

QR-3S: A High Payload QR code Secret Sharing System for Industrial Internet of Things in 6G Networks

Lizhi Xiong, Xinwei Zhong, Neal N. Xiong, *Senior Member, IEEE* and Ryan Wen Liu

Abstract—The Communication in 6G-Enabled Network In Box (NIB) needs to meet the characteristics of fast, convenient, and safe. Secret sharing scheme has become a hot topic nowadays due to unconditionally security and simple decryption. At the same time, Quick Response (QR) code as a popular carrier has been widely applied in various industrial applications because of data payload and convenience. Thus, the combination of secret sharing and QR Code provide a solution with satisfying the requirements of 6G-Enabled NIB. In this paper, we design a QR code Secret Sharing scheme with authentication to protect private data and prevent cheater. In this scheme, a secret image is firstly divided into a series of shadows based on a polynomial, and authentication bits are generated based on the generated shadows. Then shadows and the authentication bits are embedded into the cover QR codes according to the error correction redundancy and the homomorphism of Reed-Solomon code in the QR code. In addition, the secret can be restored with the qualified shares and the authentication bits could verify the authenticity of the embedded shadows. Compared with existing schemes, the proposed scheme not only guarantees high capacity, but also embeds more authentication bits to improve the authentication ability. In addition, experimental results have demonstrated that the proposed scheme is both robust and secure.

Index Terms—6G-Enabled Network in Box, QR code, error correction capability, visual secret sharing, cheater prevention

I. INTRODUCTION

6G-Enabled Network In Box (NIB) was introduced in the recent as an opportunity to combine industrial systems and the Internet in depth. NIB is a portable and self-organized device, which can provide communication services. Because NIB needs to meet the characteristics of portability and rapid deployment, the computational complexity of communication in NIB needs to be as low as possible. Moreover, the concept of ubiquitous connection and real-time connection is proposed in 6G-Enabled NIB. To meet these requirements, the NIB is developing towards low-power devices, low computing

complexity and security technology. On the other hand, the communication between different devices in the Industrial Internet needs to ensure data security, high payload, and reliability. The security of private data is also a key issue in many areas, especially in highly confidential areas such as medical and military fields [1, 2].

Visual secret sharing scheme, also called Visual Cryptography Scheme (VCS), was first introduced by Naor and Shamir [3], in which the secret is encoded and distributed a number of shares. The encoded shares will not reveal any original secret information. Finally, the secret can be restored with the qualified shares. Otherwise, the secret cannot be recovered. Therefore, VCS is also one of the techniques which transmit the secret data in public channels and provides a solution for solving the drawback of embedding all information individually. In the current mobile devices, the recovery process is feasible and reasonable. Therefore, regardless of the specific recovery operation, VCS has a feature of low computational cost. In recent years, these techniques have been widely developed [5-7].

Quick Response (QR) code [8] as a popular carrier has been widely applied in various industrial applications because of its convenience in reading, writing and fast response. Therefore, due to the popularity of QR codes, and the flexibility and security of VCS, many scholars have begun to combine VCS with QR codes for the research, which will become a safe and efficient real-time communication method in 6G networks. QR code was originally invented by the Japanese company named Denso Wave in 1994. Compared with one-dimensional codes, the application of QR code is more extensive because it has a higher storage capacity and error-correcting capabilities, such as web links, transport ticketing, payment information, electronic tickets, and so on.

In the schemes of combining QR code and VCS, the secret is not stored in a single carrier, but is divided into several meaningful cover QR codes. Each embedded cover QR code is

This work was supported in part by the National Natural Science Foundation of China under Grant 61702276, Grant 61672294; in part by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund.

Lizhi Xiong and Xinwei Zhong are with School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, Jiangsu, Peoples R. China (e-mail: lzxiong16@163.com, 846111780@qq.com). L. Xiong is also with the Engineering Research Center of Digital Forensics,

Ministry of Education, Jiangsu Collaborative Innovation Center on Atmospheric Environment and Equipment Technology, Nanjing, Jiangsu, Peoples R. China

Neal N. Xiong is with the Department of Mathematics and Computer Science, Northeastern State University, United States (e-mail: dnxiong@126.com, Corresponding author)

Ryan Wen Liu is with the School of Navigation, Wuhan University of Technology, Wuhan, Hubei, Peoples R. China (e-mail: wenliu@whut.edu.cn)

meaningful and will not disclose any secret information. Finally, the secret can be recovered by a series of qualified QR codes. Due to the characteristics of 6G networks, real-time and ubiquitous communication, the low computational complexity and the information security of communication are very important. At the same time, the scheme of combining QR code and VCS has the characteristics of low computational complexity and high security. Thus, the scheme fully meets the requirements of communication in 6G networks.

In general, a practical visual secret sharing scheme for 6G-Enabled NIB has the following features: 1) a large capacity, 2) robustness for common attacks, 3) cheater prevention. Therefore, we propose a (t, n) threshold high payload QR code Secret Sharing scheme with Authentication. Because of the characteristics of high payload and security, this scheme can be widely used in communication of 6G networks. In the proposed scheme, each t -pixel in the secret image is regarded as a group, and the coefficients of the $(t-1)$ degree polynomial are replaced by a group of t -pixels. Then, a set of shadows can be generated by inputting the private keys of participants. After that, authentication bits can be computed by the shadows. In the embedding phase, authentication bits are firstly embedded into the padding region of the QR code according to the homomorphism of Reed-Solomon (RS) code. The QR code embedded with the authentication bits does not sacrifice its error correction ability and the authentication process can check the tampered QR code before the recovery process. Then the shadows are embedded into the error correction redundancy according to the private keys of participants as the index.

The main contributions in this paper are shown as follows.

- 1) In this scheme, more authentication bits are embedded into the cover QR code. At the same time, the proposed scheme also guarantees the high secret capacity. The authentication capability is stronger compared with other schemes.
- 2) Each share is a valid QR code, which not only does not reveal the secret message, but also reduces the likelihood of attracting the attention of potential attackers. Furthermore, the robustness and payload of our proposed scheme are higher compared with other methods.
- 3) In this scheme, the key inputted into the polynomial is converted into the index of the secret embedded location, which saves a key transmission. Thus, the proposed scheme reduces the consumption of resources.

The rest of this paper is organized as follows. Section II introduces the Related works. Preliminaries are introduced in Section III. The proposed schemes are presented in Section IV. The Experiments and Comparisons are analyzed in Section V. Our conclusion and future work are presented in Section VI.

II. RELATED WORK

Recently, some researchers began to study the combination of visual secret sharing and QR code. A secret sharing method (k, n) based QR code was firstly designed by Chuang et al. [9] to protect the private data during transmission. The secret message is divided into a set of meaningless shares based on the polynomial [10], i.e., n pieces of encrypted information are

obtained. Thus, n QR codes are generated according to the n corresponding encrypted messages. When k qualified participants cooperate, they can use the polynomial interpolation to decrypt the secret. However, the generated QR codes are easy to attract the attention of attackers when transmitted, because the message stored in these QR codes is meaningless. Later, Chow et al. [11] proposed a novel (n, n) visual secret sharing scheme with the error correction capability of QR code. In Chow's scheme, the QR code with privacy is regarded as the secret. In the sharing phase, a cover QR code is randomly selected and its codeword that has not been modified is changed so that the XOR result of the codewords of all cover QR code is equal to the corresponding codeword of the secret QR code. Certainly, the number of modified codewords per block in the selected cover QR codes cannot exceed the error correction redundancy of the cover QR code. The generated shares are all valid QR codes, which can reduce the possibility of attacker's attention in transmission. Finally, the secret QR code can be reconstructed by n qualified shares with XOR each module of the shares. However, the messages stored in the cover QR codes are similar with each other, thus the secret can be partially disclosed by less than n shares. In view of this security shortcoming, Cheng et al. [12] investigated an improved VSS scheme based on QR code to avoid this shortcoming. In Cheng's scheme, the codewords in each block of the cover QR code are divided reasonably based on XOR-Visual Secret Sharing (XVSS) theory to share the secret QR code. Therefore, less than n shares will not reveal any secret. However, the participants are assumed to be honest in the above schemes. If there is the dishonesty among participants, the recovery phase will be compromised. That is to say, cheater prevention is not taken into consideration in the schemes.

Thus, Lin [13] investigated a (n, n) secret sharing scheme with cheater prevention to solve the problem. In Lin's scheme, the secret bit stream is divided into a set of shares according to the bit stream XOR operation. Then, the master key of the hash function is generated by superimposing the private keys of all participants, and the authentication stream of each participant can be obtained by the hash function with the master key and the private key of each participant. Next, the shares and the authentication streams are embedded into the carriers of common QR codes based on the wet paper code (WPC) algorithm [14]. Finally, when n marked QR codes cooperate, they may restore the secret message. In the authentication phase, only when the attacker provides a true private key and a fake stego-QR code, the attacker can be checked successfully. If the attacker provides a fake private key, the whole authentication phase will be compromised since the master key of the hash function is obtained by overlaying the private key of each participant. Besides, the key of the participant needs to be transmitted in the public channel, which maybe an insecure factor. What's more, the secret is randomly distributed to shares by Wet Paper Coding (WPC). In other word, the embedding position of the secret bits is selected randomly in WPC while the data codeword of the QR code is all in the form of consecutive 8 bits, so the embedding capacity of this scheme is not as large as that mentioned in the article. In fact, the capacity

of the Lin's scheme is from 3 bits to 1215 bits, by selecting different versions and error correction levels [15].

Recently, some researchers [18, 19] use the homomorphism of RS (Reed-Solomon) code in QR code to embed the secret into the padding region without affecting the error correction ability. In [18, 19], the secret is firstly shared into a set of meaningless shares based on traditional VCS and Sudoku, respectively. Then, these shares are embedded into the padding region of the cover QR codes with the homomorphism of RS code. However, their embedding capacity is uncertain, which is determined by the public information of QR code; in addition, their schemes have no verification ability, so they cannot prevent the attackers from cheating.

TABLE I
ERROR CORRECTION LEVELS

Error correction levels	Recovery capability, % (approx.)
L(Low)	7
M(Medium)	15
Q(Quartile)	25
H(High)	30

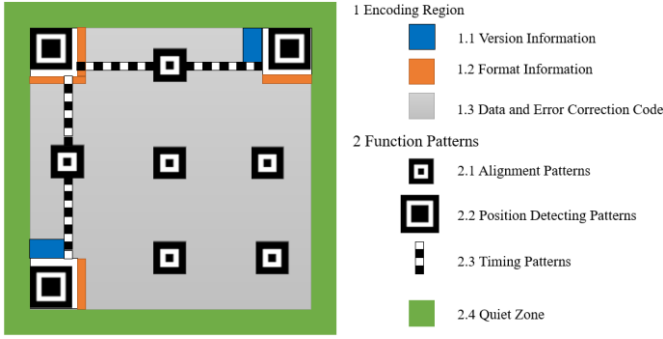


Fig. 1. The QR code structure of version 7.

III. PRELIMINARIES

QR code is a binary image, and each pixel is usually called as a module. There is a total of 40 versions of the QR code. Each version has a different size. When a part of QR code is covered or spoilt, it can also be decoded because of its error correction function. To perform the functionality of error correction, QR code standard provides four error correction levels for each version, L, M, Q, and H, as shown in Table I.

As is shown in Fig. 1, a QR code consists of two parts, encoding region and function pattern. The encoding region contain data codewords, error correction codewords, the version information, etc. While the function patterns are used to store information such as timing pattern, alignment patterns, etc.

In the decoding process, the QR codes will only be decoded in sequence according to the character count indicator, which means that the QR codes will not continue to be decoded after reaching the maximum length of the character count indicator. If the length of the public message bits does not reach the maximum length limit of the data region of the QR codes, the padding codewords needs to be appended to the public message bits to fill the data region. The area composed of padding codewords is called the padding region. The padding codewords is not important, even if the codewords is tampered with will not affect the normal use of the QR codes.

QR codes utilize the Reed-Solomon (RS) code to realize its error correction ability when a part of QR code is covered or spoilt. At the same time, the RS code has the homomorphic property [4]. In other words, the result that obtained by XORing two RS codes with the same length of data codewords and error correction codewords is still a valid RS code. Table II shows an example of error correction codewords generation. There are two RS codes, RS1 and RS2 respectively. Each of which is composed of 8 bits data, 8 bits padding code and 8 bits error correction code. Their XOR result is still a valid code.

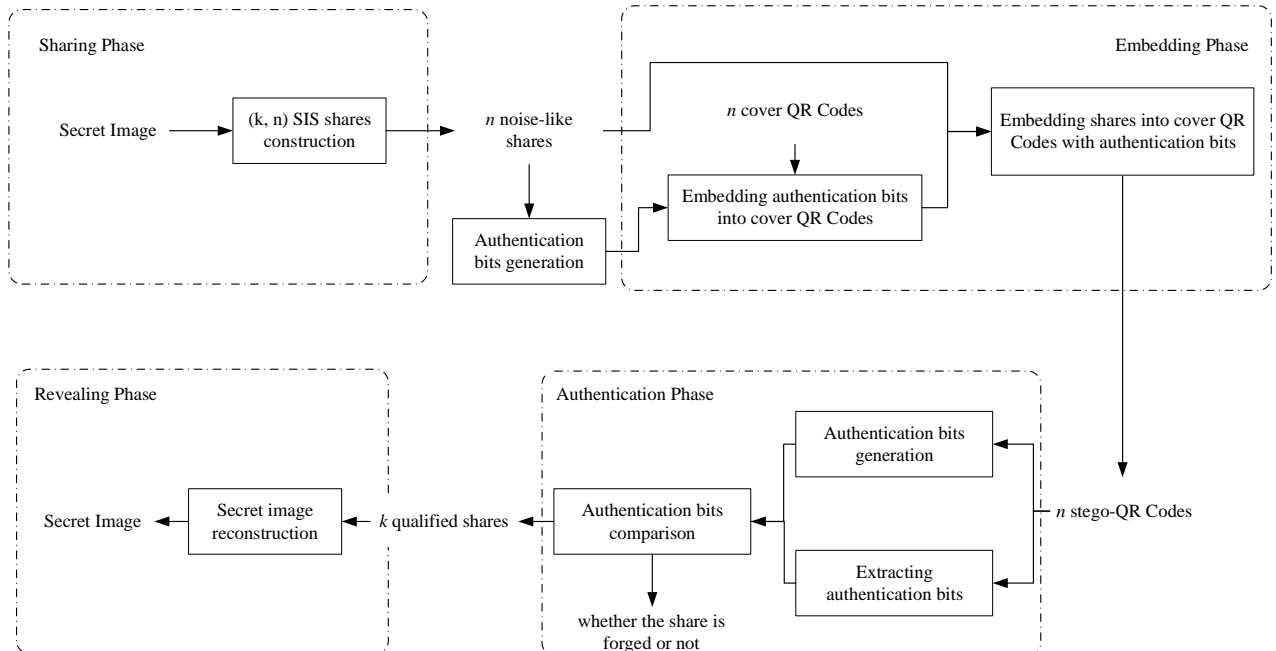


Fig. 2. The framework of the proposed scheme.

TABLE II

AN EXAMPLE OF ERROR CORRECTION CODEWORDS GENERATION

	Data region	Padding Region	Error Correction
RS code 1	10001000	00010001	10011001
RS code 2	00000000	10001000	10001000
Result	10001000	10011001	00010001

TABLE III

AN EXAMPLE OF SECRET EMBEDDING

Secret	10011001		
	Data region	Padding Region	Error Correction
RS code in QR code	10001000	00010001	10011001
The code	00000000	10001000	10001000
modified RS code	10001000	10011001	00010001

According to the above two properties, we can embed the secret into the padding region without affecting the error correction ability of the QR code. Table III shows an example of secret embedding. If we want to embed the secret bits 10011001 in the padding region. We can XOR the secret with the padding codewords of the QR code to get a code 10001000, and zeros of the same length as the data region are added in front of the code. Then, a complete RS code 000000001000100010001000 is constructed by using RS algorithm according to the generated code. Finally, the modified RS code can be obtained by XOR RS code in QR code with the code. Most important of all, the modified code is still a valid RS code. Therefore, the QR code modified in this way will not compromise its error correction ability.

IV. THE PROPOSED SCHEME

In this section, we propose a (t, n) threshold high payload QR code Secret Sharing System for Industrial Internet of Things. Next, we will describe this system from three parts: Secret Sharing Procedure, Secret Revealing Procedure, Security Analysis.

The framework of the proposed scheme is shown in Fig. 2. Firstly, n noise-like shares are generated from the secret image in the sharing phase. Secondly, the shares and authentication bits are embedded into the cover QR codes. n stego-QR codes are obtained in the embedding phase. And then, authentication bits are extracted to check the integrity of the shares. Finally, the secret image is recovered in the revealing phase.

A. Secret Sharing Procedure

1) Preliminary Phase

Before the embedding process, the length of the secret and the authentication bits needs to be calculated firstly. Suppose S is the secret, and $V_i (1 \leq i \leq n)$ is the authentication bits generated based on the shadow.

Step 1) Firstly, the length of the secret l_s is calculated according to the error correction level and version of the given QR code.

$$l_s = C \times b \times t. \quad (1)$$

where $C = \lfloor E/2 \rfloor$ is the value of modifiable capacity for the each block of the given cover QR code, E is the number of error correction codeword of each block, b is the number of blocks in the QR code, t is the threshold value of the scheme.

Algorithm I: Sharing Algorithm

Input: the cover QR code QR_i , the private key PK_i , the ID of the participant P_i , the shadow $Shadow_i (1 \leq i \leq n)$.

Output: the embedded QR code $QR_i^* (1 \leq i \leq n)$.

Foreach $i \in \{1, 2, \dots, n\}$ **do**

$V_i = Hash_k(Shadow_i \parallel P_i)$;

Unmask cover QR code QR and obtain the padding bits w ;

$B = XOR(V_i, w)$;

$BS = [8 \times R - l_v \text{ zero}, B]$; // $8 \times R - l_v$ zero should be added in the front of bit stream B to obtain a bit stream BS with length $8 \times R$.

Generate the corresponding error correction bits according to Reed-Solomon algorithm, and attach the error correction bits to the bit stream BS to obtain a new RS code NRS ;

$FRS = XOR(ORS, NRS)$; //Generate a final RS code FRS according to XORing the original RS code ORS with the new RS code NRS .

Obtain the cover QR QR_i^* after embedding the authentication bits based on FRS .

Foreach $j \in \{1, 2, \dots, b\}$ **do**

An index x of the shadow's embedded location is created based on Eq. (9);

Embed the shadow into the cover QR QR_i^* according to the index x

to obtain the final QR code QR_i^* ;

End
End

Step 2) Then, the length of the authentication bits l_v needs to be obtained according to the padding region of the cover QR code.

$$l_v = 8 \times R - \sum_{j=1}^m (M_j + I_j + D_j) - T. \quad (2)$$

where R is the total number of codewords in the data region, M_j is the number of bits of the mode indicator in each segment, I_j is the number of bits of the character count indicator in each segment, D_j is the number of bits of the input data characters in each segment, T is the number of bits of the terminator.

2) Sharing Phase

In order to recover the secret losslessly, the proposed scheme uses Galois Field $GF(2^8)$ instead of the traditional Galois Field $GF(251)$ [17], i.e.,

$$f(x) = (a_0 + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}) \bmod g(x). \quad (3)$$

In our scheme, every t pixels of the secret with length l_s is regarded as a group, and these coefficients $a_0, a_1, a_2, \dots, a_{t-1}$ of the polynomial function is replaced by t pixels in the group. Afterwards, the value of a shadow can be obtained by feeding the corresponding private key $PK_i (1 \leq i \leq n)$ of each participant. Finally, n shadows, $Shadow_i (1 \leq i \leq n)$, are obtained, each of which is $1/t$ of the size of the secret image.

3) Embedding Phase

Step 1) For the sake of preventing attackers from tampering with the shadows embedded in the cover QR code, the proposed scheme utilizes a hash function to generate the authentication bits. In our experiment, SHA-1 is the selected hash function.

Shadows are used as the input to the hash function. In addition, considering that the attacker uses the shadow of other participant to avoid the verification process, the participant ID $P_i (1 \leq i \leq n)$ should be appended to the input $Shadow_i$ to avoid this attack. After that, the length l_{V_i} of the authentication bits $V_i (1 \leq i \leq n)$ can be obtained. Thus, V_i can be defined as.

$$V_i = H_K(Shadow_i \parallel P_i). \quad (4)$$

where $P_i (1 \leq i \leq n)$ is the ID of the i -th participant. K is the key of the hash function.

Step 2) Decoding the cover QR code to obtain the padding bits $W_i (1 \leq i \leq n)$ with the length l_{W_i} . Bit stream B is obtained by XORing of the authentication bits V_i and the padding bits W_i .

$$B = XOR(V_i, W_i). \quad (5)$$

Step 3) Suppose that the data region of the cover QR code consists of R codewords in total. Since each codeword is composed of 8 bits, $8 \times R - l_{V_i}$ bits zero should be added in the front of bit stream B . After that, we can obtain a bit stream BS with length $8 \times R$. Then, the corresponding error correction bits can be obtained by Reed-Solomon algorithm, and attach the error correction bits to the bit stream BS to get a new RS code, NRS . Finally, the final RS code, FRS , can be calculated by XORing the original RS code, ORS , with the new RS code NRS and embedded into the cover QR code as follows.

$$FRS = XOR(ORS, NRS). \quad (6)$$

Step 4) Since the authentication bits are embedded into the data region, if the shadows are embedded into the data region, the authentication bits will be affected. Therefore, the shadows should be embedded into the error correction region. Suppose that the total number of error correction codewords in a block is l_{ec} . Before embedding the shadow, we need to index the location of the embedding. The index X ranges from 1 to l_{ec} . l_{ec} can be calculated by

$$l_{ec} = R - D, \quad (7)$$

where R is the total number of the codewords in a block, D is the number of the data codewords in a block.

Step 5) Since the data in the QR code will be stored in b blocks, we need to divide the shadow into b blocks first. Each block consists of l_b values in the shadow.

$$l_b = l_{Shadow} / b. \quad (8)$$

where l_{Shadow} is the total number of pixels in the shadow.

Step 6) Usually an index is generated directly according to the key, but an additional secure channel needs to be established to transmit the key, thus increasing resource consumption. In this scheme the index $X = \{x_i | 1 \leq x_i \leq l_{ec}, i = 1, 2, \dots, l_b\}$ in a block is generated according to the key $PK_j = \{k_i | 1 \leq k_i \leq 255, i = 1, 2, \dots, l_b\} (1 \leq j \leq n)$ used by participants to generate shadows. The elements in the index are obtained by modular operation of the key and the length of the error correction codewords l_{ec} . If an element in the index is

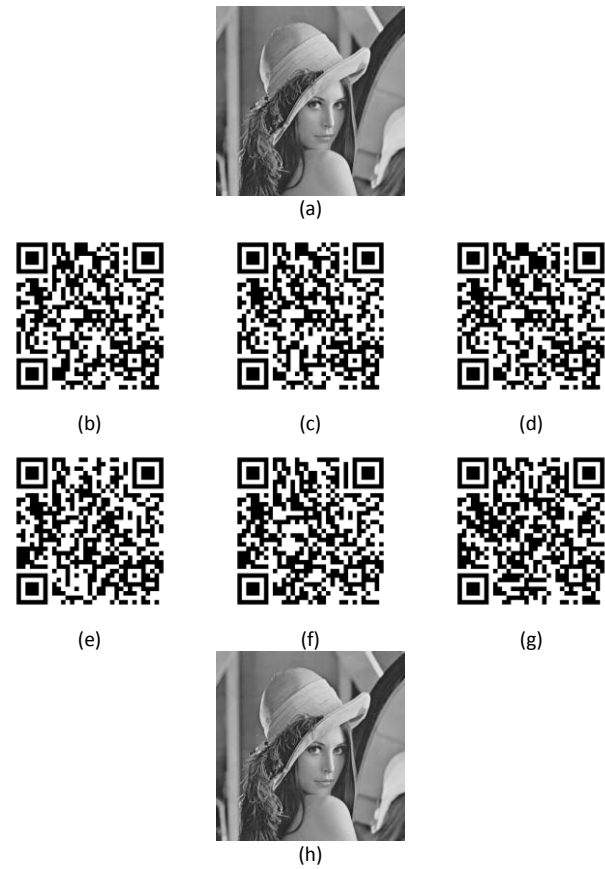


Fig. 3. (2, 3)-threshold sharing of the proposed scheme for QR version 4-H. (a) secret image with 8×8 pixels; (b) Cover QR code 1; (c) Cover QR code 2; (d) Cover QR code 3; (e) stego-QR code 1; (f) stego-QR code 2; (g) stego-QR code 3; (h) the recovered secret image.

repeated, the latter element will be increased by 1, until it is not repeated with the previous element.

$$x_i = k_i \bmod l_{ec} + D \quad (9)$$

where D is the number of the data codewords in a block. Since the shadow is embedded in the error correction region, the length of the data codewords D needs to be added at the end.

Step 7) Each value in the shadow and each codewords in the QR code is made up of 8 bits. Therefore, the shadows can be embedded directly into the QR code by index X .

The above procedures are shown in **Algorithm I**.

B. Secret Revealing Procedure

1) Cheater Identification Phase

Before the recovery phase, the authenticity of the cover QR codes need to be checked.

Step 1) The indexes of the embedded location should be first obtained by the private key of the participants. The embedded shadows $Shadow_i (1 \leq i \leq n)$ can be extracted by the indexes. Then, the authentication bits V_i' can be calculated by.

$$V_i' = H_K(Shadow_i' \parallel P_i). \quad (10)$$

where $P_i (1 \leq i \leq n)$ is the ID of the i -th participant.

Step 2) Decoding the cover QR code to obtain the embedded authentication bits V_i in the padding region. If V_i is the same as V_i' , the QR code participating in the recovery process is proved

Algorithm II: Authentication and Extraction Algorithm

Input: the embedded QR code QR^* , the private key PK .
Output: the shadow $Shadow$.
 Unmask the embedded QR code QR^* and extract the embedded authentication bits V ;
Foreach $j \in \{1, 2, \dots, b\}$ **do**
 An index of the shadow's embedded location is created based on Eq. 9;
 Extract the embedded shadow according to the index x ;
End
 Generate the authentication bits V' according to Eq. (10);
If $V' \neq V$
 Terminate the procedure;
Else
 Return $Shadow$;
End

not to have been tampered with; Otherwise, the stego-QR code has been tampered with by the attacker to deceive the recovery process.

2) Secret Retrieval Phase

If the tampering detection process is passed, the secret can be revealed by Lagrange's interpolation.

The above procedures are shown in **Algorithm II**.

C. Security Analysis

Security is an important criterion for secret sharing. As a necessary evaluation standard, security in this scheme represents that less than the qualified shares cannot reveal the data.

As we all know, the polynomial of $k-1$ degree is solved by Lagrange's interpolation method, which requires the input of k pairs. Therefore, secret information cannot be recovered with fewer than k shadows. Actually, the proposed scheme is based on Shamir's method, and its security can be guaranteed. Thus, the security of the proposed scheme is proven.

In addition, the cover QR code after embedding the shadow and authentication bits are still a valid QR code since the number of correctly recovered codewords is within the error correction redundancy, and anyone can read its public information through a QR code scanner. Besides, the stego-QR codes are robust to some extent. Therefore, they are not likely to arouse the suspicion of the attacker.

V. EXPERIMENTS AND COMPARISONS

In this section, we performed several experiments to evaluate the feasibility of our scheme. In addition, some comparisons with other related approaches are also shown.

TABLE IV
EXPERIMENT RESULTS COMPARED WITH OTHER SCHEMES

Schemes	Embedding Capacity (bit)	Authentication Bits
[11]	256	0
[13]	236	20
[19]	64	0
The proposed scheme	256×2	64

TABLE V
EMBEDDING CAPACITY COMPARED WITH OTHER SCHEMES

Scheme	Embedding capacity
[11]	C per error correction block
[13]	C per error correction block - the length of authentication bits
[19]	$8 \times R - \sum_{j=1}^m (M_j + I_j + D_j) - T$
The proposed scheme	$t \times C$ per error correction block

A. Experimental Results
















In the experiments, MATLAB language with the open source library and ZXing library are used to generate and decode the multiformat barcode for development.

In (2,3) threshold secret sharing scheme, 4-H QR code with 36 data codewords is selected as an example. Note that the proposed scheme is applicable to any version and error correction level of the QR code. Since 4-H QR code is selected, the length of the secret can be calculated as 64 pixels. Thus, the size of the secret image can be selected as 8×8 pixels. Fig. 3(a) shows the selected secret image, which is a Lena image. Fig. 3(b)-(d) show the three cover QR codes we selected. The public information stored in them is the number of Cover Quick Response Code, i , where $1 \leq i \leq 3$. According to the calculation, there are a total of 28 codewords storing public information in the cover QR codes, so the length of the remaining codewords that can be used to embed the authentication bits is 8, thus the length of the authentication bits in our scheme is 64 bits. Fig. 3 (e)-(g) show three stego-QR codes embedded with secret information and authentication bits. We can find that the public information stored in them can be read normally with the QR code reader. Therefore, it will not attract the attention of the attacker. Fig. 3(h) shows the successful recovery of the secret image through the stego-QR codes. Table IV shows a comparison with the literature [11], [13], and [19] under the same conditions. Since 4-H cover QR code can be modified a total of 32 codewords and each codewords consists of 8 bits, the embedding capacity in [11,13] is 256 bits. However, in [13], 20 bits of authentication information needs to be embedded, so the actual embedding capacity is 236 bits. In [19], the length of codewords in the padding region is 8, thus its embedding capacity is 64 bits.

B. Embedding Capacity

In this part, we analyze the difference with Chow et al. [11], Lin et al. [13] and Tan et al. [19] from the embedding capacity of cover QR codes. Table V displays the comparison between our scheme and their schemes in terms of embedded capacity. In Tan's scheme, the secret is embedded into the padding region of the QR code, so the capacity is $8 \times R - \sum_{j=1}^m (M_j + I_j + D_j) - T$. Both Chow and Lin's schemes use the error correction redundancy of the QR code to embed the shadows, thus in Chow's scheme the capacity is C per error correction block. However, in Lin's scheme the embedded information also includes authentication bits, so the capacity is C per error correction block minus the length of authentication bits. In our

TABLE VII
RESULTS OF THE 4-H STEGO-QR CODES AFTER COMMON PROCESSES

Stego-QR code			
Gaussian noise	30%	50%	70%
			
Stego-QR code			
Content	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable
Stego-QR code			
Uniform noise	30%	50%	70%
			
Stego-QR code			
Content	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable
Stego-QR code			
Gaussian blurring	Radius: 1 pixel	Radius: 2 pixels	Radius: 3 pixels
			
Stego-QR code			
Content	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable
Stego-QR code			
Rotation	45°	135°	270°
			
Stego-QR code			
Content	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable
Stego-QR code			
Compression	JPEG 50%	JPEG 70%	JPEG 100%
			
Stego-QR code			
Content	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable

proposed scheme, since the shadows are $1/t$ of the secret image, our actual embedding capacity is $t \times C$ per error correction block.

C. Authentication capability

In this paper, detection ration (DR) is used for the first time to evaluate the authentication capability of a secret sharing scheme based on QR code. DR is expressed as

$$DR = \frac{\text{Detected manipulations}}{\text{All manipulations}}. \quad (11)$$

In general, the length of authentication bits l_v in the QR code results in DR about $1 - (1/2)^{l_v}$. In our scheme, the authentication bits are embedded in the padding region of the QR code, so the length of the authentication bits is $8 \times R - \sum_{j=1}^m (M_j + I_j + D_j) - T$, where R is the total number of codewords in the data region, M_j is the number of bits of the mode indicator in each segment, I_j is the number of bits of the character count indicator in each segment, D_j is the number of bits of the input data characters in each segment, T is the number of bits of the terminator.

TABLE VI
AUTHENTICATION CAPABILITY COMPARED WITH OTHER SCHEMES

Scheme	DR	Number of authentication bits
[11]	0	0
[13]	$1 - (1/2)^{(1 + \lfloor \alpha \times \text{version} \rfloor) \times b}$	$(1 + \lfloor \alpha \times \text{version} \rfloor) \times b$
[19]	0	0
The proposed scheme	$1 - (1/2)^{8 \times R - \sum_{j=1}^m (M_j + I_j + D_j) - T}$	$8 \times R - \sum_{j=1}^m (M_j + I_j + D_j) - T$

Table VI displays the comparison between our scheme and their schemes in terms of the authentication capability. Since Tan's scheme and Chow's scheme did not embed authentication bits into the cover QR code, DR in their schemes is equal to 0. In Lin's scheme, the length of the authentication bits depends on the version and the error correction level of the QR code. The length of the authentication bits can be expressed as $(1 + \lfloor \alpha \times \text{version} \rfloor) \times b$,




where $0 \leq \alpha < \frac{(C/b-1)}{\text{version}}$. In fact, the range of embedded

authentication bits is from 1 to 3321. However, the authentication bits in the Lin's scheme is generated based on the key of the participant, and the validation process is compromised if a dishonest participant embeds a tampered shadow. At the same time, Lin's solution is to embed more authentication bits at the expense of the secret embedding capacity. However, in our scheme, the capacity of authentication bits depends on the public information of the QR code, and the maximum length of the authentication bits can reach about 9700 bits.

D. Robustness and Comparison

Considering the common attacks of noise, rotation, and compression in real-world applications, the proposed scheme is tested by the above attacks. Table VII illustrates the ability of the shares if they suffered from common attacks, such as noise,

TABLE VIII
4-H STEGO-QR CODE AFTER PRINTING AND SCANNING

Marked QR code			
	Stego-QR code 1	Stego-QR code 2	Stego-QR code 3
Print and Scan			
Content	Readable	Readable	Readable
Secret	Decodable	Decodable	Decodable

blur, rotation, and compression. Noise occurs when communicating or capturing the QR tag in the real world. Here, the Gaussian and Uniform noises are added to the marked QR code shares at 30%, 50%, and 70%. Moreover, the compression technique usually is used to compress the QR code shares for reducing the storage space. To evaluate the feasibility of the designed scheme under image compression, the JPEG 2000 loss compression is mounted to the marked QR image with quality factors (Q) of 50%, 70%, and 100%. The rotation is mounted further to the marked QR code shares to estimate the performance of the proposed scheme with the use of mobile devices. As shown in Table VII, the proposed scheme is able to resist these attacks. Note that the different barcode decoders and environments [16], such as lights, mobile devices, monitors, and non-normal conditions, could influence the decoded results of QR codes (including original and marked).

Since the QR code needs to be often published in magazines, newspapers, advertisements and other paper version of the document, we need to consider the situation of printing and scanning. Table VIII lists the printed and scanned shares for the 4-H stego-QR codes. These shares were printed by an HP LaserJet P1100 printer with 600 dpi and then scanned with 300 dpi by Konica Minolta bizhub C353 without any correction or restoration. The QR data of the three printed and scanned QR code shares are all readable by a barcode reader. In addition, the QR code shares can recover the shared secret correctly. Therefore, our proposed scheme is robust for the common print and scan operations and preserves the QR data and the secret shares in real-world application.

Table IX provides an overall comparison of the literature [11], [13], [19], and the proposed scheme. In [11], they designed a novel VCS based on XORing operation. However, In the scheme, the threshold value n must be greater than or equal to 3. Lin [13] comes up with a cheater prevention secret sharing scheme. However, according to the literature [15], the actual capacity of the Lin's scheme is from 1 to 1215 bits. In [19], Tan et al. achieved progressive (t, n) threshold secret sharing with the homomorphism of QR codes. They embed shadows in the padding region of the cover QR codes, so the embedding capacity is calculated based on the public information of the cover QR codes. However, if the public information is not stored in a proper version of the cover QR code, but in a larger version of the cover QR code, to increase the embedding capacity, it is very easy to arouse the suspicion of attackers. If the version of cover QR code is only allowed to float five levels

TABLE IX
COMPARISON OF THE CHARACTERISTICS WITH OTHER SCHEMES

Functionality	[11]	[13]	[19]	The proposed scheme
Application field	Secret sharing	Secret sharing	Secret sharing	Secret sharing
Domain	Spatial	Spatial	Spatial	Spatial
Threshold	(n, n) ($n \geq 3$)	(n, n)	Progressive (k, n)	(k, n)
Meaningful of covers	Yes	Yes	Yes	Yes
Error correction capability	Yes	Yes	No	Yes
Homomorphism of RS code	No	No	Yes	Yes
Computational complexity	Low	Mid	Low	Low
Robustness	High	High	High	High
Authentication	No	Low	No	High
Secret Capacity	QR image	Adjustable (1,1215) bits	Adjustable (1,5200) bits	High ($t, 9720 \times t$) bits

to reduce the attacker's attention, the actual embedding capacity of the scheme is about 1-5200 bits. In the proposed scheme, each cover QR code is embedded with a shadow whose size is $1/t$ of the secret image according to the error correction function, so our embedding capacity is $t \times C$ per block. In fact, the actual embedding capacity ranges from t to $9720 \times t$ bits. Assuming that five versions can be floated according to the public information in the cover QR code to avoid the attacker's attention, the length of authentication bits in this scheme could reach up to 5200 bits. Therefore, the embedding capacity and authentication capability of our scheme are higher than other schemes. In addition, the proposed scheme is suitable for other version and error correction levels of QR Code.

E. Industrial Applications

Since QR code has the characteristics of flexibility, convenience, and large capacity, QR code will become an important carrier in communication of NIB. At the same time, due to the security and low complexity of secret sharing schemes, it is an inevitable research trend to combine secret sharing schemes with QR code in communication of 6G network. However, it is not enough to satisfy the characteristics of fast and real-time communication in 6G network, it is also necessary to ensure the authenticity of communication information. Therefore, the authentication bits are embedded in the QR codes to verify the authenticity of the shadows in this scheme. In general, our algorithm is a general method that protects the security of the secret and can be applied in many areas of the industrial Internet. Fig. 4 shows an application diagram.

Medical field: with the medical industry can improve equipment security, save human resources, and expand the coverage of primary medical services to serve more patients. Doctors can send the patient's medical record information to each other in an QR code Secret Sharing scheme through the combination of the device and the Internet, thus preventing the leakage of the patient's privacy. Moreover, to match the

patient's information with the medical record image. Authentication information is embedded into the secret QR code to check the authenticity of the secret QR code. Finally, the recipient's doctor can recover the medical record image and the patient's information. This undoubtedly provides patients with safer and more efficient services.

Aviation industry: The Industrial Internet can obtain relevant information from various sensors on the aircraft in real time. The receiving data is then sent via the Industrial Internet in real time and the airline's diagnostic department. This is very helpful for the early warning and monitoring of the aircraft. It can also be remotely maintained via the Industrial Internet. If captains want to distribute confidential information to the tower, the confidential information can be replaced by a set of the QR codes that look normal and the receiver can recover the QR code containing confidential information and check the authenticity of the secret according to the authentication information. This can effectively protect the security of the data and prevent the attacker from tampering with the data to affect the correctness of the operation.



Fig. 4. Application diagram of the proposed scheme in 6G-Enabled Network in Box.

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed a high payload QR code Secret Sharing scheme with Authentication for Industrial Internet of Things. In contrast with other schemes, the proposed scheme not only guarantees high embedding capacity, but also embeds more authentication bits to improve the authentication capability. Since stego-QR codes are public, the input of the polynomial is regarded as the key. The proposed scheme uses the participant's key as the polynomial's key and the index of the embedded position of shadows, which reduces the cost of the key transmission. In addition, the authentication bits are embedded into the padding region in the proposed scheme. In this way, the proposed scheme can be applied to different security scenarios. For example, in the high security scenario,

the public information in the cover QR Codes can be appropriately reduced to improve the security of the scheme. The secret information is embedded into the error correction redundancy of the QR Code, which can ensure the high embedding capacity of the scheme. As demonstrated in the experiments, the proposed scheme has a better performance, and is both robust and secure.

In the future work, we will plan to improve the proposed method on the following aspects. Firstly, we will study new sharing methods with a lower computational complexity by replacing the traditional sharing method of the polynomial so as to improve the communication speed in the 6G networks, such as Chinese Remainder Theorem-based method. Secondly, new embedding methods based on the characteristics of QR code and the efficiency of the cheater prevention mechanism are to be further studied. Thirdly, due to the development of 6G Networks, traditional binary QR Codes may no longer meet people's needs. New QR Codes are also considered as a sharing cover in different scenario, such as artistic QR Code, which will be also a future work.

REFERENCES

- [1] K.-K. R. Choo, S. Gritzalis, and J. H. Park, "Cryptographic solutions for industrial Internet-of-Things: Research challenges and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3567-3569, 2018.
- [2] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679-3689, 2018.
- [3] M. Naor and A. Shamir, "Visual cryptography," *Lecture Notes in Computer Science*, vol. 950, no. 9, pp. 1-12, 1994.
- [4] Cox R, Qart codes. <http://research.swtch.com/qart>. Accessed 2012.
- [5] P. Tuyls, H. D. Hollmann, J. H. Van Lint, and L. Tolhuizen, "XOR-based visual cryptography schemes," *Designs, Codes and Cryptography*, vol. 37, no. 1, pp. 169-186, 2005.
- [6] C.-N. Yang and D.-S. Wang, "Property analysis of XOR-based visual cryptography," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 24, no. 2, pp. 189-197, 2014.
- [7] Y.-C. Chen, G. Horng, and D.-S. Tsai, "Comment on "cheating prevention in visual cryptography",*" IEEE Transactions on Image Processing*, vol. 21, no. 7, pp. 3319-3323, 2012.
- [8] *Information technology — Automatic identification and data capture techniques — QR code*, I. I. 18004, 2005.
- [9] 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.
- [10] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.
- [11] 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*, 2016: Springer, pp. 409-425.
- [12] 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.
- [13] 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.
- [14] Y.-J. Chiang, P.-Y. Lin, R.-Z. Wang, and Y.-H. Chen, "Blind QR code steganographic approach based upon error correction capability," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 7, no. 10, pp. 2527-2543, 2013.
- [15] 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*, pp. 1-20, 2018.
- [16] D. Munoz-Mejias, I. Gonzalez-Diaz, and F. Diaz-de-Maria, "A low-

complexity pre-processing system for restoring low-quality QR code images," *IEEE Transactions on Consumer Electronics*, vol. 57, no. 3, pp. 1320-1328, 2011.

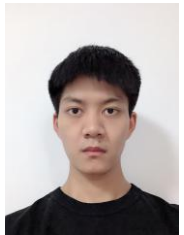
- [17] C.-N. Yang, T.-S. Chen, K. H. Yu, and C.-C. Wang, "Improvements of image sharing with steganography and authentication," *Journal of Systems and Software*, vol. 80, no. 7, pp. 1070-1076, 2007.
- [18] P. Huang, Y. Li, C. Chang, and Y. Liu, "Efficient QR code authentication mechanism based on Sudoku," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26023-26045, 2019.
- [19] 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, pp. 5719-5741, 2020.



Ryan Wen Liu received the BSc degree from the Department of Mathematics, Wuhan University of Technology, Wuhan, China, in 2009 and the PhD degree from The Chinese University of Hong Kong, Hong Kong, in 2015, respectively. He is currently an Associate Professor at the School of Navigation, Wuhan University of Technology. His research interests mainly include computational transportation science, image processing, computer vision, and machine learning.



Lizhi Xiong received Ph. D. degree in Communication and Information System from Wuhan University, China in 2016. From 2014 to 2015, he was a Joint-Ph.D. student with Electrical and Computer Engineering, New Jersey University of Technology, New Jersey, USA. He is currently an Associate Professor with School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China. His main research interests include privacy-preserving computation, information hiding, and multimedia security.



Xinwei Zhong received the B.S. degree in computer science and technology from the College of Binjiang, Nanjing University of Information Science and Technology, China, in 2018. He is currently pursuing the M.S. degree in computer science and technology from the School of Computer and Software, Nanjing University of Information Science and Technology. His research interests include visual cryptography and information security.



Neal N. Xiong (S'05–M'08–SM'12) is current an Associate Professor (6rd year) at Department of Mathematics and Computer Science, Northeastern State University, OK, USA. He received his both PhD degrees in Wuhan University (2007, about sensor system engineering), and Japan Advanced Institute of Science and Technology (2008, about dependable communication networks), respectively. Before he attended Northeastern State University, he worked in Georgia State University, Wentworth Technology

Institution, and Colorado Technical University (full professor about 5 years) about 10 years. His research interests include Cloud Computing, Security and Dependability, Parallel and Distributed Computing, Networks, and Optimization Theory.

Dr. Xiong published over 200 international journal papers and over 100 international conference papers. Some of his works were published in IEEE JSAC, IEEE or ACM transactions, ACM Sigcomm workshop, IEEE INFOCOM, ICDCS, and IPDPS. He has been a General Chair, Program Chair, Publicity Chair, Program Committee member and Organizing Committee member of over 100 international conferences, and as a reviewer of about 100 international journals, including IEEE JSAC, IEEE SMC (Park: A/B/C), IEEE Transactions on Communications, IEEE Transactions on Mobile Computing, IEEE Trans. on Parallel and Distributed Systems. He is serving as an Editor-in-Chief, Associate editor or Editor member for over 10 international journals (including Associate Editor for IEEE Tran. on Systems, Man & Cybernetics: Systems, Associate Editor for IEEE Tran. on Network Science and Engineering, Associate Editor for Information Science, Editor-in-Chief for Journal of Internet Technology (JIT), and Editor-in-Chief for Journal of Parallel & Cloud Computing (PCC)), and a guest editor for over 10 international journals, including Sensor Journal, WINET and MONET. He has received the Best Paper Award in the 10th IEEE International Conference on High Performance Computing and Communications (HPCC-08) and the Best student Paper Award in the 28th North American Fuzzy Information Processing Society Annual Conference (NAFIPS2009).