Journal of Network Intelligence ©2024 ISSN 2414-8105
Taiwan Ubiquitous Information Volume **9**, Number **4**, November **2024**

QR Code-Based Visual Secret Sharing Scheme: A Review

Shu-Chuan Chu

Information Engineering College
Guangzhou City Construction College, Guangzhou 510925, China

School of Artificial Intelligence
Nanjing University of Information Science and Technology, Nanjing 210044, China
scchu0803@sdust.edu.cn

Tao Liu

College of Computer Science and Engineering
Shandong University of Science and Technology, Qingdao 266590, China
taoliu0201@163.com

Jeng-Shyang Pan*

School of Artificial Intelligence
Nanjing University of Information Science and Technology, Nanjing 210044, China

Department of Information Management
Chaoyang University of Technology, Taichung 41349, Taiwan
jspan@ieee.org

*Corresponding author: Jeng-Shyang Pan

Received March 18, 2024, revised June 26, 2024, accepted September 20, 2024.

Abstract. *Visual secret sharing (VSS) scheme is the technology that divides a secret into shares. The decoding operation on the share is performed to restore the secret image. The quick response (QR) code is an image carrying the information. The standard of it is public. When it was obtained, anyone can decode the QR code. The VSS scheme and QR code are combined to improve the security of daily life. They can enhance the security of mobile payments, authentication, privacy data, cheater prevention, and so on. This study mainly aims to summarize previous research achievements. Comparative analysis of relevant results is conducted to illustrate the future research direction.*

Keywords: VSS, QR code, secret sharing

1. **Introduction.** Naor and Shamir designed the visual secret sharing (VSS) scheme [1]. The secret is distributed in several images (shares). Each share cannot reveal the secret alone. For the $(n,\ n)$-threshold VSS scheme, every share is a key. The key (share) is obtained to recover the secret. The VSS scheme is an encryption method, which can encrypt the secret [2–4]. They are mainly used to encrypt images. The security of the image is improved by [5–7]. Quick response (QR) codes are the image that carry information. They are used for mobile payment, carrying information, jumping to websites, and so on. To maximize their real-life application, the VSS scheme and QR codes can be contaminated. The QR code-based VSS (QR-edVSS) scheme mainly comprises three categories. One is the VSS scheme for the QR code (QRVSS scheme), in which QR codes are only

utilized as the secret; one is the VSS scheme using the QR code (VSS-QR scheme), in which QR codes are only used as shares; one is the using the QRVSS scheme for the QR code (QRVSS-QR scheme), in which QR codes are employed as secret images and shares.

QR code cannot protect itself. It owns the public standard. Anyone can decode it when a QR code is obtained. Fang employed the VSS scheme to achieve the security of QR codes [8]. The secret QR code is distributed in two shares. When two shares are obtained by the receiver, they perform an OR operation on shares to recover the image. To reconstruct the QR code in a module, the reconstructed image is processed. Cao et al. used the pseudorandom matrix to propose a new QRVSS scheme in 2016 [9]. Pan et al. designed a novel QRVSS scheme based on halftone technology [10]. The VSS scheme can be employed to encrypt QR codes.

Meaningless shares attract the attention of attackers. The VSS scheme will be insecure. QR codes carry information that users can access, achieve mobile payment, jump from one website to another, and more. Owing to its quick response and convenience, the QR code has become very popular in the daily lives of people. The QR code is employed as shares, which can decrease the suspicion of the potential attacker. Tan et al. designed a VSS-QR scheme using a color QR code to achieve lossless recovery of secret images [11]. The Chinese remainder theorem was employed to the VSS-QR scheme by [12]. Pan et al. utilized color QR code and halftone technology to propose a VSS-QR scheme [13]. Meaningful shares can enhance the security of the VSS scheme.

QR codes can be used as shares to encrypt QR codes using the QRVSS-QR scheme. In 2016, Chow et al. employed the characteristics of the error correction codeword (ECC) to propose the QRVSS-QR scheme [14]. Every share has some errors, and the recovered QR code contains some wrong codewords. The ECC can correct some errors. All shares and the recovered QR code are decoded correctly. Wan et al. designed to use big-version QR codes to share small-version QR codes [15]. Color QR codes are used as shares [16]. Using meaningful images as the share will enhance the security of the scheme.

VSS schemes based on QR codes have been proposed by numerous researchers. They can also be applied to other fields such as protecting against web phishing, secure mobile payment, authentication, cheater prevention, and information security. Kute et al. proposed one-time passwords to protect against web phishing using the VSS scheme and QR code [17]. Secure mobile payment was achieved using VSS schemes and QR codes by [18]. Based on VSS schemes and QR codes, an authentication system was proposed by [19]. Chuang et al. employed the QR code and VSS scheme to prevent cheating [20]. The VSS scheme and QR code were utilized to protect information security by Chow et al. [21]. Based on QR codes, VSS schemes can be applied to numerous fields.

This paper lists many references focusing on the VSS scheme based on the QR code. These references are systematically sorted, analyzed, and compared. All schemes are divided into three types. Each type is compared and analyzed. This study shows that an increasing number of people are interested in this field.

In this paper, Section 2 introduces the preliminaries. Section 3 presents the QRVSS schemes. Section 4 exhibits the VSS-QR scheme. Section 5 shows the QRVSS-QR schemes. Section 6 introduces the application of the QR-edVSS scheme. Section 7 provides conclusions and future work.

2. **Preliminaries.**

This section mainly discusses VSS schemes (Section 2.1) and basic knowledge about QR codes (Section 2.2).

2.1. **Visual secret sharing scheme.**

Naor and Shamir found the disadvantages of traditional cryptography. Traditional cryptography has only one key. Once this key is obtained by the attacker, the secret will be decoded by them. Based on the disadvantages of traditional cryptography, Naor and Shamir developed the VSS scheme [1]. The secret image is distributed in several shares using two basic matrices $\mathbf{B}_{\mathrm{W}}$ and $\mathbf{B}_{\mathrm{k}}$. $\mathbf{B}_{\mathrm{W}}$ and $\mathbf{B}_{\mathrm{k}}$ denote the encryption matrix of white and black pixels. Every share is a key. For the $(k,\ n)$-threshold VSS scheme (k is less than or equal to n), the receiver obtains k or more shares to recover the image. If less than k shares are obtained by the attacker, they will not reconstruct the image.

$\mathbf{R}$ denotes recovery images. $\mathbf{R}_{\mathrm{k}}$ and $\mathbf{R}_{\mathrm{W}}$ are the black and white pixels of $\mathbf{R}$, respectively. The number of pixels is denoted by the function $n(\cdot)$. For the $(k,\ n)$-threshold VSS scheme, they satisfy the following two conditions:

(a) Less than k shares are used to reconstruct the image, the reconstructed image has $n(\mathbf{R}_{\mathrm{W}}) = n(\mathbf{R}_{\mathrm{k}})$.

(b) When the amount of the share is k or more, the generated new image satisfies $n(\mathbf{R}_{\mathrm{W}}) < n(\mathbf{R}_{\mathrm{k}})$.

The condition (a) is a security condition of $(k,\ n)$-threshold VSS schemes. When attackers obtain less than k shares, they will not recover the secret image using the decoding method. The equation $n(\mathbf{R}_{\mathrm{W}}) = n(\mathbf{R}_{\mathrm{k}})$ can ensure that the recovered image contains no information. The contrast condition is the condition (b). If the receiver receives k or more shares, they reconstruct the secret. When $n(\mathbf{R}_{\mathrm{W}}) < n(\mathbf{R}_{\mathrm{k}})$, the generated new image is a meaningful image. The receiver can decode the secret from the recovered image using the human visual system (HVS). Conditions (a) and condition (b) are the basis of the design of the VSS scheme.

Given an example in [1], a (3, 3)-threshold scheme is introduced as follows:

The basic matrix is $\mathbf{B}_{\mathrm{W}} = \begin{bmatrix} \text{white} & \text{white} & \text{black} & \text{black} \\ \text{white} & \text{black} & \text{white} & \text{black} \\ \text{white} & \text{black} & \text{black} & \text{white} \end{bmatrix}$ and

$\mathbf{B}_{\mathrm{k}} = \begin{bmatrix} \text{black} & \text{black} & \text{white} & \text{white} \\ \text{black} & \text{white} & \text{black} & \text{white} \\ \text{black} & \text{white} & \text{white} & \text{black} \end{bmatrix}$. Their corresponding images are shown in Figure 1. Matrices $\mathbf{B}_{\mathrm{W}}$ and $\mathbf{B}_{\mathrm{k}}$ are the basic matrices of the (3, 3)-threshold VSS scheme. Every cow is a replaced matrix. They are used to generate shares. Secret white pixels will use the $\mathbf{B}_{\mathrm{W}}$ to distribute. The $\mathbf{B}_{\mathrm{k}}$ is used to distribute secret black pixels. The matrices $\mathbf{B}_{\mathrm{W}}$ and $\mathbf{B}_{\mathrm{k}}$ are important in the VSS scheme.

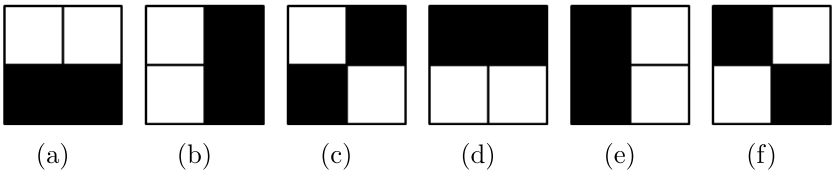


Figure 1. (a)-(c) First cow, second cow, third cow in $\mathbf{B}_{\mathrm{W}}$; (d)-(f) First cow, second cow, third cow in $\mathbf{B}_{\mathrm{k}}$.

The experimental results of the (3, 3)-threshold VSS scheme are shown in Figure 2. Figure 2 (a) shows a secret and it is divided into three shares using $\mathbf{B}_{\mathrm{W}}$ and $\mathbf{B}_{\mathrm{k}}$. Three shares are shown in Figure 2 (b)-Figure 2 (d). Every share is meaningless and does not contain any useful information. Anyone can influence the result of the reconstructed image. Any two shares cannot recover the secret, as shown in Figure 2 (e)-Figure 2 (g). Only using two shares recovers the image, which is meaningless. The restored image contains useless information. Three shares perform a stacking operation to recover the secret. The VSS scheme is mainly designed to encrypt the image.

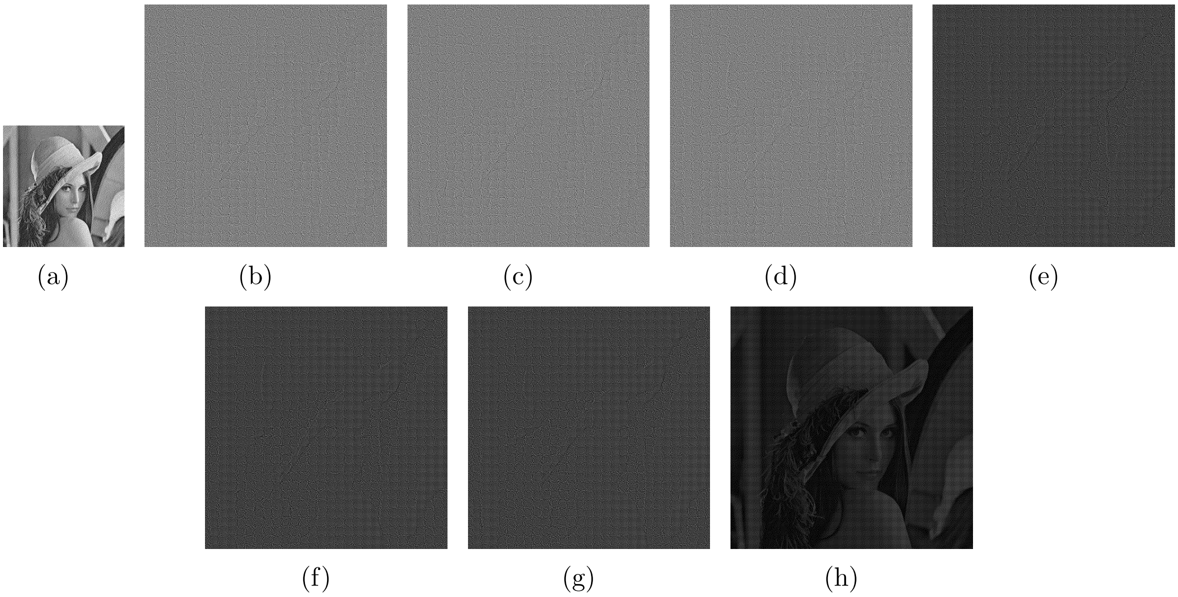


FIGURE 2. (a) The secret image (binary image); (b)-(d) Share1-Share3; (e) Stacking share1 and share2; (f) Stacking share1 and share3; (g) Stacking share2 and share3; (h) Stacking share1, share2 and share3.

The VSS scheme can generate some shares. These shares are the key. Every share is important. The receiver can only decode the secret if sufficient shares are obtained. If the attacker knows how to decode and does not have enough shares, they will not decode the secret. Compared with traditional cryptography, the number of shares is advantageous. Only a key is used in traditional cryptography. Once it is lost, the attacker will obtain the secret. VSS schemes use numerous shares to reduce this risk.

2.2. **QR code.** People utilize intelligence mobile phones to decode QR codes to acquire information, make mobile payments, and jump from one web page to another. The use of QR codes facilitates the lives of people. QR codes are popular because of their decoding speed and convenience. Encoding and decoding of QR codes are performed in accordance with the standard ISO/IEC 18004 [22]. Every QR code comprises numerous modules. The module number of each QR code is as follows:

$$l^2 = (17 + 4V)^2, \tag{1}$$

where QR codes have l^2 modules. V denotes versions of QR codes and $V \in [1,\ 40]$. The big version can contain more information. As shown in Figure 3, many modules form quiet zones, function patterns, and encoding regions.

Different modules will be combined into different codewords and will have some function. The function pattern contains finder patterns, separator, timing patterns, and alignment patterns. The encoding areas include format information, version information, and data and ECCs, as shown in Figure 3.

Every QR code can correct some errors. It has four levels, L, M, Q, and H, which are shown in Table 1. The data in the table are only general values.

The ability of error correction can be specific to codewords as shown in Table 2. The version and correction level of the QR code are 4 and H, respectively , and it has (25, 9, 8) in the correction capacity per block, which indicates that every block has 25 codewords,

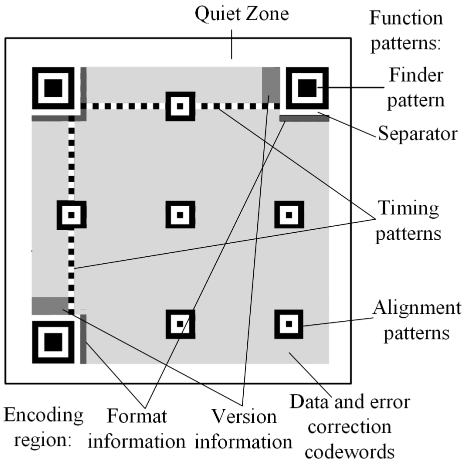


Figure 3. Structure of QR codes [22].

Table 1. Error correction levels.

Level	Correction ability
L	7%
M	15%
Q	25%
H	35%

9 data codewords, and 8 corrected codewords. Every block has eight wrong codewords that can be decoded by the decoder. Nine or more wrong codewords will cause QR codes to not be decoded correctly.

Table 2. The capacity of the ECC.

Version	Level	Amount of blocks	Correction capacity per block $(t,\ d,\ e)$
4	L	1	(100,80,10)
	M	2	(50,32,9)
	Q	2	(50,24,13)
	H	4	(25,9,8)

The $t,\ d$ and e are the amount of all codewords, the amount of data codewords and the amount of correction codewords.

QR codes have the ECC that can correct some wrong codewords. Every share has some or no errors and can be decoded by the decoder. Numerous references have utilized this characteristic to design VSS schemes using the QR code.

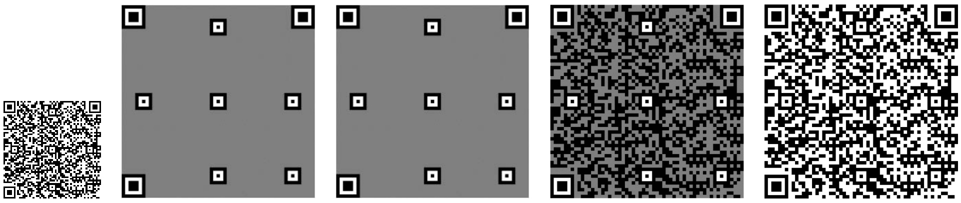
3. **QRVSS schemes.** In 1994, Naor and Shamir designed the VSS scheme [1]. Fang designed a novel reversible VSS scheme in 2007 [23]. Fang applied it to QR codes using the scheme shown in Table 3 [8]. In the distributed method, if there is a secret white pixel, the two shares are replaced by the same matrix. When there is a secret black pixel, two shares are replaced by a different matrix. These two different matrices are stacked

to recover a 4 × 4 black-pixel matrix. There is a contrast in color between the 4 black matrix and the 2 black and 2 white matrix.

Table 3. The scheme of Fang [8].

Secret	Share1	Share2	Stacking	Secret	Share1	Share2	Stacking
□	■■ □□	■■ □□	■■ □□	■	■■ □□	□□ ■■	■■ ■■
□	□□ ■■	□□ ■■	□□ ■■	■	□□ ■■	■■ □□	■■ ■■
□	□■ □■	□■ □■	□■ □■	■	□■ □■	■□ ■□	■■ ■■
□	■□ ■□	■□ ■□	■□ ■□	■	■□ ■□	□■ □■	■■ ■■
□	□■ ■□	□■ ■□	□■ ■□	■	□■ ■□	■□ □■	■■ ■■
□	■□ □■	■□ □■	■□ □■	■	■□ □■	□■ ■□	■■ ■■

The experimental results are shown in Figure 4. Referring to Table 3, the secret QR code (Figure 4 (a)) is distributed to two meaningless shares. This is a pixel-expanded scheme. Two shares (Figure 4 (b) and Figure 4 (c)) are larger than the secret image in size. Stacking Share1 and Share2 can recover the image (Figure 4 (d)). The recovered image is converted into a binary QR code (Figure 4 (e)) via post-processing.



(a) (b) (c) (d) (e)

Figure 4. (a) The secret QR code; (b)-(c) Share1-Share2; (d) Stacking share1 and share2; (e) The post-processing restored image.

Cao et al. utilized new basic matrices to design a QRVSS scheme for the QR code [9]. The schemes of Fang and Cao are (2, 2)-threshold schemes. Liu et al. improved to achieve $(n,\ n)$-threshold scheme [24]. The halftone technology was applied to design the QRVSS scheme by [10]. The size of the shares generated by the previous scheme is greater than that of the secret images. Some schemes can achieve no pixel-expanded schemes for the QR code. Liu et al. designed a new color QRVSS scheme [25]. Velumani et al. developed a new QRVSS scheme for QR codes [26]. In 2023, Pan et al. proposed a new single-pixel QRVSS scheme for the QR code [27].

Table 4 shows a comparison of these schemes. Fang and Cao utilized different basic matrices to achieve the QRVSS scheme for QR codes [8, 9], which are pixel-expansible. Secret QR codes are fully recovered in a module. Liu et al. exploited the ECC to propose a new $(n,\ n)$-threshold QRVSS scheme [24]. Although ECC is employed to design schemes, the reconstructed QR codes have no errors in the module. Shares are meaningless in the scheme of Fang, Cao, and Liu, and they can attract the attention of attackers. Halftone technology was utilized to achieve this scheme [10]. Shares are halftone images. The share of this scheme is meaningful and can decrease the suspicion of attackers. Besides, they are easy to manage for the sender and receiver.

Table 4. Comparisons of some QRVSS schemes.

Scheme	Threshold	Expansible pixel	Method
Ref. [8]	(2, 2)	Yes	Basic matrices
Ref. [9]	(2, 2)	Yes	Basic matrices
Ref. [25]	(3, 3)	No	RGB model
Ref. [24]	$(n,\ n)$	Yes	Basic matrices and ECC mechanism
Ref. [10]	(2, 2)	Yes	Halftone technology
Ref. [26]	(3, 3)	No	Super resolution convolutional neural network
Ref. [27]	$(n,\ n)$	No	ECC mechanism

These are pixel-expansible schemes [8–10, 24]. To enhance them, Pan et al. designed a new distribution scheme using the mechanism of the ECC [27]. This scheme is a single-pixel and $(n,\ n)$-threshold scheme. Secret QR codes are also recovered completely. These schemes are designed using the traditional VSS scheme. The decoding method is stacking. New decoding methods are designed for the VSS schemes. In [25], Liu et al. utilized the RGB model to propose a color QRVSS scheme. The decoding method is the RGB model. This scheme is a (3, 3)-threshold VSS without pixel-expansion. Nonnegative matrix factorization was employed to design the VSS scheme for the QR code [26]. This scheme generates three shares. The secret QR code was recovered with no errors using a super-resolution convolutional neural network.

Numerous researchers have proposed different schemes for QR codes using different methods. The traditional VSS scheme is used for QR codes to design a QRVSS scheme. Simultaneously, new methods and technologies can also be applied to the QR code to achieve the new QRVSS scheme. In the future, meaningful shares will be designed. The future trend is meaningful shares.

4. **VSS-QR schemes.** Meaningless share will attract the attention of attackers, which decreases the security of VSS schemes. QR codes were invented by Denso Wave [28]. QR codes have become increasingly popular because of their speed and convenience. Some researchers have used QR codes as shares to enhance the security of VSS schemes.

The $(k,\ n)$-threshold VSS scheme using the QR code was designed by [29]. Wan et al. designed a VSS-QR scheme for binary images [30]. QR codes are modified to become shares. Each share has some errors that can be corrected using ECC. Two shares are used in the operation stacking to reconstruct the secret. Jiang et al. achieved a new VSS-QR scheme with lossless recovery [12]. Fu et al. utilized the probabilistic sharing mode to design a VSS-QR scheme [31]. To achieve a VSS scheme using QR codes, a Reed-Solomon (RS) code was utilized to realize the scheme [32].

Based on the extended polynomial, a novel VSS scheme using QR codes was proposed [33]. Pad codewords were employed to design the (2, 2)-threshold VSS-QR scheme by [34]. Hu et al. designed a VSS-QR scheme with edge information embedded in a QR code [35]. The $(k,\ n)$-threshold VSS-QR scheme was achieved using a Chinese remainder theorem [36]. This scheme can be employed to encrypt the grayscale image. By beautifying QR codes, Ren et al. achieved the VSS scheme using QR codes [37]. Beautified QR codes are correctly decoded using a general decoder.

There are other methods to achieve the VSS scheme using QR codes. Kadam et al. designed a VSS-QR scheme using clustering and hashing techniques [38]. Tan et al. utilized color QR codes to achieve the VSS-QR scheme [11]. Using XOR operation to reconstruct the secret image without errors. Halftone technology and color QR codes were used to design a new VSS-QR scheme [13]. The color XOR is employed to decode the secret.

Figure 5 shows the RGB model. In the model, different color combinations can generate different colors. New colors can be generated using two, three, or more colors, as shown in Figure 5. A specific color can be generated using a color combination. Two, three, or more colors can generate a specific color.

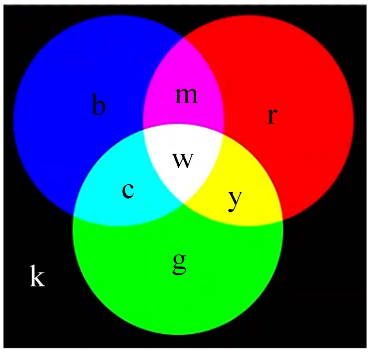


Figure 5. RGB model.

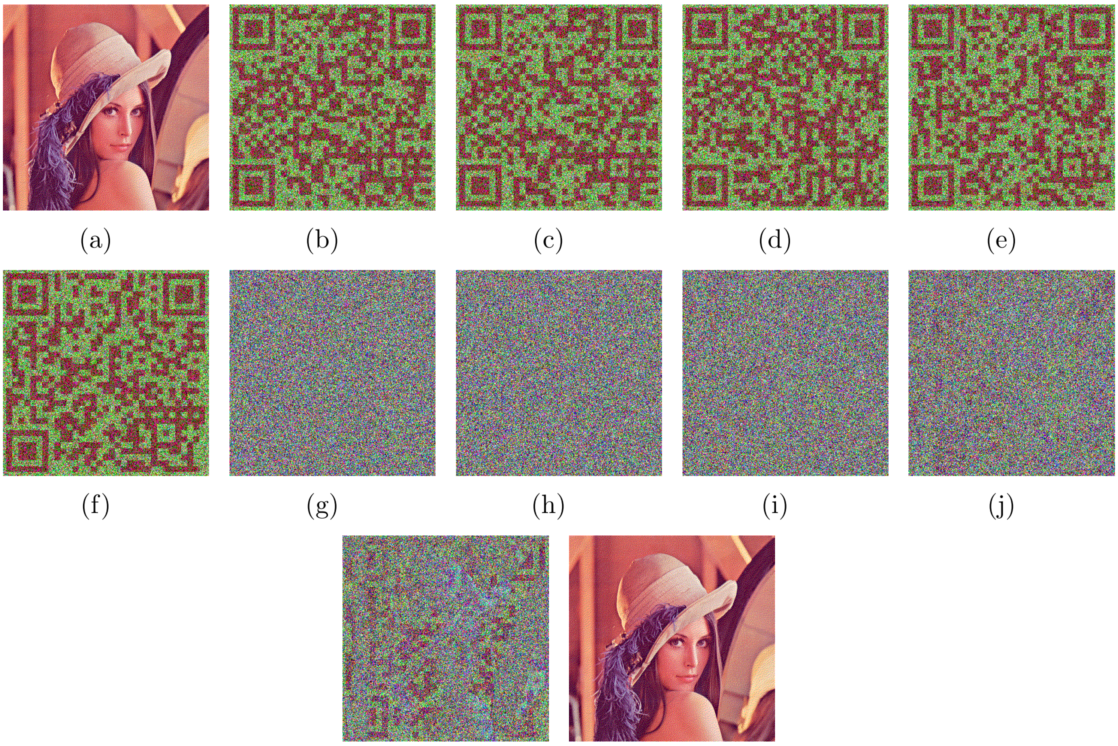
Commission on illumination (CIE) can be used to measure the brightness of colors [39]. Eight colors have different brightness levels in the RGB model. The lumen (lm) denotes a unit of brightness. $l(\cdot)$ is the brightness function. The eight colors have the following:

$$\begin{aligned} &l(\mathrm{k}) = 0\ lm,\ l(\mathrm{b}) = 0.11\ lm,\ l(\mathrm{r}) = 0.30\ lm,\ l(\mathrm{m}) = 0.41\ lm, \\ &l(\mathrm{g}) = 0.59\ lm,\ l(\mathrm{c}) = 0.70\ lm,\ l(\mathrm{y}) = 0.89\ lm,\ l(\mathrm{w}) = 1.00\ lm. \end{aligned} \tag{2}$$

The higher the value of brightness, the brighter the color. White is the brightest and black is the darkest. The eight colors have varying brightness levels. The brightness levels range from high to low as follows: w (white), y (yellow), c (cyan), g (green), m (magenta), r (red), b (blue) and k (black). Every color has a specific value of brightness. They differ in brightness levels.

The QR code decoder recognizes both light and dark. Pan et al. used eight colors (There are red, green, blue, cyan, magenta, yellow, white, and black) to replace white modules and colors (black, blue, and red) to replace black modules [13]. This color QR code is decoded correctly using a general decoder. These $n-1$ color QR codes and the n-th meaningless image are shares. The receiver obtains all shares and uses the color XOR to reconstruct the secret. The color of each share is used to generate a new color using the color XOR.

The experimental results are shown in Figure 6. The scheme of Pan is a $(n,\ n)$-threshold scheme. The (6, 6)-threshold scheme is shown in Figure 6. The picture "Lena" is the secret image (Figure 6 (a)). It is encrypted by using six shares. The five shares are the color QR codes, as shown in Figure 6 (b)-Figure 6 (f). The sixth share is a meaningless image (Figure 6 (g)). Attackers cannot restore the secret image with less than six shares as shown in Figure 6 (h)-Figure 6 (k). When six shares perform the decoding operation of the color XOR, a secret image can be recovered with errors, as shown in Figure 6 (l). The secret color image is recovered with no errors. The Pan scheme is a VSS-QR scheme that can restore color images losslessly.



(a) (b) (c) (d) (e)

(f) (g) (h) (i) (j)

(k) (l)

Figure 6. A (6, 6)-threshold scheme by [13]. (a) The secret image; (b)-(g) Share1-Share6; (h) Restored image with two shares; (i) Restored image with three shares; (j) Restored image with four shares; (k) Restored image with five shares; (l) Restored image with six shares.

These VSS-QR schemes are compared in Table 5. QR codes can correct some errors by themselves. Some researchers have utilized the ECC to design the VSS-QR scheme. The QR code can be added to some errors to satisfy the VSS scheme as the share. The $(k,\ n)$-threshold scheme was proposed by [29]. Based on the ECC, Wan et al. proposed the (2, 2)-threshold VSS-QR scheme [30]. The new $(n,\ n)$-threshold VSS scheme was achieved using the QR code with ECC [11]. Moreover, the RS and pad codewords are also used to design the VSS-QR schemes. He et al. proposed a novel VSS-QR scheme using the RS codeword [32]. Pad codewords were utilized to achieve the VSS scheme using QR codes [34].

Other schemes also utilized other methods to design VSS schemes not only the characteristic of QR codes. For example, the probabilistic sharing model was employed to achieve VSS schemes with QR codes [31]. A random grid of traditional methods was applied to the VSS-QR scheme by [35]. Kadam used clustering and hashing techniques

Table 5. The comparison of Some VSS-QR schemes.

Scheme	Threshold	Method	Type of secret image
Ref. [29]	(k, n)	ECC mechanism	Binary image
Ref. [30]	(2, 2)	ECC mechanism	Binary image
Ref. [12]	(k, n)	Chinese remainder theorem	Grayscale image
Ref. [31]	(k, n)	Probabilistic sharing model	Binary image
Ref. [32]	(k, n)	RS code	-
Ref. [11]	(n, n)	ECC mechanism	Binary image
Ref. [33]	(k, n)	Polynomial	Grayscale image
Ref. [34]	(2, 2)	Pad codewords	Binary image
Ref. [35]	(k, n)	Random grid	Binary image
Ref. [38]	(k, n)	Clustering and hashing techniques	-
Ref. [36]	(k, n)	Chinese remainder theorem	Grayscale image
Ref. [37]	(2, 2)	Limited halftone and block encryption	Binary image
Ref. [13]	(n, n)	Halftone technology and color XOR	Color image

to achieve the VSS scheme using QR codes [38]. Based on limited halftone and block encryption, a new VSS scheme using QR codes was designed [37]. Jiang et al. designed the VSS-QR scheme for the grayscale image using the Chinese remainder theorem [12]. Shares are QR codes. To improve this, Hu et al. designed a novel VSS-QR scheme using the Chinese remainder theorem [36]. The polynomial can also be used to achieve a VSS-QR scheme [33]. Pan et al. proposed not only binary and grayscale images but also a VSS-QR scheme for color images [13].

The characteristics of QR codes are important for researchers in designing VSS-QR schemes . The ECC mechanism, RS codewords, pad codewords, etc. are used to apply to VSS-QR schemes. Shares are the QR code. Meaningful shares can reduce the suspicion of others. Other schemes utilized other methods to achieve the VSS-QR scheme. Chinese remainder theorem, probabilistic sharing model, polynomial, random grid, clustering and hashing technologies, limited halftone and block encryption, halftone technology and the color XOR, and so on are all used to design the VSS-QR scheme. In the future, more characteristics of the QR code will be exploited to design VSS-QR schemes. Increasing numbers of other methods can also be applied to the VSS-QR scheme.

5. **QRVSS-QR schemes.**

QR codes are popular among people. They can scan QR codes to obtain information, jump from one website to another, make mobile payment, and so on. However, QR codes cannot ensure that these activities are safe. The VSS scheme is used to encrypt QR codes. Meaningless shares attract the attention of others that will decrease the security of the scheme. Some researchers have designed novel VSS schemes that use QR codes to encrypt the secret QR code. The QRVSS-QR scheme involves a secret QR code distributed using QR codes.

Chow et al. designed the QRVSS-QR scheme using ECC [14]. All shares and recovered QR codes have some wrong codewords, but ECC can correct them . Share is a meaningful image, and every share is a QR code. All shares that perform the operation of the XOR can reconstruct a secret QR code. Reconstructed QR codes are decoded correctly.

The scheme of Chow utilizes a mechanism to distribute secret QR codes to the share. For example, the version and correction level used are 4 and H, respectively. In Table 2, (25, 9, 8) and four blocks can be obtained. Using the method of Chow, a (3, 3)-threshold can be designed as follows:

1. When the version and correction level are 4 and H, secret QR codes can be used to encrypt by three shares. The amount of the share is greater than or equal to three. An example is a (3, 3)-threshold scheme.

2. Three QR codes are modified to be the share. Each block in every QR code contains no more than eight codewords of modified codewords. The version and correction level of the three shares are 4 and H, respectively.

3. Each modification is used to restore the secret QR codes. The amount of modified codewords for each block in the three shares is greater than or equal to 17. The amount of incorrect codewords does not exceed the ECC capacity.

Experimental results for Chow are shown in Figure 7. (3, 3)-threshold scheme uses three QR codes as shares. A secret QR code is Figure 7 (a). Three QR codes are shown in Figure 7 (b)-Figure 7 (d). The three QR codes are modified to be three shares (Figure 7 (e)- Figure 7 (g)). They can be decoded correctly because of ECC. The black pixel was employed to denote the difference, as shown in Figure 7 (i)-Figure 7 (k). All shares are performed using the decoding method to reconstruct the new QR code. The reconstructed QR code has some errors, as shown in Figure 7 (h). The difference between the secret and recovered QR codes is shown in Figure 7 (l). The recovered QR code contains errors that are corrected by ECC.

The scheme of Chow involves the researcher uses a QR code to encrypt secret QR codes. It utilizes the ECC to distribute secret QR codes to several QR codes. This scheme belongs to the $(n,\ n)$-threshold scheme and n satisfies $n \geq 3$.

The scheme of Chow is the $(n,\ n)$-threshold QRVSS-QR scheme. It was improved to a $(k,\ n)$-threshold scheme by [40]. Two decoding methods for the QRVSS-QR scheme were proposed by [41]. The recovered image has some errors when using the decoding method for stacking and no errors when using the XOR decoding method. Zhang et al. designed the VSS-QR scheme using a texture pattern [42]. The texture pattern of the QR codes is modified. They are used as shares. Tan et al. used grayscale QR codes to achieve a novel QRVSS-QR scheme [43]. Chen et al. designed a VSS-QR scheme using QR codes transparencies [44]. Shares are the QR codes that are decoded correctly. The ECC was used to achieve the QRVSS-QR scheme by [45]. Wan et al. designed a novel scheme to use the big version of QR codes to encrypt the small version of the QR code [46].

In addition, other researchers have proposed QRVSS-QR schemes. The robust $(k,\ n)$-threshold XOR-ed QRVSS-QR scheme was designed by [47]. Huang et al. achieved a $(n,\ n)$-threshold QRVSS-QR scheme using ECC [48]. Three-level QR codes were utilized to achieve the QRVSS-QR scheme by [49]. Pan et al. designed the (2, 2)-threshold scheme for the QR code using color QR codes [16]. Discrete wavelet transform (DWT), random permutation (RP) and arithmetic modulo (AM) were used to achieve the QRVSS-QR scheme by [50].

Table 6 shows some QRVSS-QR schemes. The characteristics of QR codes include the ECC mechanism, Pad codeword, and so on. They can be applied to QRVSS-QR schemes. Chow et al. designed a new $(n,\ n)$-threshold scheme [14]. n satisfies $n \geq 3$ in this scheme. The scheme of Chow was improved using the $(k,\ n)$-threshold scheme [40]. Wan et al. utilized the ECC mechanism to design schemes using two decoding methods [41]. When secret images are QR codes, the reconstructed QR codes have some wrong codewords. The ECC mechanism was used to design a QRVSS-QR scheme by [45]. The share is a QR code. Every share and the reconstructed QR code have errors that are corrected by

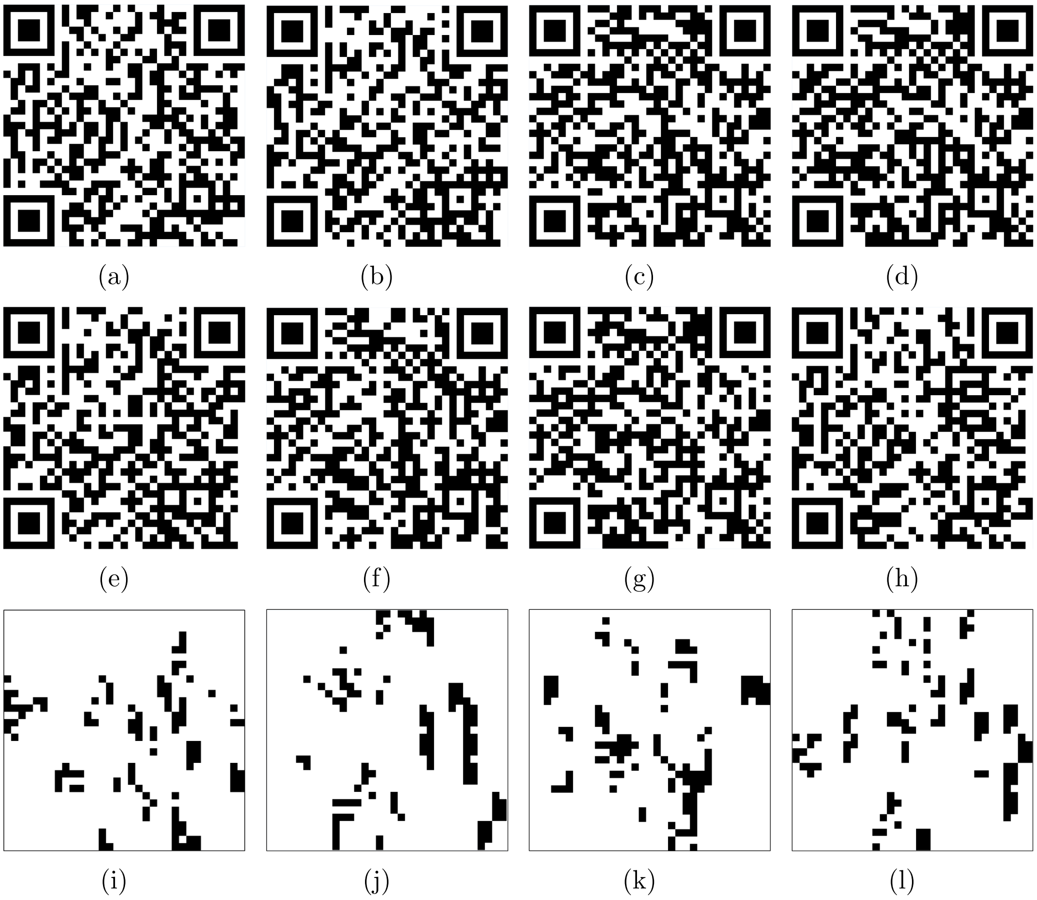


Figure 7. The experimental result of Chow. (a) The secret QR code; (b)-(d) QR code1-QR code2; (e)-(g) share1-share3; (h) Restored QR code; (i)-(l) are the difference between QR code1 and share1, QR code2 and share2, QR code3 and share3, the secret QR code and the recovered QR code, which black pixel denotes difference.

ECC. They are decoded correctly by the decoder. Huang et al. improved the security of the scheme to design a novel scheme using the ECC mechanism [48]. Most QRVSS-QR schemes cannot recover the secret QR code lossless using the ECC mechanism. The pad codeword was used to design a new QRVSS-QR scheme [47]. Recovered QR codes do not sacrifice the ECC capability.

In addition, other researchers have found other methods to achieve QRVSS-QR schemes. Zhang et al. developed a novel QRVSS-QR scheme using texture pattern design [42]. Grayscale QR codes were used to design the scheme by [43]. Chen et al. utilized QR codes transparencies to achieve the QRVSS-QR scheme [44]. The three-level QR code can also be applied to achieve the QRVSS-QR scheme by [49]. Pan et al. proposed a novel (2, 2)-threshold scheme using the RGB model [16]. DWT, RP and were combined to design the QRVSS-QR scheme [50].

The ECC mechanism can be applied to QRVSS-QR schemes. Most schemes cannot reconstruct secret QR codes without errors based on ECC. Based on pad codewords, QRVSS-QR schemes can reconstruct secret QR codes with no-errors. In the future, other characteristics of the QR code will be applied to design the QRVSS-QR scheme. Other methods can also be applied to the design of schemes. The researcher can look for other methods and apply them to achieve the QRVSS-QR scheme in the future.

Table 6. The comparison of Some QRVSS-QR schemes.

Scheme	Threshold	Method	Reconstructed QR codes without errors
Ref. [14]	$(n,\ n)$	ECC mechanism	No
Ref. [40]	$(k,\ n)$	ECC mechanism	No
Ref. [41]	$(k,\ n)$	ECC mechanism	No
Ref. [42]	$(n,\ n)$	Texture pattern design	Yes
Ref. [43]	$(n,\ n)$	Grayscale QR codes	Yes
Ref. [44]	$(k,\ n)$	QR code transparencies	No
Ref. [45]	$(k,\ n)$	ECC mechanism	No
Ref. [47]	$(n,\ n)$	Pad codeword	Yes
Ref. [48]	$(n,\ n)$	ECC mechanism	No
Ref. [49]	$(n,\ n)$	3-level QR codes	Yes
Ref. [16]	(2, 2)	RGB model	Yes
Ref. [50]	$(n,\ n)$	DWT, RP and AM	No

6. **Application of the QR-edVSS scheme.** QR-edVSS schemes can be applied to numerous fields. They are mainly applied to protection against web phishing, secure mobile payment, authentication, cheater prevention, and information security, as shown in Figure 8. QR-edVSS schemes have been applied to the daily lives of people.

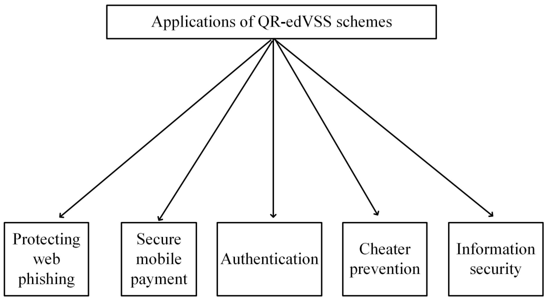


Figure 8. The application of the QR-edVSS scheme.

Table 7 shows some applications of the QR-edVSS schemes. These applications include protection against web phishing, secure mobile payment, authentication, cheater prevention, and information security.

Protection against web phishing: This protects individuals or groups from stealing personal and confidential information. Kute et al. designed a new authentication scheme for secure one-time password (OTP) distribution using the QR-edVSS scheme [17]. OTP is used to protect user from web phishing. QR code authentication was transmitted using the VSS scheme to solve the problem of phishing by [51]. The OTP was hidden in the QR code which is distributed using two shares to detect the attack [52].

Secure payment: Considering that QR codes can be used for mobile payments, QR-edVSS schemes enhance the transmission security of QR codes, and safe mobile payments can be guaranteed. To solve the problem of attackers forging the text password, a VSS scheme with reversing was proposed by [18]. Wan et al. proposed a mechanism for QR code security for anticounterfeiting using a QR-edVSS scheme [53], which can enhance secure mobile payment. Advanced encryption standards and VSS schemes have been utilized to encrypt QR codes to achieve secure payment [54].

Authentication: This means verifying whether the user has the right to access the system. The (2, 2)-threshold VSS scheme was proposed [19]. The secret is encoded into two QR codes. It is used to determine authenticity. Saha et al. designed a system to make the creation and authentication of identity documents easy and hassle-free [55]. Based on the VSS scheme, a QR code authentication protocol was proposed by [56]. To enhance service authentication, Li et al. designed two QR-edVSS schemes [57]. To achieve mobile payment authentication, Lu et al proposed three QR-edVSS schemes [58].

Furthermore, to achieve authentication, the multisecret VSS scheme and QR code were combined [59]. Symmetric keys and the QR-edVSS scheme were combined to perform authentication [21]. Liu et al. proposed a one-code-pass to achieve authentication using a QR-edVSS scheme [60]. An approach for sharing a secret leaked in a QR code adapted for a multiuser system was designed by [61], where each user can verify its share using an access structure. Zhong et al. designed a secure VSS scheme with authentication [62].A QR code was divided into equal shares, which are distributed between the user and administrator to perform secured authentication [63]. Using the Chinese remainder theorem, Wen et al. designed the QR-edVSS scheme to obtain authenticable medical images [64].

Cheater prevention: This means protecting personal and disease information from unauthorized use or access. Lin proposed a QR-edVSS scheme to protect private QR code data [65]. A new scheme with two-level information was used to protect private messages by [66]. Huang et al. proposed a Sudoku-based QR-edVSS scheme for cheater prevention [67]. To design a novel QR-edVSS scheme, the recognition patterns of QR codes and polynomials were used by [68]. Using QR codes, Huang et al. designed a scheme with cheater identification [69]. Fu et al. designed a new QR-edVSS scheme with three layers of information to protect private information [70]. A QR-edVSS scheme with authentication was designed by [71]. Huang et al. proposed an efficient $(k,\ n)$-threshold QR-edVSS scheme with cheater prevention [72].

Information security: The technical and administrative security protection established and adopted for data processing systems is designed. Chuang et al. proposed a new QR-edVSS scheme to enhance data privacy during data transmission [20]. A QR-edVSS scheme to protect the data was designed by [73]. A new two-level information protection scheme was proposed using the QR-edVSS scheme [74]. Yu et al. designed a novel VSS scheme to protect sensitive information using QR codes, Hamming codes, and wet paper codes [75]. A new QR-edVSS scheme was designed to protect information accuracy for medication administration [76]. Agrawal et al. utilized the QR-edVSS scheme to ensure the security of the electronic question paper [77]. Moreover, personal information was protected using the VSS scheme with QR codes [78]. Based on three-level QR codes and super-pixel segmentation in response, Wu et al. designed a novel VSS scheme to protect the information [79]. Watermarking and QR-edVSS schemes were utilized to protect the privacy of digital image [80]. Zhang et al. developed a novel VSS scheme that uses two-level QR codes to protect secret information [81]. Waleed et al. presented a QR-edVSS scheme using zero-watermarking for copyright protection [82].

The QR-edVSS scheme can be applied to numerous fields. It can be applied to protection against web phishing, authentication, cheater prevention, and information security. The VSS scheme is an encryption method. QR codes are popular in the daily lives of people. Combining the VSS scheme with QR codes can further improve themselves. The QR-edVSS scheme is mainly divided into three types: QRVSS scheme, VSS-QR scheme, and QRVSS-QR scheme. A (2, 2)-threshold VSS-QR scheme and QRVSS are improved to the $(n,\ n)$-threshold scheme or $(k,\ n)$-threshold scheme, respectively. QRVSS-QR schemes are widely employed to achieve the authentication. QRVSS schemes, VSS-QR schemes, and QRVSS-QR schemes are applied to the authentication. In the future, the researcher will enhance the QR-edVSS scheme. An increasing number of schemes will be applied to authentication. QRVSS schemes are rarely applied to cheater prevention, while VSS-QR and QRVSS-QR schemes have been applied. In the future, the QRVSS scheme will be applied to prevent cheating. To achieve information security widely, QR-edVSS schemes are utilized. In the future, QR-edVSS schemes will be applied to other fields.

Table 7. The comparison of Some QRVSS-QR schemes.

Scheme	Threshold	The type of scheme	Applications
Ref. [17]	(2, 2)	VSS-QR scheme	Protecting web phishing
Ref. [51]	(2, 2)	QRVSS scheme	Protecting web phishing
Ref. [52]	(2, 2)	QRVSS scheme	Protecting web phishing
Ref. [18]	(2, 2)	QRVSS scheme	Secure payment
Ref. [53]	(2, 2)	VSS-QR scheme	Secure payment
Ref. [54]	(2, 2)	QRVSS scheme	Secure payment
Ref. [19]	(2, 2)	VSS-QR scheme	Authentication
Ref. [55]	(2, 2)	QRVSS scheme	Authentication
Ref. [56]	(2, 2)	QRVSS scheme	Authentication
Ref. [57]	(2, 2)	VSS-QR scheme	Authentication
Ref. [58]	(2, 2)	QRVSS-QR scheme	Authentication
Ref. [59]	(2, n)	QRVSS-QR scheme	Authentication
Ref. [21]	(k, n)	VSS-QR scheme	Authentication
Ref. [60]	(2, n)	VSS-QR scheme	Authentication
Ref. [61]	(k, n)	QRVSS scheme	Authentication
Ref. [62]	(n, n)	QRVSS-QR scheme	Authentication
Ref. [63]	(n, n)	QRVSS scheme	Authentication
Ref. [64]	(k, n)	VSS-QR scheme	Authentication
Ref. [65]	(n, n)	VSS-QR scheme	Cheater prevention
Ref. [66]	(2, n)	QRVSS-QR scheme	Cheater prevention
Ref. [67]	(n, n)	VSS-QR scheme	Cheater prevention
Ref. [68]	(k, n)	VSS-QR scheme	Cheater prevention
Ref. [69]	(n, n)	VSS-QR scheme	Cheater prevention
Ref. [70]	(n, n)	QRVSS-QR scheme	Cheater prevention
Ref. [71]	(k, n)	VSS-QR scheme	Cheater prevention
Ref. [72]	(k, n)	VSS-QR scheme	Cheater prevention
Ref. [20]	(k, n)	QRVSS-QR scheme	Information security
Ref. [73]	(5, 5)	VSS-QR scheme	Information security
Ref. [74]	(n, n)	QRVSS-QR scheme	Information security
Ref. [75]	(n, n)	VSS-QR scheme	Information security
Ref. [76]	(n, n)	QRVSS-QR scheme	Information security
Ref. [77]	(3, 3)	VSS-QR scheme	Information security
Ref. [78]	(2, 2)	QRVSS-QR scheme	Information security
Ref. [79]	(n, n)	VSS-QR scheme	Information security
Ref. [80]	(2, 2)	VSS-QR scheme	Information security
Ref. [82]	(2, 2)	QRVSS scheme	Information security

7. **Conclusions and future work.** QR-edVSS schemes combine VSS schemes and QR codes. QR codes are utilized as the share to enhance the security of VSS schemes. The share is a QR code. Meaningful shares can reduce the suspicion of attackers. QR codes are popular because of their decoding speed and convenience. QR codes can be used

to obtain information, jump from one website to another, mobile payments, and more. However, whether QR codes are secure cannot be assured. Hence, VSS schemes can be used to encrypt the QR code to ensure transmission security. Using QR codes to share secret QR codes is a safer scheme. It can improve the transmission security of QR codes. QR-edVSS schemes can be applied to numerous fields, including protection against web phishing, secure mobile payment, authentication, cheater prevention, and information security. Shares are QR codes. Meaningful images decrease the suspicion of attackers. If the attacker cannot access the maximum amount of the share, they cannot decode the secret. Using QR codes can improve the security of schemes. In the future, QR codes will be further used in conjunction with VSS schemes. Eventually, QR-edVSS schemes will be widely used.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Workshop on the Theory and Application of Cryptographic Techniques*. Springer, 1994, pp. 1–12.

[2] T.-Y. Wu, X. Fan, K.-H. Wang, C.-F. Lai, N. Xiong, and J. M.-T. Wu, "A dna computation-based image encryption scheme for cloud cctv systems," *IEEE Access*, vol. 7, pp. 181 434–181 443, 2019.

[3] T.-Y. Wu, X. Fan, K.-H. Wang, J.-S. Pan, and C.-M. Chen, "Security analysis and improvement on an image encryption algorithm using chebyshev generator," *Journal of Internet Technology*, vol. 20, no. 1, pp. 13–23, 2019.

[4] T.-Y. Wu, X. Fan, K.-H. Wang, J.-S. Pan, C.-M. Chen, and J. M.-T. Wu, "Security analysis and improvement of an image encryption scheme based on chaotic tent map." *Journal of Information Hiding and Multimedia Signal Processing*, vol. 9, no. 4, pp. 1050–1057, 2018.

[5] Q. Yang, S.-C. Chu, C.-C. Hu, L. Kong, and J.-S. Pan, "A task offloading method based on user satisfaction in C-RANRAN with mobile edge computing," *IEEE Transactions on Mobile Computing*, vol. 23, no. 4, pp. 3452–3465, 2023.

[6] P.-C. Song, J.-S. Pan, H.-C. Chao, and S.-C. Chu, "Collaborative hotspot data collection with drones and 5G edge computing in smart city," *ACM Transactions on Internet Technology*, vol. 23, no. 4, pp. 1–15, 2023.

[7] Q. Yang, S.-C. Chu, J.-S. Pan, J.-H. Chou, and J. Watada, "Dynamic multi-strategy integrated differential evolution algorithm based on reinforcement learning for optimization problems," *Complex & Intelligent Systems*, vol. 10, no. 2, pp. 1845–1877, 2024.

[8] W.-P. Fang, "Offline QR code authorization based on visual cryptography," in *2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 2011, pp. 89–92.

[9] X. Cao, L. Feng, P. Cao, and J. Hu, "Secure QR code scheme based on visual cryptography," in *2016 2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE 2016)*. Atlantis Press, 2016, pp. 433–436.

[10] J.-S. Pan, T. Liu, B. Yan, H.-M. Yang, S.-C. Chu, M.-X. Wang *et al.*, "Novel visual secret sharing scheme for the QR code with meaningful shares," *Security and Communication Networks*, vol. 2022, pp. 1–9, 2022.

[11] L. Tan, K. Liu, X. Yan, S. Wan, J. Chen, and C. Chang, "Visual secret sharing scheme for color QR code," in *2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*. IEEE, 2018, pp. 961–965.

[12] Y. Jiang, Y. Lu, X. Yan, and L. Liu, "Extended secret image sharing with lossless recovery based on chinese remainder theorem and quick response code," in *2018 IEEE 3rd International Conference on Image, Vision and Computing (ICIVC)*. IEEE, 2018, pp. 678–683.

[13] J.-S. Pan, T. Liu, H.-M. Yang, B. Yan, S.-C. Chu, and T. Zhu, "Visual cryptography scheme for secret color images with color QR codes," *Journal of Visual Communication and Image Representation*, vol. 82, p. 103405, 2022.

[14] Y.-W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. M. Barmawi, "Exploiting the error correction mechanism in QR codes for secret sharing," in *Australasian Conference on Information Security and Privacy*. Springer, 2016, pp. 409–425.

[15] S. Wan, Y. Lu, X. Yan, H. Liu, and L. Tan, "Secret data-driven carrier-free secret sharing scheme based on error correction blocks of QR codes," in *Data Science: Third International Conference*

of Pioneering Computer Scientists, Engineers and Educators, ICPCSEE 2017, Changsha, China, September 22–24, 2017, Proceedings, Part I. Springer, 2017, pp. 231–241.

[16] J.-S. Pan, T. Liu, B. Yan, H.-M. Yang, and S.-C. Chu, "Using color QR codes for QR code secret sharing," *Multimedia Tools and Applications*, vol. 81, no. 11, pp. 15 545–15 563, 2022.

[17] M. A. Kute, M. D. Deokar, M. D. Moholkar, M. N. Kadam, and S. Kadam, "Modern method for detecting web phishing using visual cryptography (VC) and quick response code (QR code)," *International Journal of Engineering Research and Applications*, vol. 5, pp. 1–5, 2015.

[18] G. Devisree and K. Praveen, "Secretly shared QR code and its applications," in *Artificial Intelligence and Evolutionary Algorithms in Engineering Systems: Proceedings of ICAEES 2014, Volume 2.* Springer, 2015, pp. 473–480.

[19] A. Espejel-Trujillo, I. Castillo-Camacho, M. Nakano-Miyatake, and H. Perez-Meana, "Identity document authentication based on VSS and QR codes," *Procedia Technology*, vol. 3, pp. 241–250, 2012.

[20] J.-C. Chuang, Y.-C. Hu, and H.-J. Ko, "A novel secret sharing technique using QR code," *International Journal of Image Processing*, vol. 4, no. 5, pp. 468–475, 2010.

[21] Y.-W. Chow, W. Susilo, J. Tonien, E. Vlahu-Gjorgievska, and G. Yang, "Cooperative secret sharing using QR codes and symmetric keys," *Symmetry*, vol. 10, no. 4, p. 95, 2018.

[22] "Information technology. automatic identification and data capture techniques. QR code 2005 bar code symbology specification," *ISO/IEC*, vol. 18004, pp. 1–113, 2006.

[23] W. P. Fang, "Visual cryptography in reversible style," in *Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP 2007)*, vol. 1. IEEE, 2007, pp. 519–524.

[24] T. Liu, B. Yan, H.-M. Yang, S.-C. Chu, and J.-S. Pan, "A fake threshold visual cryptography of QR code," *Multimedia Tools and Applications*, vol. 81, no. 27, pp. 39 635–39 653, 2022.

[25] T. Liu, B. Yan, and J.-S. Pan, "Color visual secret sharing for QR code with perfect module reconstruction," *Applied Sciences*, vol. 9, no. 21, p. 4670, 2019.

[26] R. Velumani, H. Sudalaimuthu, G. Choudhary, S. Bama, M. V. Jose, and N. Dragoni, "Secured secret sharing of QR codes based on nonnegative matrix factorization and regularized super resolution convolutional neural network," *Sensors*, vol. 22, no. 8, p. 2959, 2022.

[27] J.-S. Pan, T. Liu, B. Yan, H.-M. Yang, and S.-C. Chu, "A lossless-recovery secret distribution scheme based on QR codes," *Entropy*, vol. 25, no. 4, p. 653, 2023.

[28] D. WAVE, "Qr code.com," http://www.qrcode.com/en/, 2003.

[29] S. Wan, Y. Lu, X. Yan, and L. Liu, "Visual secret sharing scheme with (k, n) threshold based on QR codes," in *2016 12th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN).* IEEE, 2016, pp. 374–379.

[30] S. Wan, Y. Lu, X. Yan, and L. Liu, "A novel visual secret sharing scheme based on QR codes," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 9, no. 3, pp. 38–48, 2017.

[31] Z. Fu, Y. Cheng, and B. Yu, "Visual cryptography scheme with meaningful shares based on QR codes," *IEEE Access*, vol. 6, pp. 59 567–59 574, 2018.

[32] C.-W. Hel, P.-Y. Lin, and C.-Y. Lin, "Secret sharing application for two-dimensional QR barcode," in *2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW).* IEEE, 2018, pp. 1–2.

[33] Z. Fu, S. Liu, K. Xia, and B. Yu, "Improved extended polynomial-based secret image sharing scheme using QR code," in *2018 14th International Conference on Computational Intelligence and Security (CIS).* IEEE, 2018, pp. 233–237.

[34] L. Tan, Y. Lu, X. Yan, L. Liu, and J. Chen, "(2, 2) threshold robust visual secret sharing scheme for QR code based on pad codewords," in *Security with Intelligent Computing and Big-data Services: Proceedings of the Second International Conference on Security with Intelligent Computing and Big Data Services (SICBS-2018) 2.* Springer, 2020, pp. 619–628.

[35] F. Hu, Y. Yao, W. Li, and N. Yu, "A novel visual cryptography scheme shared with edge information embedded QR code," in *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part II 6.* Springer, 2020, pp. 86–97.

[36] F. Hu, Y. Yao, W. Li, N. Yu *et al.*, "Threshold meaningful secret image sharing scheme based on QR code," *Security and Communication Networks*, vol. 2022, pp. 1–13, 2022.

[37] L. Ren and D. Zhang, "A QR code-based user-friendly visual cryptography scheme," *Scientific Reports*, vol. 12, no. 1, p. 7667, 2022.

[38] A. Kadam, P. Patil, P. Ware, S. Kutaskar, and V. Divekar, "Data hiding under QR code using visual secret sharing," *International Journal*, vol. 6, no. 4, pp. 55–59, 2021.

[39] H. S. Fairman, M. H. Brill, and H. Hemmendinger, "How the CIE 1931 color-matching functions were derived from wright-guild data," *Color Research and Application: Endorsed by Inter-Society Color Council, The Colour Group (Great Britain), Canadian Society for Color, Color Science Association of Japan, Dutch Society for the Study of Color, The Swedish Colour Centre Foundation, Colour Society of Australia, Centre Français de la Couleur*, vol. 22, no. 1, pp. 11–23, 1997.

[40] Y. Cheng, Z. Fu, and B. Yu, "Improved visual secret sharing scheme for QR code applications," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2393–2403, 2018.

[41] S. Wan, Y. Lu, X. Yan, Y. Wang, and C. Chang, "Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions," *Journal of Real-Time Image Processing*, vol. 14, no. 1, pp. 25–40, 2018.

[42] X. Zhang, J. Duan, and J. Zhou, "A robust secret sharing QR code via texture pattern design," in *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC).* IEEE, 2018, pp. 903–907.

[43] L. Tan, K. Liu, X. Yan, L. Liu, T. Lu, J. Chen, F. Liu, and Y. Lu, "Robust visual secret sharing scheme applying to QR code," *Security and Communication Networks*, vol. 2018, pp. 1–12, 2018.

[44] S.-K. Chen and Y.-W. Ti, "Visual cryptography with QR-code transparencies," in *Recent Advances in Intelligent Information Hiding and Multimedia Signal Processing: Proceeding of the Fourteenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, November, 26-28, 2018, Sendai, Japan, Volume 2 14.* Springer, 2019, pp. 19–26.

[45] Y. Cheng, Z. Fu, B. Yu, and G. Shen, "General construction for extended visual cryptography scheme using QR codes," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 11, no. 1, pp. 1–17, 2019.

[46] S. Wan, L. Qi, G. Yang, Y. Lu, X. Yan, and L. Li, "Visual secret sharing scheme with (n, n) threshold for selective secret content based on QR codes," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 2789–2811, 2020.

[47] L. Tan, Y. Lu, X. Yan, L. Liu, and X. Zhou, "XOR-ed visual secret sharing scheme with robust and meaningful shadows based on QR codes," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 5719–5741, 2020.

[48] P.-C. Huang, C.-C. Chang, Y.-H. Li, and Y. Liu, "Enhanced (n, n)-threshold QR code secret sharing scheme based on error correction mechanism," *Journal of Information Security and Applications*, vol. 58, p. 102719, 2021.

[49] Z. Fu, L. Fang, H. Huang, and B. Yu, "Distributed three-level QR codes based on visual cryptography scheme," *Journal of Visual Communication and Image Representation*, vol. 87, p. 103567, 2022.

[50] A. S. Rawat, M. Deshmukh, and M. Singh, "QR shares based secret sharing scheme using DWT, random permutation and arithmetic modulo operation for QR secret," in *2023 10th International Conference on Signal Processing and Integrated Networks (SPIN).* IEEE, 2023, pp. 772–777.

[51] S. Khairnar, "Anti-phishing framework based on extended visual cryptography and QR code," *International Journal of Computer Applications*, vol. 142, no. 5, pp. 25–28, 2016.

[52] S. Khairnar and R. Kharat, "Online fraud transaction prevention system using extended visual cryptography and QR code," in *2016 International Conference on Computing Communication Control and Automation (ICCUBEA).* IEEE, 2016, pp. 1–4.

[53] S. Wan, G. Yang, L. Qi, L. Li, X. Yan, and Y. Lu, "Multiple security anti-counterfeit applications to QR code payment based on visual secret sharing and QR code," *Mathematical Biosciences and Engineering*, vol. 16, no. 6, pp. 6367–6385, 2019.

[54] S. Goon, D. Pal, S. Dihidar, and S. Roy, "QR code-based digital payment system using visual cryptography," in *International Conference on Innovations in Data Analytics.* Springer, 2022, pp. 145–158.

[55] D. Saha, S. Sonar, P. Telore, and J. Lalit, "Secured document generation and authentication mechanism using VSS and QR code," *International Research Journal of Engineering and Technology (IRJET)*, pp. 1216–1219, 2016.

[56] M. Gayathri, A. J. Blesswin, and G. S. Mary, "An efficient QR-code authentication protocol using visual cryptography for securing ubiquitous multimedia communications," *Indian Journal of Science and Technology*, vol. 9, no. 39, pp. 1–7, 2016.

[57] L. Li, L. Li, S. Zhang, Z. Yang, J. Lu, and C.-C. Chang, "Novel schemes for bike-share service authentication using aesthetic QR code and color visual cryptography," in *Cloud Computing and Security: Third International Conference, ICCCS 2017, Nanjing, China, June 16-18, 2017, Revised Selected Papers, Part II 3.* Springer, 2017, pp. 837–842.

[58] J. Lu, Z. Yang, L. Li, W. Yuan, L. Li, and C.-C. Chang, "Multiple schemes for mobile payment authentication using QR code and visual cryptography," *Mobile Information Systems*, vol. 2017, pp. 1–12, 2017.

[59] L. Li, J. Yu, B. Wang, Q. Zhou, S. Zhang, J. Lu, and C.-C. Chang, "Multiple schemes for bike-share service authentication using QR code and visual cryptography," in *Cloud Computing and Security: 4th International Conference, ICCCS 2018, Haikou, China, June 8–10, 2018, Revised Selected Papers, Part III 4*. Springer, 2018, pp. 629–640.

[60] Y. Liu, C.-C. Chang, and P.-C. Huang, "One-code-pass user authentication based on QR code and secret sharing," *International Journal of Network Security*, vol. 22, no. 5, pp. 752–762, 2020.

[61] H. B. Errahmani and H. Ikni, "A new approach to verifying and sharing a secret QR code using elliptic curves," *Malaysian Journal of Computing and Applied Mathematics*, vol. 3, pp. 52–62, 2020.

[62] X. Zhong, L. Xiong, and Z. Xia, "A secure visual secret sharing scheme with authentication based on QR code," *Journal on Big Data*, vol. 3, no. 2, pp. 85–95, 2021.

[63] J. Valisireddy, K. A. Reddy, R. Elumalai, L. N. Mohan, and G. Anjaneyulu, "Secured authentication of online documents using visual secret sharing on QR code," *Journal of Integrated Science and Technology*, vol. 11, no. 4, pp. 568–568, 2023.

[64] W. Wen, Y. Jian, Y. Fang, Y. Zhang, and B. Qiu, "Authenticable medical image-sharing scheme based on embedded small shadow QR code and blockchain framework," *Multimedia Systems*, vol. 29, no. 2, pp. 831–845, 2023.

[65] P.-Y. Lin, "Distributed secret sharing approach with cheater prevention based on QR code," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 384–392, 2016.

[66] Y. Cheng, Z. Fu, B. Yu, and G. Shen, "A new two-level QR code with visual cryptography scheme," *Multimedia Tools and Applications*, vol. 77, pp. 20 629–20 649, 2018.

[67] P.-C. Huang, C.-C. Chang, and Y.-H. Li, "Sudoku-based secret sharing approach with cheater prevention using QR code," *Multimedia Tools and Applications*, vol. 77, pp. 25 275–25 294, 2018.

[68] S. Liu, Z. Fu, and B. Yu, "A two-level QR code scheme based on polynomial secret sharing," *Multimedia Tools and Applications*, vol. 78, pp. 21 291–21 308, 2019.

[69] P.-C. Huang, C.-C. Chang, Y.-H. Li, and Y. Liu, "Efficient secret sharing scheme with cheater identification based on QR code," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 13, no. 10, pp. 5144–5160, 2019.

[70] Z. Fu, Y. Cheng, and B. Yu, "Rich QR code with three-layer information using visual secret sharing scheme," *Multimedia Tools and Applications*, vol. 78, pp. 19 861–19 875, 2019.

[71] L. Xiong, X. Zhong, N. N. Xiong, and R. W. Liu, "QR-3S: A high payload QR code secret sharing system for industrial internet of things in 6G networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 7213–7222, 2020.

[72] P.-C. Huang, C.-C. Chang, and Y.-H. Li, "Efficient (k, n)-threshold secret sharing method with cheater prevention for QR code application," *Journal of Internet Technology*, vol. 23, no. 1, pp. 155–163, 2022.

[73] A. Vijetha, "QR code based secret sharing approach in a distributed way," *International Research Journal of Innovations in Engineering and Technology*, vol. 3, no. 10, pp. 51–55, 2019.

[74] Z. Fu, Y. Cheng, S. Liu, and B. Yu, "A new two-level information protection scheme based on visual cryptography and QR code with multiple decryptions," *Measurement*, vol. 141, pp. 267–276, 2019.

[75] B. Yu, Z. Fu, and S. Liu, "A novel three-layer QR code based on secret sharing scheme and liner code," *Security and Communication Networks*, vol. 2019, pp. 1–13, 2019.

[76] Y.-W. Ti, S.-K. Chen, and W.-C. Wu, "A new visual cryptography-based QR code system for medication administration," *Mobile Information Systems*, vol. 2020, pp. 1–10, 2020.

[77] A. Agrawal, K. Sethi, and P. Bera, "Inviolable e-Question paper via QR code watermarking and visual cryptography," in *2021 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. IEEE, 2021, pp. 266–271.

[78] N. Arora, P. Singh, S. Sahu, V. K. Keshari, and M. Vinoth Kumar, "Preventing SSRF (server-side request forgery) and CSRF (cross-site request forgery) using extended visual cryptography and QR code," in *Proceedings of Second International Conference on Smart Energy and Communication: ICSEC 2020*. Springer, 2021, pp. 215–227.

[79] W. Wu, L. Zhang, J. Zhang, C. Cui, X. Zhang, and M. Liu, "A three-level QR code sharing scheme based on SLIC and hamming code," in *2022 IEEE International Conference on Signal Processing, Communications and Computing (ICSPCC)*. IEEE, 2022, pp. 1–6.

[80] A. Arora, H. Garg, S. Shivani *et al.*, "Privacy protection of digital images using watermarking and QR code-based visual cryptography," *Advances in Multimedia*, vol. 2023, pp. 1–9, 2023.

[81] L.-N. Zhang, J.-Q. Sun, X.-Y. Zhang, Q.-P. Chen, and J. Zhang, “Two-level QR code scheme based on region matrix image secret sharing algorithm,” *Mathematical Biosciences and Engineering*, vol. 20, no. 9, pp. 16 678–16 704, 2023.

[82] J. Waleed, H. D. Jun, S. Saadoon, S. Hameed, and H. Hatem, “An immune secret QR-code sharing based on a twofold zero-watermarking scheme,” *International Journal of Multimedia and Ubiquitous Engineering*, vol. 10, no. 4, pp. 399–412, 2015.