Robust Image Watermarking Based On Quantization Index Modulation in the DCT Domain

Min Lei[1,3,5], Xiaoming Liu[2], Mian Wang[1], Yu Yang[1], Zhiguo Qu[3,4]

[1] Information Security Center, Beijing University of Posts and Telecommunications, China
[2] National Computer Network Emergency Response Technical Team/Coordination Center, China
[3] Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, China
[4] School of Computer & Software, Nanjing University of Information Science & Technology, China
[5] Guizhou Provincial Key Laboratory of Public Big Data, Guizhou University, China

leimin@bupt.edu.cn, liuxm@cert.org.cn, WangMian2015@bupt.edu.cn, yangyu@bupt.edu.cn, qzghhh@126.com

Abstract

The main drawback of the traditional quantization index modulation (QIM) watermarking is its extreme sensitivity to scaling attack. Due to scaling have a little effect on Discrete Cosine Transform (DCT) coefficients, this paper proposed a novel robust image watermarking algorithm based on QIM in the DCT domain. In the presented scheme, the medium and low frequency DCT coefficients of host signal are divided into two parts, then the watermark bits are embedded by quantizing ratio of l_p-norm of the two parts. Experimental results confirm the superiority of the proposed algorithm against common types attacks in comparison with the recently proposed scheme.

Keywords: Robust image watermarking, Quantization-based information hiding

1 Introduction

The aim of watermarking is to embed secret messages in cover medium such as text, image, audio and video to realize covert communications and intellectual property protection [1-2]. Watermarking is one of the image analysis technologies that are adjacent to Steganography. And there are lots of image analysis of steganography technologies based on different theories in the last few years which can be drawn lessons from [3-6]. Quantization-based image watermark has gained attention of researchers recently due to its good robustness. Watermark embedding algorithm based on quantization, generally, is to embed watermark according to characteristics of secret message and then to choose a specific structure quantizer to quantify the correlation coefficient of host signal to achieve the purpose of watermark embedding. The scheme is to embed useful data (watermark data) in a host signal and the perceptual quality of the host signal should not be degraded substantially during the embedding process.

Watermarking schemes fall into two categories: spread spectrum (SS) based watermarking [7-10] and QIM based watermarking [11-12]. In SS-based watermarking methods, a pseudo-random noise-like watermark is added into the host signal. It has been shown that SS-based approaches are robust aginst many types of attack. A secure algorithm and methodolgy for watermarking images which is constructed as an independent and identically distributed Gaussian random vector is presented by Cox et al. [7]. In this algorithm, robust resilience against lossy operations including scale changes is proved. Hartung and Girod firstly proposed a direct sequence spread spectrum watermarking scheme based on chip rate [8]. The wartermark is embedded into MP-2 bitstream without increasing the bit-rate, and can be retrieved from the decoded video without knowledge of original video. George et al. presented a direct sequence spread spectrum algorithm that can be applied to spatial domain and transform domain [9]. In this algorithm, at the stage of watermark extract, original cover image has to be applied in and the algorithm has a poor performance against JPEG compression and Gaussian noise attack. Kuo WeiShen et al. have used the spread spectrum technique along with chaos theory in order to enhance the obscurity and security of the watermarks [10]. Chen and Wornell firstly introduced a class of data hiding codes in 1999 known as QIM now and proposed a method referred to as distortion compensated QIM [11]. And Lee et al. proposed a method for enlarging the quantization steps of a QIM watermarking scheme to increase both the robustness and the perceptual quality of the watermarked images [12]. Different types of optimum and locally optimum decoders have been designed based on the distribution of the coefficients in the

[*] Corresponding Author: Min Lei; E-mail: leimin@bupt.edu.cn

DOI: 10.3966/160792642018031902019

watermark domain [13-14]. Ghouti et al. proposed a robust watermarking scheme based on balanced multiwavelet transform [15]. Bi et al. presented a data hiding method based on multi-band wavelet transform and empirical mode decompsition (MWT-EMD) [16].

Recently, quantization image watermarking has gained the attention of researchers due to its good robustness. The QIM watermark algorithm [11] proposed by Chen and Wornell has a higer capacity than SS-based approach [8]. Perez-Gonzlez and Balado proposed a quantization projection data hiding method based on QIM and SS [17]. Khademi and Ahadi proposed a logarithmic quantization index modulation (LQIM) method that has confirmed the superiority of perceptual better data hiding in comparison with other tradition QIM methods [18].

The disadvantage of the quantization-based digital watermarking is that it has bad performance against amplitude scaling attack. In order to solve this problem, many improved schemes have been proposed respectively, such as angle quantization index modulation (AQIM), sample projection (SP) and normalized correlation based on dither modulation Zareian Gradshteyn (NC-DM) [19-20]. Recently, a robust quantization index modulation-based approach for image watermarking (ASS-QIM) is proposed by Gradshteyn and Ryzhik [21]. From this scheme, step-size of quantization with a power-law function is adaptively selected. Besides, Zareian and Tohidypour also proposed an information hiding approach based on quantization (QIM) in discrete wavelet transform (DWT) domain and they have made some researches and explorations on DWT [22]. According to the results of simulation, the two latter algorithm ASSQIM and GIQIM have better effect against common attacks in comparison with other known algorithms. In order to against amplitude scaling attack effectively, this paper makes lots of researches on the approach of QIM proposed by Zareian and Tohidypour [23]. Thus a novel robust image watermarking algorithm based on QIM in the DCT domain is proposed in this paper and there are many researches and explorations is made on the application of this algorithm in DCT domain. And in addition, the drawback on algorithm of Zareian in the process of quantization is corrected by us.

In our scheme, we innovate the way of host signal vector generation. Gaussian low-pass filter and DCT are used to the carrier image, and then the DCT coefficients of the medium and low frequency are obtained. After that, zigzag scanning is used to get the DCT coefficients of the medium and low frequency to obtain the host signal vector *u,* and then the vector *u* is divide into two parts and the watermarking is embeded by quantizing the ratio of l_p -norm of the two parts. Finally, the watermark message which is embedded in the attacked signal u'' is extracted by using the minimum Euclidean distance scheme. The experiment results confirm the superiority of the proposed algorithm under many common attacks in comparison with many other watermarking algorithms, especially under amplitude scaling attack.

This paper is organized as follows. Section 2 is used to explain the proposed digital watermarking scheme, Section 3 is simulation and experiment on algorithm and a brief conclusion is given in Section 4.

2 Proposed Method

In this section, we introduce our blind watermarking scheme by two parts: watermark embedding and extraction.

2.1 Watermark Embedding

(1) In the first place, Gaussian low-pass filtering and discrete Cosine Transform (DCT) is done to the host carrier image to get the DCT coefficients matrix *F*. In order to get host vector signal $u=\{u_1,u_2,...,u_n\}$, zigzag scanning is done to the medium and the low frequency of *F*.

(2) Divide the host vector signal *u* into two parts: *x* and *y* which contain the even and odd indexed terms, respectively: $x_i=u_{2i}$, $y_i=u_{2i-1}$, $i=1,2,...,\frac{n}{2}$.

(3) The norm $l_x=(\frac{p}{n}\sum_{i=1}^{\frac{n}{2}}|x_i|^p)^{\frac{1}{p}}$ of two parts *x* and *y* is calculated respectively and as follows formulas, where $l_x=(\frac{p}{n}\sum_{i=1}^{\frac{n}{2}}|x_i|^p)^{\frac{1}{p}}$:

$$l_x=(\frac{p}{n}\sum_{i=1}^{\frac{n}{2}}|x_i|^p)^{\frac{1}{p}},l_y=(\frac{p}{n}\sum_{i=1}^{\frac{n}{2}}|y_i|^p)^{\frac{1}{p}} \quad \textbf{(1)}$$

The ratio z of $z=\frac{l_x}{l_y}$ norm is calculated as the following formula:

$$z=\frac{l_x}{l_y} \quad \textbf{(2)}$$

(4) And then, the quantization value z_q is calculate as the following formula:

$$z_q=Q_m(z)=\Delta round(\frac{z+m\Delta/2}{\Delta})-m\frac{\Delta}{2} \quad \textbf{(3)}$$

In the above formula, $m\in\{0,1\}$ represents watermarking message bit, Δ represents quantization step size.

In this step, it is necessary to point out clearly that $z_q=0$ is equal to zero approximately. Indeed, $z_q=0$, if $m=0$ and $\frac{z}{\Delta}<\frac{1}{2}$. In order to make assure that z_q is positive all the time, the paper deal this situation with $z_q = z_q + \frac{\Delta}{8}$.

(5) The next step, x_i and y_i are updated as x_i' and y_i' respectively as follows:

$$u' \text{ , } u' \qquad \textbf{(4)}$$

(6) Finally, we apply zigzag reverse and DCT reverse to new vector u' that contains watermark message to complete watermark embedding.

2.2 Watermark Extraction

Assuming that the received data is $l_{x''}$ at receiver side. Making Gaussian low-pass filtering and DCT to $l_{x''}$ to get a new host signal vector $l_{x''}$. After that, $l_{x''}$, $l_{y''}$ and $z''=\frac{l_{x''}}{l_{y''}}$ are calculated respectively as (1) and (2). Finally, we get watermark message data as the following formula:

$$\hat{m} = \arg\min_{t\in\{0,1\}} |u'' - Q_t(u'')| \qquad \textbf{(5)}$$

In the above formula, $\hat{m}$ represents watermark message bit.

3 Simulation and Experiment

In this section, we introduce results of simulation and experiment of proposed algorithm.

3.1 Carrier and Watermark Sample

3.1.1 Carrier Image

In order to testing the proposed algorithm accurately, the paper selects ten well-known images with the size of 512×512 as watermark carrier image: Lena, Baboon, Couple, Pirate, Barbara, Goldhill, Bridge, Peppers, Plane and Boat.

3.1.2 Watermark Sample

The paper selects binary pseudorandom sequences of 128-bit as watermark sample.

3.2 Experiment Parameters

In this paper, some experiment parameters are set as follows:

(1) PSNR: the peak of signal-to-noise ratio. In this paper, PSNR of all images 41dB.

(2) BER: bit error rate.

(3) CORR: correlation coefficient.

(4) *vlen* : 4, 8, 16, 32. It represents x and y sequence's length.s

(5) p : [1.01, 3.00]. It represents order of l_p norm and parameter p in (1).

(6) Δ : [0.01, 1.00]. It represents quantization step size.

3.3 Simulation and Experimental Results

In this part, PSNR, BER and Pearson product-moment correlation coefficient (CORR, its specific definition can be seen in Appendix A) will be used to measure the performance of the proposed algorithm.

3.3.1 Finding Optimum Parameter

The optimum *vlen, p* and $\leq$ for each image were found when the PSNR is 41dB. The results are obtained by averaging over 100 runs with 100 different watermark samples described in "Watermark Sample" part and summarized in Table 1. As can be seen, the optimum p for each image when PSNR equals to 41dB is close to 2.

Table 1. The optimum p, Δ and *vlen* for each image

Image	p	Δ	vlen
Lena	1.68	0.99	32
Baboon	1.66	0.90	32
Couple	1.67	0.60	32
Pirate	2.29	0.75	32
Barbara	2.32	0.82	32
Goldhill	1.95	0.57	32
Bridge	2.07	0.55	32
Peppers	1.72	0.52	32
Plane	2.07	0.55	32
Boat	1.84	0.55	32

Table 2. BER (%), PSNR and CORR of extracted watermark under Poisson attack

Image	BER (%)	PSNR (dB)	CORR
Lena	0	31.63	1.00
Baboon	0	31.43	1.00
Couple	0	31.66	1.00
Pirate	0	31.96	1.00
Barbara	0	31.88	1.00
Goldhill	0.78	31.90	0.98
Bridge	0.78	31.86	0.98
Peppers	0.78	32.30	0.98
Plane	0.78	30.69	0.98
Boat	0	31.50	1.00

The paper also shows PSNRs, BERs and CORRs for different vlen and $\leq$ in Figure 1 to Figure 3 with the assuming that optimum p for each image is close to 2. Seven of the original test images and their watermarked versions using the proposed with the message of 128-bit length are shown in Figure 4.

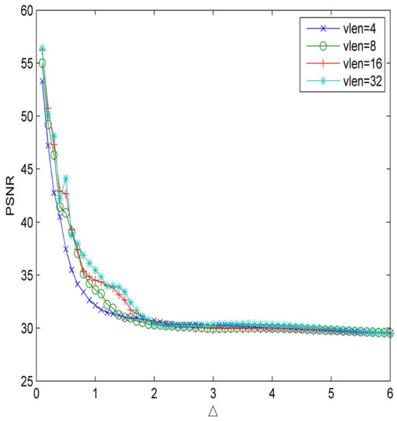

Figure 1. PSNR for different vlen and Δ with assume that optimum p for each image is same equals to 2. The results are averaged over ten well-known images

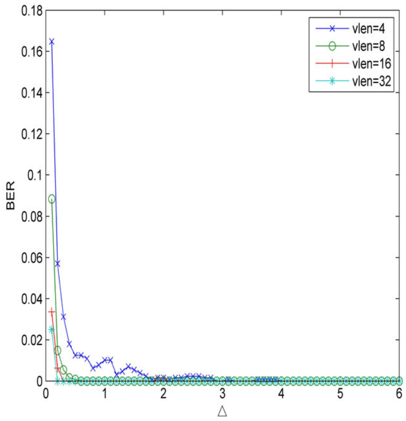

Figure 2. BER for different vlen and Δ with assume that optimum p for each image is same equals to 2. The results are averaged over ten well-known images

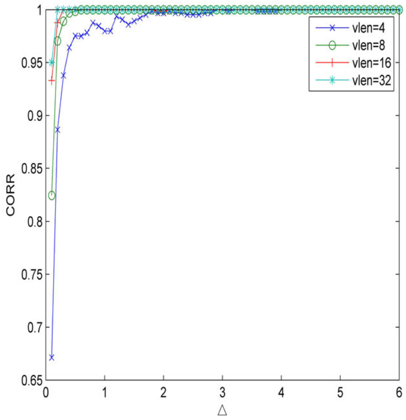

Figure 3. CORR for different vlen and Δ with assume that optimum p for each image is same equals to 2. The results are averaged over ten well-known images

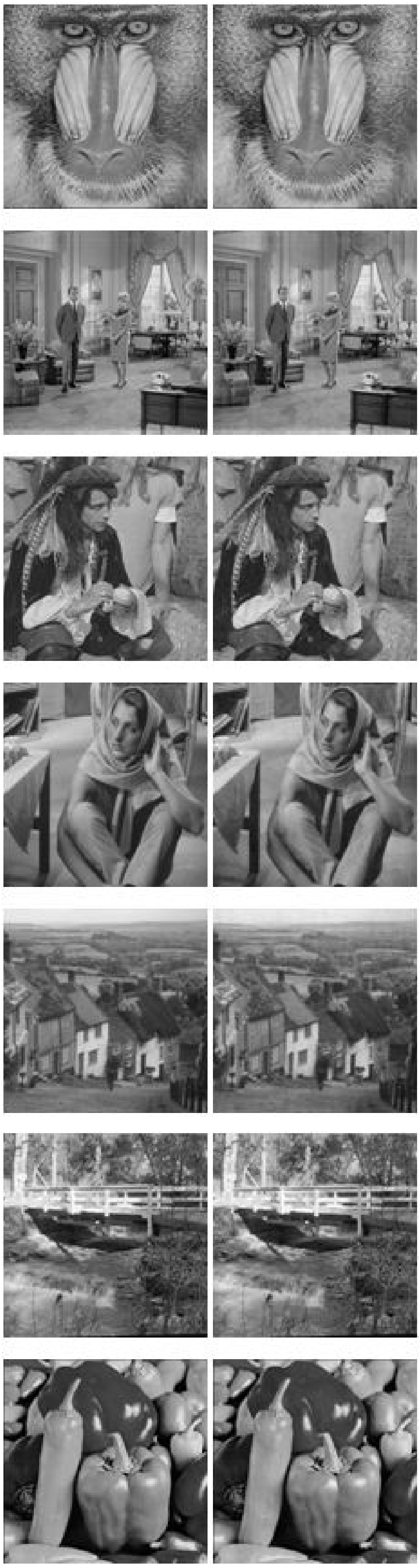

Figure 4. Original (left) and atermarked (right) test images. Up-bottom: Baboon, Couple, Pirate, Barbara, Goldhill, Bridge, Peppers

3.3.2 Performance under Attacks

In this part, the performance of the proposed scheme is tested to against several common attacks such as Poisson attack, Salt & Pepper attack, Filter attack, JPEG attack, Gaussian noise attack and Amplitude Scaling attack.

Poisson attack. As the first attack, the performance of the proposed method under Poisson attack is investigated and summarized in Table 2. As can be seen, our method has a great resistance against Poisson attack. For all of test images, the BER ≤ 0.78%, PSNR ≥ 30.00dB and CORR ≥ 0.70 are reached by our algorithm.

Salt & Peppers attack. In the second attack, the effect of Salt & Peppers noise attack (S&P noise) to the proposed watermarking scheme is investigated. In Table 3, we compare the proposed scheme with [21] for several images under the message length in both scheme is 128 bits under S &P noise with different intensity. As seen, our results are better than [21] in most cases.

Table 3. BER (%), PSNR and CORR of extracted watermark under S&P noise attack

Image	Method	S&P noise percentage		
		1%	3%	5%
Baboon	ASSQIM	0.23	1.71	5.46
	Proposed	0.00	0.78	3.12
Barbara	ASSIM	0.00	1.64	7.57
	Proposed	0.00	5.46	3.90
Bridge	ASSQIM	0.62	2.73	9.92
	Proposed	1.56	2.34	6.25
Plane	ASSQIM	0.07	2.50	9.21
	Proposed	0.00	1.56	9.37

JPEG attack. In this attack, the performance of proposed scheme is test against JPEG compression with various quality factor (QF). The BER, PSNR and CORR results are shown in Table 4. As can be seen, our scheme has reached BER = 0, PSNR ≥ 36.92dB and CORR = 1.00 under low intensity JPEG attack ($QF \geq 70$). It also gets BER = 0, PSNR ≥ 35.00dB and CORR = 1.00 under medium intensity JPEG attack ($30 \leq QF < 70$). Even under the extremely high intensity attack ($QF = 10$), the method gets BER as low as 4.60%.

Table 4. BER (%), PSNR and CORR of extracted watermark under JPEG compression. The results are averaged over ten well-known images

QF	80	70	50	30	25	20	15	10
BER(%)	0.00	0.00	0.00	0.00	0.00	0.39	1.17	4.60
PSNR(dB)	37.70	36.92	35.95	35.00	34.65	34.21	33.68	32.91
CORR	1.00	1.00	1.00	1.00	1.00	0.99	0.98	0.91

Gaussian noise attack. In the next experiment, the robustness of the proposed technique is tested against Gaussian noise attack. Table 5 shows the results for various variance (σ^2) and same mean ($\mu = 0$) of Gaussian noise attack. It is can be seen that our method is highly robust against this attack. It gets $BER \leq 1\%$ for $\sigma^2 \leq 200$. Even in extremely high noise level $\sigma^2 = 1000$, our method's BER never exceeds 12%.

Table 5. BER (%), PSNR and CORR of extracted watermark under Gaussian noise attack with mean is same zero and variance is different. The results are averaged over ten well-known images

σ^2	50	100	200	400	600	800	1000
BER(%)	0.00	0.15	0.85	3.75	5.07	8.28	11.01
PSNR(dB)	34.18	32.19	30.65	29.53	29.04	28.75	28.57
CORR	1.00	0.99	0.98	0.93	0.90	0.84	0.78

Amplitude scaling attack. The next attack is amplitude scaling attack. To investigate the robustness to this attack, the BER, PSNR and CORR results of different scaling factor (f) under the attack is reported in Table 6. As seen, our method reaches the BER of zero, PSNR ≥ 30dB and CORR = 1.00 under different scaling factor. The performance of our method is due to we used low-frequency and medium-frequency coefficients of an image, and interpolation operations and down-sampling in the scaling attack mostly wipe out the high-frequency coefficients of an image.

Table 6. BER (%), PSNR and CORR of extracted watermark for different scaling factor (f) under Amplitude Scaling attack. The results are averaged over ten well-known images

f	0.5	0.75	1.25	1.5	2
BER (%)	0.00	0.00	0.00	0.00	0.00
PSNR(dB)	34.60	36.44	38.68	38.70	38.64
CORR	1.00	1.00	1.00	1.00	1.00

Filter attack. The last attack we study is filter attack. Table VII demonstrates data extraction BERs under Gaussian low-pass filtering attack with various variances σ^2 and Median filtering attack with different window size. As can be seen in Table 7, it is obvious that our method has a better performance than ASSQIM [21] under Median filtering attack. Similar to ASSQIM [21], our approach also reaches the BER of zero for each images especially Barbara (ASSQIM: 1.56, our method: 0.00, $\sigma^2 = 2$) and Bridge (ASSQIM: 1.56, our method: 0.00, $\sigma^2 = 2$) under Gaussian low-pass filtering attack. The better performance of the proposed method is because low-frequency and medium-frequency coefficients of an image are used for watermarking, which are degraded less by low-pass filtering attacks.

Table 7. BER (%) of extracted watermark under different filter attack. The window size for Gaussian low-pass filtering attack is 3×3

Image	Method	Gaussian filter (σ^2)			Median filter		
		$\sigma^2=1$	$\sigma^2=1.5$	$\sigma^2=2$	3×3	5×5	7×7
Lena	ASSQIM	0.00	0.00	0.00	1.56	11.71	17.18
	Proposed	0.00	0.00	0.00	0.00	0.00	2.34
Baboon	ASSQIM	0.00	0.00	0.00	5.46	24.21	29.68
	Proposed	0.00	0.00	0.00	0.00	3.90	13.28
Couple	ASSQIM	0.00	0.00	0.00	0.00	8.59	21.09
	Proposed	0.00	0.00	0.00	0.00	1.56	9.37
Pirate	ASSQIM	0.00	0.00	0.00	0.00	6.25	13.28
	Proposed	0.00	0.00	0.00	0.00	0.00	3.13
Barbara	ASSQIM	0.00	0.00	1.56	0.78	9.37	22.65
	Proposed	0.00	0.00	0.00	0.00	0.00	4.68
Goldhill	ASSQIM	0.00	0.00	0.00	0.00	10.15	20.31
	Proposed	0.00	0.00	0.00	0.00	1.56	14.06
Bridge	ASSQIM	0.00	0.00	1.56	0.00	4.05	28.12
	Proposed	0.00	0.00	0.00	0.00	1.56	12.50
Peppers	ASSQIM	0.00	0.00	0.00	0.00	3.12	6.25
	Proposed	0.00	0.00	0.00	0.00	0.00	7.81
Plane	ASSQIM	0.00	0.00	0.00	0.00	8.59	27.34
	Proposed	0.00	0.00	0.00	0.00	3.90	14.06
Boat	ASSQIM	0.00	0.00	0.00	1.56	9.37	28.12
	Proposed	0.00	0.00	0.00	0.00	1.56	7.03

4 Conclusion

The paper proposed a novel robust image watermarking algorithm based on quantization index modulation in the DCT domain, for the global scaling and partial scaling have no impact on Discrete Cosine Transform (DCT) coefficients and Disperse Wavelet Transform (DWT) coefficients. The algorithm divides the DCT coefficients of medium frequency and low frequency into two parts separately, and then embedding watermark by quantizing the ratio of the two parts.

Firstly, the paper makes a lot of researches on GIQ, and proposed a novel watermarking scheme. Not only the drawback of Zareian's algorithm in the quantization is processed and corrected, but also a novel way to generate host signal vector is proposed. At the process of watermark embedding, Gaussian low-pass filtering is applied to the test image to enforce the low-frequency sub band. And then DCT was done to the test image to make it from spatial domain to frequency domain. After that, zigzag scanning is used to get the DCT coefficients of low frequency to obtain the host signal vector u, then the vector u is divide into two parts and the watermarking is embedded by quantitating ratio of l_p-norm of the two parts. At the process of extraction, the watermark on the attacked signal u' is extracted by using the minimum Euclidean distance scheme. In order to analyzing the performance of our scheme, ten well-known images are selected as carrier images and tested under many common attacks. Results of simulation can not only confirm the superiority of the proposed algorithm against common attacks (especially under amplitude scaling attack) in comparison with proposed schemes recently but also show the algorithm achieves a good transparency.

Acknowledgement

This work is supported by National Key R&D Program of China (2017YFB0802703), Guizhou Provincial Key Laboratory of Public Big Data (2017BDKFJJ017), CCF-Venustech Hongyan Research Initiative (2017-004).

References

[1] Z. Xia, X. Wang, X. Sun, B. Wang, Steganalysis of Least Significant Bit Matching Using Multi-order Differences, *Security & Communication Networks*, Vol. 7, No. 8, pp. 1283-1291, August, 2014.

[2] Y. Zheng, B. Jeon, D. Xu, Q. M. J. Wu, H. Zhang, Image Segmentation by Generalized Hierarchical Fuzzy C-means Algorithm, *Journal of Intelligent & Fuzzy Systems*, Vol. 28, No. 2, pp. 961-973, March, 2015.

[3] J. Li, X. Li, B. Yang, X. Sun, Segmentation-Based Image Copy-Move Forgery Detection Scheme, *IEEE Transactions on Information Forensics and Security*, Vol. 10, No. 3, pp. 507-518, March, 2015.

[4] Z. Xia, X. Wang, X. Sun, Q. Liu, N. Xiong, Steganalysis of LSB Matching Using Differences between Nonadjacent Pixels, *Multimedia Tools & Applications*, Vol. 75, No. 4, pp. 1947-1962, February, 2016.

[5] B. Chen, H. Shu, G. Coatrieux, G. Chen, X. Sun, J. L.

Coatrieux, Color Image Analysis by Quaternion-Type Moments, *Journal of Mathematical Imaging & Vision*, Vol. 51, No. 1, pp. 124-144, January, 2015.

[6] N. Zhou, A. Zhang, F. Zheng, L. Gong, Novel Image Compression-encryption Hybrid Algorithm Based on Key-controlled Measurement Matrix in Compressive Sensing, *Optics & Laser Technology*, Vol. 62, No. 10, pp. 152-160, October, 2014.

[7] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, pp. 1673-1687, December, 1997.

[8] F. Hartung, B. Girod, Digital Watermarking of MPEG-2 Coded Video in the Bitstream Domain, *Proceedings of International Conference on Acoustics, Speech, and Signal Processing*, Munich, Germany, 1997, pp. 2621-2624.

[9] M. George, J. V. Chouinard, N. Georganas, Digital Watermarking of Images and Video Using Direct Sequence Spread Spectrum Techniques, *Proceedings of the 1999 IEEE Canadian Conference on Electrical and Computer Engineering*, Edmonton, Canada, 1999, pp. 116-121.

[10] W.-S. Kuo, H.-T. Hu, L.-T. Lee, Rabust Two-domain Digital Image Watermarking, *Journal of Internet Technology*, Vol. 9, No. 5, pp. 337-342, December, 2008.

[11] B. Chen, G. W. Wornell, Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding, *IEEE Transactions on Information Theory*, Vol. 47, No. 4, pp. 1423-1443, May, 2001.

[12] Y.-H. Lee, S.-S. Yeo, J. Kwak, Securing Digital Images over the Internet Using a Robust Watermarking Scheme, *Journal of Internet Technology*, Vol. 11, No. 3, pp. 315-322, May, 2010.

[13] Q. Cheng, T. S. Huang, An Additive Approach to Transform-domain Information Hiding and Optimum Detection Structure, *IEEE Transactions on Multimedia*, Vol. 3, No. 3, pp. 273-284, September, 2011.

[14] M. Barni, F. Bartolini, A. De Rosa, A. Piva, Optimum Decoding and Detection of Multiplicative Watermarks, *IEEE Transactions on Signal Processing*, Vol. 51, No. 4, pp. 1118-1123, April, 2003.

[15] L. Ghouti, A. Bouridane, M. K. Ibrahim, S. Boussakta, Digital Image Watermarking Using Balanced Multiwavelets, *IEEE Transactions on Signal Processing*, Vol. 54, No. 4, pp. 1519-1536, April, 2006.

[16] N. Bi, Q. Sun, D. Huang, Z. Yang, J. Huang, Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition, *IEEE Transactions on Image Processing*, Vol. 16, No. 8, pp. 1956-1966, August, 2007.

[17] F. Perez-Gonzalez, F. Balado, Quantized Projection Data Hiding, *Proc. International Conference on Image Processing*, Rochester, NY, 2002, pp. II-889-II-892.

[18] N. K. Kalantari, S. M. Ahadi, A Logarithmic Quantization Index Modulation for Perceptually Better Data Hiding, *IEEE Transactions on Image Processing*, Vol. 19, No. 6, pp. 1504-1517, June, 2010.

[19] F. Ourique, V. Licks, R. Jordan, F. Perez-Gonzalez, Angle QIM: A Novel Watermark Embedding Scheme Robust against Amplitude Scaling Distortions, *Proc. IEEE International Conference on Acoustics, Speech, Signal Processing*, Philadelphia, PA, 2005, pp. 797-800.

[20] M. A. Akhaee, S. M. E. Sahraeian, C. Jin, Blind Image Watermarking Using a Sample Projection Approach, *IEEE Transactions on Information Forensics Security*, Vol. 6, No. 3, pp. 883-893, September, 2011.

[21] I. S. Gradshteyn, I. M. Ryzhik, *Table of Integrals, Series, and Products*, Academic, 1994.

[22] M. Zareian, H. R. Tohidypour, Robust Quantization Index Modulation-based Approach for Image Watermarking, *IET Image Processing*, Vol. 7, No. 5, pp. 432-441, July, 2013.

[23] M. Zareian, H. R. Tohidypour, A Novel Gain Invariant Quantization-Based Watermarking Approach, *IEEE Transactions on Information Forensics Security*, Vol. 9, No. 11, pp. 1804-1813, November, 2014.

Appdendix A

Pearson product-moment correlation coefficient

Pearson product-moment correlation coefficient (CORR) is used for measuring the correlation degree between two variable X and Y. Its formula is as follows:

$$corr = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \bar{Y})^2}}$$

Biographies

Min Lei received a Ph.D. degree in information security from Beijing University of Posts and Telecommunications. He is currently a lecturer at the School of Computer, Beijing University of Posts and Telecommunications. His research interests include Network security and cyber security.

Xiaoming Liu received a Ph.D. degree in information security from Beijing University of Posts and Telecommunications. He is currently a senior engineer in National Computer Network Emergency Response Technical Team/Coordination Center of China. His research interests include network security, security operation and maintenance.

Mian Wang is a postgraduate student at Beijing University of Posts and Telecommunications. His research interests includes Network security and cloud security.

Yu Yang received her Ph.D. degree in information security form Beijing University of Posts and Telecommunications. She is an associate professor at Beijing University of Posts and Telecommunications. Her research interests include Network security and information security.

Zhiguo Qu received the Ph.D. degree in information security from Beijing University of Posts and Telecommunications. He joined Nanjing University of Information and Technology in China and his research interests include quantum secure communication and digital watermarking.