2017

Covert QR codes: How to hide in the crowd

Yang-Wai Chow
University of Wollongong, caseyc@uow.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Joon Sang Baek
University of Wollongong, baek@uow.edu.au

Recommended Citation
Chow, Yang-Wai; Susilo, Willy; and Baek, Joon Sang, "Covert QR codes: How to hide in the crowd" (2017). *Faculty of Engineering and Information Sciences - Papers: Part B*. 968.
https://ro.uow.edu.au/eispapers1/968

Covert QR codes: How to hide in the crowd

Abstract

This paper investigates a novel approach of distributing a hidden message via public channels. The proposed approach employs visual subterfuge to conceal secret information within a QR code. Using a QR code reader, any individual can decode the public information contained in the QR code. However, only authorized users who have the necessary credentials will be able to obtain the secret message, which is encoded in the form of a secret QR code. We call this a Covert QR (CQR) code scheme. To embed the secret information, this approach exploits the error correction mechanism inherent in the QR code structure. By using QR codes to conceal information, the proposed scheme has the advantage of reducing the likelihood of attracting the attention of potential adversaries. In addition, the information in QR codes can be scanned and decoded through the visual channel. As such, the secret information can be distributed on printed media and is not restricted to an electronic form.

Disciplines

Engineering | Science and Technology Studies

Publication Details

Chow, Y., Susilo, W. & Baek, J. (2017). Covert QR codes: How to hide in the crowd. Lecture Notes in Computer Science, 10701 678-693. Melbourne Lecture Notes in Computer Science

Covert QR Codes: How to Hide in the Crowd

Yang-Wai Chow, Willy Susilo and Joonsang Baek

Institute of Cybersecurity and Cryptology,
School of Computing and Information Technology,
University of Wollongong, Wollongong, Australia
{caseyc, wsusilo, baek}@uow.edu.au

Abstract. This paper investigates a novel approach of distributing a hidden message via public channels. The proposed approach employs visual subterfuge to conceal secret information within a QR code. Using a QR code reader, any individual can decode the public information contained in the QR code. However, only authorized users who have the necessary credentials will be able to obtain the secret message, which is encoded in the form of a secret QR code. We call this a Covert QR (CQR) code scheme. To embed the secret information, this approach exploits the error correction mechanism inherent in the QR code structure. By using QR codes to conceal information, the proposed scheme has the advantage of reducing the likelihood of attracting the attention of potential adversaries. In addition, the information in QR codes can be scanned and decoded through the visual channel. As such, the secret information can be distributed on printed media and is not restricted to an electronic form.

Keywords: Covert message, data hiding, error correction, QR code, secret sharing

1 Introduction

Consider the scenario where the Central Intelligence Agency (CIA) needs to communicate with their agents via public channels. The agency decides to put up a poster in a public place, like a train station, where everybody can see the poster. The poster has a Quick Response (QR) code, which contains innocent-looking public information along with concealed information. To a casual observer, the QR code will not raise any suspicion. Any individual who uses a QR code reader, e.g., on a mobile phone, will only be able to obtain the public information. However, CIA agents who possess the appropriate credentials will be able to obtain the secret message by decoding the contents of a secret QR code.

This paper examines a novel approach to visual subterfuge by hiding secret information within a QR code. This provides a means for secret communication over public channels using QR codes. While any member of the public can use a standard QR code reader to decode the QR code and acquire the public information, only authorized users who have the necessary credentials will be able to recover the secret QR code and decode it to obtain the hidden message. In the proposed scheme, even if an adversary realizes that the QR code contains hidden information, the adversary will not be able to obtain the secret message without the correct key.

The motivation behind the proposed scheme is that in cryptography, if one were to encrypt a secret and distribute the ciphertext, the ciphertext can only be decrypted by receivers who know the encryption key. However, if the ciphertext itself were to be distributed using public channels, anybody who sees the ciphertext will immediately recognize that the text has been encrypted. The purpose of the proposed scheme is to adopt visual subterfuge to conceal this in the form of a QR code. Furthermore, in general, ciphertext is distributed via electronic means. The QR code approach presented in this paper allows for the secret information to be distributed in a visual form on printed media.

Our Contribution. This paper introduces a novel method of providing a means for secret communication via public channels, by employing visual subterfuge to conceal secret information in a QR code. We call this a Covert QR (CQR) code scheme. To embed secret information, the proposed scheme exploits an inherent feature of the QR code structure, which is its error correction mechanism. This feature allows correct decoding of a QR code even in the event that part of the QR code is damaged. In the proposed scheme, anybody can use a standard QR code reader to retrieve the public information contained in the QR code. Only authorized users who possess the necessary credentials will be able to recover a secret QR code, which is embedded within the CQR code, and decode it to obtain the secret message. The advantage of the proposed approach is that the QR code itself contains meaningful information, while at the same time it conceals secret information from casual observers.

2 Related Work

2.1 Visual Secret Sharing

Secret sharing is regarded as a mechanism that can be used to transfer secret information via public channels in cryptography [22]. A well known method of visual secret sharing is known as visual cryptography [15]. In visual cryptography, a secret in the form of an image is encoded into a number of shares and distributed to a group of participants. Only when a qualified number of shares are combined will the secret be revealed. Each share looks like a random pattern of pixels, and as such, a visual cryptography share is obvious even to a casual observer.

In a method known as extended visual cryptography, shares are created using meaningful cover images [2]. Therefore, each share looks like a meaningful, albeit noisy, image. The advantage of encoding the secret image into shares containing 'innocent-looking' meaningful cover images is that it reduces the likelihood of attracting the attention of attackers [19]. A QR code visual secret sharing scheme was introduced by Chow et al. [7], in which each share in the scheme is a valid cover QR code containing meaningful public information. As such, each share can be scanned using a standard QR code reader and decoded to obtain the meaningful information. When the secret sharing information in the cover QR code shares are combined, a secret QR code can be recovered and decoded to obtain the secret message. Wan et al. [18] also proposed a different visual secret sharing scheme using QR codes.

2.2 Data Hiding using QR codes

The QR code is a two-dimensional code that was invented by the company Denso Wave [9]. The use of QR codes has become ubiquitous in our everyday life. This proliferation is in part due to the QR code's convenience and ease of use. Anybody with a smartphone can obtain the information contained within a QR code. The use of QR codes has also been embraced by the information security research community. This has resulted in a variety of practical applications ranging from authenticating visual cryptography shares [20] and e-voting authentication [10], to digital watermarking [6, 13] and secret sharing [7].

There are also a number of proposed schemes that employ QR codes for data hiding and steganography. For example, Wu et al. [21] proposed a data embedding approach for hiding a QR code in a digital image. Their purpose was to camouflage the appearance of a QR code in an image so as not to degrade the visual quality of the picture.

In a different approach, Huang et al. [11] developed a reversible data hiding method for images using QR codes. The problem that they were examining was that if an image contained a QR code, the QR code would obscure a portion of the image, thus degrading its quality. The aim of their proposed scheme was to avoid the QR code from degrading the quality of an image. Their approach involved the use of reversible data hiding to replace a portion of the image with a QR code and to hide the information of this portion in the rest of the image. After the QR code has been scanned, it will be removed from the image and the original image will be restored using the data that was previously hidden in the rest of the image.

Chen and Wang [5] devised a a nested image steganography scheme using QR codes. In their approach, two types of secret data, in the form of text (lossless) and image (lossy), were embedded in a cover image. The text portion of the secret data is embedded using a QR code. A similar approach was also reported in Chung et al. [8]. Instead of first converting a secret into a QR code before embedding it in a cover image, Lin et al. [14] proposed a scheme for concealing secret data in a cover QR code. To conceal secret data, their approach capitalized on the QR code error correction redundancy property. The size of concealed secret data depends on the QR code version and its error correction level.

Bui et al. [4] also investigated the problem of hiding secret information in a QR code. In their work, they state that previous approaches of embedding secret messages in QR codes use bit embedding. They argue that this is vulnerable to modification attacks. As such, they proposed a method of using Reed-Solomon code and list decoding to hide a secret message in a QR code.

2.3 Others

This research is related to secret handshakes. The purpose of a secret handshake is to allow members from a group to identify each other [3]. Non-members of the group are not able to recognize group members and cannot perform the secret handshake. As such, secret handshakes can be used to perform mutual authentication between authorized parties [17]. In traditional secret handshake schemes, even if a casual observer does not have the appropriate credentials, the distributed ciphertext is easily recognizable. Examples of other related work include encryption on portable devices [1, 16].

3 Background

The International Organization for Standardization (ISO) has established a standard for the QR code (ISO/IEC18004) [12]. This section outlines the basic QR code structure and error correction feature as defined by the ISO standard.[1]

3.1 The QR Code Structure

A QR code symbol consists of a two-dimensional array of light and dark squares, which are referred to as modules. There are forty sizes of QR code symbol versions (i.e. version 1 to version 40). Each version comprises of a different number of modules, and as such different QR code versions have different data capacities. The appropriate version to use depends on the amount and the type of data (i.e. alphanumeric, binary, Kanji or a combination of these) to be encoded as well as the error correction level. The error correction level will be described in Section 3.2 to follow.

The QR code structure is made of up of encoding regions and function patterns [12]. An example of this depicted in Fig. 1, which shows the encoding regions and function patterns of a QR code version 7 symbol. The function patterns do not encode data, but are mainly used for obtaining information from the QR code. For example, there are three identical finder patterns located at each corner of the symbol, except for the bottom right corner. These are used by a QR code reader to recognize the QR code and to determine the rotational orientation of the symbol.

3.2 Encoding and Error Correction

The encoding region contains data codewords and error correction codewords. Message data is encoded as a bit stream that is divided into a sequence of

[1] For a comprehensive description of the QR code structure and error correction mechanism, please refer to the ISO standard (ISO/IEC18004) [12].

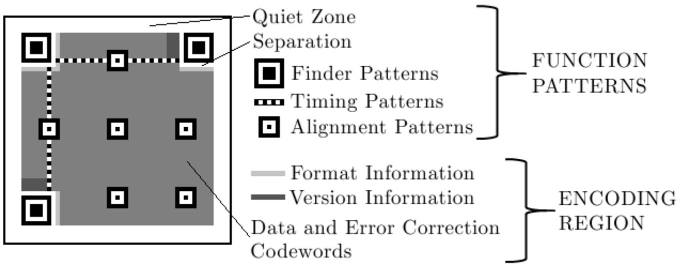


Fig. 1. QR code version 7 structure.

codewords. Codewords are 8-bits in length. The codewords are divided into a number of error correction blocks, based on the QR code version and error correction level, and an appropriate number of error correction codewords are generated for each block. Error correction allows correct decoding of the message in the event that part of the symbol is dirty or damaged. This error correction feature has also been exploited to embed art or other information in QR code symbols. For example, the QR code symbols in Fig. 2(a) and Fig. 2(b)[2] can still be decoded correctly despite the embedded text and image. It can also be seen from Fig. 2(b) that modules do not have to be black and white squares.

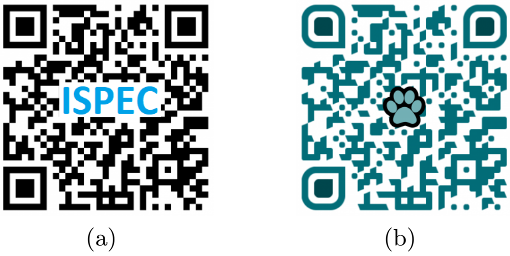


Fig. 2. (a) QR code where part of it is obscured. (b) Artistic QR code.

The QR code employs Reed-Solomon error control coding for error detection and correction [12]. There are four error correction levels (i.e. L $\sim$ 7%, M $\sim$ 15%, Q $\sim$ 25% and H $\sim$ 30%). Each level provides a different error correction capacity. Higher error correction levels improve the recovery capacity, but also increases the amount of data to be encoded. The number of data codewords, error correction blocks and error correction codewords depend on the QR code version and error correction level.

Table 1 shows these characteristics for QR code versions 4 and 5. In the table, the error correction codewords for each block is given as (c, d, e), where c is the

[2] This QR code was generated from http://www.free-qr-code.net/

total number of codewords, d is the number of data codewords and e is the error correction capacity. Note that some QR code versions have blocks with different (c, d, e) values for certain error correction levels. For example, it can be seen in Table 1 that QR code version 5 with an error correction level of Q has a total of 4 error correction blocks. The (c, d, e) values for the first 2 blocks are (33, 15, 9) while the values for the next 2 blocks are (34, 16, 9).

The codewords from the blocks are encoded in an interleaved manner, with the error correction codewords appended to the end of the data codeword sequence. This is done to minimize the possibility that localized damage will cause the QR code to become undecodable. Fig. 3 shows the data codeword and error correction codeword arrangement for QR code version 4, with an error correction level of H.

Table 1. Error correction characteristics for QR code versions 4 and 5 [12].

Version	**Total codewords**	**Error correction level**	**Number of blocks**	**Error correction codewords per block (c, d, e)**
4	100	L	1	(100, 80, 10)
		M	2	(50, 32, 9)
		Q	2	(50, 24, 13)
		H	4	(25, 9, 8)
5	134	L	1	(134, 108, 13)
		M	2	(67, 43, 12)
		Q	2	(33, 15, 9)
			2	(34, 16, 9)
		H	2	(33, 11, 11)
			2	(34, 12, 11)

4 Security Model

In this section, we define the security model of the proposed scheme. We denote assigning the output of an algorithm A, which takes $x, y, \ldots$ as input to z by $z \leftarrow \mathsf{A}(x, y, ...)$. If A is particularly randomized, we write $z \leftarrow_{\$} \mathsf{A}(x, y, ...)$. $|Q|$ indicates the cardinality of a set Q. For the sake of clarity, we use the following notations to indicate possible inputs and outputs of various algorithms we will describe shortly:

- $\mathcal{P}$: Public message
- $\mathcal{C}$: Original public QR code
- $\mathcal{C}^*$: Covert QR code
- $\mathcal{M}$: Secret message
- $\mathcal{S}$: Original secret QR code
- $\mathcal{S}^*$: Recovered secret QR code

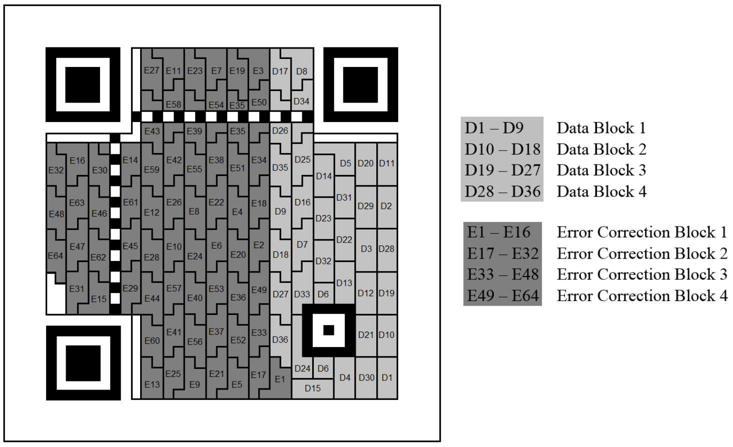

D1 – D9 Data Block 1
D10 – D18 Data Block 2
D19 – D27 Data Block 3
D28 – D36 Data Block 4
E1 – E16 Error Correction Block 1
E17 – E32 Error Correction Block 2
E33 – E48 Error Correction Block 3
E49 – E64 Error Correction Block 4

Fig. 3. Data and error correction codeword arrangement for QR code version 4 with error correction level H.

We now formally describe a covert QR (CQR) code scheme and present its security requirements.

Definition 1 (CQR). *A covert QR scheme* CQR *consists of a key generation algorithm* KeyGen*, a pseudorandom bit generator* RandGen*, a QR code encoder* QR *and decoder* InvQR*, an embedding algorithm* Emb*, an extraction algorithm* Ext *and a QR verification algorithm* QRVrfy*. The specifications of the algorithms are given as follows:*

- $k \leftarrow_{\$} \mathsf{KeyGen}(\ell)$: Taking a security parameter ℓ as input, this algorithm generates a key k.
- $\hat{k} \leftarrow_{\$} \mathsf{RandGen}(k, n)$: This algorithm takes a key k as input, and generates an array of pseudorandom bits $\hat{k} \in \{0,1\}^n$, where n is the length of the array.
- $\mathcal{R} \leftarrow \mathsf{QR}(\mathcal{T})$: Taking a message $\mathcal{T}$ as input, this algorithm generates a QR code $\mathcal{R}$ for $\mathcal{T}$. Hence, $\mathcal{C} \leftarrow \mathsf{QR}(\mathcal{P})$ and $\mathcal{S} \leftarrow \mathsf{QR}(\mathcal{M})$.
- $\mathcal{T} \leftarrow \mathsf{InvQR}(\mathcal{R})$: Taking a QR code $\mathcal{R}$ as input, this algorithm converts $\mathcal{R}$ into the message $\mathcal{T}$. Hence, $\mathcal{P} \leftarrow \mathsf{QR}(\mathcal{C})$ and $\mathcal{M} \leftarrow \mathsf{QR}(\mathcal{S})$.
- $\mathcal{C}^* \leftarrow \mathsf{Emb}(k, \mathcal{S}, \mathcal{C})$: Takes a secret key k, a secret QR code $\mathcal{S}$ and a public QR code $\mathcal{C}$ as input, and generates a covert QR code $\mathcal{C}^*$.
- $\mathcal{S}^* \leftarrow \mathsf{Ext}(k, \mathcal{C}^*)$: This algorithm takes a secret key k and a covert QR code $\mathcal{C}^*$ as input, and outputs a recovered secret QR code $\mathcal{S}^*$.
- $0/1 \leftarrow \mathsf{QRVrfy}(\mathcal{R})$: Given any QR code $\mathcal{R} \in \{\mathcal{C}, \mathcal{C}^*, \mathcal{S}, \mathcal{S}^*\}$, this algorithm outputs 1 if $\mathcal{R}$ is a valid QR code, and 0 otherwise.

Definition 2 (Correctness). *For a public QR code* $\mathcal{C} \leftarrow \mathsf{QR}(\mathcal{P})$ *where* $\mathcal{P}$ *is a public message and a covert QR code* $\mathcal{C}^* \leftarrow \mathsf{Emb}(k, \mathcal{S}, \mathcal{C})$*, the following conditions should hold:*

- $\mathsf{InvQR}(\mathcal{C}) = \mathsf{InvQR}(\mathcal{C}^*) = \mathcal{P}$

- $\mathsf{QRVrfy}(\mathcal{C}) = \mathsf{QRVrfy}(\mathcal{C}^*) = 1$

Similarly, for a secret QR code $\mathcal{S} \leftarrow \mathsf{QR}(\mathcal{M})$ *where* $\mathcal{M}$ *is a private message, and a recovered secret QR code* $\mathcal{S}^* \leftarrow \mathsf{Ext}(k, \mathcal{C}^*)$*, the following conditions should hold:*

- $\mathsf{InvQR}(\mathcal{S}) = \mathsf{InvQR}(\mathcal{S}^*) = \mathcal{M}$
- $\mathsf{QRVrfy}(\mathcal{S}) = \mathsf{QRVrfy}(\mathcal{S}^*) = 1$

Definition 3 (Security). *Let* A *be an adversary whose running time is polynomial. We say that* CQR *scheme is secure if there exists a negligible function* ϵ *such that*

$$\Pr[\mathcal{M} \leftarrow A(\mathcal{C}^*)] \leq \epsilon(\ell),$$

where $\mathcal{C}^* \leftarrow \mathsf{Emb}(k, \mathcal{S}, \mathcal{C})$*,* $k \leftarrow \mathsf{GenKey}(\ell)$*,* $\mathcal{S} \leftarrow \mathsf{QR}(\mathcal{M})$*,* $\mathcal{C} \leftarrow \mathsf{QR}(\mathcal{P})$ *and* ℓ *is the security parameter. Note that the probability is taken over the randomness used by* A*, the key generation algorithm and the pseudorandom bit generator.*

5 Proposed Covert QR Code Scheme

In this section, we describe the proposed method of implementing a Covert QR (CQR) code scheme. Fig. 4 illustrates a conceptual overview of the proposed scheme. From Fig. 4 it can be seen that first, the secret message $\mathcal{M}$ and the public message $\mathcal{P}$ are encoded in the form of QR codes, using a QR code generator, to produce $\mathcal{S}$ and $\mathcal{C}$, respectively. These QR codes along with the secret key k, will be the input of the embedding algorithm. The pseudocode for the embedding algorithm is provided in Algorithm 1, which will be described in Sec. 5.1. The output of the embedding algorithm will be the covert QR code $\mathcal{C}^*$. This CQR code contains both public and hidden information, and can be distributed via public channels.

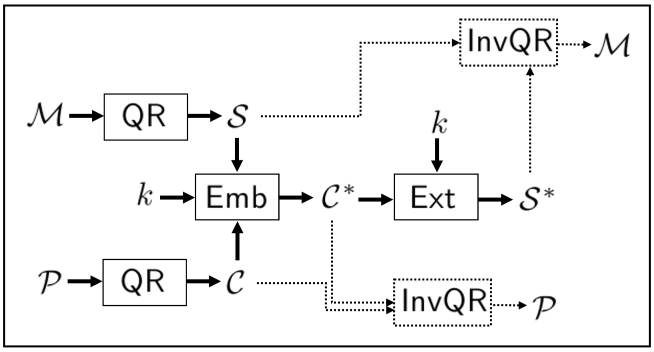


Fig. 4. Overview of the proposed CQR scheme.

Note that both $\mathcal{C}$ and $\mathcal{C}^*$ are valid QR codes. When scanned and decoded with a standard QR code reader, both QR codes will produce the public message $\mathcal{P}$. The error correction mechanism in the QR code structure makes it possible to manipulate some of the codewords in $\mathcal{C}$ to produce $\mathcal{C}^*$, while still maintaining a QR code symbol that can be decoded correctly.

For individuals who know the secret key k, the CQR code and the secret key can be provided as input to the extraction algorithm, which will be able to reconstruct a recovered secret QR code $\mathcal{S}^*$. The pseudocode for the extraction algorithm is provided in Algorithm 2, which will be discussed later. Both $\mathcal{S}$ and $\mathcal{S}^*$ are valid QR codes, that when scanned and decoded will result in the secret message $\mathcal{M}$. Note that even if the recovered secret QR code contains some errors, due to scanning errors or if $\mathcal{C}^*$ is slightly damage or obscured, the error correction mechanism inherent in the QR code symbol means that $\mathcal{S}^*$ can be still be decoded correctly as long as the error correction capacity has not be overwhelmed.

5.1 Algorithms

The embedding and extraction algorithms are described here. Pseudocode for the embedding algorithm is provided in Algorithm 1. The purpose of the embedding algorithm is to embed encrypted codewords from the secret QR code $\mathcal{S}$ into the public QR code $\mathcal{C}$, using the secret key k.

The reason why only the codewords are embedded is because the function patterns, which are fixed patterns in QR codes, will leak information about the pseudorandom bits $\hat{k}$ and consequently the secret key k. As such, the codewords in $\mathcal{S}$ must first be extracted. Then based on the number of codewords and codeword modules (each codeword is made up of 8 modules), an array of random bits can be generated using a pseudorandom bit generator by using k as the seed value. Each codeword module is encrypted by performing an XOR operation with a corresponding random bit, before embedding it in $\mathcal{C}^*$. The output of the embedding algorithm is the covert QR code $\mathcal{C}^*$, which contains both the public and private information.

For the extraction algorithm, provided in Algorithm 2, the input is the secret key k and the covert QR code $\mathcal{C}^*$. To extract the embedded information, the algorithm first decodes the CQR $\mathcal{C}^*$ to obtain the public message $\mathcal{P}$. With the public message, the algorithm generates the public QR code $\mathcal{C}$. The embedded information is obtained based on the differences between $\mathcal{C}^*$ and $\mathcal{C}$. Once the embedded codewords are extracted, the array of random bits can be generated using k and the pseudorandom bit generator. Each module is the decrypted using an XOR operation with the corresponding random bit. Thus, the secret QR code can be reconstructed and the output of the algorithm is the recovered secret QR code $\mathcal{S}^*$.

Algorithm 1 Pseudocode for the embedding algorithm (i.e. $\mathcal{C}^* \leftarrow \mathsf{Emb}(k, \mathcal{S}, \mathcal{C})$)

```
function EmbedCQR($k$, $S$, $C$)
    /* Extract the codewords from $S$ */
    $num \leftarrow$ numberOfCodewords($S$)
    $codewords[num][8] \leftarrow$ extractCodewords($S$)

    /* Generate pseudorandom bits using $k$ as the seed */
    $rbits[num \times 8] \leftarrow$ randomBitGenerator($k$, $num \times 8$)

    /* Encrypt each codeword module */
    $b = 1$
    $\mathcal{C}^* = \mathcal{C}$
    for $i = 1$ to $num$ do
        for $j = 1$ to 8 do
            /* Each codeword consists of 8 modules, $\oplus$ is an XOR operation */
            $encyptedModules[i][j] \leftarrow codewords[i][j] \oplus rbits[b]$
            $b = b + 1$

            /* Embed each encrypted module into $\mathcal{C}$ to produce $\mathcal{C}^*$ */
            $\mathcal{C}^* \leftarrow encryptedModules[i][j]$
        end for
    end for

    /* Output $\mathcal{C}^*$ */
     return $\mathcal{C}^*$
end function
```

Algorithm 2 Pseudocode for the extraction algorithm (i.e. $\mathcal{S}^* \leftarrow \mathsf{Ext}(k, \mathcal{C}^*)$)

```
function ExtractCQR($k$, $C^*$)
    /* Decode $C^*$ to obtain the public message $\mathcal{P}$, and generate $C$ */
    $\mathcal{C} \leftarrow (\mathcal{P} \leftarrow \mathsf{QR}(\mathcal{C}))$

    /* Get the difference between $C^*$ and $C$ */
    $extracted[n][8] \leftarrow$ diff($C^*$, $C$)
    $num \leftarrow$ computeSize($extracted$)

    /* Generate pseudorandom bits using $k$ as the seed */
    $rbits[num \times 8] \leftarrow$ randomBitGenerator($k$, $num \times 8$)

    /* Construct $S^*$ */
    $b = 1$
    for $i = 1$ to $num$ do
        /* Each codeword consists of 8 modules, $\oplus$ is an XOR operation */
        for $j = 1$ to 8 do
            $S^* \leftarrow extracted[i][j] \oplus rbits[b]$
            $b = b + 1$
        end for
    end for

    /* Output $\mathcal{S}^*$ */
     return $\mathcal{S}^*$
end function
```

5.2 Practical Considerations

The proposed CQR code scheme exploits the error correction mechanism in the QR code structure, by manipulating some of the codewords in $\mathcal{C}$ to produce $\mathcal{C}^*$. This will still allow the CQR code to be decoded correctly as long as the manipulated codewords does not exceed the error correction capacity. Therefore, this necessitates that the public QR code $\mathcal{C}$'s size must be large enough to accommodate the number of codewords in the secret QR code $\mathcal{S}$. In addition, based on the security discussed in Sec. 6.2 the larger the size of $\mathcal{S}$, the more difficult for an adversary to attack the CQR code. The size of a secret message that is governed by the data capacity of the secret QR code.

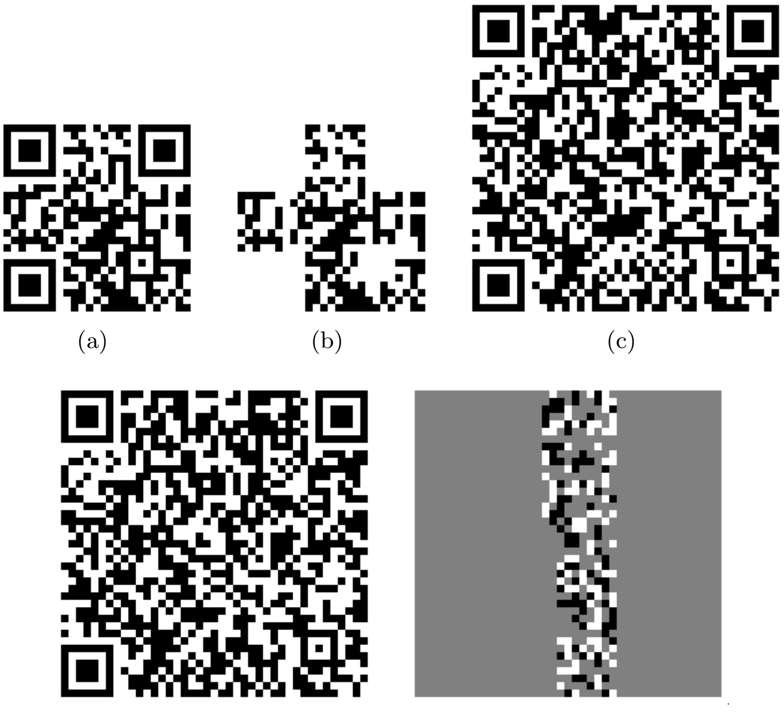
As described in Sec. 3.2, QR code symbols have different error correction levels. Furthermore, the different QR code versions determine the size of the QR code symbol and its data capacity. Each QR code version has different error correction characteristics. The appropriate size of $\mathcal{C}$, based on the size of $\mathcal{S}$, can be determined by referring to the QR code error correction characteristics. Refer to Table 1 for an example of this. A suitable QR code version for $\mathcal{C}$ requires that the error correction capacity per block, e, multiplied by the number of blocks for the specific error correction level, must be greater than the total number of codewords in $\mathcal{S}$. In practice, the chosen size should have an error correction capacity which is appropriately large to accommodate the modifications. This is so that the resulting CQR code can still be decoded in the even that it is slightly damaged or obscured.

6 Analysis and Discussion

6.1 Experiment Results

An experiment to test the scheme was performed by implementing the proposed CQR code scheme. Fig. 5 shows example results of the implementation. The secret QR code that contains a secret message is shown in Fig. 5(a). It is a QR code of version 2 and error correction level H. Fig. 5(b) depicts the codewords that are extracted from the QR code in Fig. 5(a). The total number of codewords for a QR code version 2 is 44.

Fig. 5(c) in turn shows the original public QR code, which contains the public message. It is a QR code of version 6 with error correction level H. For this version and error correction level, there are 4 encoding blocks with error correction capacity of 14. Therefore, this QR code size is suitable for the proposed scheme because $14 \times 4 > 44$. The CQR code resulting from the proposed scheme is given in Fig. 5(d). Note that the CQR shown in Fig. 5(d) is a valid QR code that can be scanned by a standard QR code reader, and will decode to the same public message as the original public QR code shown in Fig. 5(c). Finally, Fig. 5(e) shows the difference between the QR codes depicted in Fig. 5(c) and Fig. 5(d). Gray color indicates no difference, whereas the white and black modules are the original colors in Fig. 5(c) that differ from those in Fig. 5(d).



(a) (b) (c)

(d) (e)

Fig. 5. Example results; (a) QR code containing a secret message[3]; (b) Codewords of the QR code shown in (a); (c) Original public QR code that contains a public message[4]; (d) Covert QR code resulting from the proposed scheme[5]; (e) Difference image between (c) and (d).

6.2 Security Analysis

Correctness We first show that the proposed CQR scheme is correct in the sense of Definition 2.

Theorem 1. *The proposed covert QR code (CQR) scheme described in Sec. 5 satisfies the correctness requirement specified in Definition 2.*

Proof. By the construction of the proposed covert QR scheme CQR, $\mathcal{C}$ and $\mathcal{C}^*$ are valid QR codes. Hence, we have $\mathsf{QRVrfy}(\mathcal{C}^*) = \mathsf{QRVrfy}(\mathcal{C}) = 1$. Also, the

[3] Contains the secret message: "Secret Message"

[4] Contains the public message: "http://www.springer.com/gp/computer-science/lncs"

[5] Also decodes to the public message: "http://www.springer.com/gp/computer-science/lncs"

inverses of the QR codes $\mathcal{C}$ and $\mathcal{C}^*$ point to the same public message $\mathcal{P}$. As a result, we have $\mathsf{InvQR}(\mathcal{C}^*) = \mathsf{InvQR}(\mathcal{C}) = \mathcal{P}$.

In addition, $\mathcal{S}$ and $\mathcal{S}^*$ are valid QR codes. Therefore, $\mathsf{QRVrfy}(\mathcal{S}^*) = \mathsf{QRVrfy}(\mathcal{S}) = 1$, and the inverses of the QR codes $\mathcal{S}$ and $\mathcal{S}^*$ point to the same secret message $\mathcal{M}$, i.e. $\mathsf{InvQR}(\mathcal{S}^*) = \mathsf{InvQR}(\mathcal{S}) = \mathcal{M}$.

Thus, the proposed covert QR scheme satisfies the correctness requirement.

Security against Brute Force Attack The security of the proposed scheme is information theoretic: If an adversary suspects that a CQR code contains secret information, the adversary can easily obtain the embedded encrypted codewords. From this, the adversary can obtain information about the size of the secret QR code based on the number of embedded codewords. However, without the secret key k, the adversary cannot decrypt the encrypted codewords.

Nevertheless, since the secret QR code $\mathcal{S}$ must be a valid QR code, an adversary can attempt to adopt a brute force strategy to infer information about $\mathcal{M}$ or $\hat{k}$. Let S' denote a valid, or in other words 'meaningful', QR code and $\mid S' \mid$ be the cardinality of all the valid QR codes of that size. The probability of success for this attack will be bounded by $\frac{1}{\mid S' \mid}$. The space of $\mid S' \mid$ is governed by the size of data that a QR code can contain, which is determined by the specific QR code version used to encode the message. Hence, the larger the secret QR code, the larger $\mid S' \mid$ will be, which in turn lowers the success of an attack. Let d be the number of data codewords for a QR code. Since each codeword contains 8 modules, $\mid S' \mid = 2^{8d}$.

We prove this formally in the following theorem.

Theorem 2. *The proposed covert QR code scheme described in Sec. 5 satisfies the security requirement specified in Definition 3 assuming that the ℓ-bit (seed) secret key k is used to generate an array of pseudorandom bits $\hat{k} \in \{0,1\}^n$, where n is the length of the array.*

Proof. Note that by the construction of the embedding algorithm of the proposed scheme, each bit in $\hat{k}$ is XOR-ed with each codeword module in S, then embedded in C^*. This means that $\mid SP_{\mathcal{C}^*} \mid = \mid SP_{\hat{k}} \mid$, where $SP_{\mathcal{C}^*}$ and $SP_{\hat{k}}$ denote the space of the (possible) modified QR codes based on $\mathcal{C}^*$ and the random bit array space, respectively. Note that in the proposed scheme, $\mid SP_{\hat{k}} \mid = 2^n$. Hence,

$$\Pr[A \text{ outputs } \mathcal{M}] = \Pr[A \text{ finds correct } \hat{k}] \leq \frac{1}{2^n},$$

Thus, the probability that the adversary A will obtain a right message $\mathcal{M}$ is negligible for large n. This also implies that the larger the secret QR code, the larger n will be.

Visual Subterfuge One of the primary advantages of the proposed scheme stems from the fact that CQR codes are meaningful innocent-looking QR codes. This will reduce the likelihood of attracting the attention of potential adversaries.

In addition, since modules in QR codes do not have to be black and white squares, it would be aid in the visual subterfuge if the CQR code were to be constructed using an artistic QR code scheme, like the example shown in Fig. 2(b). The proposed CQR scheme will work as long as the contrast between light and dark modules can adequately be scanned by a QR code reader.

7 Conclusion

This paper presents a novel approach for distributing a hidden message via public channels using the proposed Covert QR (CQR) code scheme. By exploiting the error correction mechanism inherent in the QR code structure, the proposed scheme can embed encrypted codewords from a secret QR code into a covert QR code. The resulting CQR code can be scanned by a standard QR code reader to obtain the public information. However, authorized users who have the necessary credentials will be able to use the information embedded within a CQR code to reconstruct a secret QR code, which contains the secret message. The purpose of the proposed scheme is to employs visual subterfuge to conceal secret information within a QR code. In view of the fact that a CQR code contains meaningful innocent-looking information, the aim of this is to reduce the likelihood of attracting the attention of potential adversaries. This is unlike traditional ciphertext that can easily be recognized even by a casual observer. In addition, since the information in QR codes can be scanned and decoded through the visual channel, CQR codes are not restricted to an electronic form and can be distributed via printed media.

References

1. P. Albano, A. Bruno, B. Carpentieri, A. Castiglione, A. Castiglione, F. Palmieri, R. Pizzolante, K. Yim, and I. You. Secure and distributed video surveillance via portable devices. *J. Ambient Intelligence and Humanized Computing*, 5(2):205–213, 2014.
2. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson. Extended capabilities for visual cryptography. *Theor. Comput. Sci.*, 250(1-2):143–161, Jan. 2001.
3. D. Balfanz, G. Durfee, N. Shankar, D. K. Smetters, J. Staddon, and H. Wong. Secret handshakes from pairing-based key agreements. In *2003 IEEE Symposium on Security and Privacy (S&P 2003), 11-14 May 2003, Berkeley, CA, USA*, pages 180–196. IEEE Computer Society, 2003.
4. T. V. Bui, N. K. Vu, T. T. Nguyen, I. Echizen, and T. D. Nguyen. Robust message hiding for qr code. In *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014 Tenth International Conference on*, pages 520–523. IEEE, 2014.
5. W.-Y. Chen and J.-W. Wang. Nested image steganography scheme using qr-barcode technique. *Optical Engineering*, 48(5):057004–057004, 2009.
6. Y. Chow, W. Susilo, J. Tonien, and W. Zong. A QR code watermarking approach based on the DWT-DCT technique. In J. Pieprzyk and S. Suriadi, editors, *Information Security and Privacy - 22nd Australasian Conference, ACISP 2017, Auckland,*

New Zealand, July 3-5, 2017, Proceedings, Part II, volume 10343 of *Lecture Notes in Computer Science*, pages 314–331. Springer, 2017.

7. Y. 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 J. K. Liu and R. Steinfeld, editors, *Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Melbourne, VIC, Australia, July 4-6, 2016, Proceedings, Part I*, volume 9722 of *Lecture Notes in Computer Science*, pages 409–425. Springer, 2016.
8. C.-H. Chung, W.-Y. Chen, and C.-M. Tu. Image hidden technique using qr-barcode. In *Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on*, pages 522–525. IEEE, 2009.
9. Denso Wave Incorporated. QRcode.com, http://www.qrcode.com/en/.
10. S. Falkner, P. Kieseberg, D. Simos, C. Traxler, and E. Weippl. E-voting authentication with qr-codes. In *Human Aspects of Information Security, Privacy, and Trust*, volume 8533 of *Lecture Notes in Computer Science*, pages 149–159. Springer, 2014.
11. H.-C. Huang, F.-C. Chang, and W.-C. Fang. Reversible data hiding with histogram-based difference expansion for qr code applications. *Consumer Electronics, IEEE Transactions on*, 57(2):779–787, 2011.
12. International Organization for Standardization. Information technology — automatic identification and data capture techniques — qr code 2005 bar code symbology specification. ISO/IEC 18004:2006, 2006.
13. H.-C. Lee, C.-R. Dong, and T.-M. Lin. Digital watermarking based on jnd model and qr code features. In *Advances in Intelligent Systems and Applications-Volume 2*, pages 141–148. Springer, 2013.
14. P.-Y. Lin, Y.-H. Chen, E. J.-L. Lu, and P.-J. Chen. Secret hiding mechanism using qr barcode. In *Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on*, pages 22–25. IEEE, 2013.
15. M. Naor and A. Shamir. Visual cryptography. In A. D. Santis, editor, *EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 1994.
16. R. Pizzolante, B. Carpentieri, A. Castiglione, A. Castiglione, and F. Palmieri. Text compression and encryption through smart devices for mobile communication. In *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pages 672–677, July 2013.
17. A. Sorniotti and R. Molva. A provably secure secret handshake with dynamic controlled matching. *Computers & Security*, 29(5):619 – 627, 2010. Challenges for Security, Privacy and Trust.
18. 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*, pages 1–16.
19. D. Wang, F. Yi, and X. Li. On general construction for extended visual cryptography schemes. *Pattern Recognition*, 42(11):3071–3082, 2009.
20. J. Weir and W. Yan. Authenticating visual cryptography shares using 2d barcodes. In *IWDW*, volume 7128 of *Lecture Notes in Computer Science*, pages 196–210. Springer, 2011.
21. W.-C. Wu, Z.-W. Lin, and W.-T. Wong. Application of qr-code steganography using data embedding technique. In *Information Technology Convergence*, pages 597–605. Springer, 2013.

22. W. Yan, J. Wier, and M. S. Kankanhalli. Image secret sharing. In S. Cimato and C.-N. Yang, editors, *Visual Cryptography and Secret Image Sharing*, pages 381–402. CRC Press, Taylor and Francis Group, 2012.