

A video zero-watermarking algorithm based on LPM

De Li¹ · Luyan Qiao¹ · Jongweon Kim²

Received: 11 February 2015 / Revised: 19 April 2015 / Accepted: 3 June 2015 /

Published online: 12 June 2015

© Springer Science+Business Media New York 2015

Abstract To resist geometrical attacks, the video zero watermarking algorithm based on log-polar transform presented in this paper. In our method, an original image transformed in log-polar coordinate after transformation of 2D DWT and 3D DCT. In experiment, the proposed method was evaluated the performance of resistance against attacks such as noise attack, rotation attack, compression attack and frame attack. The experiment results show that this algorithm can effectively resist against geometric attacks, and it has high robustness to the noise, filtering, compression and other common attacks. The bit error rate of the proposed algorithm is less than 0.06 for all tested attacks.

Keywords Zero-watermark · Discrete wavelet transform · Discrete cosine transform · Log-polar transform · Logistic Map Encryption

1 Introduction

In recent years, the dissemination and exchange of digital products become more convenient, the piracy problem is growing seriously. Therefore, it is very urgent to the copyright protection of multimedia content. As an important branch of information hiding, digital watermarking technology plays an irreplaceable role in the information security field. Robust digital watermarking technology has good application value in related fields of digital content protection, such as the pirate and copyright protection, copy control.

✉ Jongweon Kim
jwkim@smu.ac.kr

De Li
leader1223@ybu.edu.cn

Luyan Qiao
leslie1295615290@163.com

¹ Department of Computer Science, Yanbian University, Yanji, China

² Department of Contents and Copyright, Sangmyung University, Seoul, South Korea

The current digital watermarking methods, whether the spatial domain watermarking algorithm, or the frequency domain watermarking algorithm, is to embed the watermarking by modifying the image information, which will lead to a certain amount of image distortion. We often reduce the watermark strength to ensure that the watermark is not visible, which will affect algorithm's robustness. In order to avoid image distortion, Wen quan [10] proposed the concept of zero watermarking, namely the use of important information to construct the watermark, but not modify any content of image. In addition, different carrier generate different watermarking, unlike that conventional watermark has a specific content, so it is necessary to establish the zero watermark database to store the watermark information. Although zero watermarking can solve the imperceptibility problem, how to find the important features of the image to construct zero watermarking has become the focus of research. The use of high order cumulant and the most significant bit to construct zero watermark, can effectively improve the robustness of the watermark against conventional attacks, but the ability to resist geometric attacks is greatly reduced. Niu Wanhong, Yan Huiqin proposed a zero watermarking algorithm based on the highest effective bit [9]. Due to the high image plane for image sensory quality has played a major role, low impact on the visual effect of image plane is small, so the selection of images of high information construct zero-watermark has certain robustness. Zhou constructs water key through the use of low frequency component obtained by Contourlet transform on the original video [17]. It can resist compression attacks well, but it is poor to the rotation attacks. Xu [11] presents a video zero watermarking algorithm based on Zernike moment, it can be very good to resist rotation attacks, but the algorithm is complex and large amount of calculation.

For the zero watermarking algorithm, the key point of the study is to extract the features characterizing the works in the digital works, and thus to construct a robust zero watermarking. In order to improve the ability to resist the attacks of watermarking, especially geometrical attack, this paper uses DWT and DCT dual transform domain to obtain the key feature information as zero watermarking, and do log-polar transform on the watermarking to resist the rotation attack.

2 Related technology

2.1 Discrete wavelet transform

Discrete wavelet transform, is a branch of science which is developed based on Fourier transform [3]. Since wavelet transform appeared, it replaced the Fourier transform position with analysis of its multi scale refinement. Fourier transform is the reflection of the frequency characteristics of the signal all the time, not information in any local time. The wavelet transform is the local transformation of time and frequency. It can be a function or signal multi-scale and multi-resolution analysis by translation and dilation operation [15], solving a lot of problems.

Wavelet transform has the multi-resolution characteristics well, interval wavelet support is not the same size square. The basic idea of DWT transform in image processing is the image multi-resolution decomposition. The image is decomposed into two parts, the low frequency and high frequency. The original carrier signal will be 4 parts through a layer of wavelet decomposition, namely, a low frequency part and three high frequency parts [7, 16]. If we decompose into two layers to the low frequency part after one layer wavelet decomposition, then will get 4 sub-band parts, and so on, we will get multi-level wavelet decomposition coefficients through multiple

decomposition. The low frequency sub-band part contains most of the information carrier, and the high frequency part can be divided into horizontal (HL), vertical (LH), and diagonal (HH) in three directions, this part describes the detail information carrier in three directions. The image of the two layer wavelet decomposition principle as shown in Fig. 1.

In the zero watermarking algorithms, generally we choose the low frequency coefficient to construct watermark [12], as it contains most of the energy of the original image. The watermark constructed by this method is robust against common attacks.

2.2 Discrete cosine transform

DCT transform is orthogonal transform based on real; it avoids the complex computation of discrete Fourier transform. The transformation is one of the core lossy image compression systems.

A pixel $s(x, y)$ in image size of $N \times N$ DCT transform as shown in (1) [1]:

$$S(u, v) = \frac{2}{N} c(u)c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} s(x, y) \cos\left(\frac{\pi u(2x + 1)}{2N}\right) \cos\left(\frac{\pi v(2y + 1)}{2N}\right) \tag{1}$$

Inverse discrete cosine transform as shown in (2):

$$s(x, y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u)c(v) S(u, v) \cos\left(\frac{\pi u(2x + 1)}{2N}\right) \cos\left(\frac{\pi v(2y + 1)}{2N}\right) \tag{2}$$

Where

$$c(u) = c(v) = \begin{cases} \frac{1}{\sqrt{2}}, & u = 0, v = 0 \\ 1, & u, v = 1, 2, \dots, N-1 \end{cases}$$

Given the image information $s(x, y)$, there are two ways of its DCT transform. One of is the image $s(x, y)$ as a two-dimensional signal, directly on the DCT transform; another kind is

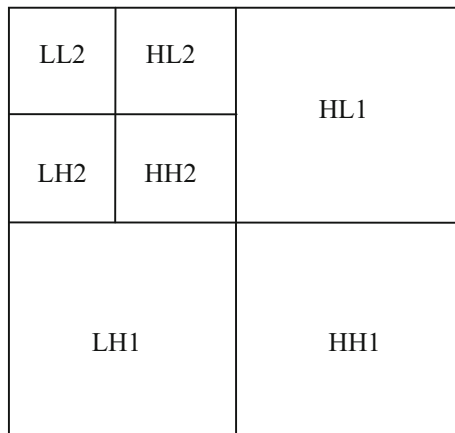


Fig. 1 Schematic diagram of two-layer wavelet decomposition

consistent with JPEG compression standard, first divides the image into 8×8 block, then for each block DCT transform. No matter for which block DCT transform, we will get DC coefficients and AC coefficients [5, 8]. DC coefficients belong to the low frequency part, it focuses on the maximum energy of the block [2, 4], and AC coefficients belong to the high frequency part.

In the zero watermarking algorithms, generally we choose the low frequency coefficient to construct watermark. As this part concentrates most of the energy of the original image, the general image processing and non-malicious compression will not change this part. So the watermark has good robustness.

2.3 The log-polar transform

The log-polar transform expresses a kind of transform image description. Descartes coordinates represents the scene plane coordinate position, as shown in Fig. 2. The log-polar transformation coordinates position, as shown in Fig. 3.

Descartes coordinate plane: $z=x+yi$

Log-polar coordinate plane: $\xi=\ln r, \psi=\theta$

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

Log-polar coordinates has two very important properties. In the axial the scale changes into log-polar lower translation. For example, a target takes the fixation as the center to amplify k times. Transform formula is as follows:

$$\xi_1 = \ln(k \cdot \rho) = \ln(k) + \ln(\rho) = \ln(k) + \xi \quad (3)$$

Among them, ξ, ξ_1 represent Y-axis in log-polar coordinate before and after the longitudinal. Equation (3) shows that the equivalent mapping moves down $\ln(k)$ units, target rotates L radian around the fixation point.

$$\psi_1 = \psi + L \quad (4)$$

Among them, ψ, ψ_1 represent X-axis in log-polar coordinate before and after the rotation. Equation (4) shows that the equivalent mapping image moves to the right L units. The two features is called distance invariability and angle invariance [6]. Namely it makes rotation and

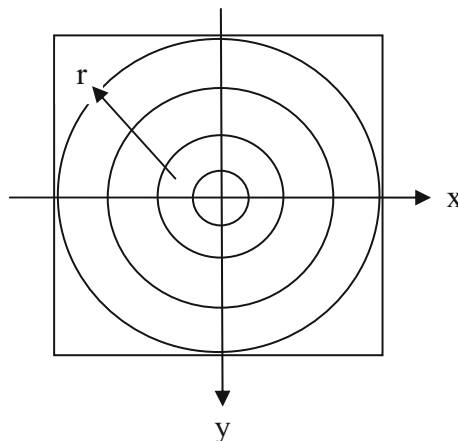


Fig. 2 Descartes coordinate

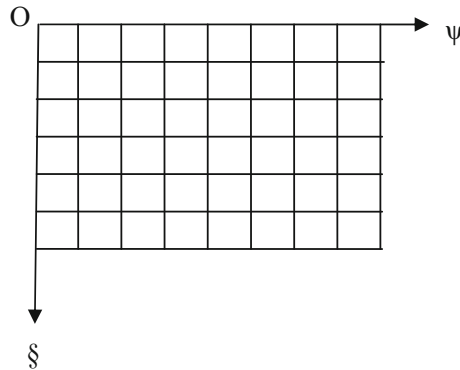


Fig. 3 Log-polar coordinate

scaling in Cartesian coordinates convert into cyclic shift [13]. In the watermarking algorithm, we can use this property to resist rotation attacks.

3 Video zero watermarking algorithm

3.1 The zero watermarking generation algorithm

At present, many watermarking algorithms are using in dual transformed domains for their robustness. As different transform domain combination has different processing effect on the carrier in 3D spatial data to process the video files. We combined the above two kind of transformation by using 2D DWT and 3D DCT method, then added the log-polar transform to generate zero watermarking. The more detail steps are described as bellows. Figure 4 shows the watermark generating flow chart in our method.

- Step 1. Reading the original video data, while selecting the key frames from the original video, then group these frames according to the size of N ;
- Step 2. 2D DWT transform for each frame of each group;
- Step 3. Divide each group of each frame of the low frequency LL coefficients into 8×8 block size;
- Step 4. 3D DCT transform for each block, and get DC coefficients matrix;
- Step 5. Log polar transform to the DC coefficients and get the LPM image;
- Step 6. Generate sequence $A \{A_1, A_2, \dots, A_M\}$ and $B \{B_1, B_2, \dots, B_M\}$ whose range within the $[0.1/2n]$ by K_1 and K_2 , this is Logistic Map Encryption [14];
- Step 7. As the range of the elements in the sequence between $[0.1]$, take $A_i = R \times A_i$, $B_i = R \times B_i$, ($i=1, 2, \dots, M$) where R is the size of the low frequency domain. We can ensure the position of the selection distribution in the low frequency domain;
- Step 8. Calculate $\{LL_{RA1}-LL_{RB1}, LL_{RA2}-LL_{RB2}, \dots, LL_{RAi}-LL_{RBi}\}$ according to the generated structural points sequence and get the difference sequence $Y \{Y_1, Y_2 \dots Y_i\}$;
- Step 9. In accordance with $Y_i \leq 0, W=0; Y_i > 0, W=1$ to generate 0.1 matrix;
- Step 10. Make the CS image and the generated 0.1 matrix do logical XOR operation, generating registered zero watermarking.

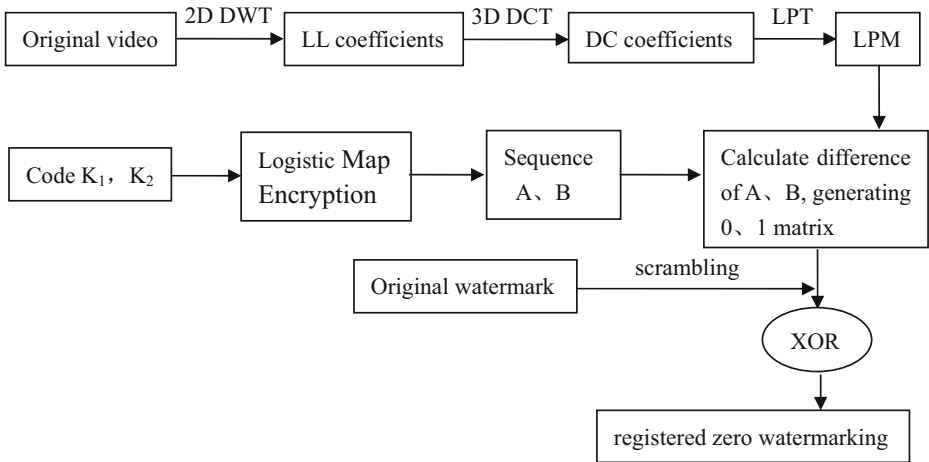


Fig. 4 Watermark generating flow chart

3.2 The zero watermarking detection algorithm

The detection processing is similar to the generation processing as in the former section. It is performed the same procedure to generate zero watermarking, and then operated logical XOR operation with registered watermarking to get the original watermark. The detecting procedure is shown in Fig. 5.

- Step 1. Reading the original video data, while selecting the key frames from the original video, then group these frames according to the size of N;
- Step 2. 2D DWT transform for each frame of each group;
- Step 3. Divide each group of each frame of the low frequency LL coefficients into 8×8 block size;

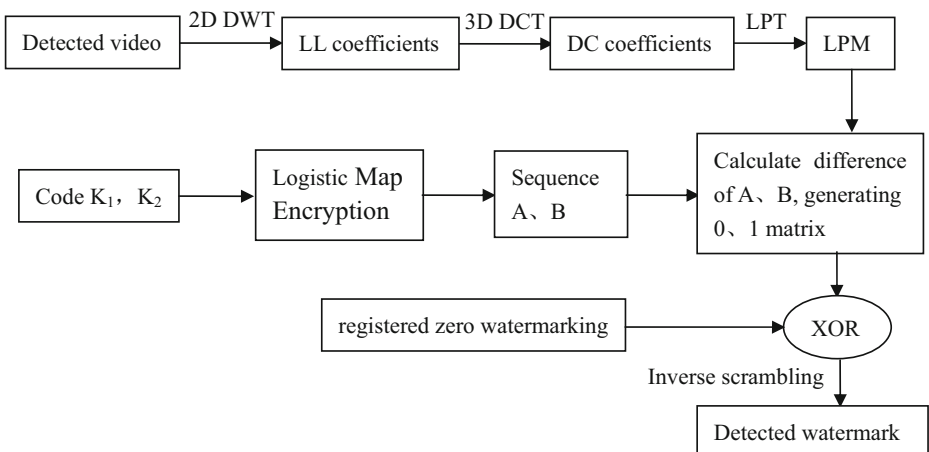


Fig. 5 Watermark detecting flow chart

- Step 4. 3D DCT transform for each block, and get DC coefficients matrix;
- Step 5. Log polar transform to the DC coefficients and get the LPM image;
- Step 6. Generate sequence $A\{A_1, A_2, \dots, A_M\}$ and $B\{B_1, B_2, \dots, B_M\}$ whose range within the $[0.1/2n]$ by K_1 and K_2 , this is Logistic Map Encryption;
- Step 7. As the range of the elements in the sequence between $[0.1]$, take $A_i=R \times A_i$, $B_i=R \times B_i$, ($i=1, 2, \dots, M$) where R is the size of the low frequency domain. We can ensure the position of the selection distribution in the low frequency domain;
- Step 8. Calculate $\{LL_{RA1}-LL_{RB1}, LL_{RA2}-LL_{RB2}, \dots, LL_{RAi}-LL_{RBi}\}$ according to the generated structural points sequence and get the difference sequence $Y\{Y_1, Y_2, \dots, Y_i\}$;
- Step 9. In accordance with $Y_i \leq 0, W=0; Y_i > 0, W=1$ to generate 0.1 matrix;
- Step 10. Remove the watermark from the registration database, by using the Boolean XOR and generated 0.1 matrix, to obtain original watermark.

4 The results and analysis of experiments

To evaluate the performance of our method, we carried out the experiments using Matlab 2010. We prepared the 100 uncompressed video files with the size of 320×240 and the binary image with the size of 20×15 as the watermark.

To verify the effectiveness of the algorithm, we selected video files that have rich high-frequency information (number 2 and 4), rich low-frequency information (number 5 and 7) and uniform distributed information (number 1.3 and 6). Table 1 shows the watermark generation and detection results without attacks.

To verify the robustness of our algorithm, we also carried out the attack experiments such as the Gauss noise, salt and pepper noise, rotation, frame exchange, frame loss, compression and other attacks.

4.1 Gaussian noise attacks

To demonstrate the robustness of this algorithm against Gaussian attacks, this paper made Gaussian attacks experiments. The results are shown in table 2.

The results of Table 2, the more noise strength is the lower, video quality. Though in distorted video image, we can still extract identifiable watermark. It means that the algorithm has good robustness to Gaussian noise attacks.

4.2 Salt & pepper noise attacks



















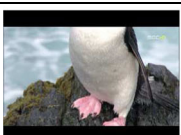























Our experimental results against Salt & pepper attacks are shown in table 3.

As see in Table 3, we can still detect the watermark well in the density of 0.5. It can be seen that the algorithm has good robustness against the Salt & pepper attacks.

4.3 Low-pass filtering attacks

To show the robustness of this algorithm against low-pass filtering attacks, we performed low-pass filtering attacks experiments. The results are shown in the Table 4.

Table 1 Effect diagram of watermark generating and detecting

Video No	Original video	Zero watermarking	Detected watermark	BER
1		CS     	CS CS CS CS CS CS	0.00
2		CS     	CS CS CS CS CS CS	0.00
3		CS     	CS CS CS CS CS CS	0.00
4		CS     	CS CS CS CS CS CS	0.00
5		CS     	CS CS CS CS CS CS	0.00
6		CS     	CS CS CS CS CS CS	0.00
7		CS     	CS CS CS CS CS CS	0.00

As seen in Table 4, we can observe that the video files are blurred after low-pass filtering attacks. But our method can still extract the watermark. It shows that the algorithm is robust against low-pass filtering attacks.

4.4 Rotation attacks

To show the robustness of this algorithm against rotation attacks, we performed rotation attack experiments. The rotation angles are 10°, 45° and 60°. The results are shown in the Table 5.

Table 2 Extracted results of Gaussian noise attacks




Gaussian	variance	0.01	0.05	0.1
Noise attack	The attacked image			
	Extracted watermark	CS CS	CS CS	CS CS
	BER	0.00	0.01	0.02

Table 3 Extracted results of salt & pepper noise attacks



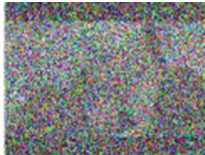
Salt & pepper	Density	0.01	0.05	0.2
Noise attack	The attacked image			
	Extracted watermark	CS CS	CS CS	CS CS
	BER	0.00	0.01	0.03

Table 4 Extracted results of low-pass filtering attacks


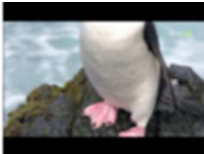
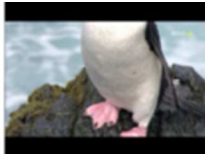



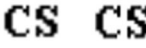
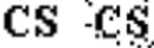

Low-pass	Frequency	10	30	50
Attack	The attacked image			
	Extracted watermark	CS CS	CS CS	CS CS
	BER	0.01	0.00	0.00

Table 5 Extracted results of rotation attacks

Rotation	Degree	10°	45°	60°
Attack	The attacked image			
	Extracted watermark			
	BER	0.00	0.06	0.00

From Table 5, we can see that this algorithm can effectively detect the watermark after log-polar transform. It proves that the algorithm has good robustness to rotation attacks.

4.5 Frame attacks

Frame attack is a common to the video watermarking attack. Exchanging the position of frames, or deleting some frames, are not easy to be perceived. To show the robustness of this algorithm against frame attacks, we performed frame attack experiments. The results are shown in the Table 6.

In Table 6, we can see that whether exchanging the frames or loss of frames, we can detect the watermark with completely and accurately.

4.6 Compression attacks

Coding is the most basic way to handle video files. At present, the most commonly used compression method is MPEG-4 standard. The video is compressed, information may be lost, which is likely to destroy the watermark. To demonstrate the robustness of this algorithm

Table 6 Extracted results of frame attacks

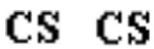

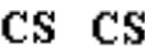


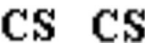
Frame switching	Switching	1st←→9st	5st←→21st	29st←→53st
	Extracted watermark			
BER	0.00	0.00	0.00	
Loss of frame	Number	3	5	15
	Extracted watermark			
BER	0.00	0.00	0.00	

Table 7 Extracted results of compression attacks

Compress	Bit rate	256Kbps	512Kbps	1024Kbps
Attack	Extracted watermark	CS CS	CS CS	CS CS
	BER	0.02	0.01	0.00

against compression attacks, this paper made compression attacks experiments. The results are shown in table 7.

From Table 7, we can see that we can still extract the watermark after compression attacks. So the algorithm can resist compression attacks well.

4.7 Comparison and analysis of the algorithm performance

In order to further verify the robustness of the algorithm, this article has carried on the contrast experiment with the literature [11, 17]. Below are the results.

From Fig. 6, we can see, compared with other two kinds of algorithms, this algorithm has strong robustness in resistance against, especially for the rotation attacks.

5 Conclusion

This paper proposed a video zero watermarking algorithm based dual transform domain and log-polar transform. We took the key features of video by using the dual transform domain as watermark, and then performed log-polar transform for the watermarking. In order to evaluate the performance of the proposed method, we performed the experiments with respect to robustness against several of attacks, such as adding Gaussian noise, rotation, low-pass

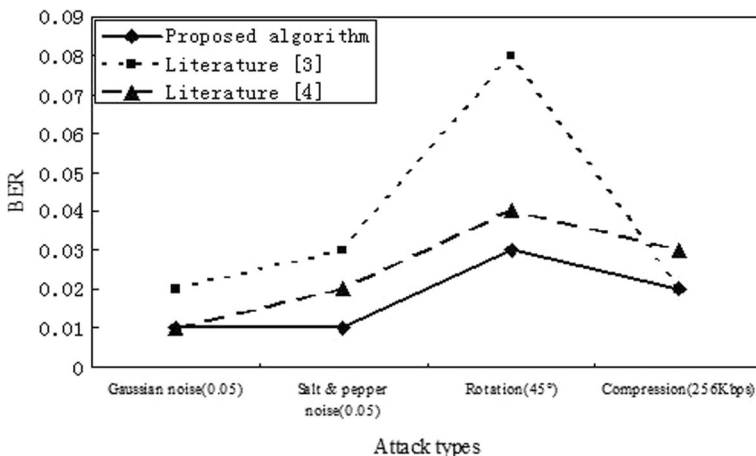


Fig. 6 Comparison of experimental results

filtering and compression. The results show that this algorithm not only can resist conventional attacks, but also is robust against geometric attacks. The bit error rates for Gaussian noise, salt and pepper noise, low-pass filtering, frame and compression attacks are less than or equal to 0.02, 0.03, 0.01, 0.06, 0.00 and 0.02 respectively.

In further studies, we should apply our method to different types of files to prove the validity of the algorithm, through the objective analysis of some performance evaluation index and experiment the different types of attacks, such as noise attack, rotation attack, cropping attack, frame attack to verify robustness.

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

References

1. Chang H, Tsan C (2005) Image watermarking by use of digital holography embedded in the discrete-cosine-transform. *Appl Opt* 44(29):6211–6219 (S0003-6935)
2. Cox J, Kilian J, Liehtonz T (1997) Secure spread spectrum watermarking for multimedia. *IEEE Trans Image Process* 6(12):1673–1687
3. Daubechies I (1992) Ten Lectures on Wavelets [M]. SIAM: Society for Industrial and Applied Mathematics, Philadelphia
4. He B (2010) Zero digital image watermarking method against rotation attack based on block DCT transform. *Microcomput Appl* 7(31):1–10
5. Hu Y, Zhu S (2008) Zero-watermarking algorithm based on PCA and chaotic scrambling. *J Zhejiang Univ (Eng Sci)* 42(4):593–597
6. Pu P, Guo X, Lei L (2008) Application of image interpolation in Log-polar transformation. *Comput Eng* 34(5):198–199
7. Ruan B (2008) Researchers of Digital Image Watermarking Algorithm Based on DWT-SVD. Master's degree thesis of Southwest Jiaotong University, pp.19-21.
8. Tao X, Zhang Y, Sun J, Zhang J, Lin Z (2009) Zero-watermarking scheme for 3D meshes based on geometric property. *J Image Graph* 14(9):1819–1824
9. Wanhong N, Huiqin Y (2009) A zero watermarking algorithm based on the MSB construction key. *Appl Comput Syst* 18(12):66–69
10. Wen Q, Sun T, Wang S (2003) The concept and application of zero watermarking. *Chin J Electron* 1(3):214–216
11. Xu D, Wang J, Wang R (2009) An object-based video zero-watermarking algorithm using Zernike moments. *J Image Graph* 14(9):1825–1831
12. Yang S, Li C, Sun F (2003) Research on zero-watermarking of images in the wavelet domain. *J Image Graph* 8(6):664–669
13. Yu B, Guo L, Zhao T (2008) Gray projection image stabilizing algorithm based on log-polar image transform. *Comput Appl* 28(12):3126–3128
14. Zhang C (2007) Research on binary text image digital watermarking technology. Master's degree thesis of Chongqing University, pp.21–22.
15. Zhang D (2009) MATLAB wavelet analysis. China Machine Press, Beijing

16. Zhao HY, Liu K, Li AJ (2011) A digital image zero watermarking algorithm based on wavelet transform. *Coal Technol* 30(11):164–168
17. Zhou Z, Yang G, Quan T, Wang Z (2010) Digital video zero-watermarking algorithm based on contourlet Transform. *Microcomput Inform* 26(12):82–84



De Li 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 Creative Content Labs, Sangmyung University. His research interests are in the areas of copyright protection technology, digital watermarking, and digital forensic marking.



Luyan Qiao 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 zero watermarking.



Jongweon Kim Received the Ph.D. degree from University of Seoul, major in signal processing in 1995. He is currently a professor of Dept. of Contents and Copyright and Chief of Creative Content Labs 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.