Image Tamper Detection Scheme Using QR Code and DCT Transform Techniques

[1]Ji-Hong Chen and [1]Chin-Hsing Chen

Abatract

This study proposes a QR code technique application in tamper detection. The QR code has error correction, which was used to detect tamper images. This scheme can be applied to evidence tampering detection. The error correction rate of QR code encoding must be carefully designed because the extracted thumbnail of a cover image is lossless. Therefore, the 25% error correction rate was suitable for this paper goal. The original image thumbnail can sustain minor perceptible distortions; thus, the authors used the 25% lower significant bits of the thumbnail image of a cover image to reduce the secret data. The simulation revealed that the authors proposed scheme can detect tampered images easily. The proposed method has two main features: 1. this study uses QR code technique nested architecture, which has the more security of the secret information. 2. the method can quickly detect a tamper image's location.

Keywords: QR code, error correction, tamper detection, watermarking.

1. Introduction

A two-dimensional barcode [1]-[6] is used to increase the encoding space. Two-dimensional barcodes, such as QR code, GS1 DataBar, Data Matrix, PDF417, and MaxiCode, are widely implemented in daily life. QR code [6] has a number of features such as large capacity encoding data, small printout size, dirt and damage resistant, readable from any angle, and structural flexibility of application. QR code can be decoded by a small program in a mobile or computer device with a built-in camera. Therefore, QR code is applied [7] in mobile value-added services such as business card by mobile, production information, commercial advertisement, bus or train tickets, passenger management, and patient identification. In general, QR codes are applied in Japan, Taiwan, Singapore, Hong Kong, China, and South Korea.

Liu et al. [8] proposed a steganography scheme stege-analysis technique based on histogram of wavelet coefficients to detect the existence of wavelet domain information hiding. Liu et al.[9] proposed a novel transform-domain image watermark based on chaotic sequences. In the approach, the secret information is concealed based on wavelet domain. Chen et al. [10] proposed a robust watermarking scheme using phase shift keying modulation with amplitude boost and low amplitude block selection. Chen et al. [11] proposed a steganography scheme based on the differential phase shift keying technique, which is widely used in digital communication systems. A combined QR code [12]-[15] technique with watermarking is also used. Because QR code has error correction feature, so it can watermark an image with more robust ability. The authors propose a tampering detection method combined with QR code and a watermarking technique.

The remainder of this paper is organized as follows: Section 2 presents the basic architecture of QR code; Section 3 presents the transformation of a thumbnail to QR code and the method to conceal it in a cover image; Section 4 presents the detecting tamper image algorithm; Section 5 provides empirical results; and finally, Section 6 offers conclusions.

2. QR Code

Barcodes are readable in optical machine, and are used to extract data from a database about the object to which they are attached. Initially, barcodes represented data by varying the widths and spacing of parallel lines, which may be referred to as linear or one-dimensional. The QR code is a two-dimensional matrix barcode and has a functional error correction to extract secret data. Therefore, in this study, QR code was used by embedding original image thumbnail.

2.1 Architecture of QR Code

The QR code is a matrix type symbol with a cell architecture arranged in the square. The QR code consists of functionality patterns to enable reading of the data area easily in which the data is stored. The QR code architecture as shown in Fig. 1, has position patterns, alignment patterns, timing patterns, quite zone, and data area. The position pattern is arranged at the three corners by a symbol, the position, the size, and the angle of which can be detected. It consists of an architecture that can be detected in all directions. Alignment pattern is highly effective for correcting nonlinear distortions. The central coordinate of the

[1]*Institute of Computer and Communication Engineering National Cheng Kung University*
jihong@ee.ncku.edu.tw; chench@eembox.ee.ncku.edu.tw

alignment pattern will be identified to correct the distortion of the symbol. The timing pattern for identifying the central coordinate of each cell in the QR Code uses black and white patterns that are arranged alternately. It is used for correcting the central coordination of the data cell when the symbol is distorted, or when an error for the cell pitch occurs. The quiet zone enables easy detection of the symbol from the image by the CCD sensor.

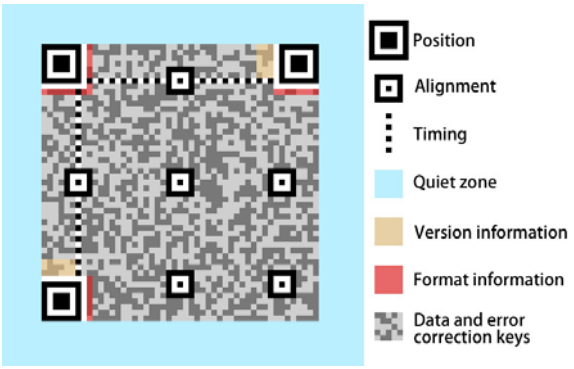


Fig. 1 The QR code architecture.

2.2 QR Code Encoding

In addition to hiding numeric, alphanumeric, and Kanji text (Chinese character used in Japan), the OR code can hide binary data. The QR code encodes without hiding the data, and has error-correcting codes. It uses the Reed-Solomon error correction algorithm with four error correction levels. The four error correction levels are as follows: in level L, 7% of symbol area can be restored; in level M, 15% of symbol area can be restored; in level Q, 25% of symbol area can be restored; and in level H, 30% of symbol area can be restored. Therefore, hiding larger data and choosing high level error correction will generate a larger size QR code. In this study, it hid 32×32 crucial thumbnail image and used level M error correction.

3.Embedding Algorithm

In the embedding process, several skills were used to achieve the goal of what the overall concealing process of embedding algorithm scheme is shown in Fig. 2. The details are described as follows:

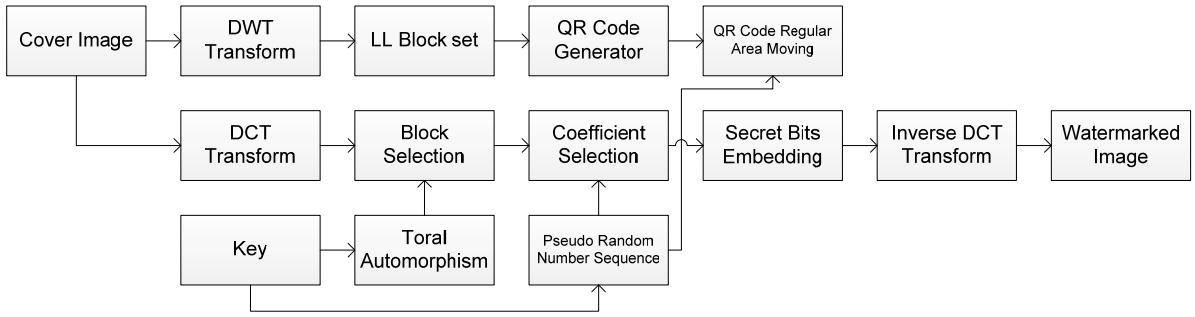


Fig. 2 Flow chart of embedding process

3.1 DWT and Thumbnail Selection

The discrete wavelet transform (DWT) is a useful digital transformation technique. The DWT can identify to a hierarchical sub-band system, in which the sub bands are logarithmically spaced in the frequency. This paper used Daubechies [16] wavelet transform, which decomposes an image into four sub bands LL, HL, LH, and HH. The wavelet transform by following formula:

$$LL[i,j] = \sum_{k_1}\sum_{k_2} h[k_1]h[k_2]a_0[2i-k_1, 2j-k_2] \quad (1)$$

$$LH[i,j] = \sum_{k_1}\sum_{k_2} h[k_1]g[k_2]a_0[2i-k_1, 2j-k_2] \quad (2)$$

$$HL[i,j] = \sum_{k_1}\sum_{k_2} g[k_1]h[k_2]a_0[2i-k_1, 2j-k_2] \quad (3)$$

$$HH[i,j] = \sum_{k_1}\sum_{k_2} g[k_1]g[k_2]a_0[2i-k_1, 2j-k_2] \quad (4)$$

where a_0 is used to decompose the image. The parameter h and g are Daubechies wavelet transform parameter, they represent DWT's low-pass filter and high-pass filter.

The LL band is called multi-resolution approximation, and represents the low frequency band of the image in detail, thus, it was used in wavelet method to compare tampered images. Fig. 3 shows the discrete wavelet transforms architecture.

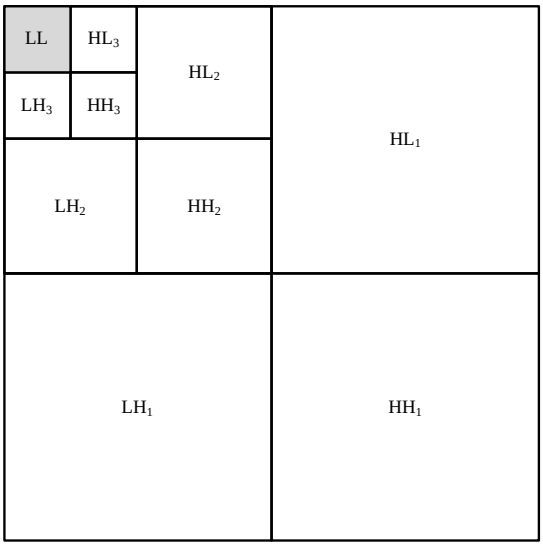


Fig. 3 Pyramidal structure of 3-level wavelet architecture

For an 8-bit grayscale image, the most significant bit (MSB) represents highest energy of the image. In other words, the least significant bit (LSB) has a low energy and can be omitted without noticeably affecting picture quality. To reduce the secret data, it preserved the higher 6 bits, as shown in the gray portion of Fig. 4. Finally, the remaining 75% of secret data was transferred to QR code.

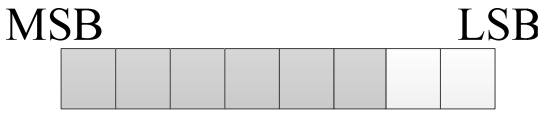
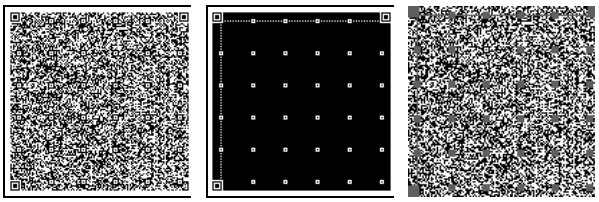


Fig. 4 Lower bits discard.

3.2 Moving of the QR Code's Regular Area

In a data hiding scheme, the secret data must be a valuable message. Because QR code has a regular pattern, several areas are useless when it serves as the secret data. The quiet zone, timing, alignment and position range are useless patterns and can be deleted. The regular format of the QR code pattern as shown Fig. 5 is useless and was deleted. In this method, regular area moving stage was implemented to eliminate the useless regions and decrease the secret data. Fig. 5 describes the regions that are useful or useless in QR code pattern. Fig. 5(a) is original QR code pattern; Fig. 5(b) shows the useless mask area of QR code; Fig. 5(c) displays secret bit of discarded useless area of the QR code.



141×141 133×133 133×133

(a) (b) (c)

Fig. 5 Useful QR code pattern: (a) the original generated QR code pattern, (b) the useless area of QR code pattern, (c) the secret data pattern of QR code.

3.3 Dimension Reduction of QR Code

In secret data embedding, this paper used a bit replacement technique to embed the secret bit into the cover image. Thus, the dimension reduction of QR code was used to convert the secret data from two dimensions into bitstream for convenient secret bit embedding. Fig. 6 shows the schematic of a reduction of QR code pattern from two dimensions to bitstream, which is essential for secret bit embedding.

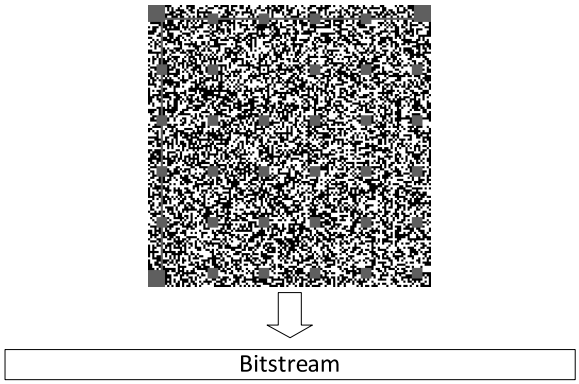


Fig. 6 Two dimensions reduction of QR code to one dimension bitstream

3.4 Toral Automorphism and Block Selection

For security, the secreted block was pre-permuted into noises by toral automorphism [17] with a user's key. Toral automorphism scatter the image shape by iterating operations less than a specified times and returning to the original shape after it has been iterated totally for the specified times. The specified times is determined by the toral automorphism parameters and the image size. In this paper, the toral automorphism is used to transfer the

shape of the original image into chaotic to protect the watermark from being stolen. The transferred functions by following formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\mathrm{mod}\ n) \qquad (5)$$

where (x, y) and (x', y') express the block number locations of the host image, k denotes the control parameter and n denotes the block number, respectively.

3.5 Coefficient Selection

The discrete cosine transform (DCT) was used to transfer the image from the spatial domain into frequency domain. The discrete cosine transform is provided by the following formula:

$$D(p,q) = 1/\sqrt{2n}\,\alpha(p)\alpha(q) \cdot \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} f(m,n)\cos\frac{(2m+1)p\pi}{2M}\cos\frac{(2n+1)q\pi}{2N} \qquad (6)$$

where

$$\alpha(p) = \begin{cases} 1/\sqrt{M}, & p = 0 \\ \sqrt{2/M}, & 1 \le p \le M-1 \end{cases} \qquad (7)$$

$$\alpha(q) = \begin{cases} 1/\sqrt{N}, & q = 0 \\ \sqrt{2/N}, & 1 \le q \le N-1 \end{cases} \qquad (8)$$

where f is original image and D is DCT transferred image. M and N are the row and column size of image f respectively. p, q, m and n are represent image D and image f coordination, respectively.

The coefficients of the DCT block with 8×8 are the values corresponding to the DCT basis. In the coefficients of the DCT block as shown Fig. 7. The upper-left coefficient is the DC value, which varies according to the luminance; the upper-left corner are the low frequency bands, in which the energy is concentrated and it is suitable for secret data concealing. The low frequency band coefficients marked B1, B2, B3, B4, and B5 (only B5 is required to exceed embed capacity) of the DCT block as shown in Fig. 7 are suitable for this paper proposed scheme.

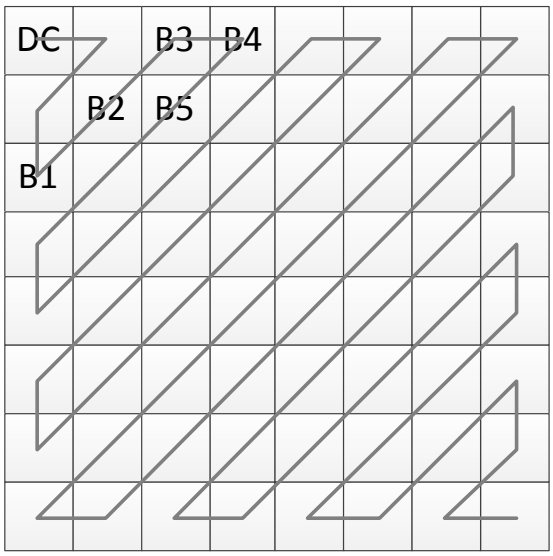


Fig. 7 Coefficients of the DCT block.

3.6 Secret Bit Embedding

In data hiding, secret bit embedding ensured that embedded information was not destroyed and added security; it scrambled the data into a chaotic state. Therefore, a chaotic mechanism is required to hash the bitstream m_s of the QR code. In this study, a fast pseudo random number traversing method was used as a chaotic mechanism to permute the bitstream m_s. The relation between the bit sequence after permutation and the bit sequence before permutation is as follows:

$$m_c(i) = m_s(i'), \quad i \ge 1, i' \le F \qquad (9)$$

$$i = permutation(i') \qquad (10)$$

where F is the length of the bit sequence. The permutation operation was accomplished by using equation (9) and a pseudo random sequence.

The discrete cosine transform was closed to DC value, that energy is most of greater, but the greater energy has seriously destroyed the host image. On the contrary, the DC value alienated was susceptible to interference. Thus, the authors used the coefficients of the DCT block B1, B2, B3, B4, and B5 (only B5 is required to exceed embed capacity) for embedding secret bits. In the embedding process, the bit replacement technique was used for concealing secret data. It selected bit 5 of DCT coefficient for secret bit replacement. There generated bitstream length of 16,478 bits, however, in this paper the DCT coefficient block had 16,384 blocks (only included B1 to B4). Thus, it required 94 blocks (in B5) to embed other secret bits.

4. Tamper Detection Algorithm

The process of a tamper detection algorithm recovers the original image from a watermarked image. Fig. 8 shows the flow chart of the tamper detection algorithm. The details of detection algorithm are described in the following paragraphs.

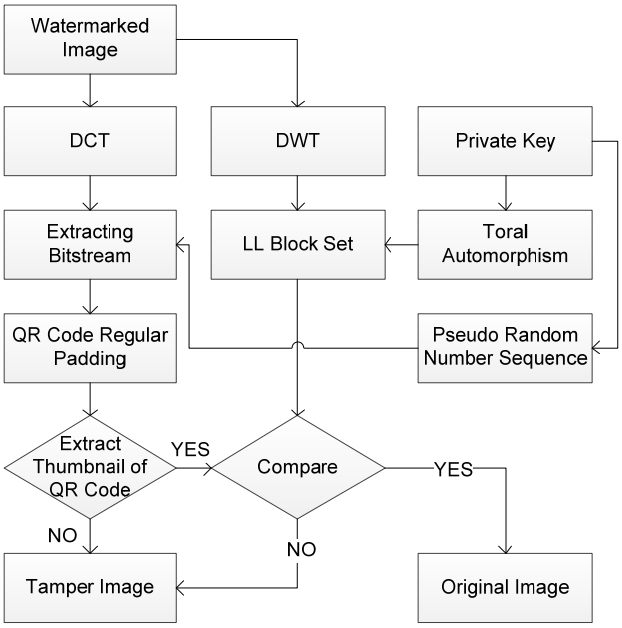


Fig. 8 The flow chart of tamper detection process

4.1 Extract Bitstream and Dimension Recovery

In the secret data embedding process, a fast pseudo random number traversing method was used as the chaotic mechanism for permutation of the bitstream. The relationship between the bit sequence after permutation and the bit sequence before permutation is described by (9) and (10). In the secret data extracting, the inverse fast pseudo random number traversing method was used as the inverse chaotic mechanism to rearrange the bitstream. It was derived by (11) and (12).

$$m_s(i') = m_c(i), \quad i \geq 1, i' \leq F \tag{11}$$

$$i' = permutation(i) \tag{12}$$

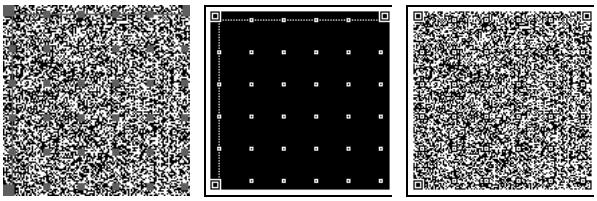
where F is the length of the bit sequence. The rearrangement operation used (12), and associated with the pseudo random sequence.

4.2 Inverse Toral Automorphism

The toral automorphism scatters the image shape into a hashed state, and the inverse toral automorphism returns the chaotic image to the original shape. According to the theory of the toral automorphism, the hashed image will return to its original shape when it is iterated totally by a specified number times. So the hashed image will return to its original shape when the sum of the number of iterations of the embedding process and that of the extracting process equals the specified number.

4.3 Regular Area Padding of the QR code

Because the regular area of QR code was not embedded into the cover image, the extracted data lacked that data. Therefore, a regular area padding of the QR code stage is required to fit the format and to recover its standard pattern for QR decoding. During the embedding step, the data of the QR code format and outer area moved is necessary. In extracting, that data must be padded. Fig. 9(a) shows the extracting QR code data rearranged into two dimension format in an incomplete state. Fig. 9(b) shows the regular area of QR code, which requires padding. Fig. 9(c) shows the image from Fig. 9(a) and (b) after merging.



133×133 133×133 141×141

(a) (b) (c)

Fig. 9 QR code extracting and padding procedure: (a) the extracted QR code rearranged into two dimension in an incomplete state, (b) the regular area of QR code, (c) the resulting image after merging (a) and (b).

4.4 Tamper detection

The working flow in the detection tamper image process is shown in Fig. 10. If QR code cannot extract thumbnail, or if the comparison between the extracted thumbnail and the original image obtains a different result, this indicates that the original image was tampered. This paper used level Q (25% error correction) QR code; which has high error corrections rate and large capacity encoding data.

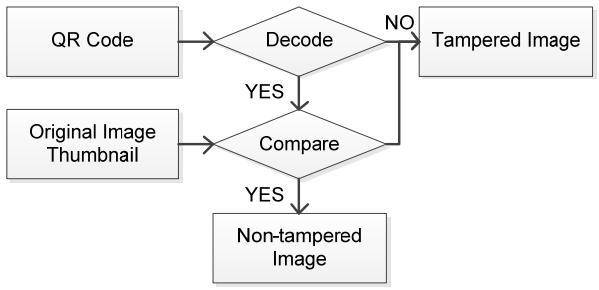


Fig. 10 Tamper detection process.

5. Experimental Results

Imperceptibility is a crucial factor in hiding QR code. The authors used peak signal-to-noise ratio (PSNR) to measure the degree of transparency. The PSNR of a watermarked image is provided by the following formula:

$$PSNR = 10\log_{10}\frac{255^2}{\frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left\|I(i,j)-K(i,j)\right\|^2} \quad (13)$$

where $I(i,j)$ and $K(i,j)$ are the grayscale values of the host image I and watermarked image K of size $n = M \times N$ at point (i,j), respectively. The PSNR is commonly used as a measurement of quality of reconstruction in image compression and watermarking image. Therefore, a quantitative measurement is necessary to provide a fair judgment of the extracted fidelity. Robustness is another crucial factor in watermarking.

In the authors used five cover images in a simulation to demonstrate the performance of the proposed scheme. The test images are shown in Fig. 11(a)-(e); their sizes are 512×512, and their transformation to thumbnail by DWT technique with size 32×32. The grayscale thumbnail images concealed 2 LSB bits, and were encoded by QR code with size 141×141. After removal of the useless area, the number of the secret data bits were equal to 16,478 bits. The DCT coefficient block of cover image has 16,384 blocks ($64\times64\times4$, as shown Fig. 7 B1-B4), and the remaining bits were used in B5. For example, the stego image, after secret data was concealed into the cover images, as shown Fig. 11(f)-(j), were PSNR=39.24, PSNR=39.36, PSNR=39.01, PSNR=39.36, and PSNR=39.41, respectively.

The simulation results are shown Fig. 12. Fig. 12(a)-(e) show tampering in various locations of the stego image. There extracted the QR code, as shown in Fig. 12(f)-(j), and extracted thumbnail in QR code. The QR code concealed secret data was useless, therefore, it can easily compared with cover image (Fig. 11 (f)-(j)). Finally, the marked part of cover image tampering is shown in Fig. 12(k)-(o).

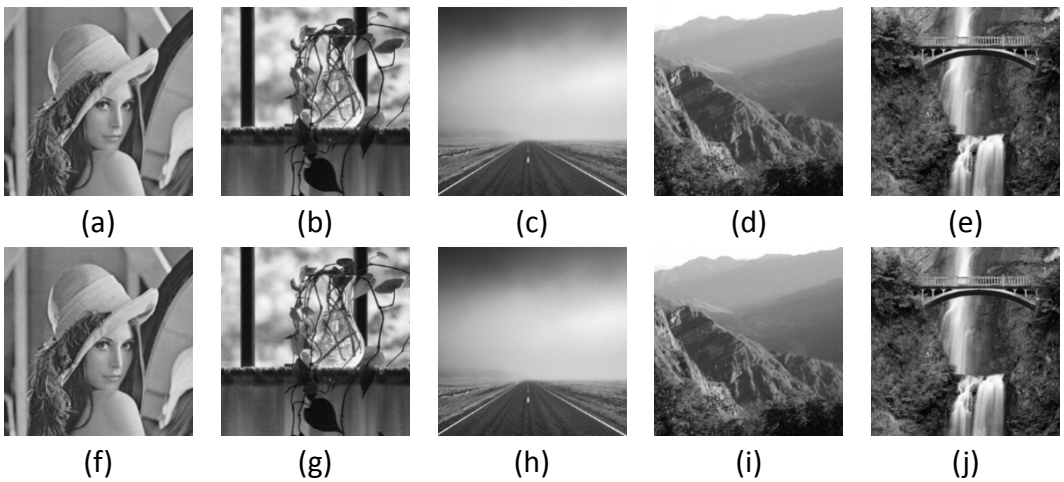


Fig. 11 The test image: (a)-(e) original test image, (f) stego image of (a) with PSNR=39.24, (g) stego image of (b) with PSNR=39.36, (h) stego image of (c) with PSNR=39.01, (i) stego image of (d) with PSNR=39.36, (j) stego image of (e) with PSNR=39.41.

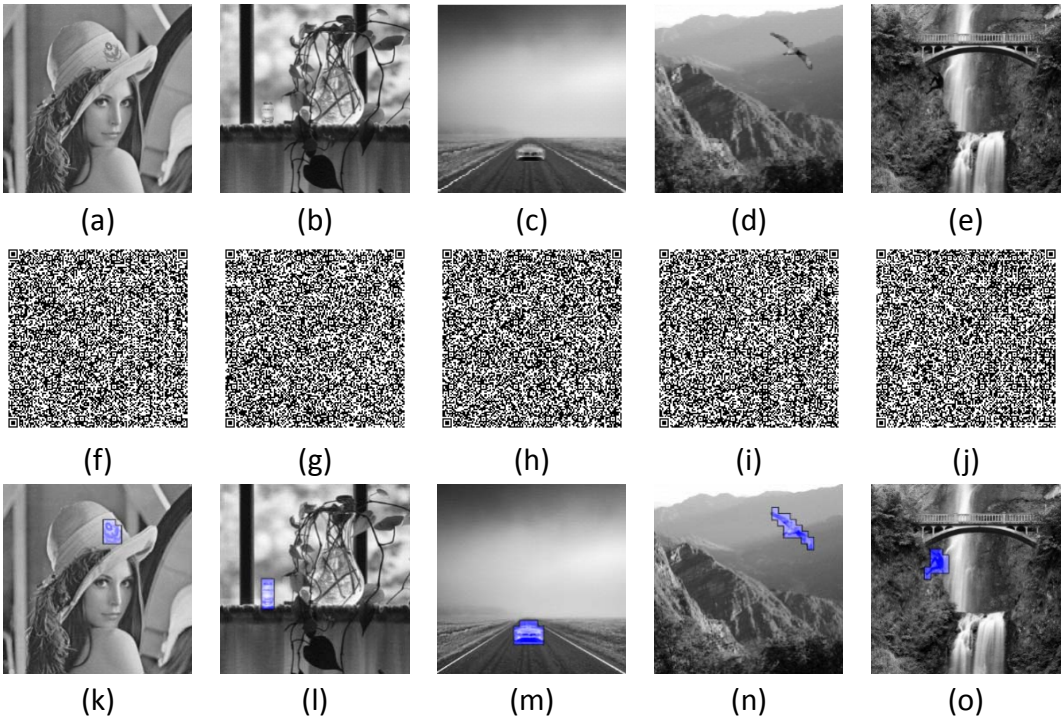


Fig. 12 (a-e) the tamper image of Fig. 11(a-e), (f-j) extract QR code of (a-e), (k-o) selection tamper area

6. Conclusions

This paper propose a tamper detection scheme by using QR code technique. The authors transferred cover image transfer to thumbnail, and subsequently transformed it into the QR code, which reduced the data in the thumbnail. The QR code contained concealed secret information; which there embedded it into the cover image. Finally, the authors used the QR code extracted data to transform to original thumbnail, and used it to compare with watermarked image detection in the tampered image. From the experimental result, combining the QR code technique and watermarking technique can achieve a successful detection tampering scheme.

References

[1] Noore, N. Tungala, and M. M. Houck, "Embedding biometric identifiers in 2D barcode for improved security," *Computer and Security*, vol. 23, pp. 679-686, 2004.

[2] M. Y. Cheng and J. C. Chen, "Integrating barcode and GIS for monitoring construction progress," *Automation in Construction*, vol. 11, pp. 23-33, Jan., 2002

[3] D. E. Gilsinn, G. S. Cheok, and D. P. O'Leary, "Reconstructing images of bar code for construction site object recognition," *Automation in Construction*, vol.13, pp. 21-35, Jan., 2004.

[4] A. Collins, A. Zomorodian, G. Carlsson, and L. J. Guibas, "A barcode shape descriptor for curve point cloud data," *Computer and Graphics*, vol. 28, pp. 881-894, 2004.

[5] T. Y. Liu, T. H. Tan, and Y. L. Chu, "2D barcode and augmented reality supported English learning system," *Conf. on Computer and Information Science, IEEE/ACIS*, vol. 6, pp. 5-10, 2007.

[6] QR-Codes, "Information technology. Automatic identification and data capture techniques. QR code 2005 bar code symbology specification," *ISO/IEC 18004:2006*, ISBN 978-0-580-67368-9, Apr., 2007.

[7] T. W. Kan, C. H. Teng, and W. S. Chou, "Applying QR code in augmented reality applications," *Conf. on Virtual Reality Continuum and Application in Industry*, pp. 253-257, 2009.

[8] S. Liu, H. Yao., and W. Gao, "Steganalysis of data hiding techniques in wavelet domain," *Conf. on Information Technology: Coding and Computing*, pp. 1-4, 2004.

[9] N. S. Liu, G. H. Yang, D. H. Guo, and L. L. Cheng, "A new wavelet watermark scheme of color image based on chaotic sequences," *Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 994-998, 2008.

[10] W. Y. Chen and C.H. Chen, "A robust watermarking scheme using phase shift keying with the combination of amplitude boost and

low amplitude block selection," *Pattern Recognition*, vol. 38, pp. 587-598, 2005.

[11] W. Y. Chen, "Color image steganography scheme using set partitioning in hierarchical trees coding, digital Fourier transform and adaptive phase modulation," *Applied Mathematics and Computation*, vol. 185, pp. 432-448, 2007

[12] W. Y. Chen and J. W. Wang, "Nested image steganography scheme using QR-barcode technique," *Optical Engineering*, vol. 48(5), pp. 057704, May, 2009.

[13] H. Chung, W. Y. Chen, and C. M. Tu, "Image hidden technique using QR-barcode," *Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 522-525, Sep., 2009.

[14] Zigomitros and C. Patsakis, "Cross format embedding of metadata in images using QR codes," *Conf. on Intelligent Interactive Multimedia Systems and Services*, pp. 113-121, Jul. 20-22, 2011.

[15] G. Coatrieux, L. Lecornu, C. Roux, and B. Sankur, "A review of image watermarking application in healthcare," *Conf. on Engineering in Medicine and Biology*, pp. 4691-4, 2006.

[16] Daubechies, "The wavelet transform, time-frequency localization and signal analysis," *IEEE trans. Information Theory*, vol. 36, pp. 961-1005, 1990.

[17] G. Voyatzis and I. Pitas, "Application of Toral Automorphism in Image Watermarking," *IEEE International Conf. on Image processing*, vol. 3, pp, 237-240, 1996.