

http://dx.doi.org/10.12785/amis/080216

Identification Recovery Scheme using Quick Response (QR) Code and Watermarking Technique

Ji-Hong Chen^{1,*}, Wen-Yuan Chen² and Chin-Hsing Chen¹

¹ Institute of Computer and Communication Engineering, National Cheng Kung University, Taiwan
² Department of Electronic Engineering, National Chin Yi University of Technology, Taiwan

Received: 20 Mar. 2013, Revised: 21 Jul. 2013, Accepted: 23 Jul. 2013 Published online: 1 Mar. 2014

Abstract: In recent years there has been increasing attention towards digital rights. Therefore, this paper proposes a matrix barcode to verify image copyrights. The copyright text, Quick Response code (QR code), and watermarking techniques are used to achieve a hidden identification scheme implementing direct sequence spread spectrum (DSSS) and modulation of the modified code division multiple access (MCDMA) to hide the QR code data. DSSS and MCDMA hash the data and QR code has a robust feature to prevent external attacks and destruction of the cover image. The QR codes information can be easily extracted by mobile devices. Even if the barcode suffers external damage, a copy of the barcode can be hidden within the image to easily recover the barcode data. Compare to the other scheme, our method has two advantages: 1) the QR code has universal, rapid identification and fault tolerance features, so it is suitable for copyright protection; and 2) using DSSS and MCDMA methods to hide information can provide more security and fault-tolerant features.

Keywords: QR code, watermarking, direct sequence spread spectrum, modified code division multiple access

1 Introduction

Currently, two-dimensional barcodes [1, 2, 3, 4, 5, 6] are used to increase encoding space. Such two-dimensional barcodes as OR code, GS1 DataBar, Data Matrix, PDF417, and MaxiCode are widely implemented in daily life. The QR code [6] has a number of features, such as large encoding data capacity, small printout size, dirt and damage resistance, readable from any angle, and structural flexibility of application. QR code can be decoded by a small program on a camera-equipped mobile device. Therefore, QR code is applied [7] in mobile value-added services, such as business cards, production information, commercial advertisement, bus or train tickets, passenger management, and patient identification. In general, QR codes are heavily implemented in Japan, Taiwan, Singapore, Hong Kong, China, and South Korea.

Liu et al. [8] proposed a steganography scheme based on the histogram of wavelet coefficients to detect the existence of wavelet domain information hiding. Liu et al. [9] introduced a novel transform-domain image watermark based on chaotic sequences. In the approach, the secret information is concealed based on the wavelet domain. Chen et al. [10] proposed a robust watermarking scheme using phase shift key modulation with amplitude boost and low amplitude block selection. Chen et al. [11] developed a steganography scheme based on the differential phase shift key technique, which is widely used in digital communication systems.

Teng [12] focused on the widely-used 2D barcode to implement a QR code based augmented reality (AR) system. Huang et al. [13] established a system for mobile cameras to capture QR codes from websites so a hyperlink corresponding to the QR code can be accessed instantly. Munoz-Mejias et al. [14] applied a complete preprocessing system for restoring low-quality QR code images. A combined QR code [15, 16, 17, 18] technique with watermarking has also been used. Because QR code has an error correction feature, it can watermark an image with further robustness. This paper proposes a tampering detection method combining QR code and watermarking techniques.

Due to QR code has error correction features and its wide used to everywhere of human life. So that, we apply it associate to the watermarking scheme to enhance the

^{*} Corresponding author e-mail: jihong@ee.ncku.edu.tw



Fig. 1: Embedding watermark process.



Fig. 2: QR code architecture.

security and convenience. This is difference from the general watermarking scheme didnt have the QR code convenience simultaneously. Therefore, we study this topics in this paper. The remainder of this paper is organized as follows: Section 2 presents the secret data embedding process; Section 3 presents detection and recovery processing; Section 4 provides empirical results; and finally, Section 5 offers conclusions and suggestions for further research.

2 Secret data embedding

The watermark embedding process involves several steps. Fig. 1 shows the overall concealing process of the proposed scheme. First, the text label is transformed to QR code; one is printed on the image as a visible watermark and the other as a secret watermark. To reduce the number of embedded secret bits, the invisible watermarks regular QR code area must be removed and important area saved. This paper used direct sequence spread spectrum and modulation of code division multiple access methods to encode secret bits to substantially increase error correction. For security, a private key is used to generate pseudo random number sequences (PRNS) PN_1 and PN_2 . PN_1 is used in DSSS generation so



Fig. 4: The schematic of the CDMA modulator.

that the secret bit sequence becomes more complex. PN_2 is used in the embedded blocks selection using two random variables making hidden information more difficult to tamper with. Therefore, this paper used text label transform to QR code and combined the DSSS and MCDMA methods to increase readability and security.

Table 1: The truth table of the MCDMA modulation.

	Input			Output				
m_a	m_b	m_c	\tilde{m}_a	\tilde{m}_b	\tilde{m}_c	\tilde{m}_d	\tilde{m}_e	
0	0	0	0	0	0	1	1	
0	0	1	0	0	1	1	0	
0	1	0	0	1	0	0	0	
0	1	1	0	1	1	0	1	
1	0	0	1	0	0	0	1	
1	0	1	1	0	1	0	0	
1	1	0	1	1	0	1	0	
1	1	1	1	1	1	1	1	

586

E N





Fig. 3: Remove regular area of QR code: (a) Original QR code; (b) Excess regular area; and (c) QR code important data area.



Fig. 6: Detection QR code process.

 \tilde{m}_a

 \tilde{m}_b

m,

m,



 \tilde{m}_{e} — m_{e}'

MCDMA

Demodulation

Fig. 7: The schematic of the modified CDMA demodulator.

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 error

correction to extract secret data.

Fig. 5: Coefficient corresponding to DCT blocks.

2.1 Architecture of QR code

Barcodes are optical machine readable and are used to extract data from a database about the object to which m'a

m



Fig. 8: QR code extracting and padding procedure: (a) The extracted QR code rearranged into two dimensions in an incomplete state; (b) The regular area of the QR code; and (c) The resulting image after merging (a) and (b).

The QR code is a matrix type symbol with a cell architecture arranged in a square. It consists of functionality patterns to enable easy reading of the data area in which the data is stored. The QR code architecture, as shown in Fig. 2, includes position patterns, alignment patterns, timing patterns, data area, and a quite zone. The position pattern is arranged at the three corners by a symbol, the position, size, and angle of which can be detected. It consists of an architecture that can be detected in all directions. The alignment pattern is highly effective for correcting nonlinear distortions. The central coordinate of the alignment pattern will be identified to correct symbol distortion. The timing pattern for identifying the central coordinate of each cell in the OR code uses black and white patterns that are arranged alternately. It is used for correcting the central coordinate 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.

2.2 Removed regular area of the QR code

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. Fig. 3 shows the regions that are useful or useless in QR code pattern. Fig. 3(a) is original QR code pattern. The quiet zone, timing, alignment and position range are non-message containing patterns and can be deleted, as shown in Fig. 3(b). A regular area moving stage was used to eliminate the useless regions and decrease the secret data. Fig. 3(c) displays the remaining significant data after the useless areas have been discarded.

For secret data embedding, this paper used a bit replacement technique to embed the secret bits into the cover image. Thus, dimension reduction of the QR code was used to convert the secret data from two dimensions into a bitstream for convenient secret bit embedding.

Table 2: The trut	n table of the MCI	DMA demodulation.
-------------------	--------------------	-------------------

	Input				(Output		
\tilde{m}_a	\tilde{m}_b	\tilde{m}_c	\tilde{m}_d	\tilde{m}_e	m'_a	$m_{b}^{\tilde{l}}$	m_c'	
0	0	0	0	0	0	1	0	
0	0	0	0	1	0	0	0	
0	0	0	1	0	0	0	0	
0	0	0	1	1	0	0	0	
0	0	1	0	0	0	0	1	
0	0	1	0	1	0	1	1	
0	0	1	1	0	0	0	1	
0	0	1	1	1	0	0	1	
0	1	0	0	0	0	1	0	
0	1	0	0	1	0	1	0	
0	1	0	1	0	0	1	0	
0	1	0	1	1	0	0	0	
0	1	1	0	0	0	1	0	
0	1	1	0	1	0	1	1	
0	1	1	1	0	0	0	1	
0	1	1	1	1	0	1	1	
1	0	0	0	0	1	0	0	
1	0	0	0	1	1	0	0	
1	0	0	1	0	1	1	0	
1	0	0	1	1	1	0	0	
1	0	1	0	0	1	0	1	
1	0	1	0	1	1	0	1	
1	0	1	1	0	0	0	1	
1	0	1	1	1	1	0	1	
1	1	0	0	0	1	1	0	
1	1	0	0	1	1	0	0	
1	1	0	1	0	1	1	0	
1	1	0	1	1	1	1	0	
1	1	1	0	0	1	1	1	
1	1	1	0	1	1	1	1	
1	1	1	1	0	1	1	1	
1	1	1	1	1	1	1	1	



Fig. 9: Recovery QR code label process.

Table 3: Performance comparison between Huangs method and proposed method.

Item	Huang's method	Proposed method		
Туре	Data hiding	Robust watermarking		
Using QR code	Yes	Yes		
Attacks testing	No	Yes		
Working domain	Spatial domain	Frequency domain		
Security ability	-	Private Key		
PSNR	22.81 dB	39.91 dB		

2.3 Direct sequence spread spectrum

Direct sequence spread spectrum (DSSS) is widely used to eliminate noise in many fields, especially in communication systems. The watermark must survive when the embedded host image encounters attacks. In this paper, we used the spread spectrum technique to enhance the robustness of the watermarking scheme. The spread spectrum expands information bit into several bits. The expanded bits are created by random values when the information bit is positive logic high. On the other hand, the expanded bits are created by the inverse of random values when the information bit is positive logic low. To randomize the expanded bits, PN sequences are used to accomplish the job. By raster scanning, post-removal regular area of the QR code is converted into a bit sequence d(j), $j = 1, 2, \dots, m$. For each d(j), we generate a pseudo random number sequence $r_i(i)$, $i = 1, 2, \dots, n$. Multiplying by $d(j), r_j(i)$ a watermark bearing bit is chopped up into chips. The expanded bit sequence is given by

$$m_j(i) = d(j)r_j(i), j = 1, 2, \cdots, m, i = 1, 2, \cdots, n,$$
 (1)

2.4 Modulation of the modified code division multiple access

The code division multiple access (CDMA) technique combines many signal bits into a code, and then transmits

the code to the receivers terminal. In the process, each signal bit is first expanded into several bits by spread spectrum to enhance security. On the other hand, each receiver uses the CDMA demodulation to extract his or her own data from the received message. In this paper, we use modified code division multiple access (MCDMA) modulation to combine the bit sequence of the three watermarks into a MCDMA code. Fig. 4 shows the schematic of the MCDMA modulator and Table 1 is its corresponding truth table. In the MCDMA, the bits of the each MCDMA code \tilde{m}_a , \tilde{m}_b , \tilde{m}_c are equal to the signal bits m_a , m_b , m_c , respectively. The bit \tilde{m}_d is the logical XNOR operator value of the signal bits m_a and m_b , and \tilde{m}_e is the logical XNOR operator value of the signal bits m_b and m_c . In this encoding rule, we can obtain a better decoding code. For example, extracted code = 00000 corresponding to the demodulation code = 010. Because, compare the code 00000 with the code of the Table 1, we found out the code = 01000 only one bit error, so its easily to decide the demodulation code = 010 (as the Table 2 shows).

2.5 DCT and Block selection

Taking the discrete cosine transform (DCT), an image is transformed from the spatial to the frequency domain. The DCT can be expressed as

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

where

$$\alpha(p) = \begin{cases} 1/\sqrt{M}, & p = 0\\ \sqrt{2/M}, & 1 \le p \le M - 1 \end{cases},$$
(3)

$$\alpha(q) = \begin{cases} 1/\sqrt{N} , & q = 0\\ \sqrt{2/N} , & 1 \le q \le N - 1 \end{cases},$$
(4)

where f denotes the original image and D is the DCT-transferred image, M and N are the row and column sizes of the image f, respectively, and the terms p, q, m, and n represent the images D and f coordinates, respectively.

In order to increase the security of the DCT blocks, we adopt pseudo random number sequence PN_2 to hash the original DCT blocks order. The hash function shows in Eq. (5)

$$B_{s}(i) = B_{o}(PN_{2}), \{i, PN_{2}\} = 1, 2, \cdots, F,$$
(5)

where B_o is original DCT blocks, $B_s(i)$ is hashed DCT blocks, and F is the length of the PN_2 sequences.

The proposal adopts a host image of 8×8 blocks whose coefficients are the values corresponding to the DCT basis. As illustrated in Fig. 5, the coefficient located





Fig. 10: Cardiac x-ray image: (a) The original cardiac x-ray image with embedded visible and invisible watermarks; (b) The horizontally-clipped original image; (c) The vertically-cropped original image; (d) The visible watermark of (a); (e) The invisible watermark extracted from (b); and (f) The invisible watermark extracted from (c).

at the upper-left corner is the DC value, which is affected by the luminance, while those marked as B1-B3 in the vicinity of the DC value are the low-frequency components, over which the energy is concentrated, and are suitable for concealing secret data in this work.

3 Detection and recovery processing

Fig. 6 is the flow chart of the QR code detection processing. First, a private key is used to generate PRNS PN_1 and PN_2 . PN_2 is used to select blocks from the post-DCT-process watermarked image. Then the demodulation of the MCDMA and inverse direct sequence spread spectrum were used to recover the QR code from the bitstream extracted from the blocks selected.

3.1 Demodulation of the modified code division multiple access

The flow chart of CDMA demodulation is shown in Fig. 7. The demodulation first mixes the extracted secret bits $(\tilde{m}_a, \tilde{m}_b, \tilde{m}_c, \tilde{m}_d, \tilde{m}_e)$ and then outputs the signal bits (m'_a, m'_b, m'_c) . Table 2 shows the truth table of the CDMA demodulation. In the CDMA demodulation, the error correction function is included by means of the arrangement of its truth table.

3.2 Inverse direct sequence spread spectrum

Since the spread spectrum expands the watermark bits before embedding, they will be contracted by inverse spread spectrum before recovery. $r_j(i)$ is generated by pseudo random number, with each bit d'(j) obtained from contracting the expanded sequences $m'_j(i)$. The value of d'(j) is obtained by

$$d'(j) = \begin{cases} 1, if \sum_{i}^{l} m'_{j}(i) \oplus r_{j}(i) < \frac{1}{2} \\ 0, if \sum_{i}^{l} m'_{j}(i) \oplus r_{j}(i) \geq \frac{1}{2} \end{cases} j = 1, 2, \cdots, n, \quad (6)$$

3.3 Regular area padding of the QR code

During the embedding process, the unnecessary data of the QR code format and outer area were removed. Therefore, a regular area padding of the QR code stage is needed to achieve the standard form for QR decoding. Fig. 8(a) is the extracted QR code data rearranged into two-dimensional format in an incomplete state. Fig. 8(b) shows the regular area of the QR code required for padding. Fig. 8(c) displays the merged image of Figs. 8(a) and (b).

3.4 Watermark verification processing

The visible watermark can be inquiry information or declaration of copyright. Because it is always visible, it is





Fig. 11: Pleural x-ray image: (a) The original pleural x-ray image with embedded visible and invisible watermarks; (b) The blackened out QR code of the original image; (c) The horizontally-clipped original image; (d) The visible watermark of (a); (e) The invisible watermark extracted from (b); and (f) The invisible watermark extracted from (c).



Fig. 12: Brain MR image: (a) The original brain MR image with embedded visible and invisible watermarks; (b) The blocked out QR code of the original image; (c) The stained QR code of the original image; (d) The visible watermark of (a); (e) The invisible watermark extracted from (b); and (f) The invisible watermark extracted from (c).

vulnerable to external attacks or tampering. Therefore, this paper proposed a scheme to hide another invisible watermark in the cover image. The flow chart of the watermark verification processing is shows in Fig. 9. Initially, the visible QR code decoded the original text label and extracted the hidden watermark from the cover image. If the visible QR code and extracted hidden QR code data are different, then recovery of the visible QR code takes place.

4 Simulation results

In this paper, several simulation images were used to demonstrate the performance of the proposed scheme. The test cover images are 512×512 pixels and the QR code label size is 45×45 pixels. Figures 10-12 are digitized medical images. Fig. 10(a) is a cardiac x-ray film, Fig. 11(a) is a pleural x-ray film, and Fig. 12(a) is a brain MR image. In each, the QR codes (d)-(f) correspond



Fig. 13: French painter Perrine Vilmot artwork: (a) The original artwork image with embedded visible and invisible watermarks; (b) The filled white block on QR code of the original image; (c) The blurred QR code of the original image; (d) The visible watermark of (a); (e) The invisible watermark extracted from (b); and (f) The invisible watermark extracted from (c).



Fig. 14: Chinese artwork: (a) The original artwork image with embedded visible and invisible watermarks; (b) The damaged QR code of the original image; (c) The stain QR code of the original image; (d) The visible watermark on (a); (e) The invisible watermark extracted from (b); and (f) The invisible watermark extracted from (c).

to images (a)-(c), respectively. The unaltered QR code is visible in the bottom-right-hand corner of (a) in each Figure. With this papers proposed scheme, the embedded visible and invisible QR code labels can be extracted and recovered when the visible QR code is removed, blackened or whitened out, or when cropping occurs. Seen from the above experiments, this scheme can be effectively applied by hospitals to store and secure digital medical images.

Fig. 13 is a French artists artwork. It has the same embedded visible and invisible watermarks as those from Figs. 10-12. An artist or publishing company can embed important text within their artworks QR code, such as the authors name, copyright, company, or contact





Fig. 15: Japanese artwork: (a) The original artwork image embedded visible and invisible watermarks; (b) The digital pen attacked QR code area of the original image; (c) The stained QR code of the original image; (d) The visible watermark of (a); (e) The invisible watermark extracted from (b); and (f) The invisible watermark extracted from (c).



Fig. 16: The error bits of the recovered watermark under JPEG attacks for the Lena and the Baboon.

information, etc. Viewers can use a mobile QR code reader to readily scan the visible watermark on the artwork to get such information. Similarly, Fig. 14 is a Chinese ink painting and Fig. 15 is a Japanese ink painting. These types of artwork usually have the artist's seal. This papers proposed method uses the DSSS and embedded block selection hashed technique to copyright data more securely. Therefore, the visible watermark can provide viewer inquiry information and the invisible watermark can reinstate the crucial copyright data more securely, even after deliberate attacks.

In order to demonstrate our scheme can suffer all kind of the attacks, several experiments are used to hit the goal. Fig. 16 shows the number of error bits of the recovered watermark under JPEG attacks for the Lena and the Baboon. The results shows the extracting QR code and secret text are all correct on the JPEG attacks. On the other hand, the results of the simulation of the attacks show in Fig. 17. Where Fig. 17(a) shows the 90



Fig. 17: The attacked watermarked image: (a) the 90 degree rotation attack, (b) the cropped attack, (c) the painted attack, (d) the noised attack.



Fig. 18: PSNR comparison between Huangs method and proposed method: (a) the watermarked Lena image by Huangs algorithm with a PSNR of 22.81 dB, (b) the watermarked Lena image by the proposed method with a PSNR of 39.91 dB.

degree rotation attack, Fig. 17(b) shows the cropped attack, Fig. 17(c) shows the painted attack, finally Fig. 17(d) display the noised attack. The extracted secret data show in Figs. 17(e)-(h) are the extracted error bits, error bit ratio, and percentage of the recovered corresponding to Figs. 17(a)-(d), respectively.

Fig. 18 shows PSNR comparison between Huangs [13] and our proposed method. Fig 18(a) is the watermarked Lena image by Huangs algorithm with a PSNR of 22.81 dB and Fig. 18(b) is the watermarked

Lena image by the proposed method with a PSNR of 39.91 dB. It is obviously our method have better quality on watermarked image. Besides, the performance comparison between Huangs method and proposed method is listed in Table 3. From the table 3, we can see that the two methods are using QR code to embed secret data. However, there something difference between two methods, like the watermarking type one is data hiding the other is robust watermarking, one is no attacks testing the other accept attacks testing, one is working on spatial



domain the other is frequency domain. From the Table 3 it shows our method is superior.

5 Conclusion

In this study, we divided the QR code into two parts, visible and invisible, and then embedded them into cover images. The visible part can directly provide users with related information; the invisible watermark can protect copyright information and reinstate the visible QR code. The QR code is universal and has fault tolerance, and is thus suitable for use as data marking and hidden information embedding. After simulation, the DSSS and MCDMA communication techniques are demonstrated, increasing watermark error correction capability and securing hidden information. Simulation results show strong evidence that this scheme is an effective identification and data correction scheme.

Acknowledgement

This work was partly supported by the National Science Council, Taiwan (R.O.C.) under contract NSC 100-2221-E-167-032.

References

- A. Noore, N. Tungala and M. M. Houck, Embedding biometric identifiers in 2D barcode for improved security, Computer and Security, 23, 679-686 (2004).
- [2] M. Y. Cheng and J. C. Chen, Integrating barcode and GIS for monitoring construction progress, Automation in Construction, 11, 23-33 (2002).
- [3] D. E. Gilsinn, G. S. Cheok and D. P. OLeary, Reconstructing images of bar code for construction site object recognition, Automation in Construction, 13, 21-35 (2004).
- [4] A. Collins, A. Zomorodian, G. Carlsson and L. J. Guibas, A barcode shape descriptor for curve point cloud data, Computer and Graphics, 28, 881-894 (2004).
- [5] T. Y. Liu, T. H. Tan and Y. L. Chu, 2D barcode and augmented reality supported English learning system, IEEE Conference on Computer and Information Science, 6, 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, (2007).
- [7] T. W. Kan, C. H. Teng and W. S. Chou, Applying QR code in augmented reality applications, Conference on Virtual Reality Continuum and Application in Industry, 253-257 (2009).
- [8] S. Liu, H. Yao and W. Gao, Steganalysis of data hiding techniques in wavelet domain, Conference on Information Technology: Coding and Computing, 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, Conference on Intelligent Information Hiding and Multimedia Signal Processing, 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, 38, 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, 185, 432-448 (2007).
- [12] C. H. Teng, Developing QR code based augmented reality using SIFT features, Conference on This paper appears in: Ubiquitous Intelligence & Computing and Autonomic & Trusted Computing (UIC/ATC), 985-990 (2012).
- [13] H. C. Huang, F. C. Chang and W. C. Fang, Reversible data hiding with histogram-based difference expansion for QR code applications, IEEE Ttransactions on Consumer Electronics, 57, 779-787 (2011).
- [14] D. Munoz-Mejias, I. Gonzalez-Diaz and F. Diaz-de-Maria, A low-complexity pre-processing system for restoring lowquality QR code images, IEEE Ttransactions on Consumer Electronics, 57, 1320-1328 (2011).
- [15] W. Y. Chen and J. W. Wang, Nested image steganography scheme using QR-barcode technique, Optical Engineering, 48, 057704 (2009).
- [16] H. Chung, W. Y. Chen and C. M. Tu, Image hidden technique using QR-barcode, Conference on Intelligent Information Hiding and Multimedia Signal Processing, 522-525 (2009).
- [17] A. Zigomitros and C. Patsakis, Cross format embedding of metadata in images using QR codes, Conference on Intelligent Interactive Multimedia Systems and Services, 113-121 (2011).
- [18] G. Coatrieux, L. Lecornu, C. Roux, and B. Sankur, A review of image watermarking application in healthcare, Conference on Engineering in Medicine and Biology, 4691-4 (2006).





Ji-Hong Chen received his BS degree in Electrical Engineering from Southern Taiwan University in 2001, the MS degree in Institute of Information and Electrical Energy from National Chin Yi University of Technology in 2004, and the Ph.D. degree in Institute of Computer and Communication Engineering

from National Cheng Kung University in Taiwan in 2013. His research interest include digital image pressing, digital watermarking and tampered image recover.



Wen-Yuan Chen Taichung, was born in Taiwan, in 1957. He received the B.S. and M. S. degrees 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 at 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.



Chin-Hsing Chen received the B.S. degree electrical engineering in National Taiwan from Taiwan. University. in 1980, and the M.S. and Ph.D. degrees in electrical and computer engineering from the University of California at Santa Barbara, in 1983 and

1987, respectively. Since 1988, he has been with the Department of Electrical Engineering at National Cheng Kung University in Taiwan, where he is now a professor. His current research interests include pattern recognition, image processing and VLSI array design. He has published over 240 papers and given more than 80 technical presentations in public in more than 15 countries.