International Journal of Security and Its Applications
Vol.8, No.6 (2014), pp.89-100
http://dx.doi.org/10.14257/ijsia.2014.8.6.09

A Zero-watermarking Scheme based on LPM and Holographic

De Li[1], LuYan Qiao[1] and JongWeon Kim[2*]

[1] *Department of Computer Science, Yanbian University, Yanji, China*
[2] *Department of Intellectual Property, Sangmyung University, Seoul, Korea*
leader1223@ybu.edu.cn, leslie1295615290@163.com, jwkim@smu.ac.kr

Abstract

This paper proposes a novel watermarking scheme against geometric attacks, combined with the holographic technology and the log-polar transform. In this paper, we first use discrete cosine transform into the original image, then do edge detection for the low frequency part, then do log-polar transform to edge image and make it binarization. We use a key to choose a certain size of the binary image to do holographic processing, then make it binarization and do logical operation with the watermarked image which do Anrold transformation, get the zero-watermarking. Finally, we register it in IPR database to obtain copyright protection. The experimental results show that compared with other zero-watermarking algorithms, this scheme has better robustness. It not only can effectively resist the noise, cropping, JPEG compression and other conventional attacks, but also can effectively resist geometric attacks such as rotation, scaling.

Keywords: *zero-watermarking, holographic technology, log-polar transform*

1. Introduction

In today's digital era, as an important method of multimedia information security and copyright protection, digital watermarking technology will inevitably subject to a variety of attacks when applicated. So the robustness is a basic requirement of digital watermarking system. Many of the existing image watermarking algorithms can resist such as image compression, filtering, noise and other common attacks, but lack of robustness to geometric attacks such as rotation and scaling. Therefore, the ability which the digital image watermarking against geometric attack is always a difficult and hot research [1].

Most of the digital image watermarking is to embed information by modifying the image spatial or frequency domain information, but these changes will make the image have a certain distortion, and causes contradiction between the robustness and non-sentience of watermark. In order to solve this problem, the concept of zero watermarking was first proposed in 2001 by Wen Quan [2]. The idea is to use the important feature information of host media to structure uniquely identify watermark. So it is considered that the original media have the ability of copyright protection because of containing the watermark. The main characteristic of zero watermarking is not to change any data of the original media, so there is no the problem that media quality decline or watermark embedding capacity restricted. In addition, due to the zero watermarks depends on the host; it is unlike conventional watermark which has a specific content. So we need to establish the zero watermarking information bases as a certificate of copyright protection [3].

* Corresponding Author

ISSN: 1738-9976 IJSIA

Although zero watermarking can solve the problem of the invisibility of the watermark, it has become a hot research that how to find the important image features to construct the zero watermarking in orders to improve the robustness of watermark. Chang proposed that generated low scale image by calculating the average value of image sub-block, and then did Sobel edge detection to the low scale image [4]. But the algorithm can't resist rotation attack very well. Liu proposed that did log-polar transform to holographic watermark, and then make it embed into the host image [5]. However, this method only can against rotation and scaling attacks, and the quality of image decreased significantly after embedded watermark. The zero watermarking schemes proposed by Cheng Sha [6] which based on edge detection and log-polar transform does not affect the image quality, but cannot against cropping attack.

Combining the above ideas, this paper presents a zero watermarking algorithm against geometric attacks by using edge detection, log-polar transform and holographic technology. Compared with the existing digital holographic watermarking algorithm and zero watermarking algorithm, the algorithm can effectively against geometric attacks such as rotation, scaling. In addition, as it doesn't change the image information during embedding process, it can reduce the contradiction between the robustness and non-sentience of watermark.

2. Research on Related Technology

2.1.Edge Detection Technology

Image edge is the most abundant image information, contains a lot of internal information (such as direction, step properties, shape *etc*.,) which represents the essential features of images. The edge is the region boundary that image gray value change dramatically. Edge detection refers to that using certain algorithm to distinguish between objects and background in the image boundary. It has an important position in digital image processing.

The classical edge detection algorithm has two main categories: differential method and optimal operator method. The differential method is that using the classical differential operator to detect image edge, including Sobel operator, Roberts's operator, and Prewitt operator. The optimal operator method is the development and optimization of differential operators, including Canny operator and LOG operator.

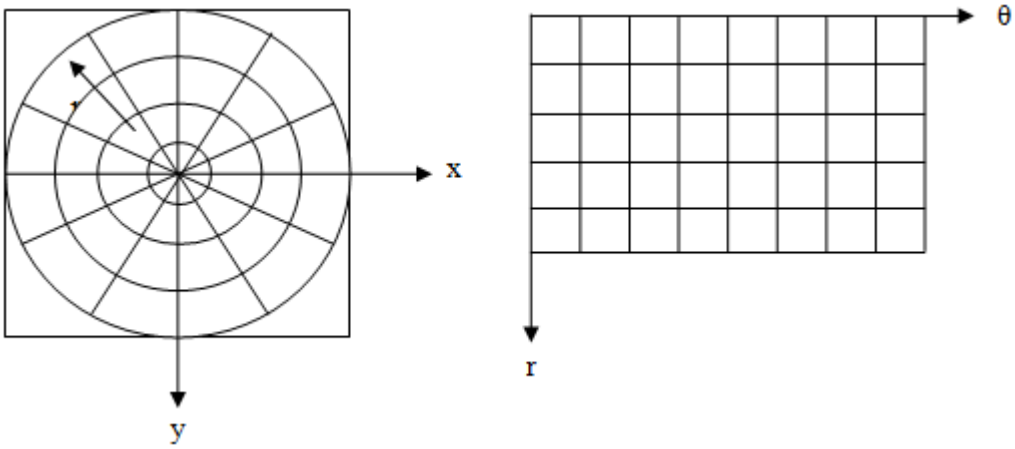
At present, the Canny operator is the better performance for detection algorithm [7]. It first filters smoothly to image by using Gauss filter and get the direction derivative that image gray along the X direction and Y direction by using the differential operator. Then get the gradient and gradient direction. By using non-maximum suppression and double threshold method for growth and refinement edge operator, get the ideal edge [8]. Therefore, the Canny operator is not interfered by noise easily. The edge location is accurate and good continuous. It has few false edges and the edge is single pixel width. It can detect the real weak edge. Therefore, we can extract the key information by applying the edge detection to the digital watermarking, in order to enhance the robustness of watermark.

2.2 The Log-polar Transform

The image of the log-polar transformation refers to that convert the image from the Cartesian coordinate to the log-polar coordinate. That is to say that the representation of the pixels in the image converts from Cartesian coordinates to polar coordinates, then take corresponding logarithm on it. The biggest characteristic of log-polar transform is that it make rotation and scaling in Cartesian coordinates convert into cyclic shift [9].

Let us define (x,y) as a point of an image in Cartesian coordinates, Then corresponding coordinate in polar coordinates is:

$$r^2 = x^2 + y^2, \theta = \arctan(y / x) \quad (1)$$



(a) The Cartesian Cordinates (b) The Log-Polar Coordinate

Figure 1. The Log-polar Transformation

Here r is the polar radius, θ is the polar angle, that is, x=rcosθ, y=rsinθ. Figure 1 shows the transform relations between the Cartesian coordinates and the log-polar, where the number of concentric circles in (a) corresponding to the polar radius in (b) and the angle divided by circular in (a) corresponding to the polar angle in (b).

In the complex plane z=x + iy, that is:

$$z = r(\cos\theta + i\sin\theta) = re^{i\theta} \quad (2)$$

Let us define D=lnz=lnr + iθ, making (x,y) scale k times while rotating Δ θ to get z_1, then:

$$D_1 = \ln z_1 = \ln(kre^{i(\theta+\Delta\theta)}) = \ln k + \ln r + i(\theta + \Delta\theta) \quad (3)$$

Compared D with D_1, we found that the scale and rotation in the Cartesian coordinates become translational motion along the polar radius r and the polar angle θ in the log-polar coordinate [9, 10].

2.3.The Digital Holography Technology

The idea of holographic technology was first proposed in 1948 by the British scientist Dennis Gabor [11]. But due to the light limitation, until the first laser was invented in Nineteen sixties, holographic technology has obtained unprecedent development [12]. Digital holography is a technique of hologram recording, processing and reproduction. It can be generated by computer or CCD collection [13]. In recent years, digital holographic technology has been applied to the field of digital watermarking and shows great potential. Japanese scholar Takai proposed digital hologram watermarking in 2002 [14]. They succeeded in embedding 2D watermark in the form of gray hologram into spatial domain of carrier image. The embedded watermark can be extracted blind from the watermark image with the method of holographic reconstruction. But because the carrier image needs low-filter, the image quality is reduced. As the digital hologram has natural encryption characteristics and can't be destroyed [15], and its resistance to cropping is very strong, it is suitable for preservation as watermark image.

Figure 2 is the process of computer generating hologram.

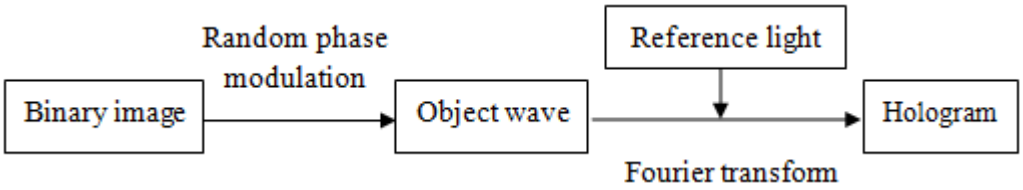


Figure 2. Computer-generated Hologram

3. Zero Watermarking Algorithm

3.1. Watermark Embedded Procedure

The basic idea is to extract features to construct watermark, and register it in IPR database to obtain copyright protection. Figure 3 displays the process of embedding algorithm.

The watermark is embedded through the following steps:

Step 1. Applying three level 2D DWT into the original image with size N×N, and choosing the low frequency coefficient to construct the low scale image with size N/8×N/8;

Step 2. Canny edge detection to the low scale image, getting the edge image;

Step 3. Lop-polar transforms to the edge image and makes it binarization, getting the LPM image;

Step 4. Selecting a part of size N/16×N/16 from the LPM image by using the key K, make it holographic and make it binarization;

Step 5. Encrypting the binary watermark image of size N/8*N/8 by using Arnold;

Step 6. Do XOR operation between binary hologram and encrypted watermark, getting the registered watermark.

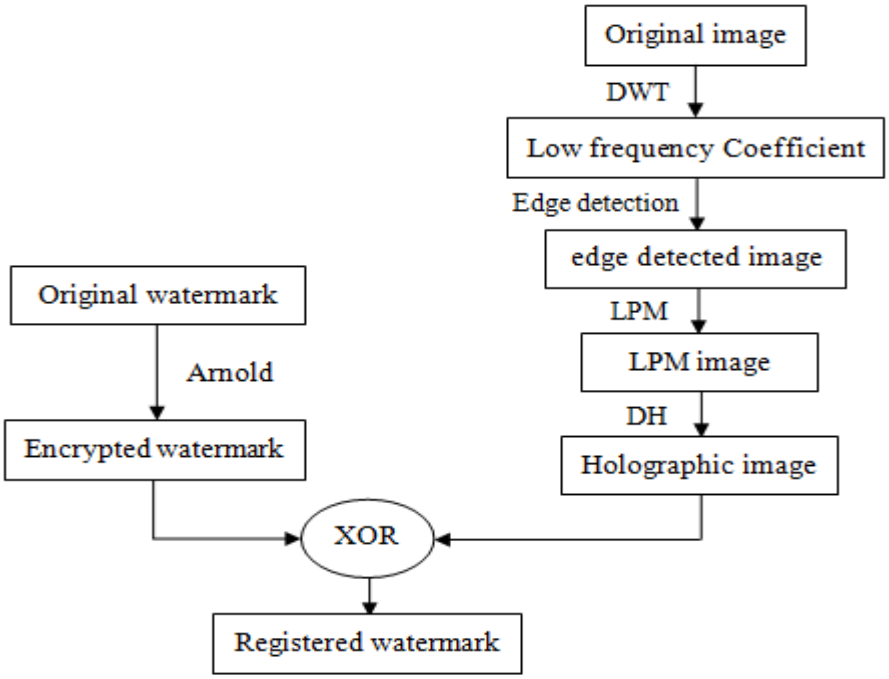


Figure 3. Diagram for Watermark Embedding Process

3.2. Watermark Detection Procedure

The watermark detection process is similar to the watermark embedding. Figure 4 displays the process of detection algorithm. The watermark is detected through the following steps:

Step 1. Applying three level 2D DWT into the detected image with size N×N, and choosing the low frequency coefficient to construct the low scale image with size N/8×N/8;

Step 2. Canny edge detection to the low scale image, getting the edge image;

Step 3. Make Lop-polar transform to the edge image and make it binarization, getting the LPM image;

Step 4. Selecting a part of size N/16×N/16 from the LPM image by using the key K, make it holographic and make it binarization;

Step 5. Get the registered image from the registry, and do XOR operation with binary hologram, then gain the reconstructed watermark by using Inverse Arnold transform.

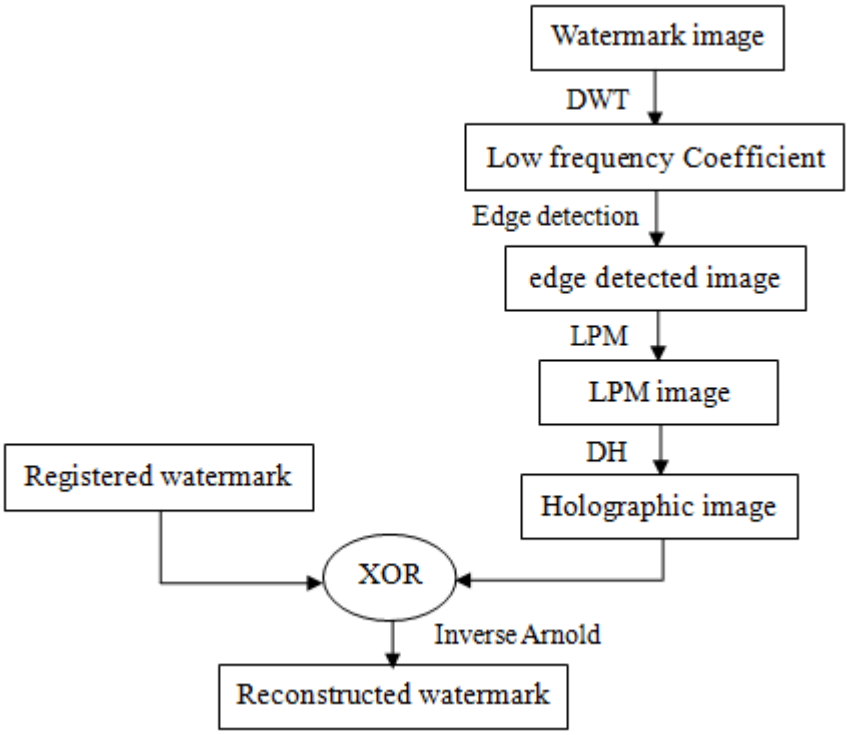


Figure 4. Diagram for Watermark Detection Process

4. The Results and Analysis of Experiments

In order to evaluate the performance of this algorithm, this paper has carried on the simulation experiment and many attack experiments in Matlab R2010. The following gives results that using the Lena image (512×512) as the original image and binary YBCS (64×64) image as watermark. To evaluate the robustness, we take BER (bit error rate) as a standard to measure the quality of watermark. Figure 5 is the detected watermark map without attacks.

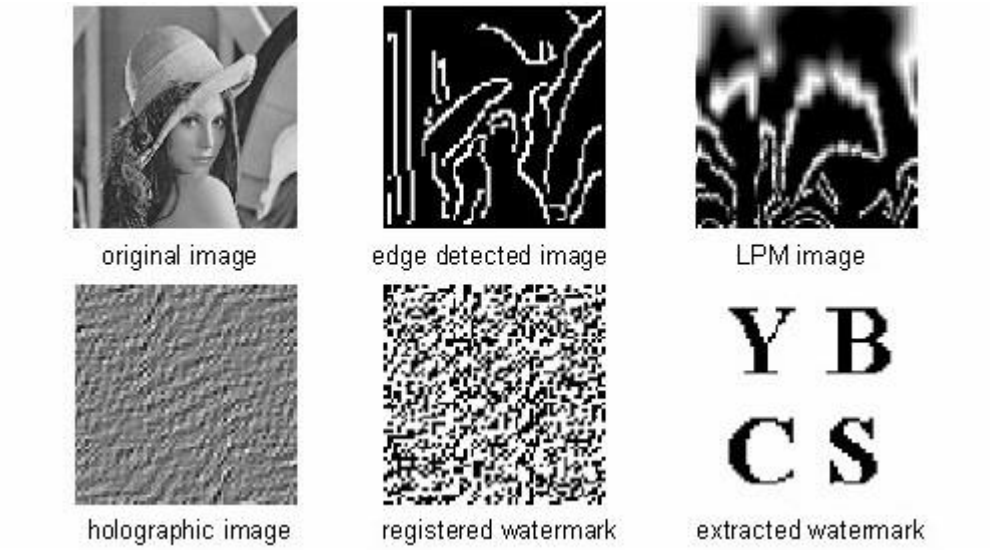


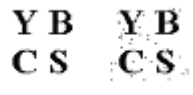
Figure 5. Detected Watermark Map without Attacks

4.1. The Results and Analysis of Attack Experiment

To demonstrate the robustness of this algorithm, this paper made a series of attack experiments such as added noise, rotation, scaling, cropping and compression.

(1) Gaussian noise attacks

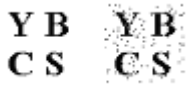
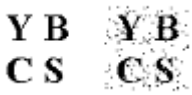
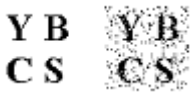
Table 1. Extracted Results of Gaussian Noise Attacks

Gaussian	**Variance**	0.005	0.05	0.1
Noise attack	The attacked image			
	Extracted watermark			
	BER	0.01	0.02	0.05

From Table 1, we can see that when the image is subjected to Gaussian noise attacks that the variance which is greater than 0.5, the quality of image becomes poor. But this algorithm can extract the watermark better. We can say it can resist Gaussian noise attacks effectively.

(2) Salt & pepper noise attacks

Table 2. Extracted Results of Salt & Pepper Noise Attacks

Salt & pepper	Density	0.005	0.01	0.1
Noise attack	The attacked image			
	Extracted watermark			
	BER	0.02	0.04	0.06

From Table 2, we can see that when the image is subjected to Gaussian noise attacks that the density which is greater than 0.01, this algorithm can extract the recognizable watermark. We can say it can resist Salt & pepper noise attacks effectively.

(3) Cropping attacks

Table 3. Extracted Results of Cropping Attacks

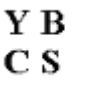
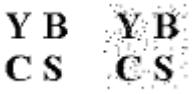
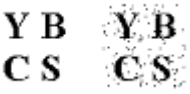
Cropping	Position	[1:256,1:256]	[150:400,150:400]	[256:512,256:512]
attack	The attacked image			
	Extracted watermark			
	BER	0.07	0.11	0.06

From Table 3, we can see that when the middle of image was cropped, as there were more pixel to be affected in the LPM image, it caused extracted watermark distorted. Compared with the upper left and lower right, its quality slightly worse. But on the whole the quality of the extracted watermark is good.

(4) Scaling attacks

Table 4. Extracted Results of Scaling Attacks

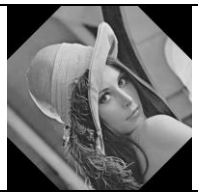
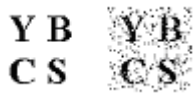
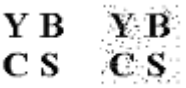
Scaling	Times	2	0.5	0.25
attack	The attacked image			

	Extracted watermark			
	BER	0.00	0.02	0.03

From Table 4, we can see that this algorithm can almost completely extract watermark for scaling attacks. So it can better resist scaling attacks.

(5) Rotation attacks

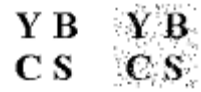
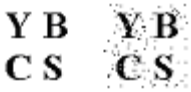
Table 5. Extracted Results of Rotation Attacks

Rotation	**Degree**	10°	45°	60°
attack	The attacked image			
	Extracted watermark			
	BER	0.02	0.07	0.03

From Table 5, we can see that when the image suffered from rotation attacks like 10°, 45° and 60°, this algorithm can extract the recognizable watermark. So it is robust to rotation attacks.

(6) JPEG Compression attacks

Table 6. Extracted Results of Compression Attacks

Compress	**Quality**	20	30	40
attack	The attacked image			
	Extracted watermark			
	BER	0.08	0.04	0.03

From Table 6, we can see that even if the quality factor of compression is 20, this algorithm can extract the recognizable watermark. So it can better resist compression attacks.

4.2. Comparison and Analysis of the Performance of the Algorithm

In order to further verify the superiority of the algorithm, we have done contrastive experiments with literature [4] and [6]. The following is the results of comparison after suffer from rotation and cropping attacks.

Table 7. Extracted Results Comparing to the Literature [4] Rotation Attacks

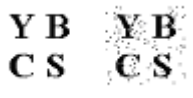
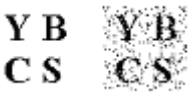
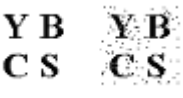
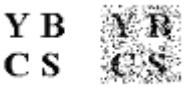
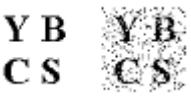
Rotation	**Degree**	10°	45°	60°
Attack Extracted Results	This algorithm			
	BER	0.02	0.07	0.03
	literature [4]			
	BER	0.09	0.13	0.08

Table 8. Extracted Results Comparing to the Literature [6] Cropping Attacks

Cropping	**Position**	[50:150,50:150]	[250:350,250:350]	[350:450,350:450]
Attack Extracted Results	This algorithm			
	BER	0.07	0.11	0.06
	literature [6]			
	BER	0.11	0.46	0.10

From the above two tables, we can see that compared with other two algorithms, this algorithm has been greatly improved in the resistance to rotation and cropping attacks. It can efficiently extract the recognizable watermark. And in the resistance to other attacks such as added noise, scaling, compression, the performance of this algorithm have been improve slightly.

5. Conclusion

In this paper, we have proposed a robust watermark algorithm based on LPM and holographic. It first obtained the key feature information of the image by using edge detection technology. Then made log-polar transformation to improve the robustness against rotation attacks. On this basis, it further improved the robustness against cropping attacks by using holographic technology. In addition, this paper used the key to obtain the specific size hologram, improve the security of the algorithm. Compared with the existing Zero-watermarking algorithms and Digital Holographic Watermarking algorithms, this algorithm not only has very strong robustness in conventional attacks, but also has a better ability to resist geometric attacks.

Acknowledgements

This research project was supported by the Ministry of Culture, Sports and Tourism (MCST) and the Korea Copyright Commission in 2014.

References

[1] P. Dong, J. G. Brankov and N. P. Galatsanos, "Digital Watermarking Robust to Geometric Distortions", IEEE Trans. On Image Processing (S1057-7149), vol. 12, no. 14, **(2005),** pp. 2140-2150.
[2] Q. Wen, T. Sun and S. Wang, "The concept and application of zero watermarking", Chinese Journal of Electronics, vol. 1, no. 3, **(2003)**, pp. 214-216.
[3] J. Shu, "Chinese text zero-watermarking technique based on statistics of part-of-speech", Master's degree thesis of Hunan University, **(2012)**, pp. 17-19.
[4] C. C. Chang and P. Y. Lin, "Adaptive watermark mechanism for rightful ownership protection", Journal of System and Software, vol. 7, no. 81, **(2008)**, pp. 1118-1129.
[5] M. Liu, G. L. Yang, H. Y. Xie, "Computer-generated hologram watermarking resilient to rotation and scaling", Opt. Eng., (S0091-3286), vol. 6, no. 46, **(2007)**, pp. 605011-605013.
[6] S. Cheng, "Study on Digital Image Zero Watermarking Algorithm", Master's degree thesis of Hangzhou University, **(2011)**, pp. 24-40.
[7] Z. Zhu, "Study on edge detection technology. Suzhou University", **(2010)**, pp. 19-21.
[8] F. J. Canny, "A Computational Approach to Edge Detection", IEEE Trans. Pattern Anal. Mach. Intell., vol. 6, no. 8, **(1986)**, pp. 679-698.
[9] B. Yu, L. Guo and T. Zhao, "Gray projection image stabilizing algorithm based on log-polar image transform Computer", Application, vol. 12, no. 28, **(2008)**, pp. 3126-3128.
[10] B. He, "Zero digital image watermarking method against rotation attack based on block DCT transform", Microcomputer Application, vol. 7, no. 31, **(2010)**, pp. 1-10.
[11] D. Gabor, "A new microscopic principle", Nature, **(1948)**, pp. 161-177.
[12] D. Zheng, Y. Zhang, J. Shen and C. Zhang, "Principle and applications of digital holography", Physics and technology, vol. 11, no. 33, **(2004)**, pp. 834-847.
[13] S. Kishk and B. Javidi, "Watermarking of three-dimensional objects by digital holography", Opt. Lett (S0146-9592), vol. 3, no. 28, **(2003)**, pp. 167-169.
[14] N. Takai and Y. Mifune, "Digital watermarking by a holographic technique", Applied Optics, vol. 5, no. 41, **(2002)**, pp. 865-873.
[15] O. E. Okman and G. B. Akar, "Quantization index modulation-based image watermarking using digital holography", Opt. Soc. Am. A (S1084-7529), vol. 1, no. 24, **(2007)**, pp. 243-253.

Authors

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.

LuYan Qiao, she is a postgraduate, major in Information Security, now studying at Yanbian University in China. Her research interests are in the areas of copyright protection technology, information security, digital watermarking and digital forensic marking.

JongWeon Kim, he received the Ph.D. degree from University of Seoul, major in signal processing in 1995. He is currently a professor of Dept. of Intellectual Property at Sangmyung University in Korea. He has a lot of practical experiences in the digital signal processing and copyright protection technology in the institutional, the industrial, and academic environments. His research interests are in the areas of copyright protection technology, digital rights management, digital watermarking, and digital forensic marking.