symmetry

MDPI

*Article*

# Cooperative Secret Sharing Using QR Codes and Symmetric Keys

**Yang-Wai Chow [1,*], Willy Susilo [1], Joseph Tonien [1], Elena Vlahu-Gjorgievska [2] and Guomin Yang [1]**

[1] Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia; wsusilo@uow.edu.au (W.S.); dong@uow.edu.au (J.T.); gyang@uow.edu.au (G.Y.)
[2] Centre of Persuasive Technology and Society, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia; elenavg@uow.edu.au
* Correspondence: caseyc@uow.edu.au; Tel.: +61-2-4221-5001

Received: 28 February 2018; Accepted: 3 April 2018; Published: 4 April 2018

**Abstract:** Secret sharing is an information security technique where a dealer divides a secret into a collection of shares and distributes these to members of a group. The secret will only be revealed when a predefined number of group members cooperate to recover the secret. The purpose of this study is to investigate a method of distributing shares by embedding them into cover Quick Response (QR) codes in a secure manner using cryptographic keys. The advantage of this approach is that the shares can be disseminated over public channels, as anyone who scans the QR codes will only obtain public information. Only authorized individuals who are in possession of the required keys will be able to recover the shares. This also means that when group members cooperate to recover a secret, the group can determine the presence of an illegitimate participant if the person does not produce a valid share. This study proposes a protocol for accomplishing this and discusses the underlying security of the protocol.

**Keywords:** cooperative; Quick Response (QR) code; secret sharing; symmetric key

## 1. Introduction

Consider the scenario where an organization requires a group of participants to cooperate on a secret task, but the group members do not know each other. The organization can split a secret into a number of pieces and distribute each piece to a different group member. Only when the pieces are combined can the secret be recovered. The organization can communicate with members of the group by sending out messages with Quick Response (QR) codes. Each QR code contains non-suspicious public information in conjunction with an encrypted piece of the secret. To an unsuspecting observer, the QR codes will not give rise to any cause for concern as anybody can use a QR code reader to retrieve the public information. Only authorized group members will be able to extract and decrypt the concealed information to obtain a piece of the secret. Group members must then cooperate to recover the secret by combining their respective pieces together. In doing so, this also verifies the identity of members of the group with each other, since only authorized individuals can obtain a correctly-decrypted piece of the secret.

Secret sharing is a technique in information security where a group of participants must cooperate to recover a secret [1]. A secret sharing scheme is a method whereby a dealer divides a secret into a collection of shares. These shares are to be distributed to members of the group. Each share by itself must not reveal any information about the secret. Only when the information from a certain number of shares is combined can the secret be recovered [2].

The motivation behind this study is due to the fact that in a number of secret sharing approaches, despite the fact that individual shares do not reveal any information about the secret, a typical share may be obvious even to a casual observer. For example, in visual cryptography schemes, shares are images consisting of seemingly meaningless random black and white pixels. Anyone who sees such an image will suspect that it is a share. This paper investigates a novel approach of distributing secret shares over public communication channels.

The proposed secret sharing protocol adopts the concept of visual subterfuge to hide and conceal shares within cover QR codes. Any member of the public can decode the resulting QR codes using an ordinary QR code reader to retrieve the public information. However, only an authorized person who possesses the correct keys can decrypt the secret share information that is meant for that individual. The purpose of this approach is to lower the probability that potential adversaries may suspect the presence of a secret. Furthermore, QR codes can be scanned and decoded by devices equipped with cameras via the visual channel. Thus, the shares can be disseminated using printed media. In addition, the proposed protocol employs a cooperate layer where participants must combine their respective shares to decrypt the secret.

This study is also related to secret handshake protocols. A secret handshake protocol aims to allow group members to mutually identify one another [3]. Since the secret handshake can only be performed by authorized members of the group, this allows for mutual authentication between authorized parties [4]. In the protocol investigated in this study, only an authorized person can obtain a correct piece of the secret. Therefore, if the group can successfully recover the secret, this means that the members are authorized persons that are part of the group. If only some of the people present can recover the secret, the other people will be identified as unauthorized and malicious.

In comparison with existing techniques involving QR codes and secrets, their differences with the method proposed in this paper are summarized as follows:

1. The objective of the proposed protocol is to encrypt and conceal shares within QR codes to be able to distribute the shares via public channels without raising suspicion. While there are a number of existing techniques for hiding a secret within a QR code, the purpose of many of these methods is for data hiding and not for secret sharing [5–9]. Hence, cooperation between a threshold number of participants to recover the secret is not incorporated in these techniques.
2. There are some drawbacks with existing QR code secret sharing approaches that are based on visual cryptography. For example, the QR code sizes that are used may have to be very large [10]. This may be useful in situations where decryption necessitates no computation; however, large QR codes are impractical and are likely to raise suspicion as these are not commonly used in public. Other approaches result in QR codes that are valid, but do not look like normal QR codes because each module is divided into smaller sub-modules in order to enable secret sharing [11].
3. There are also existing $(n, n)$ QR code secret sharing approaches where normal looking QR codes are used [12,13]. However, $(n, n)$ secret sharing requires that all participants must be present to recover the secret. The proposed protocol is for $(k, n)$ secret sharing, where $k$ can be $< n$. In other words, while a threshold number of participants is required to recover the secret, this threshold does not have to be all the participants.
4. Unlike our previous work in Chow et al. [14], in which the purpose was to use a single non-suspicious QR code to broadcast a secret to a group of authorized participants where each participant can obtain the secret themselves, the protocol proposed in this paper provides a mechanism for a shared secret using QR codes. This means that each participant can only obtain his/her respective share, which does not reveal the secret, and must cooperate with other participants before the secret can be recovered.

## 2. Background

### 2.1. Secret Sharing

Blakley [15] and Shamir [16] were the first to introduce the notion of secret sharing. Since its inception, secret sharing schemes have become vital tools that are used for many applications in cryptography and distributed computing [2]. A description of a general $k$-out-of-$n$, or ($k$, $n$), threshold secret sharing scheme can be defined as follows. Data in the form of a secret, $D$, are split into $n$ pieces, $D_1, D_2, \ldots, D_n$, where $n > 1$ [16]. The $n$ pieces of the secret are known as shares. The secret is divided into shares in a manner in which knowledge of any $k$, or more shares, will allow $D$ to be recovered, whereas knowledge of only $k - 1$, or fewer shares, makes the recovery of $D$ impossible.

The following is an example of a threshold secret sharing scheme that is based on polynomial interpolation [16]:

**Definition 1.** *In a two-dimensional plane, for k points $(x_1, y_1), \ldots, (x_k, y_k)$, there can be only one polynomial $q(x)$ of degree $k - 1$ where $q(x_i) = y_i$ for all i. Let D be a number. D can be split into shares, $D_i$, by choosing a random $k - 1$ degree polynomial $q(x) = a_0 + a_1 x + \ldots + a_{k-1} x^{k-1}$ (mod p), such that $a_0 = D$ and $D_1 = q(1), \ldots, D_i = q(i), \ldots, D_n = q(n)$, and p is a prime where $p > max(n, |D|)$.*

*With information of any k, or more, shares $D_i$ along with the respective indices, i.e., $(x_i, q(x_i))$ where $i = \{1, \ldots, k\}$, the coefficients of $q(x)$ can be interpolated to obtain the value of $D = q(0)$. This can be done using Lagrange polynomial interpolation [17]:*

$$D = q(0) = \sum_{i=1}^{k} q(x_i) \prod_{j=1, j \neq i}^{k} \frac{-x_j}{x_i - x_j} \pmod{p} \tag{1}$$

*However, with information of only $k - 1$, or fewer, $D_i$, it is impossible to determine the value of D because there is insufficient information.*

A variety of diverse secret sharing schemes with different levels of complexity have been proposed over many years. Some schemes involve complex numerical computation in the generation of shares and/or in the recovery of the secret. On the other hand, some schemes require little or no computation. For instance, visual cryptography is a commonly-known visual secret sharing method where the shares are binary images, which consist of black and white pixels. A secret image is divided into a number of shares. Each share is meant to be separately printed on a transparency. The secret is revealed when the predefined number of transparencies are stacked. This is because by stacking the transparencies, the human visual system is able to perceive the black and white pixel contributions to obtain the secret without requiring any form of computation [1,18].

However, one of the drawbacks of traditional visual cryptography is that each share is an image with a random pattern of black and white pixels. Due to the seemingly meaningless pattern of pixels, a visual cryptography share is obvious even to a casual observer. To overcome this problem, extended visual cryptography is a method of encoding shares within cover images [19]. Therefore, each share is a meaningful image. The benefit of encoding shares into "innocent-looking" meaningful cover images is that it aims to decrease the prospect of attracting the unwanted attention of attackers [20]. Nevertheless, each share in extended visual cryptography is a very noisy looking image. The approach examined in this study aims to avoid the attention of attackers by distributing shares using innocent-looking QR codes that contain both public and concealed information.

### 2.2. Quick Response Codes

A Quick Response (QR) code is a two-dimensional code that consists of light and dark squares, referred to as modules. A standard for the QR code was defined by the International Organization for Standardization (ISO): ISO/IEC18004 [21]. The standard defines forty QR code versions, where each version is made up of a different number of modules, thus giving rise to varying capacities for data. QR codes can encode various types of data including numeric, alphanumeric, binary and kanji.

Error correction is an inherent part of QR codes. It allows for correct decoding even if part of a QR code is dirty, obscured or damaged. There is a total of four error correction levels (i.e., low~7%, medium~15%, quartile~25% and high~30%), and each level provides for a different amount of error correction. Higher error correction levels increase the amount of error that can be tolerated, but also enlarges the size of the encoded data. This error correction mechanism allows for the contents of a QR code to be decoded even if part of it is obscured, so long as the amount of error does not exceed the error correction capacity. As such, many people have exploited this property for various purposes by deliberately introducing some error, like inserting a picture into a QR code.

Figure 1 shows an example of a QR code structure [21]. It can be seen that the structure is made up of encoding regions, as well as function patterns. Function patterns do not encode data and are used for retrieving specific information about the QR code, e.g., its version and error correction level. The encoding region is made up of data codewords and error correction codewords. Each codeword contains eight bits. Data are encoded in a QR code as a stream of bits, which is divided into a sequence of codewords.

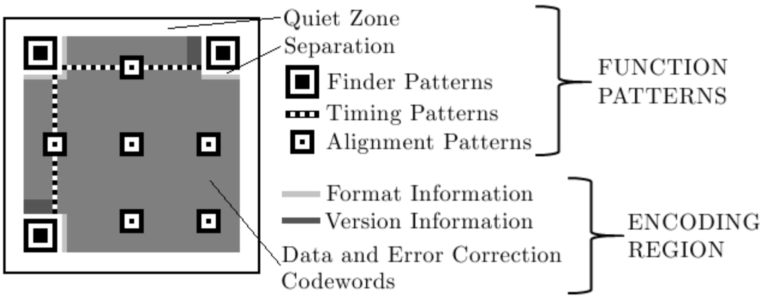

**Figure 1.** QR code Version 7 structure.

The data and error correction codewords in a QR code are divided into one or more blocks. The specific number of blocks, along with the total number of data and error correction codewords, is determined based on the QR code version and error correction level. Within each block, the error correction codewords are appended to the end of the data codeword sequence and encoded within the blocks in an interleaved manner. The purpose of this is to reduce the likelihood that localized damage will result in an undecodable QR code. Figure 2 depicts the arrangement of data and error correction codewords within a Version 4 QR code, with error correction level H.

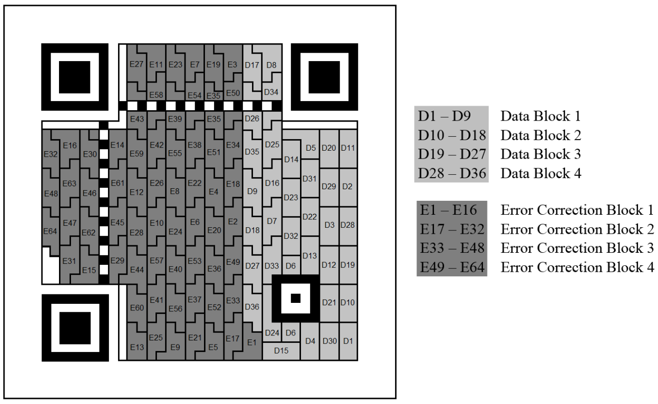
D1 – D9 Data Block 1
D10 – D18 Data Block 2
D19 – D27 Data Block 3
D28 – D36 Data Block 4
E1 – E16 Error Correction Block 1
E17 – E32 Error Correction Block 2
E33 – E48 Error Correction Block 3
E49 – E64 Error Correction Block 4

**Figure 2.** Arrangement of the data and error correction codewords within a Version 4 QR code, with error correction level H.

## 3. Related Work

The use of QR codes in information security has been proposed for a variety of different purposes, such as for authenticating visual cryptography shares [22], e-voting authentication [23], digital watermarking [24], data hiding [7] and secret sharing [10,12,13]. This section presents several studies that are related to the work in this paper.

Researchers have previously proposed steganography and data hiding techniques using QR codes. A technique for embedding data in the form of a QR code within a digital image was proposed by Wu et al. [7]. Their purpose was to conceal the existence of a QR code within a digital image in a manner that minimizes degradation of the image's visual quality. Chen and Wang [5] proposed an image steganography scheme by adopting the use of QR codes. The purpose of their scheme was to embed two types of secret data within a cover image, namely, text data (lossless) and image data (lossy). The text data were embedded in the form of a QR code. Chung et al. [6] also described a relatively similar approach.

Lin et al. [8] capitalized on the error correction redundancy mechanism of QR codes for the purpose of concealing secret data in a cover QR code. The size of secret data that can be hidden is governed by the data capacity of the QR code, which in turn is dependent on the version of the QR code that is used and its error correction level. In a different method, Bui et al. [9] proposed a method of hiding a secret message within a QR code using Reed–Solomon code, which is used in QR codes for error correction, and list decoding. Their purpose was to overcome modification attack vulnerabilities of other approaches that use bit embedding to hide secret messages in QR codes.

In previous work, a method of hiding a QR code, which contained concealed information, within a public QR code was examined in Chow et al. [14]. This approach was named covert QR codes. The objective of the approach was to employ visual subterfuge to embed a hidden secret message within a QR code and only authorized people could retrieve the secret. This would allow a dealer to disseminate a secret message to a group of authorized people over public channels. For example, a dealer could put a poster with a QR code in a public place. The casual observer will only be able to retrieve the public message, whereas all authorized people will be able to obtain the secret. This approach is useful in the situation where a dealer wants to broadcast the same secret message to all the authorized recipients. The method investigated in this paper on the other hand is intended to send a different share to each authorized participant, and the secret can only be recovered through cooperation between a threshold number of participants.

A number of methods for using QR codes in secret sharing schemes has also been proposed. Wan et al. [10] demonstrated a method of embedding visual cryptography shares within cover QR codes. They called this technique a $(k, n)$ visual secret sharing scheme based on QR codes. By embedding shares in QR codes, when a qualified number of cover QR codes was stacked, the secret could be recovered by the human visual system based on visual cryptography principles. While the advantage of this method is that no computation is required to decrypt the secret, the drawback is that the size of the cover QR codes must be very large in order to contain meaningful visual cryptography shares.

Another approach based on QR codes and visual cryptography was also proposed in Cheng et al. [11]. In their approach, the access structure of visual cryptography schemes is used for distributing and embedding secret information into QR code shares. This is done by dividing a cell into 3×3 sub-modules, where the public message in the centre sub-module remains, but the surrounding sub-modules are used to embed a visual cryptography access structure. Decryption is based on an XOR (exclusive or) operation.While the resulting QR code shares are all valid QR codes that can be scanned by a normal QR code reader, they do not look like normal QR codes due to the embedding of secret information by modifying the sub-modules.

A distributed secret sharing approach using QR codes was proposed by Lin [13]. This approach is an $(n, n)$ secret sharing scheme, where a secret is split into shares and encrypted before concealing them within marked QR codes. The secret can be retrieved when all the shares are available. A cheater prevention mechanism was also incorporated in this approach. A different $(n, n)$ QR code secret sharing technique was presented in Chow et al. [12]. This approach also exploits the error correction feature that is a characteristic part of the QR code structure by distributing and embedding information from a secret QR code within $n$ cover QR code shares. To recover the secret, the information from the QR code shares can be collated to obtain a recovered secret QR code, which can then be decoded to reveal the secret message. The advantage of this approach is that no encryption keys are required.

## 4. Protocol and Adversarial Models

To analyse the security of the proposed protocol, this section describes the protocol and adversarial models, along with the underlying assumptions.

### *4.1. Protocol Model*

The protocol is modelled based on the following entities: a dealer who knows the identities of all the participants and has access to the system that implements the encryption and concealment phase as described in Section 5.1; $n$ participants who are each equipped with a device that has a QR code reader, which holds the cryptographic keys and implements the extraction and decryption phase as described in Section 5.2.

To distribute a secret, the dealer can send QR codes over public unsecure channels, including on printed media. The protocol assumes that the secret sharing scheme implemented in conjunction with the protocol does not leak any information that can be used to determine the secret or any useful information pertaining to the secret. Furthermore, any $k - 1$, or less, shares will also not reveal any information pertaining to the secret, thereby precluding any form of collusion between participants. In addition, without losing generality, the protocol assumes that the dealer and participants have a secure channel for sharing a symmetric key. It also assumes that a public key infrastructure is in place where the dealer, who knows the identities of all the participants, can obtain digital certificates of the participants from a trusted certification authority.

### *4.2. Adversarial Model*

Based on the protocol model defined above, the adversarial model assumes that an attacker can access all communication involving the use of QR codes over public channels, including on printed media. It also assumes that the attacker can extract the hidden message from the QR codes and can obtain information about all modifications made to the cover QR codes. Since the attacker does not have the cryptographic keys, it is assumed that the attacker cannot decrypt the hidden message and cannot obtain a legitimate share. However, an attacker can try to impersonate a participant by presenting an illegitimate share to the group.

## 5. Secret Sharing Protocol Using QR codes

Figure 3 provides an overview of the proposed secret sharing protocol using QR codes and symmetric keys. The aim of the proposed protocol is to encrypt and conceal shares within QR codes in order to be able to distribute the shares via public channels without raising suspicion. Only authorized individuals who have the appropriate credentials can extract and decrypt the information to obtain the shares. Subsequently, a qualified number of group members must cooperate before the secret can be revealed. The overview depicted in Figure 3 divides the overall process in to three phases, namely the encryption and concealment phase, the extraction and decryption phase and the cooperative phase. The details of phases will be described in the subsections to follow.

### *5.1. Encryption and Concealment Phase*

In this phase, a dealer divides a secret message into a number of shares. Each group member has a private key, which is only known to them, and a corresponding public key. The dealer knows, or has a way of obtaining, each group members' public key. The individual shares are then encrypted using the group members' respective public keys and a symmetric key, which is known by the dealer and all the authorized members. This results in an encrypted message for each share.

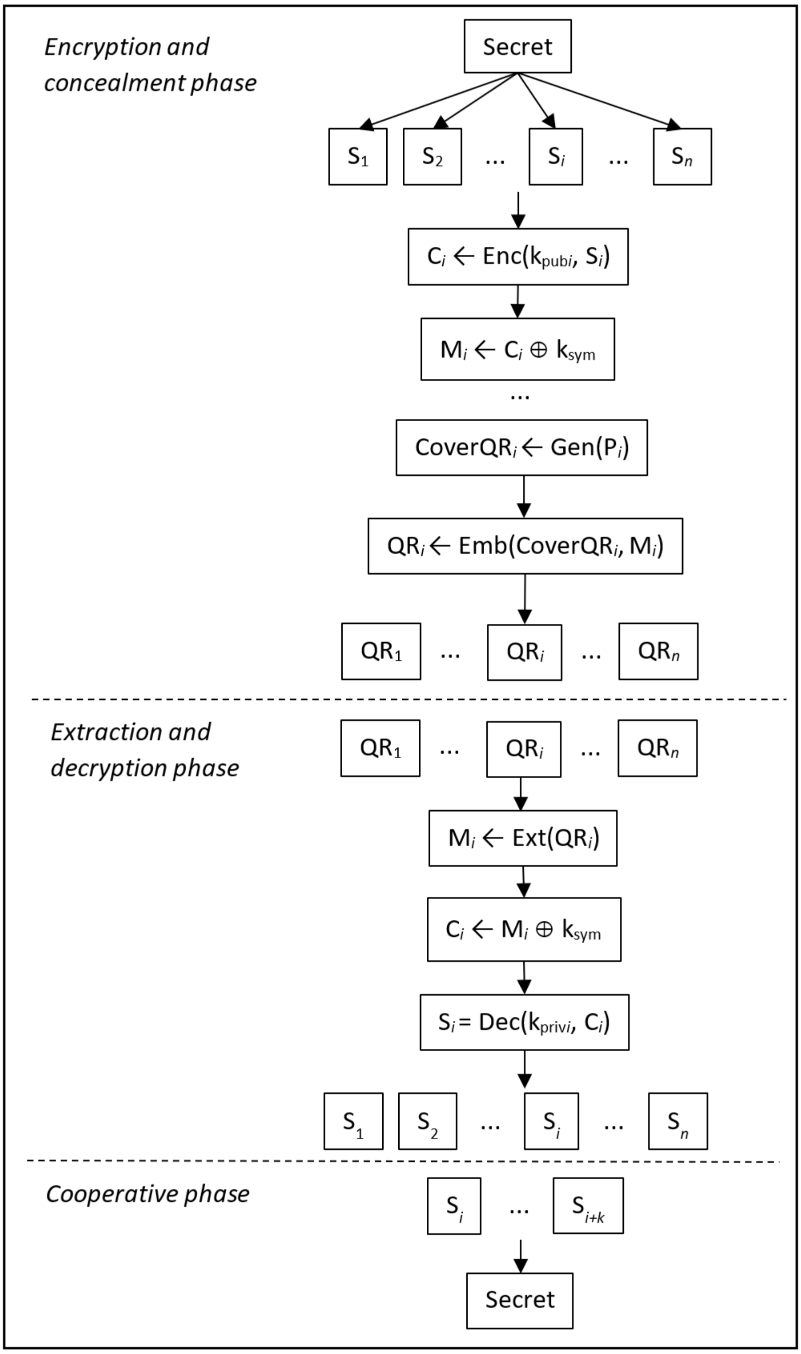

**Figure 3.** Overview of the proposed approach.

A number of cover QR codes, which contain public information, are then generated. The number of cover QR codes is the same as the number of shares. Each encrypted share is then embedded within a QR code. The resulting QR codes can then be distributed by transmitting them to the participants over public channels. To a casual observer, the QR codes look inconspicuous and can be scanned to retrieve the public information. Only authorized individuals can obtain the shares.

This phase is formally defined as follows:

**Definition 2.** *Let $S$ be the secret message and $S_i$ be the individual shares, where $i = \{1, \ldots, n\}$ and $n$ is the total number of group members. Furthermore, let $k_{pub_i}$ represent a group member's public key and $k_{priv_i}$ be the corresponding private key. $k_{sym}$ is a symmetric key that is known to the dealer and all the authorized group members. These will be used with the following algorithms.*

- *$C_i \leftarrow Enc(k_{pub_i}, S_i)$: This algorithm takes a share, $S_i$, and encrypts it using a group member's public key, $k_{pub_i}$. This results in the encrypted message, $C_i$.*
- *$M_i \leftarrow C_i \oplus k_{sym}$: This process 'XOR's the encrypted message, $C_i$, with a symmetric key, $k_{sym}$, to produce the encrypted hidden message, $M_i$, which is to be embedded in a QR code.*
- *$CoverQR_i \leftarrow Gen(P_i)$: Taking a public message, $P_i$, this algorithm generates a cover QR code, $CoverQR_i$.*
- *$QR_i \leftarrow Emb(CoverQR_i, M_i)$: This process embeds the encrypted hidden message, $M_i$, into the cover QR code, $CoverQR_i$, to produce a QR code, $QR_i$.*

*The resulting QR codes, $QR_i$, contain both public information and concealed encrypted information. These QR codes can be distributed over public channels, because only individuals with the necessary credentials can decrypt the hidden information.*

The cover QR code generation process, $Gen(P_i)$, can be implemented using any deterministic QR code generator that is based on the QR code standard. The aim is to produce a valid QR code that can be scanned and decoded by a standard QR code reader to obtain the public message, $P_i$. For the embedding process, $Emb(CoverQR_i, M_i)$, one of the inputs is an encrypted hidden message, $M_i$, which is to be embedded within the cover QR code, $CoverQR_i$. The total amount of data in $M_i$ cannot exceed $CoverQR_i$'s error correction capacity, otherwise the resulting QR code, $QR_i$, will not be valid and will be unusable. Hence, the choice of $CoverQR_i$'s version and error correction capacity must depend on the size of $M_i$. The embedding process is possible due to error correction redundancy in QR codes and can be performed by replacing some of the redundant codewords in $CoverQR_i$, as long as it maintains the integrity of the error correction mechanism. This is similar to how one can overlay an image on a QR code, and the partially obscured QR code can still be correctly decoded.

### *5.2. Extraction and Decryption Phase*

The QR codes that contain both public and hidden information will be distributed to the group members. An authorized group member who possesses all the required credentials, namely, his/her private key and the symmetric key, will be able to obtain a share for the QR code. This is done by first extracting the hidden message from the QR code, decoding the hidden message using the symmetric key, then decrypting it using the group member's individual private key. This will allow the group member to correctly obtain his/her respective share.

**Definition 3.** *The following algorithms are used in this phase.*

- *$M_i \leftarrow Ext(QR_i))$: Given the QR code with the conceal information, $QR_i$, this algorithm extracts the encrypted hidden message, $M_i$, from it.*
- *$C_i \leftarrow M_i \oplus k_{sym}$: By 'XOR'ing the encrypted hidden message, $M_i$, with the symmetric key, $k_{sym}$, the encrypted message, $C_i$, can be obtained.*
- *$S_i \leftarrow Dec(k_{priv_i}, C_i)$: This process obtains the share $S_i$ by decrypting the encrypted message, $C_i$, using the private key, $k_{priv_i}$.*

*By extracting and decrypting the hidden information from the QR code, group member i will be able to obtain his/her respective share, $S_i$.*

QR codes constructed based on the QR code standard [21] are deterministic. Therefore, if a valid, but modified, QR code is scanned and decoded by a normal QR code reader, the user will be able to obtain the public message. The public message can then be used to reproduce the original, non-modified, QR code. Thus, the difference between the original and modified QR code can be determined by comparing the two. This is the underlying notion governing the hidden information extraction process, $Ext(QR_i)$. While an adversary can also obtain this, the hidden information is encrypted and cannot be decrypted without the key.

### *5.3. Cooperative Phase*

During this phase, group members would have already obtained their respective shares. To reveal the secret message that was distributed by the dealer, a qualified number of group members must cooperate by combining their shares together. For recovery of the secret message, in a $(k, n)$ threshold secret sharing scheme, $k$ or more shares must be present before the secret can be revealed. Any $k - 1$, or less, shares will not be able to reveal the secret. The method of recovery is dependent on the secret sharing scheme that is used. For example, if the secret sharing scheme that was defined in Definition 1 is employed, then Equation (1) will be used for recovering the secret message.

## **6. Analysis and Discussion**

### *6.1. Implementation Guidelines*

An implementation of the proposed protocol will require the use of a QR code embedding technique in conjunction with a secret sharing scheme. It should be noted that the resulting QR codes, i.e., $QR_i$, must be valid QR codes. In other words, anybody with a standard QR code reader must be able to scan $QR_i$ and obtain the public message. Furthermore, the public message should be the same as the message in the cover QR code. The extraction process, i.e., $M_i \leftarrow Ext(QR_i)$, capitalizes on this fact, in that once the public message is obtained, the cover QR code can be reproduced by generating a QR code using the public message. Hence, the difference between the cover QR code and the $QR_i$ can be used to extract the concealed information.

In view of the fact that this embedding process exploits the QR code error correction mechanism, this means that the size of the encrypted share cannot be larger than the size of the cover QR code's error correction capacity. Otherwise, the resulting QR code will not be valid and cannot be decoded. This necessitates that the size of the cover QR code be significantly larger than the size of the encrypted share. As such, the appropriate cover QR code version and error correction level is reliant on the size of the shares that must be embedded.

An appropriate version and error correction level can be determined as follows. The data in QR codes are encoded within one or more blocks. An example of this was previously depicted in Figure 2. The number of blocks, $b$, depends on the QR code version and error correction level, as defined in the QR code standard [21]. Each block is made up of a number of codewords, $c$, which consist of data codewords, $d$, and error correction codewords, $e$. Each block also has an error correction capacity, $r$, which is the maximum number of codewords in that block that can be in error. If the number of codewords within a block that are in error exceeds, $r$, the data in that block cannot be decoded, and hence, the whole QR code cannot be decoded correctly. This means that to embed hidden information within a QR code, the size of the embedded message, $m$, must be such that $m < b \times r$. Otherwise, the error introduced by embedding the encrypted share, i.e., $QR_i \leftarrow Emb(CoverQR_i, M_i)$, within $CoverQR_i$, will overwhelm the error correction capacity of that QR code version and error correction level, resulting in an invalid $QR_i$.

The covert QR code approach described in Chow et al. [14] is a method that can be used to hide the shares. This approach has the advantage that the hidden information itself uses a QR code, which means that both the hidden QR code and the cover QR code have error correction redundancy. This minimizes the chances of the hidden QR code being undecodable due to a dirty or damage to the covert

QR code. Figure 4 provides an illustration of how this technique can be used to embed a encrypted share. Figure 4a shows a QR code that was generated with a secret message that is to be hidden in a cover QR code. Only the data and error correction codewords should be embedded, as shown in Figure 4b, because the function patterns can potentially leak information. Figure 4d shows the resulting QR code after the embedding process, i.e., the covert QR code. The covert QR code contains both the public message and the hidden information. The difference between the cover QR code and the resulting QR code with the embedded information is shown in Figure 4e. Note that both the QR codes shown in Figure 4c,d are valid QR codes that can be decoded by a normal QR reader. In addition, they will both decode to the same public message.

An approach for implementing $M_i \leftarrow C_i \oplus k_{sym}$ and its reverse $C_i \leftarrow M_i \oplus k_{sym}$ is to use a deterministic random number generator. Since the size of $C_i$ varies depending on the length of the encrypted message, using the same seed, a random number generator can produce a deterministic sequence of random bits, which can be used for the XOR operation. This will ensure that the dealer and all participants will be able to perform the XOR operation with the same random bit sequence. However, an adversary will not be able to obtain this sequence of bits and thus will not be able decrypt the information.

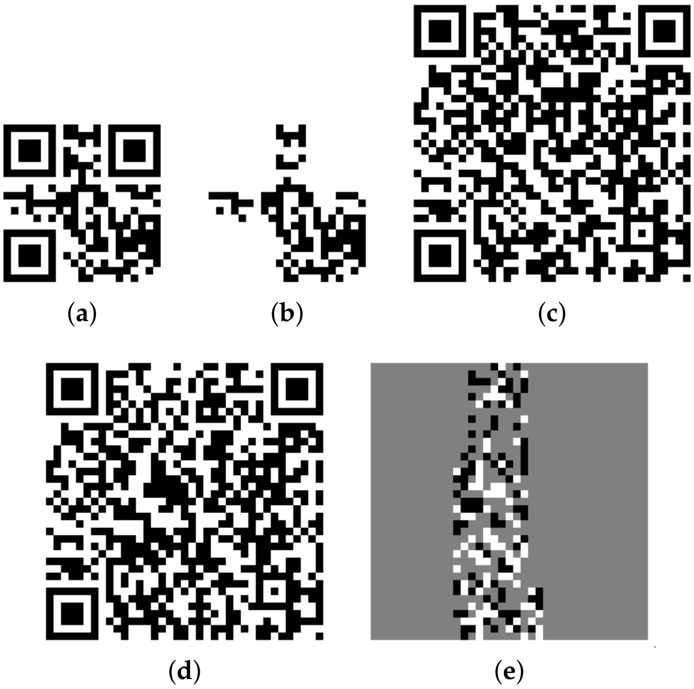

**Figure 4.** Example of embedding a hidden QR code message within a cover QR code; (**a**) QR code containing a message to be embedded; (**b**) codeword modules of the QR code presented in (**a**); (**c**) cover QR code containing a public message; (**d**) resulting QR code containing a public message and an embedded hidden message; (**e**) differences in modules between the QR codes shown in (**c**,**d**).

### *6.2. Security*

Numerous secret sharing schemes can be used in conjunction with the proposed protocol. For example, the secret sharing scheme provided in Definition 1 can easily be incorporated into the protocol. Since the security of the protocol relies on the implemented techniques, the security of the proposed protocol is discussed as follows.

**Theorem 1.** *Shares in the proposed secret sharing protocol using QR codes as defined in Section 5 are secure.*

**Proof of Theorem 1.** Security of the shares in the protocol is based on the underlying symmetric key and public key infrastructure that are used to encrypt the shares before transmission. Since the shares are embedded within a cover QR code, $CoverQR_i$, the resulting QR code, $QR_i$, will be modified and different from $CoverQR_i$. This means that an adversary who suspects that $QR_i$ contains a hidden message can reconstruct $CoverQR_i$ using the public information decoded from $QR_i$ and subsequently find the difference between them. Nevertheless, the only information that will be revealed is the potential length of the share, based on the number QR code codewords that were modified. No other information can be extracted, because the adversary cannot decrypt the encrypted information without the keys. Let $C'$ represent the number of modified codewords in $QR_i$, and the probability of success of a brute force attack is governed by $\frac{1}{8\times|C'|}$, since each codeword contains eight modules. □

The protocol described in Section 5 assumes that a public key infrastructure is in place where the dealer can obtain digital certificates of the group members from a trusted certification authority. Otherwise, instead of using a public key approach, an identity-based encryption method can easily replace the public key encryption.

**Theorem 2.** *The secret in the protocol defined in Section 5 is secure assuming that the underlying secret sharing scheme implemented in the protocol is secure. This means that any $k-1$ or less shares will reveal no information about the secret.*

**Proof of Theorem 2.** A variety of secret sharing schemes can be implemented in conjunction with the protocol. The security of the secret in the protocol is based on the security of the secret sharing scheme such that if $n$ shares are generated and distributed, any $k-1$, or less, shares will reveal no information about the secret. This is a fundamental requirement of a $(k, n)$ secret sharing scheme. As such, the proposed protocol is secure without information of $k$, or more, shares. □

In the proposed protocol described in Section 5, if the group members cannot correctly recover the secret despite having $k$ or more shares, This means that there is at least one unauthorized and malicious person among the group. If the implementation requires cheater detection, which refers to the ability to be able to detect whether a group member is malicious or a illegitimate individual is trying to tamper with the shares, a verifiable secret sharing scheme like Feldman's scheme [25] can be used. Such a verifiable secret sharing scheme will allow the other legitimate group members to identify the malicious individual(s) who did not provide valid share(s).

A practical consideration when using the protocol is that since shares by themselves do not reveal useful information, an authorized user may not know whether the share was decrypted correctly. As such, in practice, a human-readable string should be appended to the share and encrypted together with it. In this manner, if decrypting the hidden message produces a readable string, this will imply that the share was also successfully decrypted.

## 7. Conclusions

This study investigated a secret sharing protocol for distributing secret shares over public channels. The proposed approach is secure as only authorized individuals who have the necessary credentials can extract and decrypt the concealed information from the QR codes. Furthermore, the QR codes will not look suspicious to a casual observer, as they are valid QR codes that can be scanned and decoded by a normal QR code reader. However, without the required credentials, one can only obtain public information from the QR codes. With the correctly-decrypted shares, group members will have to cooperate to recover the secret. During the secret recovery process in the proposed protocol, unauthorized participants will be revealed as they will not have valid shares. The security underlying the protocol was examined, and it was shown to be secure. Since many diverse secret sharing schemes can be used in conjunction with the proposed approach, a thorough implementation to compare the incorporation of several such schemes with the protocol will be the topic of future research.

**Acknowledgments:** The authors would like to acknowledge the support of the UOW UICInternational Links Grant 2017 that was awarded for this research.

**Author Contributions:** The authors' names are sorted in alphabetical order. Yang-Wai Chow, Willy Susilo and Guomin Yang conceived of the idea. Joseph Tonien and Elena Vlahu-Gjorgievska defined and analysed the protocol. Yang-Wai Chow wrote the paper.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Chow, Y.; Susilo, W.; Yang, G. Cooperative Learning in Information Security Education: Teaching Secret Sharing Concepts. In *Lecture Notes in Computer Science, Proceedings of the 14th International Conference Cooperative Design, Visualization, and Engineering (CDVE), Mallorca, Spain, 17–20 September 2017*; Luo, Y., Ed.; Springer: Berlin, Germany, 2017; Volume 10451, pp. 65–72.
2. Beimel, A. Secret-Sharing Schemes: A Survey. In *Lecture Notes in Computer Science, Proceedings of the Third International Workshop Coding and Cryptology (IWCC), Qingdao, China, 30 May–3 June 2011*; Springer: Berlin, Germany, 2011; Volume 6639, pp. 11–46.
3. Balfanz, D.; Durfee, G.; Shankar, N.; Smetters, D.K.; Staddon, J.; Wong, H. Secret Handshakes from Pairing-Based Key Agreements. In Proceedings of the 2003 IEEE Symposium on Security and Privacy (S & P 2003), Berkeley, CA, USA, 11–14 May 2003; pp. 180–196.
4. Sorniotti, A.; Molva, R. A provably secure secret handshake with dynamic controlled matching. *Comput. Secur.* **2010**, *29*, 619–627.
5. Chen, W.Y.; Wang, J.W. Nested image steganography scheme using QR-barcode technique. *Opt. Eng.* **2009**, *48*, 057004.
6. Chung, C.H.; Chen, W.Y.; Tu, C.M. Image hidden technique using QR-barcode. In Proceedings of the Fifth IEEE IIH-MSP'09 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, 12–14 September 2009; pp. 522–525.
7. Wu, W.C.; Lin, Z.W.; Wong, W.T. Application of QR-Code Steganography Using Data Embedding Technique. In *Information Technology Convergence*; Springer: Berlin, Germany, 2013; pp. 597–605.
8. Lin, P.Y.; Chen, Y.H.; Lu, E.J.L.; Chen, P.J. Secret Hiding Mechanism Using QR Barcode. In Proceedings of the 2013 IEEE International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Kyoto, Japan, 2–5 December 2013; pp. 22–25.
9. Bui, T.V.; Vu, N.K.; Nguyen, T.T.; Echizen, I.; Nguyen, T.D. Robust Message Hiding for QR Code. In Proceedings of the 2014 IEEE Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Kitakyushu, Japan, 27–29 August 2014; pp. 520–523.
10. Wan, S.; Lu, Y.; Yan, X.; Wang, Y.; Chang, C. Visual secret sharing scheme for (k, n) threshold based on QR code with multiple decryptions. *J. Real Time Image Process.* **2018**, *14*, 25–40.
11. Cheng, Y.; Fu, Z.; Yu, B.; Shen, G. A new two-level QR code with visual cryptography scheme. In *Multimedia Tools and Applications*; Kluwer Academic Publishers: Boston, MA, USA, 2017.
12. Chow, Y.; Susilo, W.; Yang, G.; Phillips, J.G.; Pranata, I.; Barmawi, A.M. Exploiting the Error Correction Mechanism in QR Codes for Secret Sharing. In *Part I, Lecture Notes in Computer Science, Proceedings of the 21st Australasian Conference Information Security and Privacy (ACISP), Melbourne, Australia, 4–6 July 2016*; Liu, J.K., Steinfeld, R., Eds.; Springer: Berlin, Germany, 2016; Volume 9722, pp. 409–425.
13. Lin, P. Distributed Secret Sharing Approach With Cheater Prevention Based on QR Code. *IEEE Trans. Ind. Inform.* **2016**, *12*, 384–392.
14. Chow, Y.; Susilo, W.; Baek, J. Covert QR Codes: How to Hide in the Crowd. In *Lecture Notes in Computer Science, Proceedings of the 13th International Conference Information Security Practice and Experience (ISPEC), Melbourne, Australia, 13–15 December 2017*; Liu, J.K., Samarati, P., Eds.; Springer: Berlin, Germany, 2017; Volume 10701, pp. 678–693.
15. Blakley, G. Safeguarding cryptographic keys. In Proceedings of the 1979 AFIPS National Computer Conference, New York, NY, USA, 4–7 June 1979; pp. 313–317.
16. Shamir, A. How to Share a Secret. *Commun. ACM* **1979**, *22*, 612–613.
17. Dawson, E.; Donovan, D. The breadth of Shamir's secret-sharing scheme. *Comput. Secur.* **1994**, *13*, 69–78.

18. Naor, M.; Shamir, A. Visual Cryptography. In *Eurocrypt*; Santis, A.D., Ed.; Lecture Notes in Computer Science; Springer: New York, NY, USA, 1994; Volume 950, pp. 1–12.
19. Ateniese, G.; Blundo, C.; De Santis, A.; Stinson, D.R. Extended capabilities for visual cryptography. *Theor. Comput. Sci.* **2001**, *250*, 143–161.
20. Wang, D.; Yi, F.; Li, X. On general construction for extended visual cryptography schemes. *Pattern Recognit.* **2009**, *42*, 3071–3082.
21. International Organization for Standardization. *ISO/IEC 18004:2006—Information Technology—Automatic Identification and Data Capture Techniques—QR Code 2005 Bar Code Symbology Specification*; International Organization for Standardization: Geneva, Switzerland, 2006.
22. Weir, J.; Yan, W. Authenticating Visual Cryptography Shares Using 2D Barcodes. In *Lecture Notes in Computer Science, Proceedings of the 10th IWDW 2011 International Workshop, Atlantic, NY, USA, 23–26 October 2011*; Springer: Berlin, Germany, 2011; Volume 7128, pp. 196–210.
23. Falkner, S.; Kieseberg, P.; Simos, D.; Traxler, C.; Weippl, E. E-voting Authentication with QR-codes. In *Human Aspects of Information Security, Privacy, and Trust*; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8533, pp. 149–159.
24. Chow, Y.; Susilo, W.; Tonien, J.; Zong, W. A QR Code Watermarking Approach Based on the DWT-DCT Technique. In *Part II, Lecture Notes in Computer Science, Proceedings of the 22nd Australasian Conference Information Security and Privacy (ACISP), Auckland, New Zealand, 3–5 July 2017*; Pieprzyk, J., Suriadi, S., Eds.; Springer: Berlin, Germany, 2017; Volume 10343, pp. 314–331.
25. Feldman, P. A Practical Scheme for Non-interactive Verifiable Secret Sharing. In Proceedings of the 28th Annual Symposium on Foundations of Computer Science, Los Angeles, CA, USA, 27–29 October 1987; pp. 427–437.