

A Spread Spectrum Zero Video Watermarking Scheme based on Dual Transform Domains and Log-Polar Transformation

DaYou Jiang¹, De Li^{1*} and JongWeon Kim²

¹Department of Computer Science, Yanbian University
133002, Yanji, China

²Department of Intellectual Property, Sangmyung University
110743, Seoul, Korea

ybdxgxy13529@163.com¹, leader1223@ybu.edu.cn¹, jwkim@smu.ac.kr²,

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

Abstract

This paper proposes a zero-video watermark scheme based on 2D-DWT and pseudo 3D-DCT, otherwise Singular Value Decomposition and log-polar transform are applied. The method makes no changes to original images while embedding the owner information of images so as to achieve high transparency. The log-polar transform ensures that the method is robust to rotation operations. In order to achieve the high robustness and security, we use chaotic logistic mapping and spread spectrum (CLMSS) to spread the watermark information. we also use the visual cryptography (VC) scheme to split the secret image into two shares. In the scheme, we use spread spectrum to encode the watermark to a Code Division Multiple Access watermark and use dual transform and log-polar to generate the feature values. Then the visual cryptography scheme is applied to generate the secret image from the feature values and the watermark. In the extraction scheme, we use the secret image which is registered to certification authority and the feature values extracted from the examined image with visual cryptography scheme to generate the CDMA watermark, and then decrypt it to get the watermark information.

The experimental are conducted to verify the robustness through a series of experiments.

Keywords: Zero-video watermarking, Log-Polar Transformation, Spread Spectrum, Visual Cryptography, Singular Value Decomposition

1. Introduction

Digital watermarking technique is an effective method to solve the copyright protection problems of digital media. Many existing digital watermarking schemes by using discrete Fourier transform [1], discrete cosine transform [2], the discrete wavelet transform [3], fractional Fourier transform [4], radon transform [5], and singular value decomposition [6] perform well against common signal processing operations such as addition of noise, and signal filtering.

Video watermarking introduces some issues not present in image watermarking. On one hand, video signals are highly susceptible to pirate attacks such as frame dropping, frame averaging and frame swapping. On the other hand, the three dimensional characteristic of the video make it harder to provide an imperceptibility of the watermark. Most of the current video watermarking technique insert watermark directly to uncompressed or compressed video sequences [7]. Niu and Sun proposed a wavelet based watermarking method that embeds decomposed watermark at different resolution in the corresponding resolution of the decomposed video by means of multirotation solution signal decomposition [8]. Barni *et al.* proposed a robust watermarking scheme for raw video that alters the DFT coefficients of the brightness components of the to-be-marked frames. The

scheme is robust against filtering, scaling and cropping attacks [9]. Th.Rupachandra *et al.* proposed a video watermarking scheme based on visual cryptography, scene change detection and DWT. The scheme uses an identical sub-band watermark for the same scene, but different parts in different scenes [10].

We proposed a new video zero-watermarking scheme based on dual domains and log-polar transformation in this paper. The log-polar transformation can be invariant to rotation attack. In order to improve the transparency and the imperceptibility of the watermarked video, the watermark scheme is one of blind zero-watermarking approaches. The VC scheme and CLMSS are also used to achieve the high robustness and security of the watermark.

The rest of the paper is organized as follows: in Section 2, CLMSS, 2D-DWT and pseudo 3D-DCT transform and VC are briefly proved. Details of the proposed embedding and extracting scheme are described in Section 3. Section 4 presents a variety of simulation experimental results, which illustrate the effectiveness of the proposed algorithm. Finally we conclude the paper in Section 5.

2. Background

In this section, the concepts of Chaotic Logistic map and Spread Spectrum, 2D-DWT and pseudo 3D-DCT, Log-Polar transformation and Visual Cryptography are briefly described.

2.1 Chaotic Logistic Map and Spread Spectrum Transform

In this paper, we use chaotic logistic map and spread spectrum transform to generate a spread spectrum and chaotic logistic watermark.

Chaos based encryption techniques are considered good for practical use as these techniques provide a good combination of speed, high security, complexity, reasonable computational overheads and computational power [11].

The chaotic logistic map (CLM) which we employed to achieve the goal of image encryption is as follow [12]:

$$X_{n+1} = \lambda X_n(1 - X_n) \quad (1)$$

Here, λ and X_n which respectively falls in the interval $[0, 4]$ and $(0, 1)$. When λ is within the range between 3.569945 and 4, the logistic map is chaotic. Chaotic sequence generated by the logistic map highly depends on the initial conditions; also its properties of auto-correlation and cross-correlation are good. The properties will enable us to use the initial conditions such as system parameter λ and sequence initial value X_0 as the cipher keys.

Pickholtz [13] define spread spectrum (SS) communication firstly. Results from the SS systems are capable of approaching the Shannon limit for reliable communication; they are increasingly widely applied to digital watermarking [14].

A form of Direct Sequence Code Division Multiple Access (DS-CDMA) spread spectrum communications was employed in the paper. Suppose the encrypted watermark sequence E_n is denoted as follow:

$$m = \{b_i \mid b_i \in \{0,1\} \} i = 1,2, \dots, N \times M \quad (2)$$

Then we employ the quadrature amplitude modulation (QAM) to the sequence, the generated binary polarity sequence of $\{-1, 1\}$ is denoted as follow:

$$m' = \{b'_i \mid b'_i \in \{-1,1\} \} i = 1,2, \dots, N \times M \quad (3)$$

If we define the pseudo-random noise pattern as follow:

$$P = \{P_{i,j}(k) | k = 1, 2, \dots, N \times M\} \quad (4)$$

Where $P_{i,j}(k)$ is 2-D pseudo-random binary sequence of $\{-1, 1\}$ with zero mean generated using the key as the seed.

Then the CDMA watermark will be

$$w = P \cdot m' = \sum_{k=1}^{N \times M} P_{i,j}(k) b_k \quad (5)$$

Figure 1 shows an example of this method.

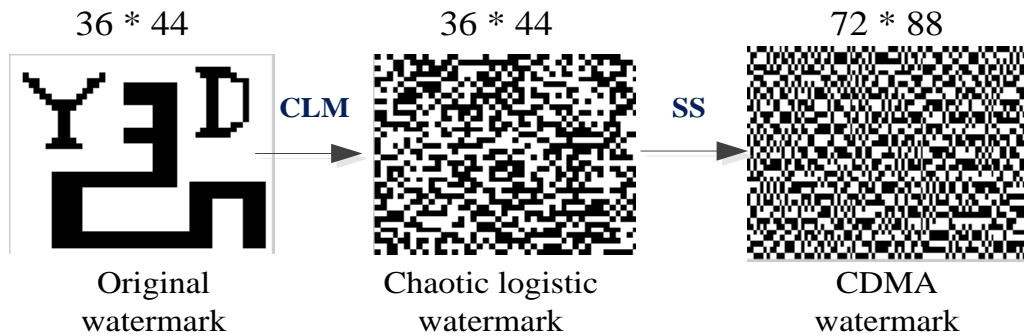


Figure 1. An Example of Chaotic Logistic Map and Spread Spectrum

2.2 2D-DWT and Pseudo 3D-DCT

Considering that the DWT preserves the local edges and noise reduction in the low frequency domain after the image decomposition and the DCT is obviously to decrease the correlation of the video image. In this paper, we combined the DWT and DCT to process video image. Firstly, we choose key-frame of the raw video sequence and separate them into groups, and each group consists of N frames. Secondly, we select the Y sample of each frame and take 2D-DWT to each frame of every group. Then divide the LL coefficients into 8×8 blocks of all frames. At last, take pseudo 3D-DCT transform to each blocks of the group.

2.3 Log-Polar Transform

The Log-Polar mapping (LPM) which maps the Cartesian coordinate system into the polar coordinate system. Let (x, y) and (r, θ) denote a point in Cartesian coordinate system and its corresponding polar coordinate, respectively. The mapping formulas are specified as follow:

$$r = \sqrt{(x - x_c)^2 + (y - y_c)^2} \quad (6)$$

$$\theta = \tan^{-1} \frac{y - y_c}{x - x_c} \quad (7)$$

Where (x_c, y_c) stands for the origin of the Cartesian system. Figure 2 illustrates the example for the properties of the LPM transformation. Through the experience, it is easy

to observe that the image just move along vertical and horizontal lines after rotation, scaling and transform operations.

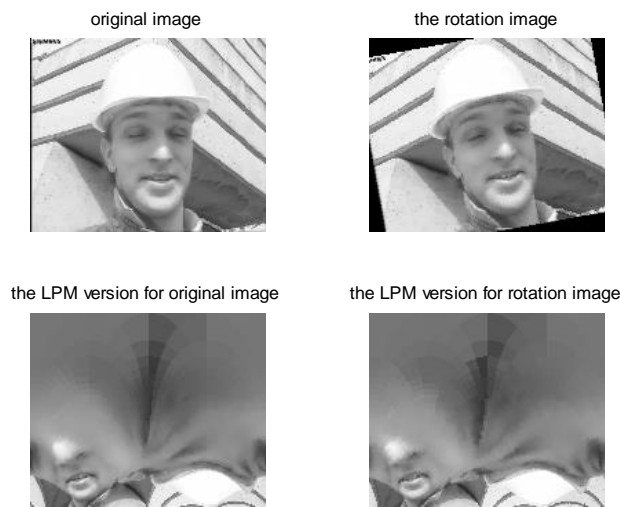


Figure 2. The Example for the Properties of the LPM Transformation

2.4 Visual Cryptography

Visual cryptography is 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) scheme, called visual cryptography [15]. 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 or more than k shadows. VC which achieves requirements of robustness, imperceptibility, security, blindness is widely used as a kind of loss-less watermarking.

Considering the convenience and security of the scheme, in this paper, we employed a $(2, 2)$ 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. Binary map, and the binary map is generated by a Table.1 shows the concept of $(2, 2)$ VSS scheme. An example of the scheme is shown in Figure 3.

Table 1. Concept of $(2, 2)$ VSS Scheme











Pixel color	White Pixel 	Black Pixel 
Share 1	 	 
Share 2	 	 



Figure 3. An Example of (2, 2) VSS Scheme

3. Proposed Zero Video Watermarking Scheme

In this section, we explain the proposed zero video watermarking scheme in detail.

3.1 Watermark Embedding Process

Figure 4 shows the process of the embedding scheme. The main steps of the embedding procedure are described as follow:

Step1: Watermark image preconditioning

- (1) Select the binary image with 36×44 pixels as watermark information.
- (2) Apply CLMSST described in 2.1 to the watermark.

Step2: YUV video preconditioning

- (1) Select 256 frames of the raw YUV video, then select key-frames in every 4 frames and separate each 4 key-frames into groups.
- (2) Select Y samples of each key-frame of each group. Then apply LPM transformation described in 2.3 and 2D-DWT and pseudo 3D-DCT described in 2.2 and SVD in orderly to those frames in each group to get the feature value.

Step3: Employ VC technique described in 2.4 to generate the secret information from the feature value and the watermark, and then register the secret information to certification authority (CA).

3.2 Watermark Extraction Process

The extraction process is similarity to the embedding process. The difference is that do the Log-Polar transformation and 2D-DWT and pseudo 3D-DCT to the protected video to get the feature value, then using VC technique to generated the watermark from the feature value and the secret image. Then do the decryptions process of CLMSST to decrypt the extracted watermark. Figure 5 shows the process of the extraction scheme.

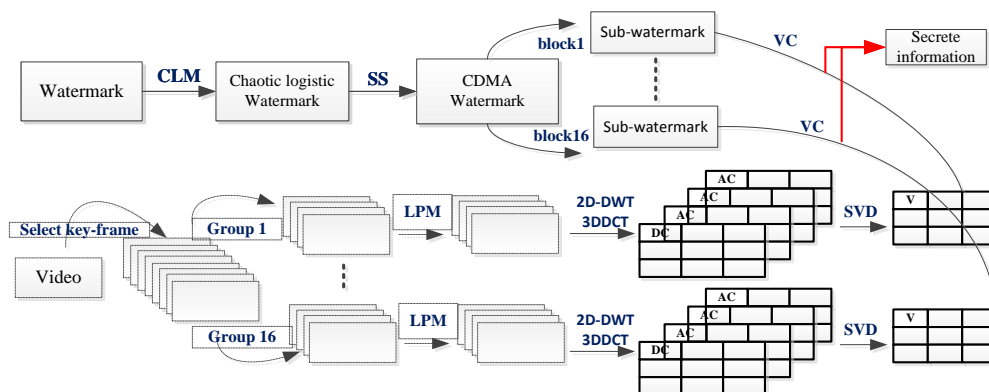


Figure 4. Process of the Embedding Scheme

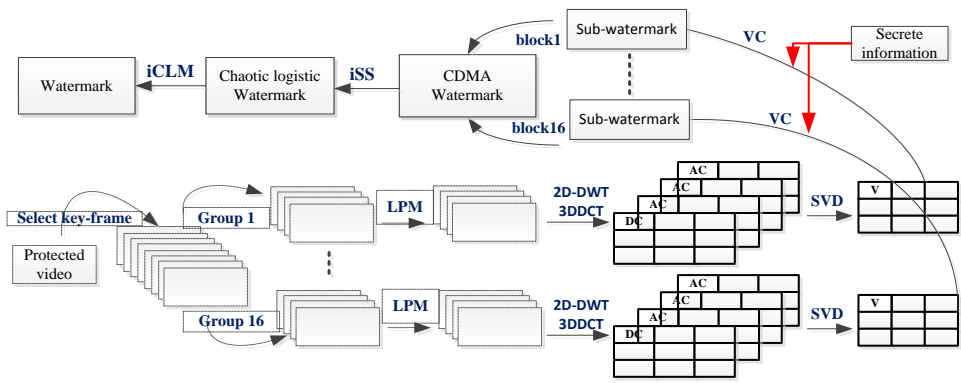


Figure 5. Process of the Extraction Scheme

4. Experiment Results and Analysis

To evaluate the performance of the proposed scheme, we used 4 video sequences with CIF format and 30 FPS. All video sequences have 300 frames which are available in [16]. The watermark image is denoted by a binary image, the size of which is 36×44 . Table 2 shows watermark and video sequences used for evaluation of the proposed method.

Table 2. The Video Sequences and Watermark Image

watermark	foreman	news	container	bus

In this paper, Bit Error Rate (BER) and normalized cross-correlation (NC) are used to evaluate the similarity between an original watermark and the extracted watermark.

The high NC and low BER convey high robustness. When using the proposed algorithm for watermark embedding, by reason of the method is loss-less, there is no difference between the watermarked video and the cover video. In addition, for all video sequences, the results show that NC is 1 while the BER is 0. It is evident that the proposed algorithm can accurately extract the watermark without error.

In order to assess the embedded watermark robustness, the watermark video sequences are attacked using some common signal processing and frame-based attacks. In the proposed method, the watermark is embedded into Y samples of each key-frames with static step size of the video scene. All the attacks are performed in these key-frames.

The watermarked video sequences are subject to signal process attacks including noise contamination such as Gaussian noise attack (shown in Table 3) and salt & pepper noise (shown in Table 4), Gaussian low-pass filtering ,median filtering, averaging filtering (shown in Table 5),rotation(shown in Table 6) and cropping (shown in Table 7).

Additionally we evaluated the proposed scheme against frame-based attacks. A video sequence contains lots of temporal redundancy, so frame-based attacks, such as frame dropping (shown in Table 8) ,frame averaging (shown in Table 9) and frame swapping(shown in Table 10 and Table 11),are efficiently done to remove the watermark sequence without cause significant quality degradation.

Table 3 and Table 4 show the result of proposed method under noise contamination. We set Gaussian noise at zero mean and its variances ranging from 0.005 to 0.02. The salt & pepper noise density is set ranging from 0.01 to 0.04. It is found that the watermark is

clearly identifiable. It is because the high frequency components are affected by the noise, while the low frequency components in LL sub band is the least affected.

Table 5 shows the result of proposed method under different filtering such as Gaussian low-pass filtering, median filtering and averaging filtering. The values of window sizes are all set 3×3. The results show that the proposed method is highly robust to filtering attacks.

Table 6 shows the result of the proposed method under rotation attack at different rotation angle from 10° to 60° in counter clockwise direction. Even though the BER value is up to 0.1452, the extracted watermark is still identifiable. Since the returned image is cropped to fit the same size as the original image, the results value of BER is within acceptable limits. By using Log-Polar transformation, the results show that the method is robust under rotation attack.

Table 7 shows the result of the proposed method under cropping attack. The percentage of cropping is ranging from 12.5% to 43.75%. 12.5% cropping corresponds to removing 36 horizontal lines per frame in the video. Since it's a video sequences, in order to make sure that the cropped video is still attractive for people to watch, we purposely crop the video from outside to inside from all directions. Doing so, even the cropping percentage is up to 43.75%, the result still shows that the method is robust under cropping attack.

Table 8 shows the result of the proposed method under frame dropping attack. In the method, the dropping key-frames are selected from each group. The number of groups is ranging from 3 to 15 (nearly 25% percentage of all key-frames). The results show that the BER value is less than 0.03, so the method is robust under frame dropping attack.

Table 9 shows the result of the proposed method under frame averaging attack. In the method, the averaging key-frames are selected from each key-frame. The number of frames is ranging from 6 to 16 (25% percentage of all key-frames). We collect a number of frames, then replacing each pixel' value of each frame by the estimated average value of each pixel. The results show that the method is robust under frame averaging attack.

Table 10 and Table 11 show the result of the proposed method under frame swapping attack. The frame swapping attack is divided into two types, one is within-group, the other is inter-group. Table 10 shows that the within-group swapping program has no effect on the BER value which illustrate that the watermark is embedded into the frame group. To maximize the BER, while doing the inter-group swapping program, the key-frames are selected from each group firstly (each group can only select one frame), then select contiguous groups to swap (such as group 1 and group2, group 3 and group 4). In the program, the number 5 of swapping frames means that 10 frames from different 10 groups are swapped. Even though, the watermark is clearly identifiable.

Table 3. Extracted Results of Gaussian Noise Attacks









variance	0.005	0.010	0.015	0.020
Attacked Frame				
Extracted Watermark				
NC	0.9816	0.9816	0.9839	0.9774
BER	0.0253	0.0253	0.0221	0.0309

Table 4. Extracted Results of Salt and Pepper Noise Attacks









density	0.01	0.02	0.03	0.04
Attacked Frame				
Extracted Watermark				
NC	0.9986	0.9936	0.9936	0.9918
BER	0.0019	0.0088	0.0088	0.0114

Table 5. Extracted Results of Filtering




type	Gaussian low-pass filtering	Averaging filtering	Median filtering
Extracted Watermark			
NC	1.0000	0.9991	0.9982
BER	0	0.0013	0.0025

Table 6. Extracted Results of Rotation Attacks













angle	10	30	45	60
Attacked Frame				
Extracted Watermark				
NC	0.9839	0.9439	0.9160	0.8896
BER	0.0221	0.0758	0.1117	0.1452

Table 7. Extracted Results of Crop Attacks

percentage	Crop 12.5%	Crop 25%	Crop 23.44%	Crop 43.75%
Attacked Frame				





Extracted Watermark				
NC	0.9931	0.9307	0.9961	0.9798
BER	0.0095	0.0928	0.0051	0.0278

Table 8. Extracted Results of Frame Dropping





group	1-3	1~7	1~11	1~15
Extracted Watermark				
NC	0.9982	0.9830	0.9830	0.9775
BER	0.0025	0.0234	0.0234	0.0309

Table 9. Extracted Results of Frame Averaging





numbers	6	9	12	16
Extracted Watermark				
NC	0.9853	0.9835	0.9803	0.9529
BER	0.0202	0.0227	0.0271	0.0644

Table 10. Extracted Results of Frame Swapping (within-group swapping)









within-group	2	4	6	8
Extracted Watermark				
NC	1.0000	1.0000	1.0000	1.0000
BER	0	0	0	0

Table 11. Extracted Results of Frame Swapping (inter-group swapping)

inter-group	2	3	4	5
Extracted Watermark				
NC	0.9886	0.9597	0.9592	0.9355
BER	0.0158	0.0549	0.0556	0.0871

5. Conclusion

In this paper, we proposed a zero video watermarking technique robust against several signal processing distortions and frame-based attacks. The watermark is implicitly hidden in the secret key instead of the image contents. To improve robustness and security of the method, the chaotic logistic map, spread spectrum and visual cryptography are used. During watermark embedding, it first finds out the feature characteristics of host video by applying log-polar transformation, 2D-DWT and pseudo 3D-DCT, SVD in orderly. Secondly the watermark is encoded by chaotic logistic map and spread spectrum. Finally the visual cryptography is used to generate the secret image for authentication. Although the proposed scheme still has limitations such as a need for a trusted third party to store the secret images. But it is blind and also has high imperceptibility and robustness. Future work will focus on applying a method without the correct security key.

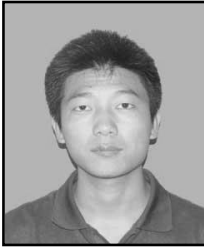
Acknowledgements

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

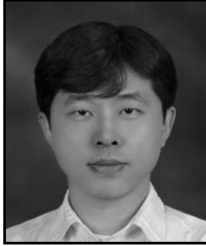
References

- [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; Beijing, China. pp. 1039-1044.
- [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; Wuhan, China, pp. 34-36.
- [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; Chengdu, China. pp. 163-166.
- [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. pp. 659-663.
- [5] L. Cai, S. D. Du and D. T. Gao, "Geometrically Invariant Watermarking based on Radon Transformation", JOURNAL OF ELECTRONICS, (2005) May, vol. 22, no. 3, 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] G. Doerr and J. Dugelay, "A guide tour if video watermarking", Signal Processing Image Communication, vol. 18, no. 4, (2003), pp. 263-282.
- [8] X. Niu and S. Sun, "A new wavelet based digital watermarking for video", In: Proc. IEEE Digital Signal Processing Workshop, (2000) October, Texas, USA.
- [9] M. Barni, F. Bartolini, R. Caldelli, AD. Rosa and A. Piva, "A robust watermarking approach for raw video", In: Proc. 10th International Packet Video Workshop, (2000), May 2; Cagliari, Italy.
- [10] Th. Rupachandra Singh, Kh. Manglem Singh and Sudipta Roy, "Video watermarking scheme based on visual cryptography and scene change detection", Int. J .Electron. Commun., (AEU), vol. 67, no. 8, (2013) August, pp. 645-651.
- [11] N. K. Pareek, V. Patidar and K. K. Sud, "Image Encryption using Chaotic Logistic Map, Image and Vision Computing", vol. 24, no. 9, (2006), pp. 926-934.
- [12] T. Kohda and T. Suneda, "A Pseudo noise sequences by chaotic nonlinear maps and their correlation properties [J]", IEICE Trans communication, E762B vol. 8, (1993), pp. 855-862.
- [13] R. L. Pickholtz, D. L. Schilling and L. B. Milstein, "Theory of Spread Spectrum Communications- a tutorial", IEEE Trans. Commun. COM-30 vol. 5, (1982) May, pp. 855-884.
- [14] A. Baharak, K. Fatih, M. Peter and B. Ahmed, "Spread Spectrum Watermarking based on the Discrete Sheralet Transform", EUVIP University of Paris, (2013) June, pp. 178-183.
- [15] M. Naor and A. Shamir, "Visual cryptography", in: Proceedings of the Advance in Cryptology-EUROCRYPT'94, Lecture Notes in Computer Science, Spring-Verlag, vol. 950, (1995), pp. 1-12.
- [16] <<http://trace.eas.asu.edu/yuv/index.html>>.

Authors



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



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.

