

Brief Report

A Confidential QR Code Approach with Higher Information Privacy

Pei-Yu Lin ^{1,2}, Wen-Shao Lan ², Yi-Hui Chen ^{3,4,*} and Wen-Chuan Wu ^{5,*}

¹ Department of Electrical Engineering, National Kaohsiung University of Science and Technology, Kaohsiung 807618, Taiwan; pagelin3@gmail.com or pagelin@nku.edu.tw

² Department of Information Communication, Yuan Ze University, Taoyuan 320315, Taiwan; wenshao0303@gmail.com

³ Department of Information Management, Chang Gung University, Taoyuan 333323, Taiwan

⁴ Kawasaki Disease Center, Kaohsiung Chang Gung Memorial Hospital, Kaohsiung 833401, Taiwan

⁵ Department of Computer Science and Information Engineering, National Ilan University, Yilan 260007, Taiwan

* Correspondence: cyh@gap.cgu.edu.tw (Y.-H.C.); wenn@niu.edu.tw (W.-C.W.)

Abstract: In present times, barcode decoders on mobile phones can extract the data content of QR codes. However, this convenience raises concerns about security issues when using QR codes to transmit confidential information, such as e-tickets, coupons, and other private data. Moreover, current secret hiding techniques are unsuitable for QR code applications since QR codes are module-oriented, which is different from the pixel-oriented hiding manner. In this article, we propose an algorithm to conceal confidential information by changing the modules of the QR Code. This new scheme designs the triple module groups based on the concept of the error correction capability. Additionally, this manner can conceal two secret bits by changing only one module, and the amount of hidden confidential information can be twice the original amount. As a result, the ordinary data content (such as URL) can be extracted correctly from the generated QR code by any barcode decoders, which does not affect the readability of scanning. Furthermore, only authorized users with the secret key can further extract the concealed confidential information. This designed scheme can provide secure and reliable applications for the QR system.

Keywords: information security; QR code; error correction capability; sensitive information; secret data



Citation: Lin, P.-Y.; Lan, W.-S.; Chen, Y.-H.; Wu, W.-C. A Confidential QR Code Approach with Higher Information Privacy. *Entropy* **2022**, *24*, 284. <https://doi.org/10.3390/e24020284>

Academic Editors: Udaya Paramalli and Tetsuya Kojima

Received: 13 December 2021

Accepted: 13 February 2022

Published: 16 February 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Quick Response (QR) codes are widely used in our daily lives since they are convenient and can accommodate a large amount of data [1,2]. Mobile devices can scan the QR code and obtain the data content for public transmission. However, when the information requires privacy for the individual (e.g., e-coupons and e-tickets), current QR Code technologies cannot address the security problems [3–6]. For example, in 2011, Taiwan High Speed Rail (THSR) released a trial of e-ticketing, in which users could download a QR code after purchasing a ticket via smartphones. These codes replaced paper tickets for entering and exiting the train gate. However, although e-ticketing makes the ride smoother and more environmentally friendly, it also makes it easier for people with bad intentions to forge fake tickets. The security of QR code e-tickets thus remains an unsolved question. Accordingly, it is necessary for companies or e-ticketing systems to hide or protect sensitive QR code content, allowing only authorized users to retrieve it [7].

However, many studies on concealing confidential information have focused on protecting the ownership of digital images or on embedding secrets into digital images [8–11]. These approaches applied steganography techniques based on traditional media instead of embedding or protecting the QR code directly. Moreover, QR codes have standard encoding and decoding specifications and need to be quickly decoded by scanning devices

such as cell phones, tablets, or barcode scanners. In other words, general research on secret image hiding is unsuitable for protecting QR codes.

These schemes [12,13] have explored the security of QR codes, proposing ownership protection via image processing techniques, including the discrete wavelet transform (DWT), the discrete cosine transform (DCT), or the discrete Fourier transform (DFT). These techniques transform QR images into the frequency domain and embed watermarks into the special coefficients of QR images. However, such approaches require computer assistance and are unsuitable for printed QR codes, such as posters or hard paper. In addition, due to the scanning environment of the camera instrument, the generated QR code image may be distorted. Watermarks in the frequency domain may encounter capture problems and cause incorrect watermark results.

Researchers such as [14,15] directly embed the watermark into the barcode by adjusting the height and width of the barcode modules. The module is the black or white square of the barcode. Although such methods directly embed secrets into the barcode modules, the generated barcode still requires additional equipment to calculate the height and width of the modules. In addition, the available barcode scanners cannot directly identify and extract the secrets of the generated QR code, which reduces the practicability.

Different from the schemes presented in [12–15], Chiang et al. proposed a blind QR code steganographic approach based on the error correction capability [16]. Their method [16] effectively exploits the error correction properties of QR codes and adapts the QR module to embed secrets. A typical scanning device can read the QR data content from the generated QR code. In particular, the authorized recipients can additionally extract secrets from the tagged QR codes. Chiang et al.'s scheme is practical and can be applied to standard mobile devices and scanning devices. However, the maximum payload of the secret is equal to the error tolerance of the QR code. To increase the payload of embeddable secrets, the method proposed by Luo et al. [17] can effectively reduce the modification of the QR module when embedding secrets into QR codes. As a result, the secret payload embedded in the method of Luo et al. is 1.5 times higher than that of the method proposed by Chiang et al.

Based on the above observations, there is a considerable lack of research on protecting the confidential information of QR codes. Anyone can easily scan and retrieve QR data content through barcode readers [16–19]; therefore, the protection of private data is critical. Traditional image hiding or watermarking techniques require additional image processing processes/computers that are not suitable for real-time scanning and direct retrieval of QR codes by barcode readers. In this article, we aim to design a system to embed secrets into QR codes and to address the following issues: the confidentiality of QR codes and the payload of the confidential information that can be embedded. This proposed method can effectively preserve the original readability of QR codes, significantly reduce the modification of QR modules, and increase the embeddable capacity of secrets in QR codes. Moreover, the embeddable secret payload is superior to related studies [16,17]. Finally, we perform a theoretical analysis to prove the proposed method and discuss its implications.

2. The Proposed Confidential QR Approach Based on the Triple Module Group

The designed system integrates three QR modules into a group and changes the modules by utilizing the concept of the error correction propriety of QR codes. As a result, the new system can change only one of these modules to hide two confidential information bits for enhancing the confidential capacity. The generated QR code still maintains its virtual QR appearance and readability to reduce tamper risk. Only the authorized user with the secret key can retrieve the hidden secret of the QR code. Figure 1 shows the flowchart of the proposed approach, and below that the algorithm is presented.

2.1. Preliminary Process

A QR code is given with data content (such as URL) and the confidential stream. According to QR specification, let E be the number of error correction codewords of the

QR code and B_i be the i -th block of QR code, in which $i = 1, 2, \dots, n$. Based on the error correction propriety of QR codes, this new scheme limits the change amount of QR modules to less than half of E . As a codeword consisting of eight modules, we can calculate the maximum change amount of the QR modules C as

$$C = \lfloor E/2 \rfloor \times 8. \tag{1}$$

Let S be the confidential stream encrypted with the key K . Here, K is the secret key of the system dealer. Then the length of S , l_s , can be determined as follows:

$$l_s = 2 \times C. \tag{2}$$

As shown in Table 1, QR version 3 and error correction level Q can be taken as an example. Using the number of error correction codewords, $E = 36$, we can learn that $C = 144$ and that the length of the confidential stream S is $l_s = 288$.

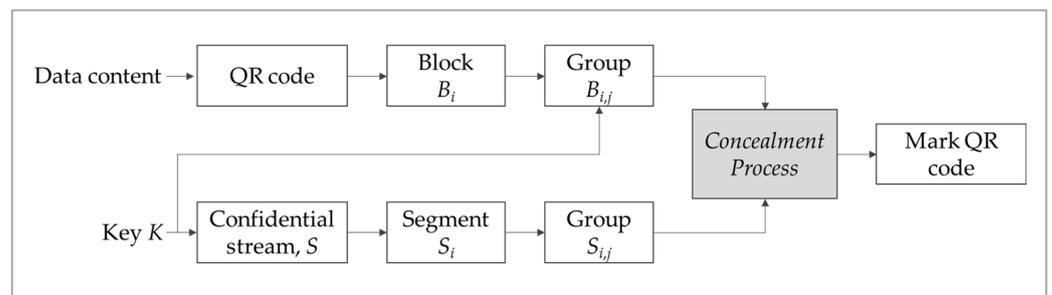


Figure 1. The framework of the proposed QR code approach.

Table 1. The error correction characteristics for QR code version 3.

Error Correction Level	Number of Error Correction Blocks (n)	Total Number of Codewords	Number of Data Codewords	Number of Error Correction Codewords (E)
L	1	70	55	15
M	1	70	44	26
Q	2	70	34	36
H	2	70	26	44

To make S evenly embedded in the QR code, the proposed system firstly divides S into n segments, S_i , where $i = 1, 2, \dots, n$. Hence, each segment S_i has l_s/n bits. Each segment S_i is subsequently divided into groups, in which each group consists of two bits. Assume that group $S_{i,j}$ indicates the j -th group of the i -th segment, for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, C/n$. With the key K , the system can randomly select $3C/n$ modules from the block B_i of the QR code, $i = 1, 2, \dots, n$. The selected modules afterward are divided into groups, in which each group consists of three modules. Assume that group $B_{i,j}$ is the j -th group of the i -th block, for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, C/n$. $B_{i,j} = 0$ means the QR module is white, and $B_{i,j} = 1$ means the QR module is black.

Take QR version 3 and error correction level Q. For example, $C = 144$ and $l_s = 288$. Due to the number of blocks being two ($n = 2$), S is divided into segments S_1 and S_2 . Each segment has $l_s/n = 288/2 = 144$ bits. The 144 bits of each segment can be paired to derive 72 groups. That is, there are $S_{1,1}, S_{1,2}, \dots, S_{1,72}$ for S_1 and $S_{2,1}, S_{2,2}, \dots, S_{2,72}$ for S_2 . On the other hand, the system with the key K can randomly choose $3C/n = 216$ modules from blocks B_1 and B_2 of the QR code. These 216 modules afterward can be divided into $216/3 = 72$ groups, that is, $B_{1,1}, B_{1,2}, \dots, B_{1,72}$ for B_1 and $B_{2,1}, B_{2,2}, \dots, B_{2,72}$ for B_2 .

2.2. Concealment Process

Figure 2 shows the flowchart of the concealment process. The confidential segment $S_{i,j}$ can be embedded into the corresponding QR block $B_{i,j}$ for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, C/n$. Let the bits of $S_{i,j}$ be $\{s_2, s_1\}$ and the modules of $B_{i,j}$ be $\{b_3, b_2, b_1\}$. The difference value, d , can be learned by using $S_{i,j}$ and $B_{i,j}$:

$$d = \sum_{k=1}^2 b_k \oplus s_k. \tag{3}$$

Here, the notation \oplus indicates the exclusive-or (XOR) operator. First, consider the value of b_3 : when $b_3 = 0$, adjust a module according to the following formula:

- Case 1: if $d = 0$, unchanged.
- Case 2: if $d = 1$,
if $b_1 = s_1$, then set the value of $b_2 = s_2$; otherwise $b_1 = s_1$.
- Case 3: if $d = 2$, the $b_3 = 1$.

when $b_3 = 1$, adjust it according to the following formula:

- Case 4: if $d = 0$, the $b_3 = 0$.
- Case 5: if $d = 1$,
if $b_1 = s_1$, then change the value of $b_1 = \bar{s}_1$, otherwise $b_2 = \bar{s}_2$.
- Case 6: if $d = 2$, unchanged.

Repeat the above algorithm to process $S_{i,j}$ and $B_{i,j}$, for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, C/n$. As a result, the designed system can finally generate the marked QR code with private information. It is worth noting that general users can only obtain the data content (such as URL) on the QR code by using familiar barcode readers but will not know the private information hidden in it. Furthermore, QR codes are meaningless images to the human eye. Thus, changing the QR modules does not cause any suspicion to users. Due to the proposed approach modifying the modules within the limit of the error correction capability, the readability of the generated marked QR code can be guaranteed.

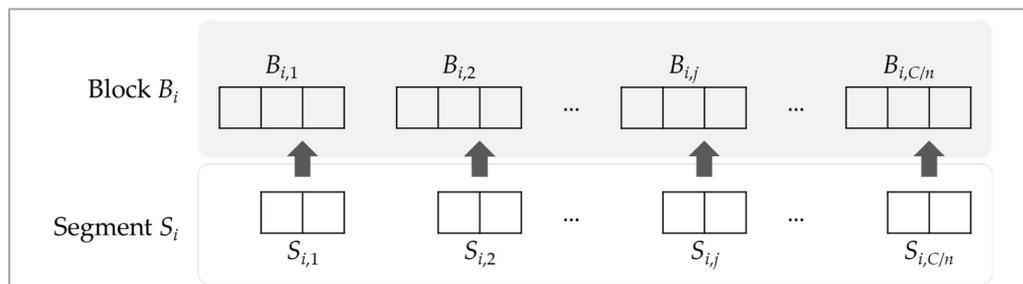


Figure 2. The concealment of segments S_i and the corresponding block B_i .

2.3. Extraction Process

To retrieve the confidential stream, the authorized users with the key K are allowed to further reveal the S from the generated QR code in the following way. According to the QR version and the error correction level, the extraction process can learn the number of error correction codewords E , the number of error correction blocks n , and the values of C and l_s by Equations. (1) and (2).

Firstly, the system can extract the assigned $3C/n$ modules for each QR block, B_i , by using the key K , where $i = 1, 2, \dots, n$. The $3C/n$ modules, afterward, are divided into groups by gathering three modules into one group. Thereby, there are C/n groups for each block B_i . Let $B_{i,j}$ be the j -th group of the i -th block, for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, C/n$. $B_{i,j} = 0$ means the QR module is white, and $B_{i,j} = 1$ means the QR module is black.

Assuming $\{b_3, b_2, b_1\}$ are the QR modules of group $B_{i,j}$, one can extract the corresponding confidential bits $\{s_2, s_1\}$ with the following equation:

$$\begin{aligned} &\text{if } b_3 = 0, \text{ then } s_1 = b_1, s_2 = b_2 \\ &\text{else } s_1 = \overline{b_1}, s_2 = \overline{b_2}. \end{aligned} \quad (4)$$

The results $\{s_2, s_1\}$ are the confidential groups corresponding to $S_{i,j}$. The group $S_{i,j}$ indicates the j -th group of the i -th segment, for $i = 1, 2, \dots, n$ and $j = 1, 2, \dots, C/n$. Repeat all the steps according to the above decoding method and extract all $\{s_2, s_1\}$ from $B_{i,j}$, for $i = 1, 2, \dots, n$, and $j = 1, 2, \dots, C/n$. Finally, the authorized users with the key K can decrypt S and obtain the confidential stream.

3. Experimental Results

The designed concealment QR system can embed confidential information and retain the readability of the generated QR code. In particular, the proposed algorithm takes three modules as a group, and only one module being changed can help hide two bits of confidential information. Therefore, this method can effectively reduce the adjustment to the QR modules, enhance the embedded sensitive information, and retain the error correction capability of the QR code. In the following, the essentials of the confidential capacity, the probability of modified QR modules, and the readability of the generated marked QR code are discussed.

3.1. Capacity

Table 2 shows the payload of the confidential stream under QR code versions 1, 10, 20, 30, and 40. The larger the QR version is, the more QR size and data content there are. There are four error correction levels, L, M, Q, and H, for all QR versions. With a larger level, the value of C is higher as defined in Equation (1). For instance, in QR version 10, C is 288 modules for error correction level L, and C is 896 modules for error correction level H.

Table 2. The capacity of the confidential stream under different QR code versions.

Version	Error Correction Level	C	Confidential Capacity, l_s (bit)
1	L	24	48
	M	40	80
	Q	48	96
	H	64	128
10	L	288	576
	M	520	1040
	Q	768	1536
	H	896	1792
20	L	896	1792
	M	1664	3328
	Q	2400	4800
	H	2800	5600
30	L	1800	3600
	M	3248	6496
	Q	4800	9600
	H	5760	11,520
40	L	3000	6000
	M	5488	10,976
	Q	8160	16,320
	H	9720	19,440

The designed triple module group system can enhance the maximum amount of confidential information to $l_s = 2 \times C$. The last column of Table 2 lists the capacity of confidential information l_s under different QR versions. Since the proposed approach can reduce the changes to the QR modules, it can significantly increase the amount of

embeddable confidential information. Furthermore, it can be observed that increasing the QR version and error correction level can help embed more confidential stream l_s (bits). In QR version 10, the embeddable payload $l_s = 576$ bits when the error correction level is L, and $l_s = 1792$ bits when the error correction level is H. Therefore, the developers can embed more confidential information by increasing the QR code version and error correction level.

3.2. Modification

The notation M in Table 3 indicates the total number of QR modules (except the function pattern modules, the format, and the version information modules). The value of C/M denotes the percentage of maximum changeable modules for QR codes. We can note that the rates are around 10%, 19%, 28%, and 32% for error correction levels L, M, Q, and H, respectively. The modification ratio γ in Table 3 represents the average rate of the changed modules of our generated QR code. We can observe that the values of γ are lower than that of C/M for different QR versions and error correction levels. Here, the theoretical value γ can be calculated as:

$$\gamma = \frac{2}{3}C (\%) \tag{5}$$

Table 3. The average change rates of QR code versions 1, 10, 20, 30, and 40.

Version	QR Modules, M	Error Correction Level	C/M (%)	Modification Ratio, γ (%)
1	208	L	12%	8%
		M	19%	13%
		Q	23%	15%
		H	31%	21%
10	2768	L	10%	7%
		M	19%	13%
		Q	28%	18%
		H	32%	22%
20	8683	L	10%	7%
		M	19%	13%
		Q	28%	18%
		H	32%	21%
30	17,483	L	10%	7%
		M	19%	12%
		Q	27%	18%
		H	33%	22%
40	29,648	L	10%	7%
		M	19%	12%
		Q	28%	18%
		H	33%	22%

In the concealment process, each group B_{ij} will meet one of the conditions from case 1 to case 6. Considering cases 2 to 5, the probability of each group being changed is $2/3$. The other $1/3$ chance is that the original modules remain unchanged in case 1 and case 6. Therefore, the modification ratio γ of the proposed approach can be derived as $2/3C$.

3.3. Readability

Based on the error correction level of QR code specification, if the damaged module is under C/M module changes, the original QR data content can be recovered correctly. As the results in Table 3 demonstrate, the γ values of the designed method are less than the values of C/M under all QR versions and error correction levels. Therefore, it can guarantee that one can correctly decode and reveal the original QR data content (such as URL). Moreover, the readability of the generated marked QR code can reduce the risk of suspicion. Furthermore, the receivers with the key K are authorized to extract the confidential stream of the marked QR code.

3.4. Comparison

The schemes [12,13] transform the QR image into the frequency domain and requires computer assistance. Additionally, the watermark in the frequency domain may encounter capture problems, resulting in incorrect watermark results. Methods [14,15] use the adjustment of the module's height and width to embed the watermark. Their generated barcodes require additional equipment to calculate the module's height and width differences. Moreover, existing barcode scanners cannot directly identify and extract the secrets of their generated barcodes, thus reducing practicality [12–15].

In contrast, the schemes [16,17] and our approach conceal the secrets in QR codes by adjusting the QR modules directly. The computational complexity of the methods [16,17] and our system is lower than the related works [12–15]. Our designed concealment and extraction operations are based on the QR code specifications and can be utilized on mobile applications or scanning devices without additional equipment. A typical scanning device can read the QR modules directly from the generated QR code.

Figure 3 demonstrates the proposed system with the related QR module modification schemes regarding the embeddable capacity of the confidential secrets. The X-axis represents the four error correction levels under different QR versions, and the Y-axis represents the confidential stream (bits) that can be carried. The payload of the confidential stream of Chiang et al.'s method [16] is equal to the maximum changeable QR modules C (as in Equation (2)). For the same QR version, Luo et al.'s scheme [17] can embed more payloads of the confidential stream into the QR code. The embedding capacity of the method presented in [17] is $3/2 \times C$, i.e., 1.5 times that of the method presented in [16].

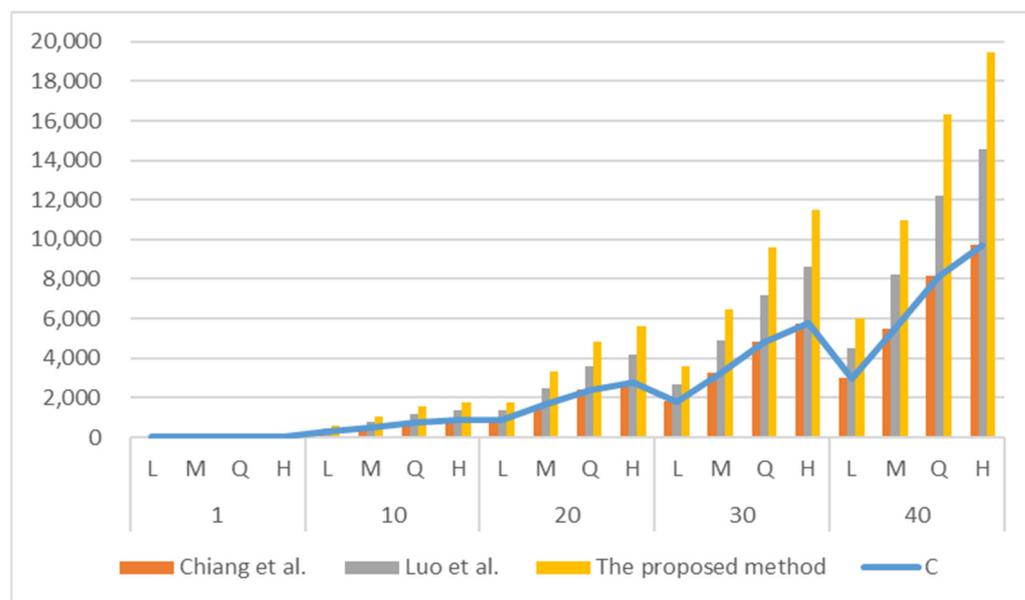


Figure 3. The comparisons of the embeddable payload of confidential stream between the proposed approach and the related schemes.

Our designed triple module group approach can effectively reduce the alteration to the QR modules. Therefore, the proposed method can enhance the embedding capacity of the confidential information to $l_s = 2 \times C$. Figure 3 shows that the embeddable confidential stream of our proposed system is higher than methods [16,17]. In addition, the new system can effectively hide more secrets with larger QR versions and higher error correction levels.

Only an authorized recipient with the key K can further decode and achieve the confidential streams S correctly in terms of security. However, the intruder may use the brute-force attack to infer the contents of S without knowing the key K . We used the brute-force attack to evaluate the security of the related QR methods [16,17] and the proposed system. Table 4 lists the computations required for the brute-force attack in different QR

versions and error correction levels. Since the confidential payloads l_s of methods [16,17] are C and $1.5C$, respectively, the cracking probability ρ is 2^{-C} and $2^{-1.5C}$. On the other hand, the l_s of our proposed method is $2C$, and the cracking probability ρ is 2^{-2C} . Accordingly, the security of the proposed method is higher than that of the methods presented in [16,17] in the brute-force attack. Furthermore, as the QR code version and the error correction level increase, the security also increases.

Table 4. The amount of computation required for the brute-force attack under different QR versions.

Version	Error correction level	Cracking Probability ρ		
		[16]	[17]	Ours
1	L	2^{-24}	2^{-36}	2^{-48}
	M	2^{-40}	2^{-60}	2^{-80}
	Q	2^{-48}	2^{-72}	2^{-96}
	H	2^{-64}	2^{-96}	2^{-128}
10	L	2^{-288}	2^{-432}	2^{-576}
	M	2^{-520}	2^{-780}	2^{-1040}
	Q	2^{-768}	2^{-1152}	2^{-1536}
	H	2^{-896}	2^{-1344}	2^{-1792}
20	L	2^{-896}	2^{-1344}	2^{-1792}
	M	2^{-1664}	2^{-2496}	2^{-3328}
	Q	2^{-2400}	2^{-3600}	2^{-4800}
	H	2^{-2800}	2^{-4200}	2^{-5600}
30	L	2^{-1800}	2^{-2700}	2^{-3600}
	M	2^{-3248}	2^{-4872}	2^{-6496}
	Q	2^{-4800}	2^{-6700}	2^{-9600}
	H	2^{-5760}	2^{-8640}	$2^{-11,520}$
40	L	2^{-3000}	2^{-4500}	2^{-6000}
	M	2^{-5488}	2^{-8232}	$2^{-10,976}$
	Q	2^{-8160}	$2^{-12,240}$	$2^{-16,320}$
	H	2^{-9720}	$2^{-14,580}$	$2^{-19,440}$

According to the results, the designed approach is feasible for embedding a confidential stream into QR codes. The generated QR code can satisfy the requirements of reducing the amount of the modification of QR modules, thus increasing the capacity of the embeddable confidential information, maintaining the readability of the QR data code, and authorizing the users to decrypt and retrieve the confidential information with K .

4. Conclusions

Conveying the confidential information of QR codes has been a significant issue recently. Many mobile devices apply QR codes for mobile payments, e-tickets, e-bonuses, and digital signatures. As a result, the private information needs to be protected from casual scanning. The designed concealment process is based on the error correction capability of QR codes, which can preserve the readability of the generated marked QR code. General users can scan to bring the QR data content to avoid being suspected and maliciously attacked by others. Only authorized users with the secret key can further extract the confidential stream with scanners or mobile applications.

The designed triple module grouping approach conceals two confidential bits by changing only one QR module. Accordingly, the new approach can effectively reduce the alteration of the QR modules and improve the embeddable confidential capacity of a QR code. The confidential payload of the new system is twice the error correction capability of a QR code, which can solve the issue of insufficient private payload, and the performance is better than the related schemes. Moreover, the decoder and extraction operations of the proposed system are based on the QR specification. A usual scanning device can read the QR modules (including the QR data content and the encrypted secret S) directly from the generated QR code. Therefore, the extraction of S is the same as the original

QR operation. However, the new scheme needs to decrypt S . Encryption and decryption can be determined according to system requirements. Here, we can utilize a one-way hash function for encryption and decryption to reduce the time complexity. Therefore, the computational complexity of the designed system is low and can be widely applied on mobile applications or scanning devices. The algorithm can also be practical for various two-dimensional barcodes with error correction capabilities.

Author Contributions: Conceptualization, P.-Y.L. and W.-S.L.; methodology, P.-Y.L. and W.-S.L.; software, Y.-H.C.; validation, Y.-H.C.; formal analysis, W.-C.W.; resources, P.-Y.L.; writing—original draft preparation, P.-Y.L. and W.-S.L.; writing—review and editing, P.-Y.L. and Y.-H.C.; visualization, W.-C.W.; supervision, W.-C.W.; project administration, P.-Y.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Ministry of Science and Technology, Taiwan, under Grant MOST 110-2221-E-992-097-MY3.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: We want to thank Chong-Wen Chen for his full support that helped complete this paper.

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

References

1. Denso Wave. 2003. Available online: <http://www.qrcode.com/en/index.html> (accessed on 15 January 2022).
2. ISO/IEC 18004. *Information Technology Automatic Identification and Data Capture Techniques Bar Code Symbology QR Code*; ISO: Geneva, Switzerland, 2000.
3. Wada, T.; Kishimoto, Y.; Nakazawa, E.; Imai, T.; Suzuki, T.; Arai, K.; Kobayashi, T. Multimodal user interface for QR code based indoor navigation system. In Proceedings of the IEEE 9th Global Conference on Consumer Electronics (GCCE), Kobe, Japan, 13–16 October 2020; pp. 343–344.
4. Xiong, L.; Zhong, X.; Xiong, N.N.; Liu, R.W. QR-3S: A High Payload QR Code Secret Sharing System for Industrial Internet of Things in 6G Networks. *IEEE Trans. Ind. Inform.* **2021**, *17*, 7213–7222. [[CrossRef](#)]
5. Zhou, Y.; Hu, B.; Zhang, Y.; Cai, W. Implementation of Cryptographic Algorithm in Dynamic QR Code Payment System and Its Performance. *IEEE Access* **2021**, *9*, 122362–122372. [[CrossRef](#)]
6. Hung, S.H.; Yao, C.Y.; Fang, Y.J.; Tan, P.; Lee, R.R.; Sheffer, A.; Chu, H.K. Micrography QR code. *IEEE Trans. Vis. Comput. Graph.* **2020**, *26*, 2834–2847. [[CrossRef](#)] [[PubMed](#)]
7. Barron, I.; Yeh, H.J.; Dinesh, K.; Sharma, G. Dual Modulated QR code for Proximal Privacy and Security. *IEEE Trans. Image Processing* **2021**, *30*, 657–669. [[CrossRef](#)] [[PubMed](#)]
8. Lin, P.-Y. Imperceptible visible watermarking base on postcamera histogram operation. *J. Syst. Softw. Arch.* **2014**, *95*, 194–208. [[CrossRef](#)]
9. Lin, P.-Y. Distributed Secret Sharing Approach With Cheater Prevention Based on QR Code. *IEEE Trans. Ind. Inform.* **2016**, *12*, 384–392. [[CrossRef](#)]
10. Puteaux, P.; Puech, W. Rebuttal. On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 2445–2446. [[CrossRef](#)]
11. Puteaux, P.; Puech, W. A Recursive Reversible Data Hiding in Encrypted Images Method with a Very High Payload. *IEEE Trans. Multimed.* **2021**, *23*, 636–650. [[CrossRef](#)]
12. Chung, C.H.; Chen, W.Y.; Tu, C.M. Image Hidden Technique Using QR-Barcode. In Proceedings of the 2009 Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kyoto, Japan, 12–14 September 2009; pp. 522–525.
13. Vongpradhip, S.; Rungraungsilp, S. QR Code Using Invisible Watermarking in Frequency Domain. In Proceedings of the 2011 Ninth International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, 12–13 January 2012; pp. 47–52.
14. Xue, L.Q.; Chao, Y.H.; Liu, L.S.; Zhang, X.J. Information Hiding Algorithm for PDF417 Barcode. In Proceedings of the 2009 Fifth International Conference on Natural Computation, Tianjian, China, 14–16 August 2009.
15. Wu, D.C.; Wu, Y.M. Covert Communication via the QR Code Image by a Data Hiding Technique Based on Module Shape Adjustments. *IEEE Open J. Comput. Soc.* **2020**, *1*, 12–34. [[CrossRef](#)]
16. Chiang, Y.J.; Lin, P.Y.; Wang, R.Z.; Chen, Y.H. Blind QR Code Steganographic Approach Based upon Error Correction Capability. *KSII Trans. Internet Inf. Syst.* **2013**, *7*, 2527–2543.
17. Luo, M.; Wang, S.; Lin, P.Y. QR Code steganography mechanism with high capacity. In Proceedings of the 2016 International Conference on Communication Problem-Solving (ICCP), Taipei, Taiwan, 7–9 September 2016.

-
18. Alajmi, M.; Elashry, I.; El-Sayed, H.S.; Allah, O.S.F. Steganography of Encrypted Messages inside Valid QR code. *IEEE Access* **2020**, *8*, 27861–27873. [[CrossRef](#)]
 19. Mohammed Ali, A.; Farhan, A.K. Enhancement of QR Code Capacity by Encrypted Lossless Compression Technology for Verification of Secure E-Document. *IEEE Access* **2020**, *8*, 27448–27458. [[CrossRef](#)]