Nested image steganography scheme using QR-barcode technique

Wen-Yuan Chen
National Chin-Yi University of Technology
Department of Electronic Engineering
35 Lane 215
Section 1, Chung-Shan Road
Taiping City, Taichung County 411 Taiwan
E-mail: cwy@ncut.edu.tw

Jing-Wein Wang
National Kaohsiung University of Applied Sciences
Institute of Photonics and Communications
415 Chien Kung Road
Kaohsiung 807 Taiwan

Abstract. In this paper, QR bar code and image processing techniques are used to construct a nested steganography scheme. There are two types of secret data (lossless and lossy) embedded into a cover image. The lossless data is text that is first encoded by the QR barcode; its data does not have any distortion when comparing with the extracted data and original data. The lossy data is a kind of image; the face image is suitable for our case. Because the extracted text is lossless, the error correction rate of QR encoding must be carefully designed. We found a 25% error correction rate is suitable for our goal. In image embedding, because it can sustain minor perceptible distortion, we thus adopted the lower nibble byte discard of the face image to reduce the secret data. When the image is extracted, we use a median filter to filter out the noise and obtain a smoother image quality. After simulation, it is evident that our scheme is robust to JPEG attacks. Compared to other steganography schemes, our proposed method has three advantages: (i) the nested scheme is an enhanced security system never previously developed; (ii) our scheme can conceal lossless and lossy secret data into a cover image simultaneously; and (iii) the QR barcode used as secret data can widely extend this method’s application fields.

Subject terms: QR code; steganography; error correction; JPEG; image processing.

Paper 080983R received Dec. 18, 2008; revised manuscript received Mar. 5, 2009; accepted for publication Mar. 18, 2009; published online May 6, 2009.

1 Introduction

The barcode patterns pasted on commodities in supermarkets are European Article Number Barcodes (EAN-13 barcode), also known as international barcodes. They were developed by 12 industrialized countries in Europe in 1977. The barcode has several advantages. It is not as easily worn down as magnetic cards, it has very low rate of error, and it is very cheap and easy to fabricate. Recently, barcodes have become used for the identification of commodities and are massively used in various markets.

The two-dimensional barcode is currently being developed to increase the encoding space. The QR code, Maxicode, Datamatrix code, and pdf417 are widely implemented in daily life. In fact, the QR code has six desirable features: high capacity encoding of data, small printout size, Chinese/Japanese (kanji and kana) capability, dirt and damage resistance, readability from any direction in 360°, and a structure append feature. Specifically, its capacity can encode 7089 numeric characters for numeric data.

As the usage of the Internet becomes extremely popular, online data exchange becomes extremely easy as well. While people gain great benefits through the Internet, they also encounter many serious problems with it. Piracy of private data is one good example. In order to remedy the drawback of data communication through the Internet, many data security techniques have been proposed. However, steganography is a suitable method used for protecting nontext data.

In general, there are two types of data security schemes, i.e., steganography and watermarking. Steganography techniques conceal secret data into a cover image so that other people cannot find it. Liu et al. used a steganalysis technique on the basis of histogram analysis on the wavelet coefficients to detect the very existence of wavelet domain information hiding. In the approach, the secret message was embedded via quantizing wavelet coefficients.

Fig. 1 The pattern of a QR barcode.
Furthermore, by means of histogram analysis of subband wavelet coefficients from stego-images, several statistical discrepancies are obtained. Finally, the discrepancies are passed through fast Fourier transform to generate a quantitative criterion and then used to determine whether a secret message has been embedded. Wang proposed a steganography scheme that used modulus operation to incorporate secret data into a cover image in which half of the size and a quarter of the size of the chosen host-image were used to demonstrate that the secret image can be totally embedded while preserving a high-quality image. Based on an embedded zerotree wavelet compression method and bit-plane complexity segmentation skill, Spaulding et al. proposed a steganography scheme. From his experimental results, it achieved a large embedding capacity of around 255 of the compressed image size with little noticeable degradation in image quality.

Noore et al. present an approach for embedding uncompressed image in a standard pdf417 (2-D barcode) using a blind digital watermarking. The text is encoded in the 2-D barcode with error correction, while the face image is watermarked in the encoded 2-D barcode. In this paper, a 2-D QR barcode (as in Fig. 1) shows a QR barcode from which image-processing techniques were used to construct a nested steganography scheme. Then the QR barcode pattern and a face image serve as the secret data which are embedded into the cover image without degradation of quality. The remainder of this paper is organized as follows: In Section 2, the introduction to the QR barcode is presented. The secret data embedding algorithm is described in Section 3. The secret data extracting algorithm is illustrated in Section 4. Empirical results are presented in Section 5. Section 6 concludes this paper.

2 QR Barcode

2.1 QR Barcode Structure

The QR barcode is a 2-D symbology developed by Denso Wave in 1994. The code contains information in both the x- and y-axis, whereas traditional barcodes contain data in one direction only. The QR barcode therefore stores a considerably greater volume of information than a normal bar code. The main structure of the QR barcode is shown in Fig. 2. The outer range is the quiet zone. The upper-left, upper-right, and left-bottom square areas are used for position detection and pattern separators for positioning. There are

---

**Fig. 2** The structure of QR barcode.

---

Furthermore, by means of histogram analysis of subband wavelet coefficients from stego-images, several statistical discrepancies are obtained. Finally, the discrepancies are passed through fast Fourier transform to generate a quantitative criterion and then used to determine whether a secret message has been embedded. Wang proposed a steganography scheme that used modulus operation to incorporate secret data into a cover image in which half of the size and a quarter of the size of the chosen host-image were used to demonstrate that the secret image can be totally embedded while preserving a high-quality image. Based on an embedded zerotree wavelet compression method and bit-plane complexity segmentation skill, Spaulding et al. proposed a steganography scheme. From his experimental results, it achieved a large embedding capacity of around 255 of the compressed image size with little noticeable degradation in image quality.

Noore et al. present an approach for embedding uncompressed image in a standard pdf417 (2-D barcode) using a blind digital watermarking. The text is encoded in the 2-D barcode with error correction, while the face image is watermarked in the encoded 2-D barcode. In this paper, a 2-D QR barcode (as in Fig. 1) shows a QR barcode from which image-processing techniques were used to construct a nested steganography scheme. Then the QR barcode pattern and a face image serve as the secret data which are embedded into the cover image without degradation of quality. The remainder of this paper is organized as follows: In Section 2, the introduction to the QR barcode is presented. The secret data embedding algorithm is described in Section 3. The secret data extracting algorithm is illustrated in Section 4. Empirical results are presented in Section 5. Section 6 concludes this paper.

2 QR Barcode

2.1 QR Barcode Structure

The QR barcode is a 2-D symbology developed by Denso Wave in 1994. The code contains information in both the x- and y-axis, whereas traditional barcodes contain data in one direction only. The QR barcode therefore stores a considerably greater volume of information than a normal bar code. The main structure of the QR barcode is shown in Fig. 2. The outer range is the quiet zone. The upper-left, upper-right, and left-bottom square areas are used for position detection and pattern separators for positioning. There are

---

**Fig. 3** Hiding text data into barcode: (a) the text data I, (b) generated QR barcode I, (c) the text data II, and (d) the generated QR barcode II.

---

**Fig. 4** A bigger QR barcode pattern: (a) the encoding text and (b) the corresponding QR barcode pattern with size 279×279.

---

**Fig. 5** Flow chart of nested image steganography embedding.

---
### 2.2 QR Barcode Encoding

The QR barcode can be generated by English, Chinese, or Japanese text. The text data shown in Figs. 3(a) and 3(c) are used for input. The generated QR barcode, as Figs. 3(b) and 3(d) show, are the QR encoding output. Because the size of QR barcode is varied by encoding input data, larger text data will generate a larger size QR code. In Fig. 3(b), the size of the QR barcode is 159 × 159 and it is encoding from Fig. 3(a). It is a part of the secret data in our scheme and will be embedded into a cover image. Figure 4 shows a bigger QR barcode pattern. Figure 4(a) is the encoding text, and Fig. 4(b) is the corresponding QR barcode pattern of 279 × 279 size.

### 3 Embedding Algorithm

In the embedding process, the working flow is divided into three parts as Fig. 5 shows. The upper path is the text data encoding flow; it first transfers the text into a 2-D barcode pattern (QR code) and then embeds it into the cover image. The middle path is the face image embedding flow. The lower path is preparing the cover image for secret data embedding. At the beginning, the text data is used generate a QR barcode pattern at the barcode encoding (BCE) stage. Because the QR barcode is a regular format of data blocks, it can be eliminated for decreasing the secret data. Thus, the regular area moving (RAM) is designed for moving the redundancy. For enhancing the security, a chaotic mechanism (CM) provides hashing of the secret data. Furthermore, the dimension reduction (DR) stage is used to map 2-D barcode patterns into 1-D data for convenient secret data embedding. A lower nibble byte discarding (LNBD) stage is used to keep the kernel data of the face image and eliminate the unimportant message. However, the key and a pseudorandom number sequence (PRNS) generator are used to generate the pseudorandom sequences. On the cover image, a discrete cosine transform (DCT) is adopted to convert the image from the spatial domain to frequency domain for robustness. Simultaneously, a block selection (BS) and coefficient selection (CS) are used to hash the order, thereby increasing the security. Once all of these processes have been prepared, the secret bits embedding (SBE) step is used to hide the secret data into the cover image. After all the secret data is embedded, an inverse discrete cosine transform (iDCT) returns the cover image to the spatial domain from the frequency domain. Then the secret data embedding is complete.

#### 3.1 Moving of the QR Barcode’s Regular Area

For the data hiding scheme, the secret data must be a valuable message. Because a barcode has a regular pattern, several areas are useless while it serves as the secret data. The outer range is a useless white pattern and can be deleted. The regular format of the QR pattern shown in Fig. 6(c) is useless and can be removed. In our approach, a RAM stage is implemented to eliminate the useless regions and decrease the secret data. Figure 6 describes which regions are useful or useless in the QR barcode pattern. Figure 6(a) is the original generated barcode pattern; Fig. 6(b) shows the resulting image after discarding the white outer-range area.

---

**Fig. 6** Useful QR barcode pattern: (a) the original generated barcode pattern, (b) the resulting image after discarding the outer range, (c) the useless area of the barcode pattern, and (d) the test pattern that can be used as the secret data.

**Fig. 7** 2-D reduction of a QR barcode to one dimension bit stream.

**Fig. 8** LNBD of an 8-bit grayscale image.

**Fig. 9** Coefficients of the DCT block.
Figure 6(c) shows the regular format area of the barcode pattern. Figure 6(d) displays the test pattern that can be used as the secret data; its size is 15,147 bits.

### 3.2 Chaotic Mechanism

In data hiding, we want the data to be chaotic because chaotic data is not easy to attack. Therefore, it needs a chaotic mechanism to hash the output streams $m_i$. In this paper, a fast pseudorandom number-traversing method is used as the chaotic mechanism to permute the output streams $m_i$. The relation between the bit sequence after permutation and the bit sequence before permutation is presented in the following formulas:

$$m_i(i) = m(i'), \quad 1 \leq i, \quad 1 \leq i' \leq F$$

$$i = \text{permutation}(i'),$$

where $F$ is the length of the bit sequence. The permutation operation is accomplished by using Eq. (1) and the PN$_1$ sequence.

### 3.3 Dimension Reduction of QR Barcode

In secret data embedding, we use a bit replacement technique to embed the secret data into a cover image. Thus, a dimension reduction (DR) of QR barcode is used to convert the secret data from two dimensions into bit streams for convenient secret bit embedding. Figure 7 shows the schematic of a QR barcode pattern from two dimensions being reduced to bit streams. However, having a bit stream is essential for secret bit embedding.

### 3.4 Lower Nibble Byte Discard (LNBD)

For an 8-bit grayscale image, the high nibble byte represents 88% of each pixel’s energy. In other words, the low nibble bytes possess only a little energy and can be omitted without noticeably effecting picture quality. In order to reduce the secret data, we preserve the high nibble byte data and discard the low nibble byte of the face image. After the LNBD, we have a 50% reduction of secret data for the face image. From the simulation results, we find the face image is acceptable under the adopted LNBD strategy. Figure 8 shows the schematic of an LNBD.

### 3.5 Block Selection and Coefficients Selection

DCT is used to transfer the image from the spatial domain into the frequency domain. The coefficients of the DCT block with size $8 \times 8$ are the values corresponding to the DCT basis. In the coefficients of the DCT block as shown in Fig. 8, the upper-left coefficient is the DC value, varies according to the luminance, and is not suitable for bit embedding. Where the coefficients in the upper-left corner are the low-frequency bands, the energy is concentrated and is suitable for secret data concealing. The low-frequency band coefficients marked P1, P2, D1, and D2 of the DCT block in Fig. 9 are suitable for use in our scheme. In our ap-
proach, the locations P1 and P2 are used to conceal the face image. Simultaneously, the locations D1 and D2 are used to embed the QR barcode pattern.

### 3.6 Secret Bit Embedding

There are two types of secret data (text and image) which need to be embedded into a cover image. In our approach, we use the coefficients of the DCT block D1 and D2 for secret text, and P1 and P2 for secret image embedding, respectively. The locations of the D1, D2, P1, and P2 are shown in Fig. 9. In the embedding process, the bit replacement technique is used for secret data concealing. In fact, we select bit 4 and bit 5 of selected DCT coefficients for secret bit replacement. There are two sizes (512×512 and 1024×512) of cover images used for simulation. When the size of the cover image is 512×512, we use two bits (bit 4 and bit 5) from each selected DCT coefficients (D1 and D2) for the placement of secret text (meaning the QR pattern) embedding. P1 and P2 are used for the placement of secret image embedding. When the size of the cover image is 1024×512, only bit 5 of the selected DCT coefficients (D1, D2, P1, and P2) is used for the placement of secret data embedding. Because 1024×512 is exactly twice the size of 512×512, therefore only one bit is needed.

### 4 Extracting Algorithm

In the extracting process, the inverse of the concealing process is used to extract the secret image. A flow chart of the extracting process is shown in Fig. 10. The stego-image $R'$ is transferred to $\hat{R}$ by DCT. The locations are exactly the same as were used in the embedding and were selected by means of the BS, CS, and the $PN_3, PN_4$ sequence with its private key. Once the locations are determined, a bit capture is used to extract the secret data. When the secret bits are all extracted, they are immediately concatenated into two bit sequences $\{m_1^t\}$ and $\{m_2^t\}$ by a rearranging operation. Then $\{m_1^t\}$ is contracted by an inverse chaotic mechanism (ICM). Furthermore, the regular area padding of the extracted QR code is used to reconstruct the complete QR code. Then a QR decoder is used to extract the original text. Additionally, $\{m_2^t\}$ is contracted by ICM. Following execution, low nibble byte padding the recovered face image is obtained. Because the extracted face image includes noise, a median filter is used to filter out the noise and output an acceptable face image. The details of the secret data extracting is described below.

<table>
<thead>
<tr>
<th>JPEG quality</th>
<th>Not compressed</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>QR barcode</td>
<td>Extracted error bits</td>
<td>72</td>
<td>1645</td>
<td>980</td>
<td>655</td>
<td>618</td>
</tr>
<tr>
<td></td>
<td>After error correction</td>
<td>0</td>
<td>36</td>
<td>9</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>100% text decoding</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Face image</td>
<td>Extracted error bits</td>
<td>156</td>
<td>1023</td>
<td>759</td>
<td>501</td>
<td>495</td>
</tr>
</tbody>
</table>
### 4.1 ICM

In the secret data embedding process, a fast pseudorandom number-traversing method is used as the CM to permute the output streams. The relationship between the bit sequence after permutation and the bit sequence before permutation is described by Eqs. (1) and (2). In the secret data extracting, the inverse fast pseudorandom number-traversing method is used as the ICM to repermute the output streams. It is given by Eqs. (3) and (4),

\[
m(i') = m_c(i), \quad 1 \leq i, \quad i' \leq F
\]

\[
i' = \text{permutation}(i), \quad 1 \leq i \leq F
\]

where \( F \) is the length of the bit sequence. The repermutation operation uses Eq. (4) and is associated with the \( PN \) sequence.

#### 4.2 Regular Area Padding of the QR Code

Because the regular area of QR code was not embedded into the cover image, the extracted data lacks that data. Therefore, a regular area padding (RAP) of the QR code stage is needed to fit the format and recover its standard pattern for QR decoding. During the embedding step, we moved away the necessary data of the QR format and outer white area. Therefore, in extracting, we must pad that data. Figure 11 shows the QR barcode extracting and padding procedure. Figure 11(a) denotes the extracted QR barcode data restored into 2-D format in an incomplete state. Figure 11(b) displays the regular area of a QR code which is needed for padding. Figure 11(c) is the resulting image after merging (a) and (b). Finally, Fig. 11(d) shows a complete extracted barcode with outer white area. Its format can be accepted for QR decoding.

#### 4.3 Error Bit Correction of the QR Barcode Pattern by MBC

Since the QR barcode pattern consists of blocks with size \( 3 \times 3 \), we can correct some error bits by the majority bit check (MBC) technique. Figure 12 shows the error correction schematic of the QR barcode by MBC. Figure 12(a) is the extracted pattern I; there are five bits which are 0 (black) and four bits 1 (white). Figure 12(b) illustrates the resulting pattern after MBC is applied to Fig. 12(a); we obtain nine bits with value 0. On the contrary, Fig. 12(c) is the extracted pattern II; there are five bits belonging to white and four bits belonging to black. Applying the MBC to Fig. 12(c), we obtain nine bits belonging to white, as Fig. 12(d) shows.

#### 4.4 Low Nibble Byte Padding of the Face Image

In order to reduce the secret data, we discard the lower nibble byte data of the face image during the embedding process. On the contrary, we need to pad the low nibble

---

**Table 2** The extracted error bits of the stego-image Peppers with PSNR=37.67 under JPEG attacks.

<table>
<thead>
<tr>
<th>JPEG quality</th>
<th>Not compressed</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>QR barcode</td>
<td>Extracted error bits</td>
<td>71</td>
<td>1869</td>
<td>1345</td>
<td>728</td>
<td>931</td>
</tr>
<tr>
<td></td>
<td>After error correction</td>
<td>0</td>
<td>18</td>
<td>0</td>
<td>0</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>100% text decoding</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Face image</td>
<td>Extracted error bits</td>
<td>123</td>
<td>1147</td>
<td>865</td>
<td>725</td>
<td>833</td>
</tr>
</tbody>
</table>

**Table 3** The extracted error bits of the stego-image Baboon with PSNR=38.20 under JPEG attacks.

<table>
<thead>
<tr>
<th>JPEG quality</th>
<th>Not compressed</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>QR barcode</td>
<td>Extracted error bits</td>
<td>101</td>
<td>2106</td>
<td>1574</td>
<td>1076</td>
<td>1276</td>
</tr>
<tr>
<td></td>
<td>After error correction</td>
<td>0</td>
<td>45</td>
<td>9</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>100% text decoding</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Face image</td>
<td>Extracted error bits</td>
<td>122</td>
<td>1195</td>
<td>1010</td>
<td>727</td>
<td>815</td>
</tr>
</tbody>
</table>
byte data in the extracted face image. In our approach, we use the zero padding technique to restore the low nibble byte data of the face image.

4.5 Median Filter

The median filter, a nonlinear spatial filter, is a powerful tool for removing outlying-type noise. It is not suitable for preserving the edges of an image. The filter mask simply defines what pixels must be included in the median calculation. The computation of the median filter starts by ordering those \( n \) pixels defined by the filter mask, in the order from minimum to maximum value of the pixels, as given in Eq. (5),

\[
F_0 \leq F_1 \leq F_2 \cdots \leq F_{n-2} \leq F_{n-1},
\]

where \( F_0 \) denotes the minimum and \( F_{n-1} \) is the maximum value of all the pixels in the filter calculation. The output of the median filter is the median of these values and is given by

\[
F_{\text{med}} = \begin{cases} 
  \frac{F_{n/2} + F_{n/2-1}}{2} & \text{for even } n \\
  F_{n/2} & \text{for odd } n 
\end{cases}
\]

Typically, an odd number of filter elements is chosen to avoid the additional step in averaging the middle two pixels of the order set when the number of elements is even. In this scheme, we select a mask with size \( 3 \times 3 \) used to filter out the noise.

5 Experimental Results

Imperceptibility is an important factor in steganography. In this paper, we employ peak signal to noise ratio (PSNR) to measure the degree of transparency. The PSNR of \( Y \) is given by the following formula:

\[
\text{PSNR} = 10 \log_{10} \left( \frac{255^2}{MSE} \right)
\]

where \( MSE \) is the mean squared error between the original and stego images.

Table 4 The extracted error bits of the stego-image (X-ray of chest) with PSNR=36.39 under JPEG attacks.

<table>
<thead>
<tr>
<th>JPEG quality</th>
<th>Not compressed</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Extracted error bits</td>
<td>35</td>
<td>3167</td>
<td>1551</td>
<td>321</td>
<td>492</td>
</tr>
<tr>
<td>Extracted error bits</td>
<td>0</td>
<td>2025</td>
<td>153</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>QR barcode</td>
<td>After error correction</td>
<td>OK</td>
<td>X</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Face image</td>
<td>100% text decoding</td>
<td>OK</td>
<td>X</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Face image</td>
<td>Extracted error bits</td>
<td>77</td>
<td>255</td>
<td>643</td>
<td>241</td>
<td>393</td>
</tr>
</tbody>
</table>

Fig. 14 The test images: (a) cover image X-ray of hand, (b) stego-image of (a) with PSNR=36.34, (c) cover image X-ray of chest, (d) the stego-image of (c) with PSNR=36.39, (e) cover image X-ray of cranium, and (f) the stego-image of (e) with PSNR=36.21.

Fig. 15 The stego-image X-ray of chest under JPEG attacks: (a1)–(a6) are the extracted QR barcode pattern; (b1)–(b6) are after error correction of (a1)–(a6); (c1)–(c6) are the extracted face image; and (d1)–(d6) are the after median filter of (c1)–(c6).
of error bits to indicate the extracted fidelity.

The extracted error bits of the stego-image sailboat for the embedding image is NCUT logo with PSNR=36.23 under JPEG attacks.

The number of the secret bits is equal to 15,147+64×64 ×4=31,531. The total number of blocks is equal to (512×512)÷(8×8)=4096. Therefore, the number of coefficients of each selected block is four, and each coefficient conceals 2 bits for embedding secret bits.

In order to demonstrate that our scheme can sustain interference on the Internet, we use JPEG compression to attack the stego-image. For example, the stego-image after secret data was concealed into the cover images Lena and Sailboat are PSNR=37.76 and PSNR=37.97, respectively. Table 1 is the extracted error bits of the stego-image F16 with PSNR=37.69 under JPEG attacks. In JPEG attacks, we use several quality degrees (no compression, 8, 9, 10, 11, 12) for simulation. The simulation results are listed in two parts (QR barcode and face image) in Table 1. In the QR barcode we listed three kinds of results: extracted error bits, the error bits after error correction by MBC, and whether it can be fully decoded. According to Table 1, we see that the secret text can obtain perfect recovery under JPEG attacks. Although the extracted face image has noise, we can clearly identify it, as Fig. 13 shows. Likewise, Tables 2 and 3 are the test results of the still images Peppers

\[
\text{PSNR} = 10 \log_{10} \frac{255^2}{\frac{1}{N \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} [X(i,j) - Y(i,j)]^2}.
\]

where \(X(i,j)\) is the grayscale value of the host image \(X\) at point \((i,j)\), and \(Y(i,j)\) is the grayscale value of the stego-image \(Y\) of size \(n \times n\) at point \((i,j)\). We use the number of error bits to indicate the extracted fidelity.

The cover images Lena (512×512), Peppers (512×512), F16 (512×512), Sailboat (512×512), Baboon (512×512), X-ray of hand (1024×512), X-rays of chest (1024×512), and X-ray of cranium (512×512) are used in simulation for demonstrating the performance of the proposed scheme. The texts as shown in Figs. 3(a) and 3(c) were first encoded by the QR barcode with size 159×159, and face images as shown in Figs. 13(d) and 15(d), and Fig. 16(d) with size 64×64 were used as the secret images. The block size used in the simulation was 8×8. The QR barcode pattern size was shrunk to 135×135 first, and then a RAM stage was implemented to eliminate the useless regions and shrink the secret data. Finally, it was converted into a bit stream (15147 bits) by dimensional reduction.

The stego-image sailboat under JPEG attacks: (a1)–(a6) are the extracted QR barcode pattern; (b1)–(b6) are after error correction of (a1)–(b6); (c1)–(c6) are the extracted NCUT logo image; and (d1)–(d6) are the after median filter of (c1)–(c6).

![Fig. 16 The stego-image sailboat under JPEG attacks: (a1)–(a6) are the extracted QR barcode pattern; (b1)–(b6) are after error correction of (a1)–(b6); (c1)–(c6) are the extracted NCUT logo image; and (d1)–(d6) are the after median filter of (c1)–(c6).](image)

Table 5 The extracted error bits of the stego-image sailboat for the embedding image is NCUT logo with PSNR=36.23 under JPEG attacks.

<table>
<thead>
<tr>
<th>JPEG quality</th>
<th>Not compressed</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>QR barcode</td>
<td>Extracted error bits</td>
<td>87</td>
<td>1941</td>
<td>1559</td>
<td>1083</td>
<td>1229</td>
</tr>
<tr>
<td></td>
<td>After error correction</td>
<td>0</td>
<td>36</td>
<td>9</td>
<td>18</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>100% text decoding</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>Face image</td>
<td>Extracted error bits</td>
<td>164</td>
<td>1051</td>
<td>1087</td>
<td>1123</td>
<td>1703</td>
</tr>
</tbody>
</table>

Table 6 Comparison between the state-of-the-art steganalysis method and the proposed method.

<table>
<thead>
<tr>
<th>Item</th>
<th>State-of-the-art steganalysis method</th>
<th>Proposed method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedding capacity</td>
<td>Large</td>
<td>Large</td>
</tr>
<tr>
<td>Can sustain JPEG attacks</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Nested structure</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Include lossless and lossy secret data</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Application range</td>
<td>Median</td>
<td>Wide (because of the 2-D barcode)</td>
</tr>
</tbody>
</table>
pers and Baboon, respectively. Figure 14 shows the test on medical images. Figures 14(a) and 14(b) are the cover image X-ray of a hand and its stego-image with PSNR = 36.34. Figures 14(c) and 14(d) are the cover image X-ray of a chest and its stego-image with PSNR = 36.39. Figures 14(e) and 14(f) are the cover image X-ray of a cranium and its stego-image with PSNR = 36.21. Figure 15 and Table 4 are the test results of the medical images chest X-ray.

In order to demonstrate that the secret image can be any kind of image, we selected the National Chin-Yi University of Technology (NCUT) logo used for simulation. Table 5 shows the simulation results. We see that the secret text can obtain perfect recovery under JPEG attacks. In image testing, the simulation results demonstrate that the effectiveness is the same as when the secret image is a face. Figure 16 shows the detail patterns extracted from the cover image under JPEG attacks. From Fig. 16, we can clearly identify the logo, although the extracted image has a little noise. According to the above experimental results, it is evident that our method is an effective steganography scheme.

Figure 17 shows the curves comparing the number of error bits of the extracted QR barcode pattern under noise-added attacks for the Lena, Sailboat, X-ray of chest, and X-ray of cranium images.

Figure 18 shows the curves comparing the number of error bits of the extracted face image under noise-added attacks for the Lena, Sailboat, X-ray of chest, and X-ray of cranium images.
boat, X-ray of chest, and X-ray of cranium images. From the curves in Fig. 18, the extracted face images are all clearly identified. As Figs. 13 and 15 show, under JPEG techniques to propose a nested steganography scheme. In 2-D barcode that can be used in any field.

application range of the proposed scheme is wider than ods embed only one of the two types at a time. Finally, the simultaneous, but the state-of-the-art steganalysis meth-

ods have large concealing ability. It is likely that the two sys-
tems can sustain JPEG attacks and have high security; how-
ever, there are some different features which exist in the two systems. First, our scheme is a nested structure which is different from the state-of-the-art steganalysis method. Next, our scheme can embed lossless and lossy secret data simultaneously, but the state-of-the-art steganalysis meth-
ods embed only one of the two types at a time. Finally, the application range of the proposed scheme is wider than state-of-the-art steganalysis, because our scheme includes a 2-D barcode that can be used in any field.

6 Conclusions
In this paper, we use QR barcode and image-processing techniques to propose a nested steganography scheme. In our approach, two types of data (text and image) serve as the secret data which are embedded into a cover image. To demonstrate the robustness, JPEG compression is used to attack the stego-image. However, the extracted text data cannot have any distortion compared to the original. Thus, QR encoding and decoding must be carefully designed. In considering extraction error, we use a 25% error correction rate of QR barcode; it has been shown to be suitable for our cases after experimental testing. Because the QR barcode consists of a small $3 \times 3$ block, we use a majority bit check criterion to correct the error bits and obtain an effective result. In image embedding, because it can sustain some distortion, we discard the lower nibble byte of the face image to reduce the secret data. After image extraction, we pad the lower nibble byte and use the median filter to filter out the noise. Results show that we obtain a smoother face image. From the experimental results, it is evident that combining the image-processing techniques and QR barcode can achieve an excellent nested steganography scheme, even when encountering JPEG attacks.

References
7. See (http://www.denso-wave.com/qrcodeqrfeature-e.html).

Wen-Yuan Chen received his BS and MS in Electronic Engineering from National Taiwan University of Science and Technology in 1982 and 1984, respectively, and the Ph.D. degree in Electrical Engineering from National Cheng Kung University in Tainan, Taiwan, in 2003. Since 2007 he has been a professor in the Department of Electronic Engineering at National Chin-Yi University of Technology. His research interests include digital signal processing, image compression, pattern recognition, and watermarking.

Jing-Wein Wang received his BS and MS in Electronic Engineering from National Taiwan University of Science and Technology in 1986 and 1988, respectively, and the PhD degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 1998. From 1992 to 2000, he was a principal project leader at Equipment Design Center of Philips, Taiwan. In 2000 he joined the faculty of National Kaohsiung University of Applied Sciences, where he is currently an associate professor at the Institute of Photonics and Communications. His current research interests are combinatorial optimization, pattern recognition, and wavelets and their applications.