet the security requirements, although our method reduces the image quality after binarization, the measurement results are roughly the same as the standard halftone technology, with a difference of about 6.

Table 2 shows feature comparisons among our proposal and related works. Naor's revolutionary work has many shortcomings. Later work to try to solve some of these problems. Many methods combine QR codes and VCS. However, these methods use XOR operation, which makes it impossible for human eyes to restore secret images by simply superimposing images. Our method adopts the limited halftone method to present an expansion-free EVCS. At the same time, it keeps the meaning and printability (computation-free) of EVCS, which is not available in other methods.

Many proposed schemes use the error correction function of QR codes to embed shared pixels. However, the fault tolerance rate of the highest level H of the error correction code is only 30%, that is, the damaged area of the two-dimensional code cannot exceed 30% of the whole image, which also limits the use of the whole two-dimensional code to transmit images. The error correction ability of the QR code can only reach the claimed error correction ratio in the case of continuous large-scale errors. For random noise errors, the error correction ability of the QR code is much lower than the claimed error correction ratio.

Contrast analysis. The contrast of the image restored by our method is the same as that of the underlying EVCS. In the halftone processing of secret images, we use sub-pixels with 3/4 black pixels to represent white pixels, and sub-pixels with 4/4 black pixels to represent black pixels. The contrast of the image to be encrypted is 4/4–3/4 = 1/4. In the two cover images, we use 2/4 sub-pixels with black pixels to represent white pixels, 3/4 sub-pixels with black pixels, and the contrast of the processed cover images is 3/4–2/4 = 1/4.

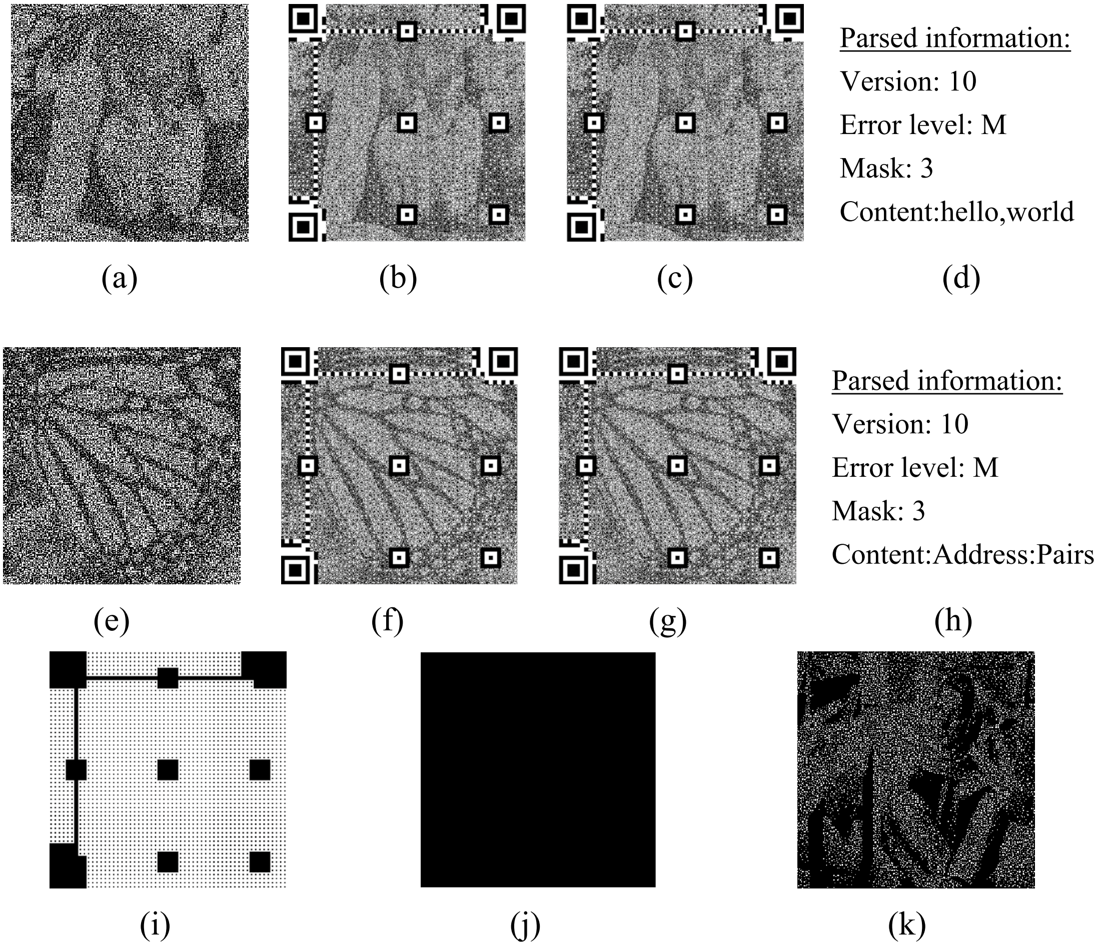


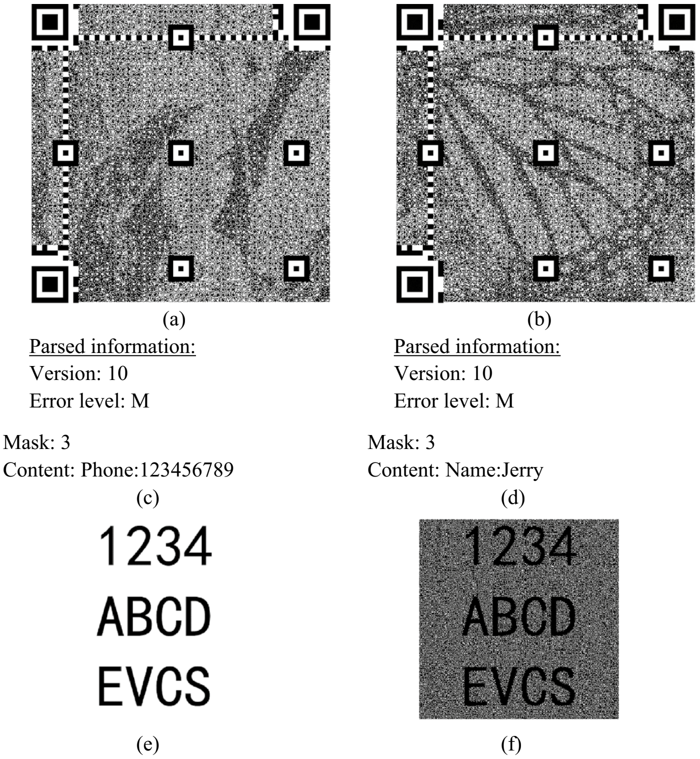
Figure 3. The experimental results of encryption, embedding, and recovery images. Halftoned cover images (**a**,**e**); cover images mixed with QR codes (**b**,**f**). Cover images embedded with overlayed pixels (**c**,**g**); parsed information with the zxing[16] tool (**d**,**h**); mask image for QR codes (**i**); (**j**) is the difference between (**f**,**g**); recovery image (**k**).

Security analysis. QEVCS can be divided into three steps. The first step is limited halftone processing, which is done independently by each image, so the information of the secret image will not be revealed. The second step is to encrypt the image with the underlying EVCS, which has been proved to be safe. The third step is pixel embedding, and this step is only related to the share images and QR codes, and will not reveal the information of the secret image. Therefore, QEVCS is secure.

Conclusion

Visual cryptography perfectly combines the threshold characteristics of secret sharing with images, providing an effective solution to preserve the privacy of images. After printing shares on transparencies, HVS can recover the secret images without using any device. In this paper, we proposed a QR code-based expansion-free extended visual cryptography scheme (QEVCS). This scheme generates visually appealing QR codes for transmitting meaningful shares when keeping the printing friendliness of VCS. By the limited halftone and block encryption, QEVCS can reuse existing EVCS methods for constructing encryption matrices without pixel expansion. The experimental results show the effectiveness of QEVCS.

In the future, we will further improve the quality of restored images. To keep VCS friendly to HVS, our proposal sacrifices the contrast of images. Second, we will explore the combination of VCS with quantum computing[20] since classical cryptography methods cannot resist quantum attacks. Last but not least, we are also working on the optimized pixel embedding method for overlaying shares into QR codes.



Parsed information:
Version: 10
Error level: M
Mask: 3
Content: Phone:123456789

Parsed information:
Version: 10
Error level: M
Mask: 3
Content: Name:Jerry

Figure 4. The experimental result of a plain text image. Cover images (**a**,**b**); parsed information by the zxing tool (**c**,**d**); secret image (**e**); recovery image (**f**).

	Barbara			Peppers			Butterfly		
version	PSNR	MSE	SSIM	PSNR	MSE	SSIM	PSNR	MSE	SSIM
8	21.12	502.44	6.23	21.01	515.32	6.23	21.23	489.87	6.22
10	20.12	632.53	6.24	20.20	620.98	6.24	20.32	604.06	6.23
14	21.34	477.62	6.24	21.49	461.40	6.25	21.39	472.15	6.24
16	21.19	494.40	6.28	21.59	450.90	6.28	21.23	489.87	6.26
30	21.89	420.80	6.30	22.10	400.94	6.29	22.31	382.01	6.28
35	22.40	374.18	6.29	22.41	373.32	6.31	22.52	363.98	6.32

Table 1. The performance of the proposed scheme for three secret images.

Scheme	Size-invariant	Meaningful	Transmission	Computation-free
Naor[6]	No	No	No	No
Pan[9]	Yes	No	Yes	No
Tan[11]	Yes	No	Yes	No
Cheng[13]	Yes	No	Yes	Yes
Zhang[18]	Yes	No	No	Yes
Zhang[19]	No	No	Yes	No
Our proposal	Yes	Yes	Yes	Yes

Table 2. Feature comparisons among our proposal and previous schemes.

Received: 28 January 2022; Accepted: 19 April 2022
Published online: 10 May 2022

References

1. Tan, Y., Qin, J., Tan, L., Tang, H. & Xiang, X. A survey on the new development of medical image security algorithms. In *Cloud Computing and Security*, vol 11065 (eds Sun, X. *et al.*) 458–467 (Cham, 2018). https://doi.org/10.1007/978-3-030-00012-7_42.
2. Eichelberg, M., Kleber, K. & Kämmerer, M. Cybersecurity in PACS and medical imaging: An overview. *J. Digit. Imaging* **33**(6), 1527–1542. https://doi.org/10.1007/s10278-020-00393-3 (2020).
3. Lin, J. *et al.* A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet Things J.* **4**(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200 (2017).
4. Thanh, T. M. & Tanaka, K. An image zero-watermarking algorithm based on the encryption of visual map feature with watermark information. *Multimed. Tools Appl.* **76**(11), 13455–13471. https://doi.org/10.1007/s11042-016-3750-2 (2017).
5. Selva Mary, G. & Manoj Kumar, S. A self-verifiable computational visual cryptographic protocol for secure two-dimensional image communication. *Meas. Sci. Technol.* **30**(12), 125404. https://doi.org/10.1088/1361-6501/ab2faa (2019).
6. Naor, M. & Shamir, A. Visual cryptography. In *)Advances in Cryptology—EUROCRYPT'94* , vol 950 (ed. De Santis, A.) 1–12 (Springer, 1995). https://doi.org/10.1007/BFb0053419.
7. Cai, H., Liu, X. & Yan, B. Beautified QR code with security based on data hiding. In *Advances in Computational Intelligence Systems*, vol 1043 (eds Ju, Z. *et al.*) 423–432 (Springer, 2020). https://doi.org/10.1007/978-3-030-29933-0_35.
8. Chu, H.-K., Chang, C.-S., Lee, R.-R. & Mitra, N. J. Halftone QR codes. *ACM Trans. Graph.* **32**(6), 1–8. https://doi.org/10.1145/2508363.2508408 (2013).
9. Pan, J.-S. *et al.* Visual cryptography scheme for secret color images with color QR codes. *J. Vis. Commun. Image Represent.* **82**, 103405. https://doi.org/10.1016/j.jvcir.2021.103405 (2022).
10. Wan, S., Lu, Y., Yan, X., Wang, Y. & Chang, C. Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions. *J. Real-Time Image Proc.* **14**(1), 25–40. https://doi.org/10.1007/s11554-017-0678-3 (2018).
11. Tan, L. *et al.* Robust visual secret sharing scheme applying to QR code. *Secur. Commun. Netw.* **2018**, 1–12. https://doi.org/10.1155/2018/4036815 (2018).
12. Cheng, Y., Fu, Z., Yu, B. & Shen, G. A new two-level QR code with visual cryptography scheme. *Multimed. Tools Appl.* **77**(16), 20629–20649. https://doi.org/10.1007/s11042-017-5465-4 (2018).
13. Cheng, Y., Fu, Z. & Yu, B. Improved visual secret sharing scheme for QR code applications. *IEEE Trans. Inform. Forensic Secur.* **13**(9), 2393–2403. https://doi.org/10.1109/TIFS.2018.2819125 (2018).
14. Ren, L. A novel raster map exchange scheme based on visual cryptography. *Adv. Multimed.* **2021**, 1–7. https://doi.org/10.1155/2021/3287774 (2021).
15. Askari, N., Heys, H. M. & Moloney, C. R. An extended visual cryptography scheme without pixel expansion for halftone images. In *2013 26th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*, Regina, SK, Canada, May 2013, pp 1–6. https://doi.org/10.1109/CCECE.2013.6567726.
16. Wang, Y. Intelligent Invoice Identification Technology Based on Zxing Technology. In *Innovative Computing* vol 791 (eds Hung, J. C. *et al.*) 87–93 (Springer, 2022). https://doi.org/10.1007/978-981-16-4258-6_11.
17. Hore, A., & Ziou, D. Image Quality Metrics: PSNR vs. SSIM. In *2010 20th International Conference on Pattern Recognition*, Istanbul, Turkey, Aug. 2010, pp. 2366–2369. https://doi.org/10.1109/ICPR.2010.579.
18. Zhang, D., Zhu, H., Liu, S. & Wei, X. HP-VCS: A high-quality and printer-friendly visual cryptography scheme. *J. Vis. Commun. Image Represent.* **78**, 103–186. https://doi.org/10.1016/j.jvcir.2021.103186 (2021).
19. Zhang, L., Dang, X., Feng, L. & Yang, J. Efficient secret image sharing scheme with authentication and cheating prevention. *Math. Probl. Eng.* **2021**, 1–11. https://doi.org/10.1155/2021/9274415 (2021).
20. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**(3), 2002. https://doi.org/10.1103/PhysRevA.65.032302 (2002).

Acknowledgements

This work is supported in part by the Guangdong Basic and Applied Basic Research Foundation of China (2022A1515011542).

Author contributions

D.Z. wrote the manuscript text and performed the experiment. L.R. helped perform the analysis with constructive discussions and performed the data analyses.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to D.Z.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.