I.J. Computer Network and Information Security, **2011, 1, 11-17**
Published Online February 2011 in MECS (http://www.mecs-press.org/)

Application of CL multi-wavelet transform and DCT in Information Hiding Algorithm

Tao ZHANG
College of Automation, Northwestern Polytechnical University, Xi'an 710072, Shaanxi, China
Email: zt904@foxmail.com

Shuai REN
School of Information Engineering, Chang'an University, Xi'an 710064, Shaanxi, China
Email: maxwellren@qq.com

***Abstract*—Taking advantage of a feature that allows the energy of an image would gather and spread on four components (LL_2, LH_2, HL_2 and HH_2) in the sub-image after first-order CL multi-wavelet transform, and Using the advantage of Discrete Cosine Transform in application of information hiding, propose an Information Hiding scheme based on CL multi-wavelet transform and Discrete Cosine Transform (abbreviated as CL-DCT). LL_2 is embedded module of robust parameters (optimized code of *Chebyshev* scrambling and *Hash* value of embedding information). Embed hiding Information in LH_2 and HL_2 with RAID1 and fragile sign in HH_2. Select a different range of DCT coefficients in LH_2, HL_2 and HH_2. The embedding sequence of each bit plane is traversal according to Knight-tour rout. Experimental results indicate that the proposed scheme can increase invisibility and robustness separately by 5.24% and 28.33% averagely. In particular, the scheme has better ability against cutting attacks. The scheme has certain ability against steganalysis such as Higher Order Statistics based on wavelet coefficients. Moreover, the scheme has excellent sensitivity of image processing.**

***Index Terms*—algorithms; wavelet transforms; information hiding; CL multi-wavelet transform; Discrete Cosine Transform; Chebyshev scrambling; genetic algorithm; Knight-tour rout**

I. INTRODUCTION

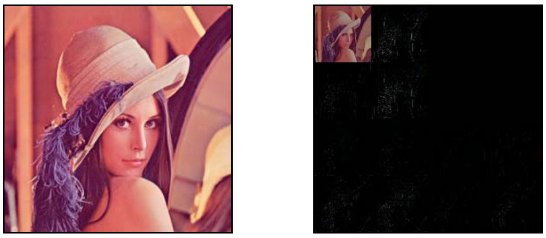
How to make the Information Hiding scheme have a better performance in terms of invisibility, robustness, sensitivity and anti-steganalysis becomes a research hotspot. Currently, the algorithm has not achieved four performances at the same time. The scheme based on space domain are good at invisibility, but can not meet the requirements of robustness and anti-steganalysis at the same time [1][2]. The scheme based on transform domain are good at robustness. Zhang *et al* [3] and Zhu *et al* [4] proposed Information Hiding scheme and digital watermarking scheme respectively based on discrete cosine transform (DCT) and discrete wavelet transform (DWT). They are robust enough against compression, but they are costly and low robust against cutting. and However, most algorithm are not strong in anti-steganalysis, and does not increase significantly [5][6].

Combination of different technologies can bring new ideas into Information Hiding. Taking advantage of the CL multi-wavelet transforms and Discrete Cosine Transform in application of information processing, propose an Information Hiding scheme based on CL multi-wavelet transform and Discrete Cosine Transform. In particular, CL multi-wavelet transform can process multi-transformation at the same time, and satisfy compact sup-port and symmetry of the image processing. This new scheme is named as CL-DCT. Experiment results illustrate that CL-DCT is better than traditional algorithms as DWT-DCT and DCT-LSB in invisibility and robustness against image attacks such as JPEG2000, cutting, filtering and noise. Has certain ability against steganalysis such as Higher Order Statistics based on wavelet coefficients. Moreover, the CL-DCT has excellent sensitivity and against cutting to image attacks.

II. INFORMATION HIDING ALGORITHM DESIGN

A. Embedding region

In digital image processing based on the multi-wavelet transform, the energy distribution due to the order of decomposition and the direction of components. The energy distribution of CL multi-wavelet transform [7] provides a flexible information hiding strategy. Fig. 1 shows CL multi-wavelet first-order transformation to *Lena* image.



(a) *Lena* Normal (b) *Lena* CL first-order

Figure 1. First-order CL multi-wavelet transform

Energy ratio of four First-order CL Multi-wavelet Transform sub-images is approximately as TABAL I [8].

TABLE I.
ENERGY DISTRIBUTION OF FIRST-ORDER CL MULTI-WAVELET

CL transform LL_1 sub-image energy percentage of total image energy	Each component energy distribution of LL_1 sub-image (%)			
	LL_2	LH_2	HL_2	HH_2
97.36	96.53	2.51	0.62	0.34

After CL multi-wavelet transform, the most energy not only concentrated in the first-order sub-image (LL_1), but also concentrated in the first component of first-order sub-image (LL_2).Based on the energy distribution of CL, Generating CL-DCT embedding region have four steps:

Step1. Transform the cover image with first-order CL multi-wavelet to obtain four sub-images. Embed robust parameters in LL_2. Embed hiding Information in LH_2 and HL_2. Embed fragile sign in HH_2. See Fig. 2;

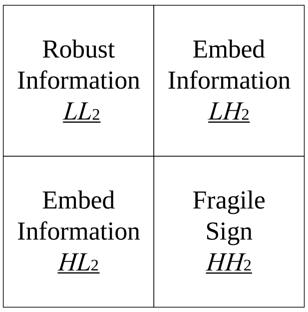


Figure 2. Embedded region strategy

Step2. Transform LL_2 component ($N \times N$) with DCT. Choose the interval distribution $[(N^2/4)-1, N^2-1]$ of DCT coefficient as embedding region in LL_2;

Step3. Transform LH_2 and HL_2 ($N \times N$) with DCT. Choose the interval distribution $[(N^2/4)-1,(N^2/2)-1]$ of DCT coefficient as embedding region in LH_2 and HL_2;

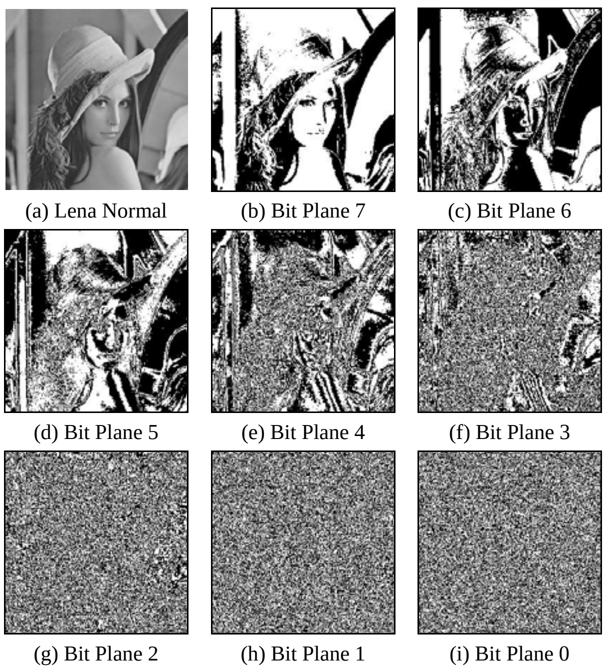


Figure 3. Bit Plane decomposition of 256 gray-scale Image

Step4. Decomposed HH_2 into $l\alpha\beta$ color component and transform the β component into gray image [9]. Bit plane decompose to the gray image. The Bit Plane 2 is the embedding region in HH_2. Fig. 3 shows a bit plane decomposition of normal *Lena* as a 256 gray-scale image.

B. Embedding rules

The embedded rules of CL-DCT are as follows:

Rule1. Odd and Even of DCT coefficient separately stand for 0 and 1;

Rule2. Embed information into LH_2 and HL_2 with RAID1, as shown in Fig. 4;

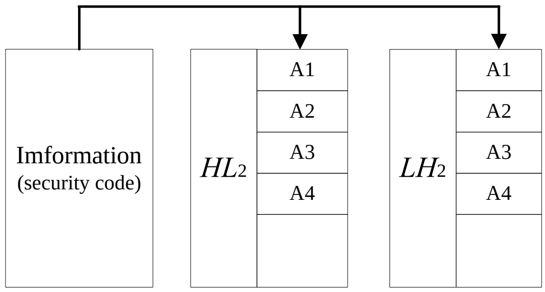


Figure 4. Knight-tour route

Rule3. Order by $[(N^2/4)-1, N^2-1]$ to embed information into LL_2, and order by $[(N^2/4)-1,(N^2/2)-1]$ in LH_2 and HL_2;

Rule4. Order by Knight-tour route traversal to embed information into HH_2. The Matrix of 9×9 Knight-tour is *T*. In the matrix *T*, "1" stands for the initial point of Knight-tour rout [10].

$$T=\begin{bmatrix} 1 & 34 & 3 & 16 & 31 & 42 & 37 & 14 & 29 \\ 4 & 17 & 32 & 43 & 36 & 15 & 30 & 41 & 38 \\ 33 & 2 & 35 & 64 & 69 & 54 & 39 & 28 & 13 \\ 18 & 5 & 68 & 73 & 44 & 65 & 46 & 53 & 40 \\ 81 & 74 & 63 & 70 & 67 & 72 & 55 & 12 & 27 \\ 6 & 19 & 80 & 75 & 62 & 45 & 66 & 47 & 52 \\ 79 & 76 & 61 & 22 & 71 & 56 & 51 & 26 & 11 \\ 20 & 7 & 78 & 59 & 50 & 9 & 24 & 57 & 48 \\ 77 & 60 & 21 & 8 & 23 & 58 & 49 & 10 & 25 \end{bmatrix}.$$

According to the matrix *T*, Fig. 5 shows the Knight-tour route of 9×9 image.

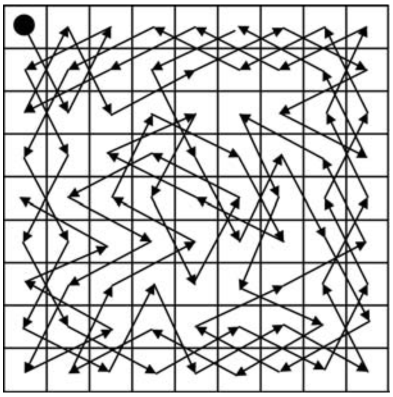


Figure 5. Knight-tour route

C. Embedding process

Information hiding scheme based on CL Multi-wavelet and CL-DCT divided into seven steps. Fig. 6 shows general process:

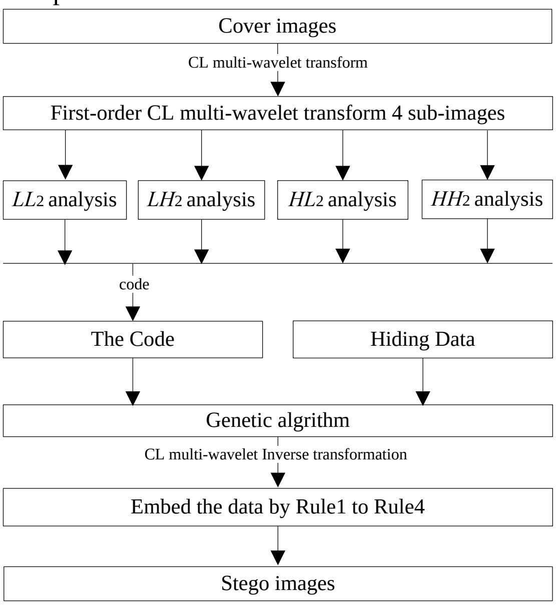


Figure 6. Embedding process for CL-DCT

Step1. Transform the cover image with first-order CL multi-wavelet to obtain four LL_1 sub-images;

Step2. Transform the LH_2 and HL_2 component ($N \times N$) with DCT. Draw the data from DCT coefficient of LH_2 and HL_2 order by $[0,(N^2/2)-1]$ according to Rule2. The data separately denoted as $CLL_1^{(2)}$ and $CLL_1^{(3)}$. $CLL_1^{(2)} = x_1^{(2)}, x_2^{(2)}, \cdots, x_m^{(2)}$ and $0 \le m \le N^2/2$. $CLL_1^{(3)} = x_1^{(3)}, x_2^{(3)}, \cdots, x_n^{(3)}$ and $0 \le n \le N^2/2$. The final analysis result denoted as C;

$$C = (x_1, x_2, \cdots, x_i) = \left(x_1^{(2)}, x_2^{(2)}, \cdots, x_m^{(2)}, x_1^{(3)}, x_2^{(3)}, \cdots, x_n^{(3)}\right) \quad (1)$$

Step3. Use *Chebyshev* mapping [11] of chaotic map algorithm to optimize information, as defined in (2) and (3). Suppose the parameter is μ, η and x_k. The chaotic sequence after the *Chebyshev* mapping is C_h. The Pre-hiding bit series is C_{pre}. Scrambling formula is defined in (4), $C_{IN}^x = (b_1, b_2, \cdots, b_i) = \left(b_1^x, b_2^x, \ldots b_{m+n-1}^x, b_{m+n}^x\right)$;

$$\begin{cases} 1 \quad , \quad -1 \le x_{k+1} < \eta \\ 0 \quad , \quad \eta \le x_{k+1} \le 1 \end{cases} \quad (2)$$

$$x_{k+1} = \cos\left(\mu \arccos(x_k)\right) \quad (3)$$

$$C_{IN}^x = C_{pre} \oplus C_h \quad (4)$$

Step4. In order to optimize the sequence of embedded bits with genetics algorithm [12], suppose F as the amount of the same bit value in matched positions between C_{IN}^x and C. The optimization model based on CL-DCT is (5). Get the optimal solution x_n' 、 η' and μ' by genetic algorithms optimization;

$$F(x_n, \eta, \mu) = Max \sum (x_i \,\bar{\oplus}\, b_i) \quad (5)$$

Step5. Bring x_n' 、 η' and μ' into (2) (3) and (4) to get optimization embedded bits C_{IN}^y, $C_{IN}^y = b_1^y, b_2^y, \ldots b_{n-1}^y, b_n^y$. Embed C_{IN}^y into DCT coefficients of LH_2 and HL_2 between $(N^2/4)-1$ and $(N^2/2)-1$;

Step6. Transform the LL_2 component ($N \times N$) with DCT. LL_2 is the most robust region in four LL_1 sub-images. In order to judge and recover the imperfect information, The CL-DCT embed the check code of RAID1, optimized code of *Chebyshev* scrambling (x_n' 、 η' and μ') and *Hash* value of embedding information (recorded as R^L) into DCT coefficient between $(N^2/4)-1$ and N^2-1;

Step7. HH_2 is the most vulnerable region in four sub-images. Embed the *Hash* of embedding information (recorded as R^H). Receiver can judge whether the stego image is attacked by comparing R^H and R^L.

D. Extracting information

Extracting information is divided into five steps. Fig. 7 shows general process:

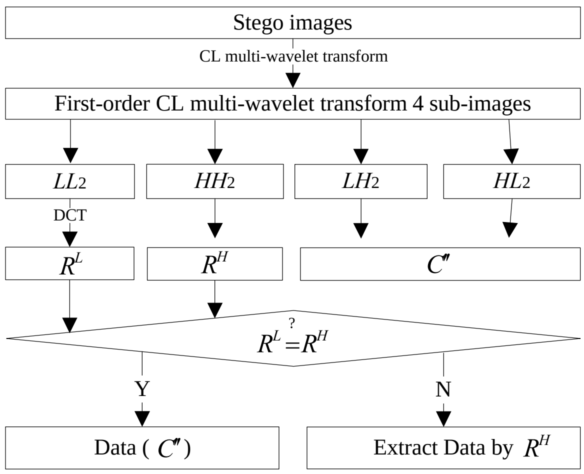


Figure 7. Process for Extracting Information

Step1. Transform the cover image with first-order CL multi-wavelet and get four LL_1 sub-images;

Step2. Transform LL_2, LH_2 and HL_2 component with DCT. Draw the R^L from LL_2 component. Draw the data from LH_2 and HL_2 component with the order in the Knight-tour route, and denoted as C''. Draw the R^H from HH_2;

Step3. if $R^L = R^H$ .The C'' is the secret information. if $R^L \neq R^H$ .The process continues;

Step4. if $R^L = R^H$ .The C'' is the secret information. if $R^L \neq R^H$ .The process continues;

Step5. Draw the check code of RAID1 from LL_2 component and use them to process C'' and get final secret information.

III. Information Hiding Algorithm design

A. Invisibility and Robustness Analysis

Use high energy component LL_1 as information hidden area, the energy percentage of which is about 97.36% in the total image energy. This feature satisfies robust basic requirement of hiding area.

Main hidden area of information are LH_2 and HL_2 components, the energy of which is much lower than the energy of LL_2 (energy distributions of LL_1 are 2.51% and 0.62%, energy percentages of the total energy are 2.51% and 0.60%).

This characteristic meets the invisible basic condition of hiding area. Choose high frequency of DCT coefficients in high energy component LL_2, meeting invisible hiding area rule of DCT. Choose low frequency of DCT coefficients in medium energy components LH_2 and HL_2, which qualifies robust hiding area rule of DCT. The general design idea of information hiding algorithm based on CL multi-wavelet and DCT is hiding information in low energy area of high energy component. This design can satisfy robustness and invisibility and solve the opposition between them well.

B. Anti-Steganalysis Analysis

The information hiding analysts generally use "all black" characteristic of LH_2 and HL_2 in CL component to analyze hidden information. Without obvious texture and pattern feature, information hidden in LH_2 and HL_2 is easily to expose.

Considering about the above, choose high frequency coefficient interval of DCT as hiding area to avoid information hiding analysis effectively. With consistent statistical properties of *Chebyshev* traversal and Knight-tour route, zero mean white noise [13, 14], hidden information is of good distribution and hidden characteristics, thus improve the anti-steganalysis of algorithm. β components of HH_2 in $l\alpha\beta$ color space are grayed to satisfy sensitive perceptivity and anti-steganalysis based on general LSB analysis.

C. Sensitivity Analysis

Hide *Hash* value in LL_2 robust unit with highest energy and LL_2 fragile sign unit with lowest energy. By contrast judgment on *Hash* value, the system can have sensitive perception against distortion.

IV. Simulation Experiment

Simulation environment of the algorithm is Matlab7.0.0.19920. Cover image is *Lena* (256×256) as shown in Fig. 8(a). Stego image is binary image Baboon (64×64) as shown in Fig. 8(b).

A. Invisibility Experiment

Fig. 8(c) shows stego image based on CL-DCT. PSNR value equals 41.3295. It shows that this method is of better invisibility.

(a) Cover image (b) Hiding information (c) Stego image

Figure 8. Hiding and result of CL-DCT

Invisibility is determined by Information content. Embed information in 200 images randomly. 2^k is used to denote bit quantity ($0 \leqslant 2^k \leqslant 4096$). Fig. 9 shows the PSNR of different embedding quantity. The experimental results indicated that when $k \leqslant 12$, it is of better invisibility (PSNR$\geqslant$41.3295).

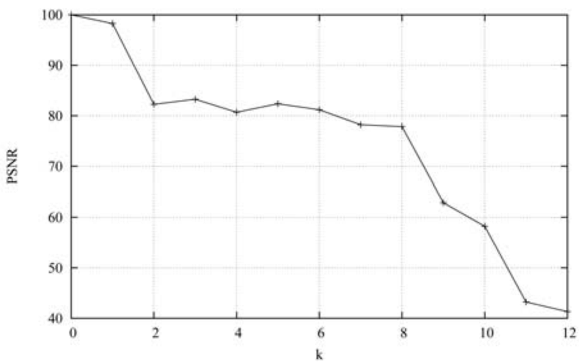


Figure 9. Experiment of embedding dense and corresponding Invisibility

B. Robustness Experiment

Define texture evaluation and modification rate of binary image (n×n pixels) separately in (6) and (7).

$$w = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \oplus f(i+\mu, j \pm \eta)}{2n^2} \tag{6}$$

$$p = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \oplus f'(i,j)}{n^2} \tag{7}$$

Where $n = N/2^d$, $d \in \{1,2,\cdots,\log_2(N-1)\}$. $f(i,j)$ and $f'(i,j)$ are separately for the pixel at (i,j) of normal and extraction image with $n\times n$ pixels.

Robustness test algorithm is defined in (8). Q is robustness test value and $Q \in [0,1]$. In the following experiments, μ=η=1. Expand Q 100 times to accommodate judgment habit.

$$Q = w(1-p) \tag{8}$$

Fig. 10 shows the result of different attacks such as JPEG2000 compression, cutting, filtering and noise.

(a) JPEG2000_60% Q=50.30 (b) cutting_25% Q=63.75

(c) mean filter_[3,3] Q=73.01 (d) wiener2 filter_[3,3] Q=61.36

(e) *Gaussi*_μ=0,σ^2=0.003 Q=75.79 (f)'*salt & pepper*'_d=0.15 Q=45.30

Figure 10. Results of robustness experiment

Images are vulnerable to compression and cutting attacks, Fig. 11 shows the Q's value corresponding to ratio of these attacks.

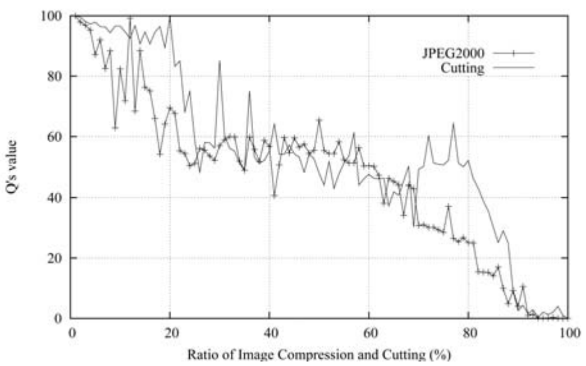


Figure 11. JPEG2000 and cutting experiment

According to experiment, embedded information can be identified when Q reach about 30. Fig. 10 and Fig. 11 show that CL-DCT is robust against JPEG2000 compression below 75%, cutting below 83%, common filtering and adding noise.

C. Experiment of ability against steganalysis

Higher order statistics detection algorithm based on wavelet coefficients (HOSWC) is a general detection algorithm [15]. Use the algorithms above-mentioned to analyze the performance of CB2-CFS. Experiment results are shown in Fig. 12 and Fig. 13.

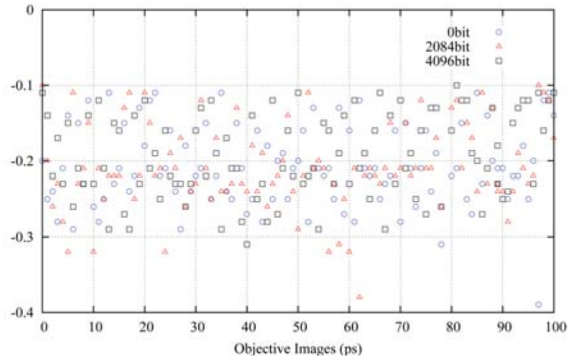


Figure 12. Steganalysis experiment result of HOSWC to CL-DCT

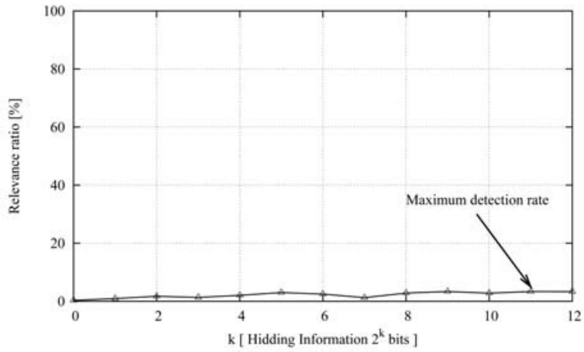


Figure 13. Steganalysis detection rate of HOSWC to CL-DCT

Fig. 12 shows there is no one or more threshold value found to recognize which pictures embedded information in 100 images. Use 1000 images to test, as shown in Fig. 13, largest detection rate below 3.3%. Experiments show that CL-DCT is of better anti-steganalysis.

D. Experiment of sensitivity to image attacks

Sensitivity to image attacks is the peculiar characteristic in CL-DCT. Comparing R^L with R^H indicates the algorithm has excellent sensitivity of image processing. TABLE II lists the detectable rate when JPEG2000 compression ratio is 5%, random cutting ratio is 5%, [3, 3] median filter, *Gaussian* (μ=0, σ^2=0.003) and '*salt & pepper*'(d=0.15). The average of detectable rate is 99.72%.

TABLE II.
DETECTABLE RATE OF ATTACKS

ATTACKS	JPEG2000	Cutting	Filtering	Gaussian	'*salt pepper*'
Detectable rate	99.98%	99.94%	99.98%	98.79%	99.92%

E. Experiments of invisibility comparison

According to PSNR, CL-DCT has advantages in invisibility compared with DWT-DCT and DCT-LSB. TABLE III shows that invisibility increases by 6.00% averagely when embedding rate is 25%.

TABLE III.
INVISIBILITY COMPARISON BASED ON PSNR

Algorithm	CL-DCT	DWT-DCT	DWT-LSB
PSNR	41.3295	38.3270	39.9501

F. Experiments of robustness comparison

Fig. 14, Fig. 15 and TABLE IV show robustness comparison results when embedding rate is 25% based on the Q's value.

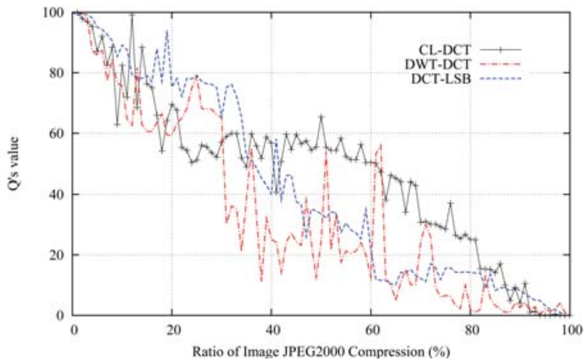


Figure 14. Compression comparison

The Q's value of CL-DCT in JPEG2000 compression is 44.7315. DWT-DCT is 32.9980, and DCT-LSB is 42.6989. Indicate CL-DCT is better robustness at JPEG2000.

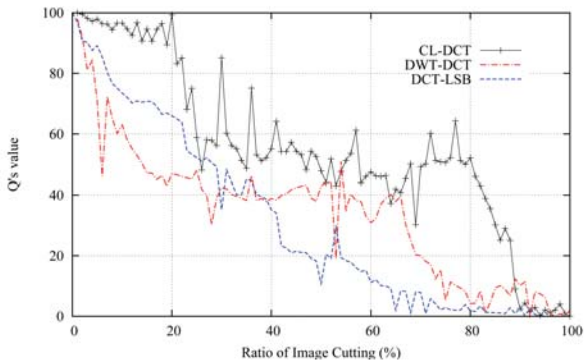


Figure 15. Cutting comparison

The Q's value of CL-DCT in cutting is 50.4678. DWT-DCT is 33.7810, and DCT-LSB is 31.0311. Indicate CL-DCT is better robustness at cutting.

TABLE IV.
RTV COMPARISON OF FILTERING AND NOISE

Attacks	Information Hiding Algorithm		
	CL-DCT	DWT-DCT	DCT-LSB
[3,3] median filter	72.11	45.33	60.11
[3,3] wiener2 filter	60.54	58.74	49.60
Gaussi(μ=0, σ^2=0.003)	72.17	46.90	60.14
'*saltpepper*'(d=0.15)	43.54	53.48	42.15

TABLE IV show that CL-DCT have better performance in robustness under filter and noise except compared with '*salt & pepper*' noise of DWT-DCT.

V. CONCLUSIONS

Propose an Information hiding scheme based on CL and DCT. Take advantage of the energy distribution ratios in the four sub-images after first-order CL multi-wavelet transformation, and use DCT to generate the DCT coefficients. Change the DCT coefficient to achieve information hiding. Chose LL_1, the energy of which accounts for 97.36% of the total image energy, as the algorithm hiding area. The feature of LL_1 can meet the basic requirement of robustness hiding area. The main information hiding areas are LH_2 and HL_2, the energy of which is much lower than the energy of $LL2$. The energy of LH_2 and HL_2 separately account for 2.51% and 0.62% of LL_1, and approximately account for 2.44% and 0.60% of the image total energy. The energy feature of LH_2 and HL_2 can meet the basic requirement of invisibility hiding are. Choose high frequency DCT coefficients of LL_2 component according to invisibility rule of DCT hiding area. Choose low frequency DCT coefficients of LH_2 and HL_2 according to robustness rule of DCT hiding are. The statistical properties of *Chebyshev* traverse and zero mean white noise are consistent [16], which is of good distribution and hiding characteristics to improve anti-steganalysis. Decompose HH_2 according to $l\alpha\beta$ color space. Hide information with LSB method in β components after gray-scaling which can meet the requirement of sensitivity and anti-steganalysis against common analysis based on LSB.

The future work is focus on alternating selection of bit plane, choosing embedded module and robustness parameters in LL_2 in order to improve invisibility, robustness and tampering perception. Especially research on applications in information hiding based on the theory of Image Multiscale Geometric Analysis [17].

ACKNOWLEDGMENT

This work was supported by The Graduate Starting Seed Fund of Northwestern Polytechnical University (NPUZ2010). This work also has been supported by the National Defense Fund of China (C2720061361) and the

National Science and Technology Major Special Project (2008ZX03006)

The authors wish to thank all the reviewers for their valuable comments and suggestions that improved the quality of this paper.

REFERENCES

[1] Chang Chin-Chen, Tseng Hsien-Wen. Data hiding in images by hybrid LSB substitution, Proceedings of the 3rd International Conference on Multimedia and Ubiquitous Engineering (MUE 2009), 2009：360-363.

[2] Li Xiao-long, Zeng Tie-yong, Yang Bin. Improvement of the embedding efficiency of LSB matching by sum and difference covering set, Proceedings of the 2008 IEEE International Conference on Multimedia and Expo (ICME 2008), 2008：209-212.

[3] Daqi Zhang, Shiru Qu, and Baosheng Kang, “A More Secure Information Images Using Hiding Technology for Digital DWT and DCT”, Journal of Northwestern Polytechnical University, Northwestern Polytechnical University Press, Xi’an, P.R.China, 2007, 25(3), pp. 378-382.

[4] Gengming Zhu, Nong Sang, Desheg Xiang, Shaobo Zhang, “Watermark Algorithm Research and Simulation Based on Different Frequency Coefficients”, in Proceedings of International Conference on Advanced Computer Theory and Engineering (ICACTE 2008), Phuket, THAILAND, IEEE COMPUTER SOC, USA, 2008, pp. 271-275.

[5] Sun, X.. Robust adaptive image watermarking using visual models in DWT and DCT domain, Information Technology Journal, 2010, 9(3)：460-466.

[6] Lu Wei, Sun Wei, Lu Hong-tao. Robust watermarking based on DWT and nonnegative matrix factorization, Computers and Electrical Engineering, 2009, 35(1)：183-188.

[7] Chui C. K., Lian J. A. A Study of orthonormal multi-wavelets, Applied Numerical Mathematics, 1996, 20(3)：273-298.

[8] HUANG Zhuo jun, MA Zheng-ming. Statistical Analysis of Multiwavelet Image Transform, Journal of Image and Graphics, 2001.12, (6A):1198-1203.(in Chinese)

[9] TaiYu-wing, Jia jia-ya, Tang Chi-keung. Proceedings of the 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, (2005), 1:747.

[10] Paris, L., “Heuristic strategies for the knight tour problem”, in Proceedings of IC-AI 2004 & MLMTA 2004, CSREA PRESS, Athens, 2004, pp. 1121-1125.

[11] Boyd J. P.. Chebyshev and Fourier spectral methods. Canada: General Publishing Company, 2001.

[12] Goldberg, D.E., Genetic Algorithms in Search, Optimization, and Machine Learning, Addison Wesley Publishing Company, PISCATAWAY, USA, 2007, pp. 237-251.

[13] Prasadh K., Ramar K., Gnanajeyaraman, R. Public key cryptosystems based on chaotic-chebyshev polynomials, Proceedings of the 2009 International Conference on Intelligent Agent and Multi-Agent Systems (IAMA2009), 2009, Article number：5228035.

[14] SHI Jun. Chaotic and Its Performance Analysis Based on Chebyshev Mapping, Modern Electronics Technique, 2008, 31(23): 93-96. (in Chinese)

[15] Hany F., Siwei L. Higher-order Wavelet Statistics and their Application to Digital Forensics, IEEE Workshop on Statistical Analysis in Computer Vision, 2003, 8: 94.

[16] Prasadh K., Ramar K., Gnanajeyaraman, R. Public key cryptosystems based on chaotic-chebyshev polynomials, Proceedings of the 2009 International Conference on Intelligent Agent and Multi-Agent Systems (IAMA2009), 2009.

[17] Licheng Jiao, Biao Hou, Shuang Wang, and Fang Liu, Image Multiscale Geometric Analysis: Theory and Applications Beyond Wavelets, Xidian University Press, Xi’an, P.R.China, 2008.

Tao Zhang received the Bachelor and Master of Engineering in Computer Science and Technology from the Northwestern Polytechnical University, Xi'an, P.R.China respectively in 2005 and 2009. She is a full-time PhD student in Control Theory and Engineering of the Northwestern Polytechnical University at present.

During her master study, she helped to achieve a project named "Information security risk assessment for a bank". Her research interests include information security assessment, information hiding and network security control.

Shuai Ren received the Bachelor, Master and PhD of Engineering in Computer Science and Technology from the Northwestern Polytechnical University, Xi'an, P.R.China respectively in 2005 and 2010.

Currently he was the lecture of Information Engineering College of Chang'an University, Xi'an, P.R.China. His research interests include information hiding, network control, and pattern recognition. He has participated and accomplished 3 projects and published 13 papers, 7 were indexed by EI.

