

An Immune Secret QR-Code Sharing based on a Twofold Zero-Watermarking Scheme

Jumana Waleed^{1,2}, Huang Dong Jun¹, Sarah Saadoon³, Saad Hameed⁴, Hiyam Hatem¹

¹*School of information Science and Engineering, Central South University, Changsha, 410083, China*

jumana_waleed@yahoo.com, djhuang@csu.edu.cn,

²*College of Science, University of Diyala, Iraq*

³*Computer Science/ Technical college of Management-Baghdad, department of IT, Middle Technical University, Iraq*

⁴*College of Information Science and Engineering, Hunan University, Changsha, China*

hiamhatim2005@yahoo.com¹, Sarah_sm88@yahoo.com³, saad@hnu.edu.cn

Abstract

A robust twofold zero-watermarking scheme for secret QR-Code (Quick Response Code) sharing is proposed in order to increase the security of commercial activities on the internet and media. In this paper we will present a twofold scheme for zero-watermarking to be used for copyright protection, implemented in discrete wavelet transform (DWT) as the first fold and discrete cosine transform (DCT) as a second fold for color images in which the visual secret sharing is used to generate unexpanded master and secret shares for the same QR-Code watermark. The experimental results indicate that the proposed scheme is highly robust and the QR-Code can be decodable even after different types of attack being applied.

Keywords: *QR-Code; Visual Secret Sharing; Discrete Wavelet Transform; Discrete Cosine Transform*

1. Introduction

The digital watermarking is one of the most commonly used techniques for copyright protection and digital data ownership. Nowadays, many watermarking techniques based on manipulating both spatial and frequency domains render the digital data with high distortion. On the other hand, an emerging technique which known as a zero-watermarking is proposed, this technique relies on extracting a specific features that could identify the digital data uniquely and could contribute with the construction of the watermark, then registering these features into a third party database for safe keeping. This database is an intellectual properties rights for digital media. Zero-watermark technology's merit include: preserving the image primitives (invisibility is good and robustness is strong) and well balanced watermarked algorithm (between robustness, inserting information content and invisibility contradiction) [1]. Recently, many researchers have gone through this field to protect the copyrights of digital images. Literature [2] constructs two watermarks from remote sensing image, one is constructed from low-frequency coefficients in discrete wavelet transform (DWT) domain of the host image, and the other is constructed from that of the log-polar mapping image of the host image. In [3], a proposed scheme constructs a watermarking from the image features which is extracted from the original image by applying the DWT and the singular value

decomposition (SVD). While [4] uses discrete cosine transform (DCT) and SVD combined with contourlet transform to construct a zero-watermark. In [5] a robust zero-watermarking scheme has been proposed to protect image copyrights. This scheme uses the random projection characteristic of compressive sensing. Observations can represent the feature of original image fully and succinctly. The features and meaningful copyright information are combined to construct a zero-watermark.

The QR-Code (The Quick Response Code) is a type of 2D code being developed from the 1D barcode, which has been used in advertising, manufacturing, logistics, and retailing. QR codes have become very popular in digital watermarking in the recent years. The QR code is used with digital watermarking as a cover image as in [6] and [7] to identify the owners of the data in the QR codes. While [8] presents a zero-watermarking scheme with SVD domain for unambiguous authentication of medical images, proposing a patient identification details and a link to patient data encoded into a Quick Response (QR) code serves as the watermark. Also, the QR-Code is used as a watermark as shown in [9] to provide a new way for giving medical image authentication and improved radiology readings. In the proposed scheme the QR-Code is used as a watermark for providing copyright protection.

The visual secret sharing is a technique to share secret images, proposed by Naor and Shamir [10]. In its basic model, a binary image is encrypted into n separate images, which reveal the original image when overlaid. If the user does not have the complete n images then no information about the encrypted image can be retrieved. Some researchers used the concept of visual secret sharing of two participants with the zero-watermarking technique to protect the copyrights of digital images. [11] Proposed a novel copyright protection scheme for gray-level images based on sampling distribution of means and expanded visual cryptography to achieve the requirements of robustness and security. Also in [12] a gray-level image copyright protection scheme using expanded visual cryptography is presented, and this scheme is based on SVD technique. While [13] proposed a novel copyright protection scheme based on DWT, noticing that this scheme does not expand the shares.

In this paper, a twofold zero-watermarking scheme was proposed using the visual secret sharing to generate unexpanded secret and master shares for the QR-Code watermark, and this scheme extract the feature bits by utilizing the most important parts in the DWT and DCT of the color image to get semi-perfect results and obtained a highly robust and decodable QR-Code watermark. The rest of the paper is organized as follows: the method description is given in the subsequent section. Section 3 is the explanation of the proposed twofold zero-watermarking scheme for the secret QR-Code sharing. In Section 4, we show the presentation of experiments to demonstrate the performance of the proposed scheme. In Section 5 we have the conclusions of our scheme and the findings obtained.

2. Method Description

2.1. QR-Code

The acronym QR stands for Quick Response and QR Code is a type of two-dimensional symbol (2-D barcode) that can be used to store information and attached to an object. The purpose of QR code is to identify the object and to provide related information. It was created by Toyota subsidiary, Denso-Wave, in 1994. Then, six years later (2000), QR code is standardized as ISO/IEC 18004 [14]. A QR code exhibits efficient features such as high capacity encoding of data that can encode 7089 numeric characters for numeric data, small printout size, Chinese and Japanese character representation (kanji and kana capability), resistance to dirt

and damage, readability from any direction in 360 degrees (high speed reading), varied error correction levels, and a structure append feature. Figure 1 shows the structure of the QR code.

QR Code is comprised of black and white patterns on geometric plane surface in the two dimensions. It uses black pattern to stand for binary number 1, and white pattern to represent binary number 0. QR Code has a function of an error correcting for miss reading that white is black. Error correcting is defined in 4 levels (L, M, Q and H); level L: about 7% or less errors can be corrected, level M: about 15% or less errors can be corrected, level Q: about 25% or less errors can be corrected, and level H: about 30% or less errors can be corrected [15].

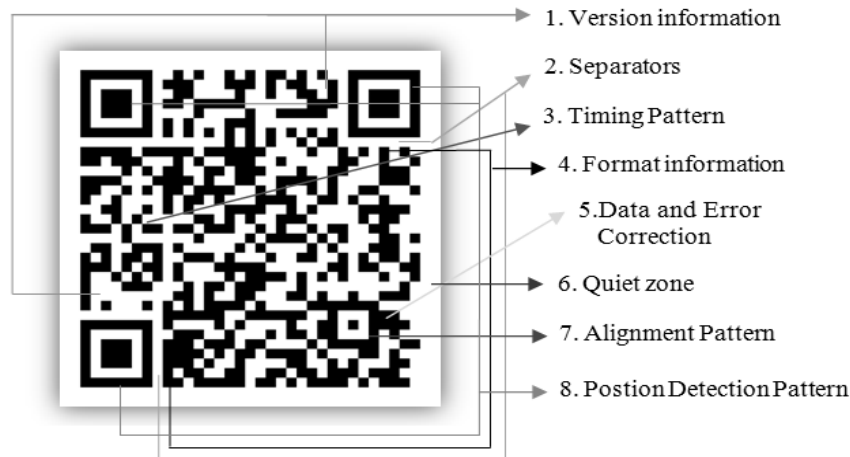


Figure 1. Structure of QR-Code

2.2. Visual Secret Sharing

The visual secret sharing technique is a visual cryptographic protocol which has the ability for sharing images in secure way, and restores it without the use of complex computations [10]. Any black and white printed material such as text or images etc. are considered as images and can be split into n different share images. By stacking out a set of qualified images k where ($k \in n$) the image can be obtained from this k set of images, knowing that even $k-1$ would not reveal the image at all, not even close to the watermark image. Recently, a 2-of-2 visual secret sharing schemes are widely used in protecting the copyrights of high precision digital images. In the traditional (2, 2) visual secret sharing scheme, a secret image is encrypted in two transparencies. When stacking these two transparencies, content of the secret image is visible. In this model, six 2×2 binary codewords are involved as shown in Figure 2, one pixel of the secret image is encrypted into two codewords. Also, there is another model of (2,2) visual secret sharing in which each pixel in the secret image is replaced by two sub-pixels in each share, the width of the decoded image is twice that of the original image as shown in Figure 3. These models increase the size of each share and result in loss of contrast in the recovered image. In this paper, XOR-based (2, 2) visual secret sharing is used without expansion in the secret image pixels. The secret QR-Code image is split into two unexpanded master and secret shares.

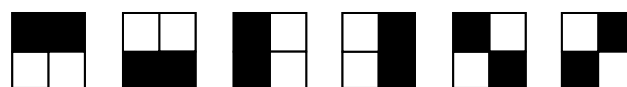


Figure 2. 2×2 Binary Codewords

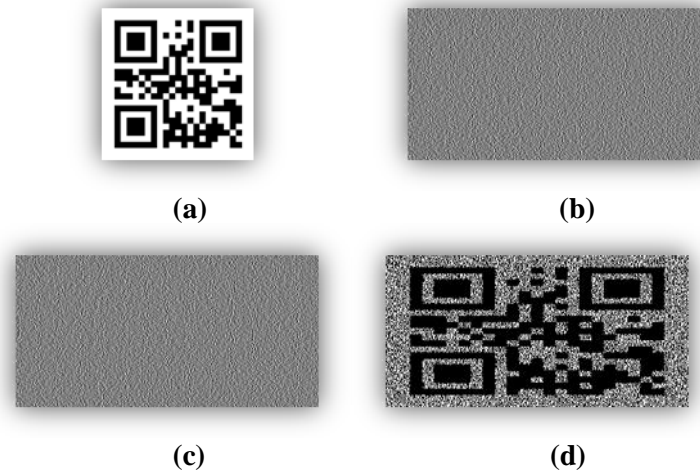


Figure 3. An Example of (2, 2) Visual Secret Sharing Technique, for (a) Secret QR-Code Image, (b) First Share, (c) Second Share, (d) Overlapped Expanded QR-Code Image

2.3. Discrete Wavelet and Cosine Transforms

The wavelet transform describes a multi-resolution decomposition process in terms of expansion of an image onto a set of wavelet basis functions. DWT has its own excellent space frequency localization property. Application of DWT in two-dimensional (2D) images corresponds to 2D filter image processing in each dimension. The input image is divided into four non-overlapping multi-resolution sub-bands by the filters, namely LL_1 (approximation coefficients), LH_1 (vertical details), HL_1 (horizontal details) and HH_1 (diagonal details). The sub-band (LL_1) is processed further to obtain the next coarser scale of wavelet coefficients, until some final scale 'N' is reached. When 'N' is reached, $3N + 1$ sub-bands are obtained consisting of the multi-resolution sub-bands. Which are LL_x and LH_x , HL_x and HH_x where 'X' ranges from 1 until 'N'. Generally, most of the image energy is stored in the LL_x sub-bands [16]. The low-frequency sub-band represents the best approximation of the original image under the condition of the largest scale and the minimum resolution decided by DWT decomposition level. Its statistical characteristics are similar to the original image, and most of the energy of the image is concentrated in it. While the high frequency sub-bands represent the details of the original image in different scales and resolutions. The lower the resolution is, the higher the proportion of useful information is [17].

DCT is a typical scene for image processing and digital signal processing with advantages of high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity [6]. The DCT block is consisted of several frequency bands; The single direct current (DC) coefficient, the low frequency coefficients of the block (BL), the height frequency band (BH) and the middle frequency coefficients of the block (BM). Since the (DC) coefficients represent the average brightness of the image, those coefficients are chosen for generating the feature matrix bits.

3. The Proposed Twofold Zero-watermarking Scheme

In this section, we propose a twofold copyright protection scheme for zero-watermarking using visual cryptography technique and working on QR-Code as a

watermark. There are two procedures of proposed method; Embedding Procedure and Extracting Procedure.

3.1. Embedding Procedure

The embedding procedure uses the YCbCr color space for zero watermarking to achieve maximum robustness against majority of attacks. To generate the secret shares for the QR-Code watermark, there are two stages (folds); in the first stage a 4-level Discrete Wavelet Transform is performed to the Y component and the feature matrix bits will be extracted from the low frequency band (LL4) since it is almost not changed by any of the common attacks so that features extracted from the low frequency coefficients contains better robustness. The second stage performs the DCT to the Y component, and selects the most important part (DC) coefficient to extract the feature matrix bits. The embedding procedure can be described as the following steps; Figure 4 is the representation of these steps.

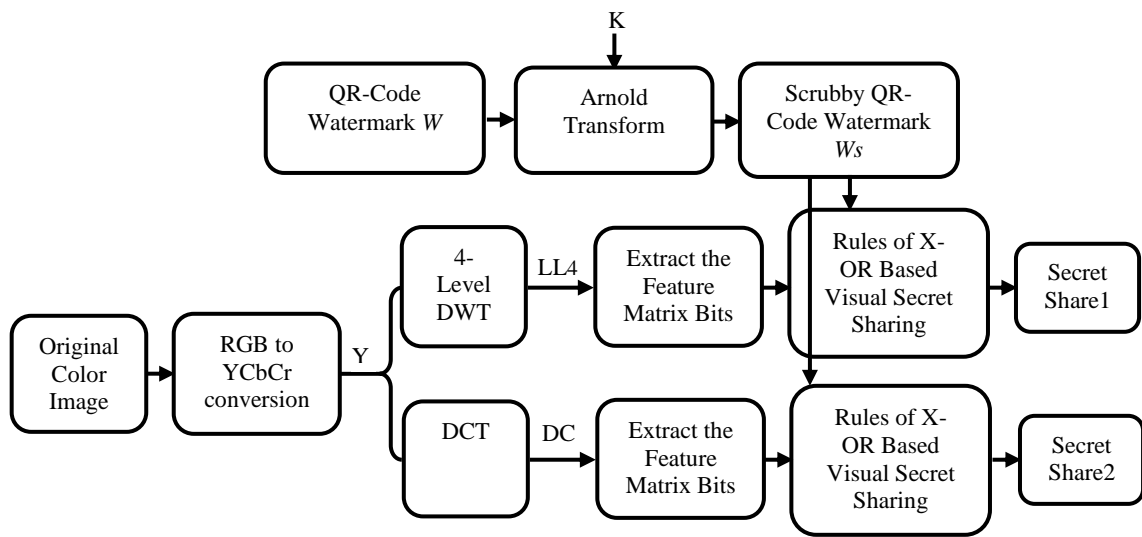


Figure 4. Embedding Procedure

Step1: Generate a QR-Code image with company name of size $n \times n$. To decrease the relationship of pixel space in the QR-Code watermark image, the watermark W is spread out evenly using Arnold transform with the scrambling time K . Empirical value of K is 20 which applied on the watermark W to obtain spread out watermark W_s as in (1).

$$W_s(i, j) = W \left(\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} i \\ j \end{bmatrix} \text{mod } n \right) \quad (1)$$

where: $W(i, j), W_s(i, j) \in \{0,1\}, 1 \leq i, j \leq n$

Step2: Convert the color image of size $m \times m$ from RGB domain to its equivalent YCbCr domain; The Y component represents the luminance while the Cb and Cr components represent the chrominance. Here, only the Y component is used to extract the features.

Step3: In the first stage (fold), Decompose Y component into discrete wavelet domain with four-levels, and select the LL4 to generate the feature matrix bits. Split the LL4 and divide it into non-overlapping blocks of dimension 4×4 , B_1, B_2, \dots, B_b . where b is the number of blocks. Then, extract the feature matrix bits, this process is done by computing the average for each block B , and compare each element in each block with the average of that block. The feature matrix F_l is constructed by using (2), and (3).

$$\text{Average}(p) = \text{average} \left(B_p(x, y) \right), 1 \leq x, y \leq 4, 1 \leq p \leq b \quad (2)$$

$$F_1(i,j) = \begin{cases} 1, & \text{Average}(p) < B_p(x,y), \\ 0, & \text{Otherwise} \end{cases} \quad (3)$$

where: $F_1(i,j) \in \{0,1\}, 1 \leq i,j \leq n$



Step4: In the second stage (fold), the selected component Y will be divided into 8×8 sub-blocks. To extract the feature matrix bits; these blocks are converted into the frequency domain using the two dimensional DCT, $B = \{B_1, B_2, \dots, B_t\}$, where t is the total number of blocks. Since the number of QR-Code watermark bits ($n \times n$) are very less as compare to total number of blocks (t), $2(n^2)$ blocks need to be selected from B . A random matrix RM having dimension $2(n^2)$ is generated, $RM = \{r_1, r_2, \dots, r_{2(n^2)}\}$, where r lies in between 1 and t . the blocks whose block number matches with r are separated from B . For each selected block the (DC) coefficient is selected to obtain the two (DC) matrices DC_1 and DC_2 , each of size (n^2) . Then, each element in DC_1 will be compared with the corresponding element in DC_2 . The feature matrix F_2 is constructed by using (4).

$$F_2(i,j) = \begin{cases} 1, & DC_1(i,j) \geq DC_2(i,j), \\ 0, & \text{Otherwise} \end{cases} \quad (4)$$

where: $F_2(i,j) \in \{0,1\}, 1 \leq i,j \leq n$

Step5: Generate the secret share by using the rules given in Table 1. The secret share is then registered into a third parity database for safe keeping. This database is an intellectual properties rights for digital media.

Table 1. Construction Rules of X-OR Based Visual Secret Sharing

QR-Code Watermark Pixel	White		Black	
Bit in Feature Matrix F	0	1	0	1
Master Share Pixel				
Secret Share Pixel				
Master Share X-OR Secret Share				

3.2. Extracting Procedure

For both stages (folds), the inputs to the extraction procedure are a color controversialial image and the secret share image. The output is a QR-Code watermark image W' . To extract the features of controversialial color image, the owner uses the same process which is used in the embedding procedure. Then, the master share is constructed by using the rules given in Table 1. The X-OR logic function is then applied between secret and master shares to reveal the Scrubby QR-Code watermark W 's. Finally, Arnold transform is applied K times to W 's to obtain W' which is used to verify the copyright. Note that, the size of the shares and the extracted watermark is exactly same since there is no pixel expansion. Figure 5 represent the extracting procedure.

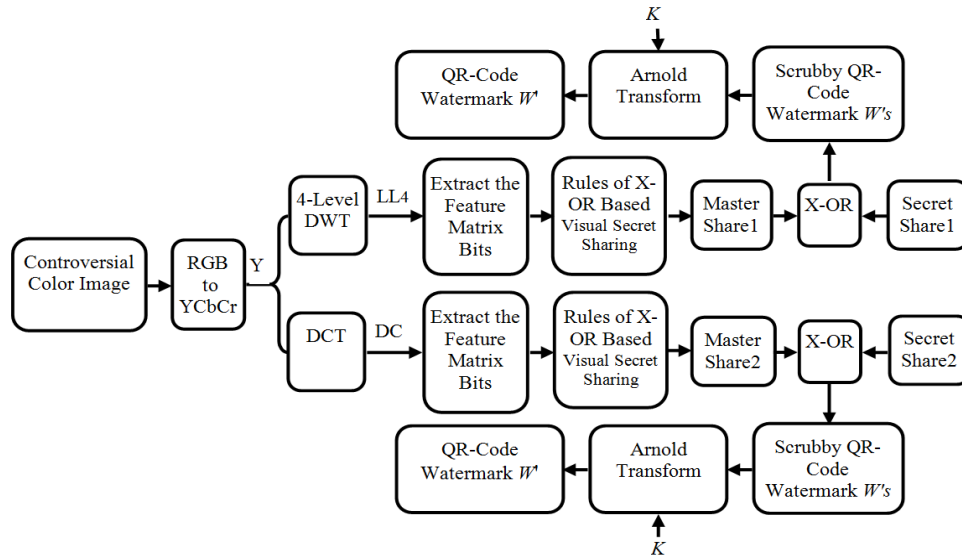


Figure 5. Extracting Procedure

4. Evaluation of the Proposed Scheme

To evaluate the proposed scheme fidelity, we measure the similarity between the original and attacked images by using the Peak Signal to Noise Ratio.

$$PSNR = 10 \log_{10} \left(\frac{255^2}{\frac{1}{m \times m} \sum_{i=1}^m \sum_{j=1}^m [I(i,j) - I'(i,j)]^2} \right) \quad (5)$$

Where: $m \times m$ is the size of the image, and $I(i, j)$, $I'(i, j)$ are the pixel values of the host and the attacked images.

In order to measure the robustness of the zero-watermarking system, the normalized correlation coefficient (NC) of the extracted watermark W_i is applied in conjunction to the original one W_i ; the maximum value of this measure is 1 which determines the best robustness of the watermarking process.

$$NC = \frac{\sum_{i=1}^N w_i w_i'}{\sqrt{\sum_{i=1}^N w_i^2} \sqrt{\sum_{i=1}^N w_i'^2}} \quad (6)$$

Where: N is the size of the original and extracted QR-Code watermark bits.

For testing performance of the proposed twofold zero-watermarking scheme, the results of the experiments are obtained using MATLAB. The proposed scheme is tested on a color image of size 512×512 (Lena image.png) which is shown in Figure 6(a). The binary QR-Code watermark image of size 32×32 that decode the word "Jumana" as shown in Figure 6(b). The resultant Master and Secret Shares for the first stage (fold) are shown in Figure 7(a), and (b). The recovered QR-Code watermark from an unaltered color image for the first stage is shown in Figure 7(c). The Master share, Secret Share, and the recovered QR-Code watermark for the second stage (fold) are shown in Figure 8(a), (b), and (c). Note that the size of all these images is same as the original QR-Code watermark and looks like random scatter of black and white pixels.



Figure 6. (a) The Original Color Image (Lena), (b) QR-Code Watermark (32x32)



Figure 7. The Resultant Images of the First Stage, (a) Master Share, (b) Secret Share, (c) Reconstructed QR-Code Watermark



Figure 8. The Resultant Images of the Second Stage, (a) Master Share, (b) Secret Share, (c) Reconstructed QR-Code Watermark

To check the robustness of the proposed scheme, some common image processing attacks were performed on the original color image. The impact of the attacks on the original color image is shown in Figure 9 which demonstrates the values of PSNR for the color image with respect to each attack type. Noise added image is obtained by adding 1% and 5% salt and pepper noise to the original image. Gaussian noise is obtained with mean=0 and variance=0.0005. Median filtering is performed with window size 3x3. And, Gaussian low pass filtering of the image was done with a window of size 2x2. Gamma Correction 1.5, Intensity Adjustment ([0 0.8], [0 1]), and histogram equalization are applied to the original image. The JPEG compression attack is performed by compressing the image with quality factors 15 and 10. The scaling of an image is done by first reducing the original host image size from 512x512 pixels to 256x256 pixels, and then zoomed to its original size by means of pixel replication. The cropped image is obtained by cropping 15% of the original image.

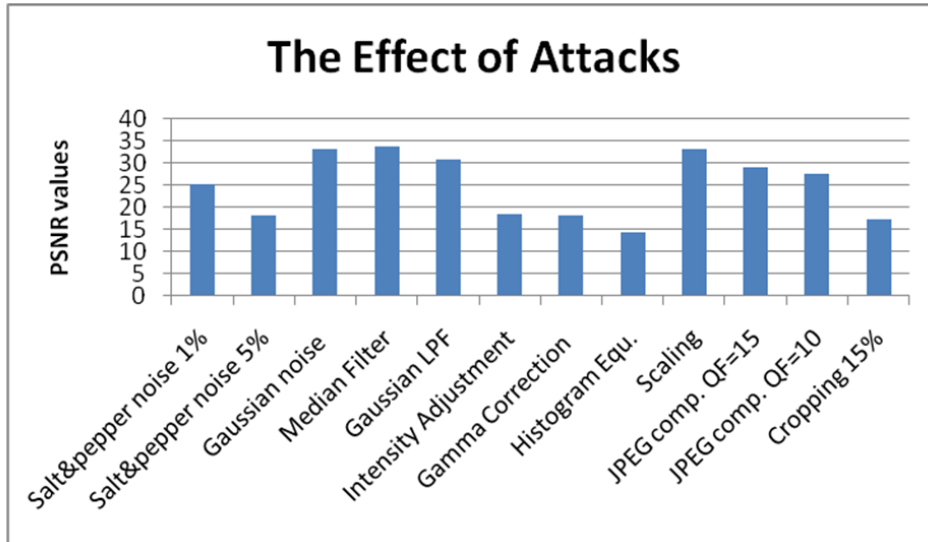




Figure 9. The Values of PSNR for the Color Image with Respect to Each Attack Type

Table 2 and Table 3 show the NC values of the reconstructed QR-Code watermark for the first and second folds under different types of attack to decode the word "Jumana". The NC values of the second fold are better than the first fold in adding the salt & pepper noise and Gaussian noise. While, the NC of the first fold gives better value than the second fold in Gaussian low pass filtering attack. In the median filtering, the two folds are approximately the same. The NC values of the reconstructed QR-Code watermark under intensity adjustment, gamma correction, and histogram equalization are better in the second fold. The scaling attack involves the resizing of the image. Here, the results show that the proposed folds is robust against the scaling attack, and the tables show the NC vales are equal in the two folds (NC=0.9992). The folds have shown good results for the JPEG compression with quality factors 15 and 10, but the reconstructed QR-Code watermark is not decodable in the first fold under quality factors 10. Cropping is used to cut a part of an image from a picture so that the extracted feature matrix is corrupted. The proposed folds resist the cropping attack with size 15%, but the reconstructed QR-Code watermark is not decodable in the first fold under this size of cropping.

Table 2. Test of Reconstructed QR-Code Watermark for the First Fold under Different Types of Attack to Decode the Word "Jumana"

Attacks	NC	Reconstructed QR-Code watermark under attacks	Decoded QR-Code "Jumana"
Salt and Pepper Noise 1%	0.9969		Decodable
Salt and Pepper Noise 5%	0.9889		Decodable

Gaussian Noise	0.9992		Decodable
Median filter (3×3)	0.9968		Decodable
Gaussian low pass filter(2×2)	0.9936		Decodable
Intensity Adjustment	0.9944		Decodable
Gamma Correction	0.9897		Decodable
Histogram Equalization	0.9873		Decodable
Scaling	0.9992		Decodable
JPEG compression QF=15	0.9905		Decodable
JPEG compression QF=10	0.9841		Not decodable
Cropping 15%	0.9753		Not decodable

Table 3. Test of Reconstructed QR-Code Watermark for the Second Fold under Different Types of Attack to Decode the Word "Jumana"

Attacks	NC	Reconstructed QR-Code watermark under attacks	Decoded QR-Code "Jumana"
Salt and Pepper Noise 1%	0.9976		Decodable
Salt and Pepper Noise 5%	0.9944		Decodable
Gaussian Noise	1		Decodable
Median filter (3×3)	0.9976		Decodable
Gaussian low pass filter(2×2)	0.9881		Decodable
Intensity Adjustment	0.9968		Decodable
Gamma Correction	0.9952		Decodable
Histogram Equalization	0.9936		Decodable
Scaling	0.9992		Decodable

JPEG compression QF=15	0.9897		Decodable
JPEG compression QF=10	0.9834		Decodable
Cropping 15%	0.9880		Decodable

5. Conclusion

In this paper, we have proposed an immune secret QR-Code sharing based on a twofold zero-watermarking scheme that extracts the feature bits from the most important parts in the host color image instead of embedding watermark into that image to protect the copyright information in a robust way. The feature bits are used to split the QR-Code watermark in to unexpanded master and secret shares. The proposed schemes generate two different secret shares to the same QR-Code watermark from host color image during the embedding procedure. One is constructed from low-frequency coefficients in discrete wavelet transform domain of the host image, and the other is constructed from that DC coefficient in DCT domain of the host image. The secret shares are then registered in a third-part database for copyright protection. While, the master shares are constructed from the controversial color image during the extracting procedure. The obtained results of NC and PSNR values show that the proposed scheme is robust against different kinds of attack. It also results in high quality extracted QR-Code watermark.

Acknowledgements

This work was supposed by the project of National Science Fund of China (No. 60873188).

References

- [1] Y. Wang, K. Luo and W. Gao, "Overview on Zero-watermarking Techniques", International Conference on Mechanical Engineering and Automation, vol. 10, (2012), pp. 259-264.
- [2] L. Jing, Y. Zhang and G. Chen, "Zero-watermarking for Copyright Protection of Remote Sensing Image", IEEE 9th International Conference on Signal Processing ICSP, Beijing, China, (2008) October 26-29, pp. 1083-1086.
- [3] W. Wang, A. Men, B. Yang and X. Chen, "A novel robust zero watermarking scheme based on DWT and SVD", IEEE 4th International Congress on image and Signal Processing (CISP), Shanghai, China, vol. 2, (2011) October 15-17, pp. 1012-1015.
- [4] D. Li, H. Shi and J. W. Kim, "The Contourlet Domain Comic Zero Watermarking Algorithm based on Discrete Cosine Transform and Singular Value Decomposition", International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 10, (2014), pp. 183-196.
- [5] S. Hao, X. Zhu, G. Zhu and G. Li, "A Robust Zero-watermarking Scheme for Image Based on Block Compressive Sensing and Arnold Transformation", Journal of Information & Computational Science, vol. 11, no. 8, (2014), pp. 2505-2516.
- [6] S. Vongpradhip and S. Rungraungsilp, "QR Code Using Invisible Watermarking in Frequency Domain", IEEE Ninth International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, (2012), January 12-13, pp. 47-52.

- [7] C. Skawattananon and S.Vongpradhip, "An Improved Method to Embed Larger Image in QR Code", IEEE 10th International Joint Conference on Computer Science and Software Engineering (JCSSE), Maha Sarakham, Thailand, (2013) May 29-31, pp. 64-69.
- [8] V. Seenivasagam and R. Velumani, "A QR Code Based Zero-Watermarking Scheme for Authentication of Medical Images in Teleradiology Cloud", Computational and Mathematical Methods in Medicine, vol. 2013, Article ID 516465, (2013), 16 pages.
- [9] R. Velumani and V. Seenivasagam, "Study of QR Code Zero Watermarking Systems in Contourlet-SVD and SVD Domains under Noise Attacks", Research Journal of Information Technology, vol. 6, no. 4, (2014), pp. 270-290.
- [10] M. Naor and A. Shamir, "Visual Cryptography", Advances in Cryptography Eurocrypt'94, Lecture Notes in Computer Science, Springer-Verlag, Berlin, vol. 950, (1995), pp. 1-12.
- [11] C.-S. Hsu and Y.-C. Hou, "Copyright protection scheme for digital images using visual cryptography and sampling methods", Optical Engineering, vol. 44, no. 7, (2005), pp. 1-10.
- [12] M.-S. Wang and W.-C. Chen, "Digital image copyright protection scheme based on visual cryptography and singular value decomposition", Optical Engineering, vol. 46, no. 6, (2007), pp. 1-8.
- [13] B. Surekha, G. Swamy and K R. L. Reddy, "A Novel Copyright Protection Scheme based on Visual Secret Sharing", IEEE Third International Conference on Computing Communication & Networking Technologies (ICCCNT), Coimbatore, India, (2012) July 26-28, pp. 1-5.
- [14] P. Makhapun, K.Sangthongpattana, S. Jantarapatin and C. Mitrpant, "The Embedding of Thai in QR Code", IEEE 8th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTICON), Khon Kaen, Thailand, (2011) May 17-19, pp. 516-519.
- [15] P. Sutheebanjard and W. Premchaiswadiv, "QR-Code Generator", IEEE Eighth International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, (2010) November 24-25, pp. 89-92.
- [16] M. Khalili and D. Asatryan, "Colour spaces effects on improved discrete wavelet transform-based digital image watermarking using Arnold transform map", Institution of Engineering and Technology, IEEE, vol. 7, no. 3, (2013), pp. 177 – 187.
- [17] Y. Wang, X. Bai and S. Van, "Digital Image Watermarking Based on Texture Block and Edge Detection in the Discrete Wavelet Domain", IEEE International Conference on Sensor Network Security Technology and Privacy Communication System (SNS & PCS), Nangang, Taipei, Taiwan, (2013) May 18-19, pp. 170-174.

Authors



Jumana Waleed, she is a Ph.D. student in the School of information science and Engineering at Central South University, Changsha, China. Her research activity focuses on image processing, and information security working on digital watermarking. She received the B.S. degree in computers sciences from the Al-Yarmouk University College, Iraq, in 2004, and the M.S. degree in Computer Science/Data Security from the University of Technology, Baghdad, Iraq, in 2009.



Huang Dong Jun, he is a professor at Central South University. He received his PHD degree in computer science and technology from the Central South University, China, in 2004. He worked as a visiting academic to University of Glasgow, UK, from 2007 to 2008. Currently, he is the director of the Department of Computer Engineering, Central South University and the member of the IOT Education Expert Group of the Ministry of Education, China. His research interests include computer networks, multimedia technology, image and video processing, video conferencing system and video surveillance techniques.



Sarah Saadoon, she is a lecturer at Computer Science/ Technical College of Management-Baghdad, department of IT, Middle Technical University, Iraq. She received the B.S. degree in computers sciences from the Al-Yarmouk University College, Iraq, in 2004, and the M.S. degree in Computer Science from the University of Technology, Baghdad, Iraq, in 2008.



Saad Hameed, he was born in Baghdad – Iraq in 7 June 1979, he received his B.Sc. Degree in computer science at AL-Mansour University College 2001, and Masters Degree in computer Sciences, Iraqi committee for computer and informatics in 2004, he continued working in academic teaching in AL-Mansour University College for 11 years, through that time all of his research was self-funded and concentrated in automation and control, he has been promoted from assistant Lecturer to Lecturer in 2011, he is now a Ph.D. degree student at Hunan University in P.R. China.



Hiyam Hatem, she received the BS degree from the department of computer science, Baghdad University, Iraq, 2003. She received the master degree from Huazhong University of science and technology Wuhan, China, in 2010. Currently, she is a PhD student in School of information science and Engineering at Central south university, Changsha, China. Her research interests include face processing and recognition, object detection, pattern recognition, computer vision, and biometrics.