

## A Blind Holographic Image Watermarking Algorithm based on Dual Transform Domains and Visual Cryptography

Xiao Luo, DaYou Jiang and De Li\*

Department of Computer Science, Yanbian University  
133002, Yanji, China

*lxazy123@163.com, ybdxgxy13529@163.com, leader1223@ybu.edu.cn*

### Abstract

*In this paper, we propose a blind watermarking scheme based on dual transform domains of discrete wavelet transform and discrete fractional random transform. In order to achieve the robustness and security, we also use the visual secret sharing scheme to split the secret image into two shares and use hologram quantization to spread the watermark information and analyze the cover image detail. For the purpose of widely practical application, we use a QR code for the watermark information. The QR code is decomposed into two shares, the first share is generated by the random seed, and the second share is generated with the help of secret image and the first share. Firstly, the two shares are respectively transformed into a hologram by using the hologram quantization, and then a discrete fractional random transform is applied to them. The cover image is decomposed by two-dimension discrete wavelet transform. The subband generated watermark then is embedded into the intermediate frequency components of the cover image. The watermark extraction process is the reverse of the embedding process.*

*Because of the spectrum characteristic and tear resistant of the hologram, the algorithm has good invisibility. The experimental results show that the proposed algorithm is effective and robust against JPEG loss compression, cropping, rotation and noise.*

**Keywords:** *Hologram, Visual Cryptography, Discrete Fractional Random Transform, Discrete Wavelet Transform, QR code*

### 1. Introduction

During the last decade, the availability of information in digital form has increased rapidly. The success of the internet, cost-effective recording and storage devices have made it possible to easily create, replicate, transmit, and distribute digital content. However, the information security, authentication of data and protection of intellectual property rights have also become an important issue. Digital watermarking is one of the popular mechanisms that have been used for the copyright protection of digital media. The method for image authentication is to insert secret sensitive information into the digital image and then authenticate the credibility of the digital content using embedded information. It is generally believed that the digital watermarking should be security, imperceptibility, robustness and provable, but also for the sake of convenient application it can realize blind extraction. Up till the present moment, the study of digital watermarking has made great achievements. In spatial domain watermarking

---

\*Corresponding author: De Li (*leader1223@ybu.edu.cn*)

schemes, the watermark is embedded by directly modifying the pixel values of the image. Transform domain watermarking schemes apply transformation techniques, such as the discrete Fourier transform (DFT) [1], discrete cosine transform (DCT) [2], the discrete wavelet transform (DWT) [3], fractional Fourier transform (FFT) [4], radon transform [5], and singular value decomposition (SVD) [6] to an image. Watermark is then embedded by modifying the transform coefficients. As compared to spatial domain techniques, these techniques show better robustness and security.

In this paper, a new blind holographic image watermarking algorithm based on dual transform domains and visual cryptography is proposed. At first, the host image is divided into  $8 \times 8$  nonoverlapping blocks. Then we apply single-level discrete 2-D wavelet transform to each block and get the mean energy value of each block. Then we divide the  $8 \times 8$  blocks into  $4 \times 4$  blocks and get the minimum energy value of each block. After that a  $4 \times 4$  energy quantization table is formed and used to be the reference values for hologram quantization later. We apply visual secret sharing scheme (VSS) to the watermark. The first share is constructed by using random seed. The second share is then generated by using the first share together with the watermark. Transform the two shares separately using the DFRNT and then using hologram quantization separately to generate holograms. Then add each hologram quantization block to corresponding subimage. At last apply inverse discrete wavelet transform to those subimages.

The rest of the paper is organized as follows. In Section 2, a brief background about QR code, visual cryptography, DFRNT and hologram quantization is proved. Details of the proposed scheme are given in Section 3. The experimental results are presented in Section 4. Finally, the conclusions are drawn in Section 5.

## 2. Background

In this section, the concepts of visual cryptography, discrete fractional random transform and hologram quantization are briefly described.

### 2.1 QR code

QR code was invented by Denso Wave and released in 1994. QR code can encode in much type of characters such as numeric, alphanumeric character, symbols, binary, and control codes. Features of QR code are high capacity and error correction. Error correction helps to restore when symbol is dirty or damaged [7].

QR code is a matrix symbol that contains of an array of nominally square modules arranged in an overall square pattern. QR code includes unique finder pattern located at three corners of the symbol and intended to assist in locating its position, size and inclination easily. A wide range of size of symbol is provided for together with four levels of error correction.

For its special features, QR Code has been widely used in the digital watermarking in recent years [8].

In this paper, we use a QR code for the watermark information. Its size is  $25 \text{ modules} \times 25 \text{ modules}$  and its level of Reed-Solomon error correction allowing recovery the codewords in 15%.







### 2.2 Visual cryptography

A secret sharing scheme allows a secret to be shared among a set of participants. In 1995, Naor and Shamir proposed the concept of  $(k, n)$  VSS scheme, called visual cryptography (VC) [9]. A  $(k, n)$  threshold scheme for  $k$  out of  $n$  shadow images is used to encode a secret image into  $n$  shadows, namely shares. It can visually recover the secret image by stacking  $k$  shadows,

while no information of the secret image could be obtained for less than k shadows. For this reason, VC is widely used in many digital watermarking schemes [10-11].

Considering the convenience and security of the scheme, in this paper, we proposed a pseudo-(2, 2) VSS method. A secret image is just divided into two shares, but the size of them is the same as the secret image. In the encryption process, every secret pixel is turned into two blocks, and each block belongs to the corresponding share image. At last, two share images are obtained. In the decryption process, two corresponding blocks of a pixel are stacked together to retrieve the secret pixel. This paper proposes method for adding watermark that is hiding information into QR code. The share 1 is constructed by using the binary map, and the binary map is generated by a random seed. Table 1 shows the concept of pseudo-(2, 2) VSS scheme. An example of the scheme is shown in Figure 1.

**Table 1. Concept of Pseudo-(2, 2) VSS Scheme**

Pixel color	White Pixel 	Black Pixel 
Share 1		
Share 2		



(a) Original secret image      (b) First share image      (c) Second share image

**Figure 1. An Example of Pseudo-(2, 2) VSS Scheme**

### 2.3 DFRNT

DFRNT was proposed by Z. Liu, H. Zhao and S. Liu in 2005 [12]. DFRNT originates from discrete fractional Fourier transform (DFrFT) [13]. DFrFT has the same eigenvectors as DFT, but with fractional power eigenvalues. Meanwhile, DFRNT has the same eigenvalues as DFrFT, but with random eigenvectors. In DFRNT domain, high amplitude spectrum and low amplitude spectrum components carry different information of original image.

A symmetric random matrix  $Q$  is written as

$$Q_{mn} = Q_{nm}, \quad Q = (P + P^T) / 2, \tag{1}$$

The matrix  $P$  is an  $N \times N$  real random matrix. The kernel transform matrix  $R^\alpha$  of the DFRNT is defined in a commutative way that

$$QR^\alpha = R^\alpha Q, \tag{2}$$

Eigenvectors  $\{V_{Rj}\}$  ( $j = 1, 2, \dots, N$ ) of  $R^\alpha$  are all real and orthonormal to another. Then we use the Schmidt standard normalization procedure to normalize the  $\{V_{Rj}\}$  to  $\{V_{Rj}\}$ . Eigenvector matrix  $V_R$  is composed of  $N$  column vectors  $\{V_{Rj}\}$

$$[V_R] = [V_{R1}, V_{R2}, \dots, V_{RN}], \quad V_R V_R^T = I, \tag{3}$$

If we apply singular value decomposition to the matrix  $Q$ , we can get the  $V_R$  that we wanted. The process is as

$$[V_R, S, L] = svd(Q), \quad (4)$$

Coefficient matrix corresponding to eigenvalues of DFRNT is defined as

$$D_{R_i} = \text{diag}\{[1, \exp(-2i\pi a/t), \dots, \exp(-2i\pi a(N-1)/t)]\}, \quad (5)$$

The  $t$  indicates periodicity of DFRNT. Thus,  $R^a$  can be constructed as

$$R^a = V_R D_{R_i} V_R^T, \quad (6)$$

DFRNT for a 1-D and 2-D signals can be written as matrix multiplications as follows

$$X_{R(\alpha)}(n) = R^a x(n), \quad X_{R(\alpha)} = R^a x(R^a)^T. \quad (7)$$

The DFRNT needs these parameters, such as integer periodic quantity  $M$ , fractional order  $\alpha$ , random seed  $\beta$  and the encrypted image. Without knowing the correct parameters in the decryption process, it is impossible that we can get the accurate secret image. So we can also use the DFRNT to ensure the security of the algorithm.

## 2.4 Hologram Quantization

The holographic concept was first proposed by Dennis Gabor in 1947. As for improvements in holographic technique, Leith and Upatnieks proposed the off-axis geometry in the early 1960s. After the invention of the off-axis hologram and the discovery of Laser, holography took on lots of new features. J. W. Goodman brought forward the concept of digital holography in 1960s. Its principle was used the light-sensitive electronic component to replace the conventional holographic plate for recording hologram, and reconstructed numerically. Digital hologram can be used to image objects, such as in the digital image watermarking region. Hologram as watermark data is embedded into the cover image, for improving the performance of the conventional watermarking system against some attacks such as noise, cropping and so on.

In this paper, we use the lensless Fourier transform hologram [14]. Supposing that the object point source and the reference point source are on the same plane namely  $x_0y_0$  plane. The CCD plane is named  $xy$  plane. The recording distance between the two planes is  $d$ . Suppose the complex amplitude of the object is  $O_0(x_0, y_0)$  and the reference point source is  $(-b, 0)$ .

According to the Fresnel diffraction theory and ignoring the constant factor, the complex amplitude of the object wave in the CCD plane is defined

$$O(x, y) = \iint_{\infty} O_0(x_0, y_0) \exp\left\{\frac{jk}{2d}[(x-x_0)^2 + (y-y_0)^2]\right\} dx_0 dy_0, \quad (8)$$

The complex amplitude of the reference wave in the CCD plane is defined

$$R(x, y) = \exp\left[\frac{jk}{2d}(x^2 + y^2)\right] \exp\left[-\frac{jk}{d}(xx_r + yy_r)\right], \quad (9)$$

The intensity distribution of the interference pattern in the hologram plane is

$$H(x, y) = |O + R|^2 = |O|^2 + |R|^2 + O^*R + OR^*, \quad (10)$$

Where  $*$  denotes the complex conjugate.

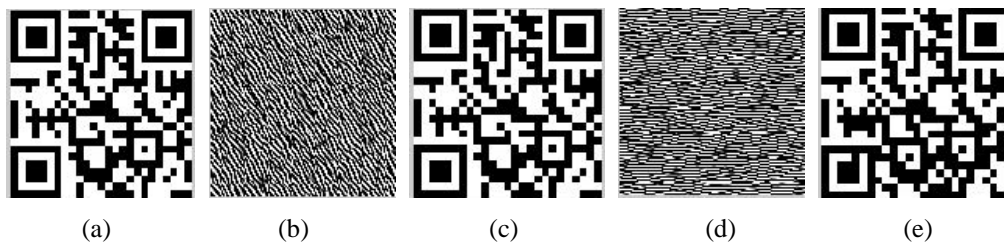
A spherical reference wave is used as the reconstruction wave to illuminate the hologram and can be written

$$C(x, y) = \exp\left[\frac{jk}{2d}(x^2 + y^2)\right], \quad (11)$$

Then the complex amplitude of the reconstructed wave in the image plane can be written

$$I_i(x_i, y_i) = \iint_{\infty} C(x, y)H(x, y) \exp\left\{\frac{jk}{2d}[x_i - x]^2 + (y_i - y)^2\right\} dx dy. \quad (12)$$

Through the experimental study of lensless Fourier transform digital hologram, the angle of the incident of the reference light, the light wavelength of the incident light and the distance between the object plane and CCD plane are proved to be main factors of reconstruction of hologram. In order to obtain the high-resolution reconstruction image, under the condition of satisfying the sampling theorem, the distance between the object plane and CCD plane should be narrow as far as possible. In this paper, QR code is measured by using lensless Fourier transform digital hologram shown in Figure 2 (a). The generated hologram image is shown in Figure 2(b) and the reconstruction image is shown in Figure 2(c). When the reconstruction distance is a little longer, the generated hologram image and the reconstruction image are shown respectively in Figure 2(d) and Figure 2(e). It can be seen that the longer the reconstruction distance is, the bigger the object image changes.



**Figure 2. Hologram Image and Reconstruction Image at Different Reconstruction Distance**

### 3. Proposed Watermarking Scheme

In this section, we explain the proposed watermarking scheme in detail. Figure 3 shows the process of the embedding scheme. The main steps of the embedding procedure are described as follow:

Step1: Watermark image preprocessing

- (1) Select the binary image with 25 pixels  $\times$  25 pixels as watermark information.
- (2) Generate the binary map image with 25 pixels  $\times$  25 pixels by using the random seed and select it as the share 1 image.
- (3) Apply the visual secret sharing scheme to split the QR code into two shares, generate the share 2 image by using the share 1 image together with the QR code.
- (4) Generate the hologram images of share 1 and share 2 respectively.
- (5) Transform the two hologram images by using the DFRNT separately.

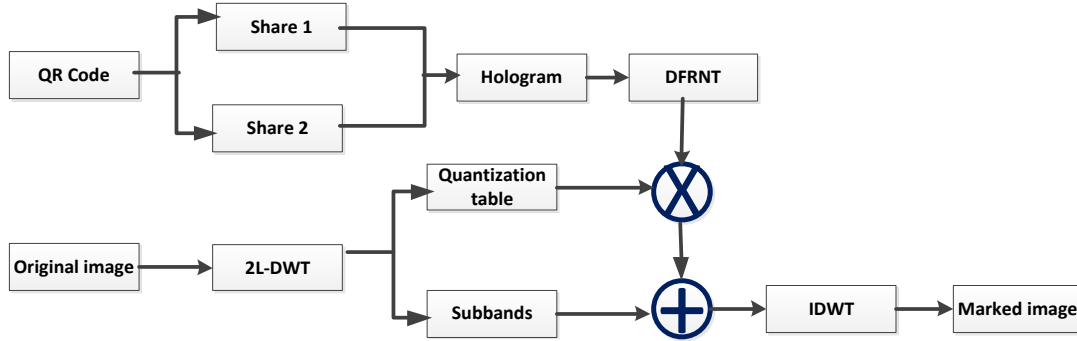
Step2: Cover image preprocessing

- (1) Select the cover image with 512 pixels  $\times$  512 pixels.
- (2) Transform the cover image by using a two-dimension DWT and apply the same transform to the LH1, HL1.
- (3) Divide the cover image into 8 $\times$ 8 blocks. Each 64 pixels  $\times$  64 pixels block's average energy is calculated by the following rule:

$$f_{energy} = \sum_{i=1}^M \sum_{j=1}^N \frac{f(i, j)}{M \bullet N} \quad (13)$$

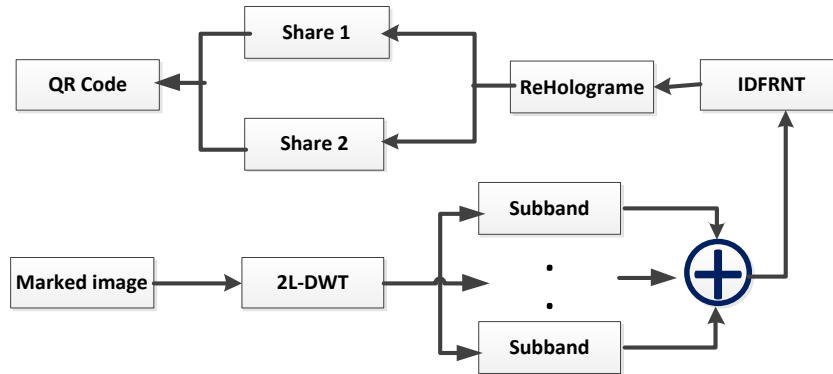
- (4) Divide the 8 $\times$ 8 blocks into 4 $\times$ 4 blocks. Calculate the minimum average energy of each 2 $\times$ 2 blocks. Form an energy table based on the (4, 4) matrix of average energy.

Step3: Generate the hologram quantization table based on the energy Table.  
 Step4: Add the hologram quantization block and the matrix of the HL1-LH2, HL1-HL2 subbands and the LH1-LH2, LH1-HL2 subbands separately.  
 Step5: Transform them by using inverse two-dimension DWT.



**Figure 3. Process of the Embedding Scheme**

The extraction process is just the opposite of the embedding process. Fig.4 shows the process of the extraction scheme.



**Figure 4. Process of the Extraction Scheme**

## 4. Experiment Results and Analysis

### 4.1 Experimental Results

In this paper, peak signal-to-noise ratio (PSNR) is used to analyze the visual quality of the watermarked image  $I'$ , in comparison, the original image is named  $I$ . PSNR is measured physically in decibels and defined as

$$PSNR = 10 \lg \left( \frac{255^2}{MSE} \right) dB \quad (14)$$

Mean squared error (MSE) between the original image  $I$  and the watermarked image  $I'$  is given by

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [I(i, j) - I'(i, j)]^2 \quad (15)$$

Bit error rate (BER) is used to measure the similarity between the extracted secret image and the original secret image. It is defined as

$$BER = \frac{\sum_{i=1}^m \sum_{j=1}^n S_{i,j} \oplus S'_{i,j}}{m \times n} \quad (16)$$

where  $S_{i,j}$  and  $S'_{i,j}$  represents the original and extracted secret images respectively,  $\oplus$  denotes the exclusive-or (XOR) operation and  $m \times n$  is the secret image size.

Various experiments are carried out in this section, to ass the performance of the proposed algorithm. Four images, “Lena”, “Baboon”, “Airplane” and “Peppers” of size  $512 \times 512$  are used as cover image. A QR code of size  $25 \times 25$  is used as secret image. All the cover images and the marked images are shown in Figure 5.



**Figure 5. Cover Images (Left) and Marked Images (Right)**

From the two sets of images, we can get the conclusion that there is no obvious difference between the cover images and the marked images, which proves that the imperceptibility of the proposed algorithm is good.

The PSNR and BER values corresponding to the cover images are listed in the Table 2.

**Table 2. PSNR and BER Values for Various Cover Images**

	PSNR(dB)	BER (%)
Lena	37.52	0
Baboon	33.20	0.32
Peppers	38.14	0
Airplane	38.32	0.16

Although the PSNR value is less than 40 dB, the watermark is invisible if the cover image has mainly high-frequency components. For cover image “Lena”, without any attack, we can extract the watermark exactly with BER = 0.

In the following experiments, the robustness of the proposed scheme is estimated by performing several image processing attacks, including noise addition, JPEG compression, geometric rotation and cropping. All attack simulations were made using Matlab platform.

All the results obtained by performing the proposed scheme on the “Lena” image. Table 3-6 shows the results of those attacks. The attacks are described as follows:







**Noise addition:** A sets of noise images are obtained by adding 0.1%, 0.5% and 1% Gaussian noise to the original image. The PSNR of the corresponding noise images is 28.85 dB, 22.86 dB and 20.47 dB. The BER of the corresponding extracted watermark is 0, 0.0048 and 0.0424.

**JPEG compression:** We compressed the image by JPEG with quality factor 80%, 60% and 40% respectively. The PSNR of the corresponding compressed image is 32.84 dB, 32.09 dB and 26.56 dB. The BER of the corresponding extracted watermark is 0.0224, 0.0520 and 0.1042.







**Geometry rotation:** The image is rotated respectively by 10°, 30° and 45°. The PSNR of the corresponding rotated image is 16.84 dB, 13.54 dB and 13.28 dB. The BER of the corresponding extracted watermark is 0.0080, 0.0220 and 0.0823.

**Cropping:** The image is cropped respectively by 10%, 20% and 30%. The PSNR of the corresponding rotated image is 16.97 dB, 14.52 dB and 13.04 dB. The BER of the corresponding extracted watermark is 0, 0 and 0.

**Table 3. Noise Addition Attack**







		Variance	0.001	0.005	0.01
Gaussian	Noised image				
	Extracted watermark				
BER			0	0.0048	0.0424

**Table 4. JPEG Compression Attack**

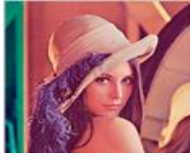





		Quality factor	80%	60%	40%
JPEG compression	Compressed image				
	Extracted watermark				
BER			0.0224	0.0520	0.1042



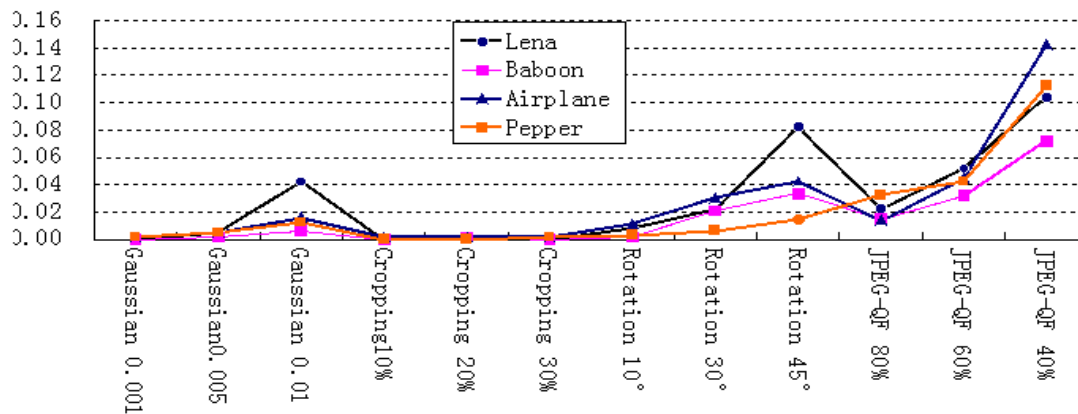
**Table 5. Geometry Rotation Attack**

		Angle	10°	20°	30°
Geometry rotation	Rotated image				
	Extracted watermark				
BER			0.0080	0.0220	0.0823

**Table 6. Cropping Attack**

		Scale	10%	20%	30%
Cropping	Cropped image				
	Extracted watermark				
BER			0	0	0

The proposed scheme that is robust to several types of attack is shown in Figure 6.



**Figure 6. BER Values Corresponding to Various Attacks**

## 4.2. Experimental Analysis

Robustness and security are the two most important properties that a watermarking scheme should hold. After those attacks listed before, the results show that the scheme has good invisibility and fair robustness. For different cover images, the extracted watermarks are very close to the original watermarks. The maximum BER value of the extracted watermark in our experiment is 0.1423, which is still in the error correction range of the QR code we used as the secret image.

The security of the scheme is ensured by using the VSS and DFRNT. VSS needs its key shares to reconstruct the secret image, each of them is vital. DFRNT is very much sensitive to its transform order, without knowing the correct transform order nobody can extract the correct watermark.

## 5. Conclusion

In this paper, a blind holographic image watermarking scheme based on dual transform domains and visual cryptography is proposed. The robustness of the scheme is tested by performing various image processing attacks. The QR code is used as the secret image, it is not only a widely used information medium, but also it has high capacity and error correct. Besides, the VSS and DFRNT can ensure the security of the scheme. The hologram has the ability to restore the image even the image is torn up. Also by analyzing the spectral characteristic of the hologram and using DWT to cover image, we can choose the appropriate regions to embed the watermark. Result from that, a good invisibility and high robustness of the algorithm are ensured.

## Acknowledgements

This research project was supported by the National Natural Science Foundation of China (Grant No. 61262090).

## Reference

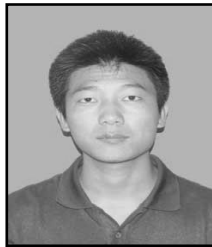
- [1] X. He, C. Q. Zhu and Q. S. Wang, "The Blind Watermarking Model of the Vector Geospatial Data Based on the DFT of QIM", Proceedings of 2009 IEEE international Conference on Network Infrastructure and Digital Content, (2009) November 06, pp. 1039-1044, Beijing, China.
- [2] S. F. Sun and L. Jian, "A New General Binary Image Watermarking in DCT Domain", Proceedings of 2008 International Seminar on Future Biomedical information Engineering, (2008) December 18, pp. 34-36, Wuhan, China.
- [3] T. M. Gu and Y. J. Wang, "DWT-based Digital Image Watermarking Algorithm", Proceedings of IEEE 2011 10th International Conference on Electronic Measurement & Instruments, (2011) August 16, pp. 163-166, Chengdu, China.
- [4] L. Jun and J. Y. Sun, "Digital Watermarking Algorithm based on Hyperchaos and Fractional Fourier Transform", Proceedings of 2012 IEEE 14th International Conference on Communication Technology, (2012) November 09, Chengdu, China.
- [5] L. Cai, S. D. Du and D. T. Gao, "Geometrically Invariant Watermarking based on Radon Transformation", JOURNAL OF ELECTRONICS, vol. 22, no. 3, (2005) May, pp. 301-306.
- [6] J. L. Wang, "Digital Watermarking Algorithm based on SVD Decomposition and Wavelet Transform", Proceedings of the Third International Symposium on Test Automation & Instrumentation vol. 3, (2010) May 12, Xiamen, China.
- [7] "Information Technology Automatic Identification and Data Capture Techniques Bar Code Symbolology QR Code", ISO/IEC 18004:2000(E), (2000).
- [8] R. Suppat, K. Mahasak, S. Pruch and V. Sartid, "Data Hiding Method for QR Code based on watermark by comparing DCT with DWT domain", International Conference on Computer and Communication Technologies, (2012) May 26-27, Phuket, Thailand.

- [9] M. Naor and A. Shamir, "Visual cryptography", in: Proceedings of the Advance in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, (1995).
- [10] R. Snjay and R. Balasubramanian, "A Blinded Watermarking Algorithm based on Fractional Fourier Transform and Visual Cryptography", Signal Processing, vol. 92, (2012), pp. 1480-1491.
- [11] D. C. Lou, H. K. Tso and J. L. Liu, "A Copyright Protection Scheme for Digital Images Using Visual Cryptography Technique", Science Direct, Computer Standards & Interface, vol. 29, (2007), pp. 125-131.
- [12] Z. Liu, H. Zhao and S. Liu, "A Discrete Fractional Random Transform", Opt. Comm., vol. 255, (2005), pp. 357-371.
- [13] S. C. Pei and M. H. Yeh, "Improved Discrete Fractional Fourier Transform", Opt. Lett., vol. 22, (1997), pp. 1047-1049.
- [14] H. Cui, D. Y. Wang, Y. X. Wang, J. Zhao and Y. Z. Zhang, "Phase Contrast Imaging of Biologic Cells based on Lensless Fourier Transform Digital Holography", First International Conference on Cellular, Molecular Biology, Biophysics and Bioengineering, (2010), pp. 303-306.

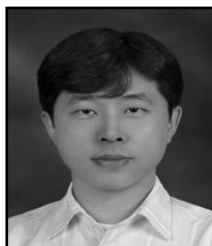
## Authors



**Xiao Lu**, he is a postgraduate, major in Information Security, now studying at Yanbian University in China. He research interests are in the areas of copyright protection technology, information security, digital watermarking and digital forensic marking.



**DaYou Jiang**, he is a postgraduate, major in Information Security, now studying at Yanbian University in China. He research interests are in the areas of copyright protection technology, information security, digital watermarking.



**De Li**, he received the Ph.D. degree from Sangmyung University, major in computer science in 2005. He is currently a professor of Dept. of Computer Science at Yanbian University in China. He is also a Principal Researcher at Copyright Protection Research Institute, Sangmyung University. His research interests are in the areas of copyright protection technology, digital watermarking, and digital forensic marking.

