http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (15): 3260-3266, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.3260.3266

An High Performance Information Hiding Scheme Based on CL multi-wavelet and Color Transfer Theory for Secret Communication

[1]Tao Zhang, [1]Yong-Feng Ju, [2]Shuai Ren and [2]Jing-Xiang Lei
[1]School of Electronic and Control Engineering, Chang'an University, Xi'an 710064, China
[2]School of Information Engineering, Chang'an University, Xi'an 710064, China

Abstract: Take advantage of the feature that the energy of the 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. Make use of the color control ability of lαβ color space in color transfer theory. Propose a reversible information hiding algorithm named as CL-CTT. Use color transfer theory to generate the embedding rule. Embed robust parameters in the LL_2, hiding Information in LH_2 and HL_2 with RAID4 and fragile sign in HH_2. Improve the consistence of the embedded data bits' order and the coding of the sub-image with the chaotic map and the genetic algorithm. Experimental results indicate that CL-CTT can increase imperceptibility by 19.40% averagely and robustness at least 19.99% and have excellent sensitivity of image processing.

Key words: Algorithms, wavelet transforms, information hiding, CL multi-wavelet transform, color transfer theory, chebyshev chaotic map, genetic algorithm

INTRODUCTION

Information Hiding is an important way to achieve secret communication. The balance between invisibility and robustness in Information Hiding based on digital image becomes a research hotspot. Currently, the space and frequency domain are the main methods of Information Hiding. LSB is the basic algorithm of space domain methods, but the schemes based on LSB almost have drawbacks under embedding great amount of information (Lai and Tsai, 2011). DCT and DWT which are based on frequency domain, have certain robustness but are costly and low robust against rotating attacks (Yuan *et al*., 2011)?

New technologies bring new ideas into Information Hiding. Chui and Lian (1996) proposed CL multi-wavelet transform which can satisfy compact sup-port and symmetry of the image processing. (Li *et al*., 2005) proposed a color transfer theory which can transfer color from one image to another in the lαβ color space. Using CL multi-wavelet transform technology and color transfer theory, propose an Information Hiding scheme based on CL and color transfer theory: Firstly, transform the cover image with first-order CL multi-wavelet and use four first-order sub-images (LL2, LH2, HL2 and HH2) as information host; Then get the optimal embedded code from the four sub-images; Scramble pre-hiding information with chaotic map (Ye, 2010) and search the optimal scrambled parameters with genetic algorithm (Deb *et al*., 2002) in order to improve the consistency between pre-hiding information and the best embedded code; Finally, embed hiding information with RAID4 according to embedding rule based on color transfer theory and the optimal scrambled order. Simulation experiment results illustrate that CL-CTT is better than traditional algorithms in invisibility and robustness against image attacks such as JPEG2000, cutting, rotation, filtering and noise. Moreover, the CL-CTT has excellent sensitivity to image attacks.

CL MULTI-WAVELET TRANSFORM

CL multi-wavelet transform is the earliest and most widely used in multi-wavelet transform field, has distinctive characteristics such as compact sup-port, second-order approximation, integer translation and orthogonality of scalar function. Figure 1 shows CL multi-wavelet first-order transformation to Lena image.

Energy ratio of four sub-images after first-order CL Multi-wavelet transform is approximately 284:7:2:1. Based on the feature, embedding region strategy of CL-CTT is as follows: LL2 is robustness module; LH2 and HL2 are data embedded modules and HH2 is a fragile sign module.

COLOR TRANSFER THEORY

Embedded process: Color Transfer is the new issue in the field of digital image processing. Image A and B are

Corresponding Author: Tao Zhang, School of Electronic and Control Engineering, Chang'an University, 710064, Xi'an, China

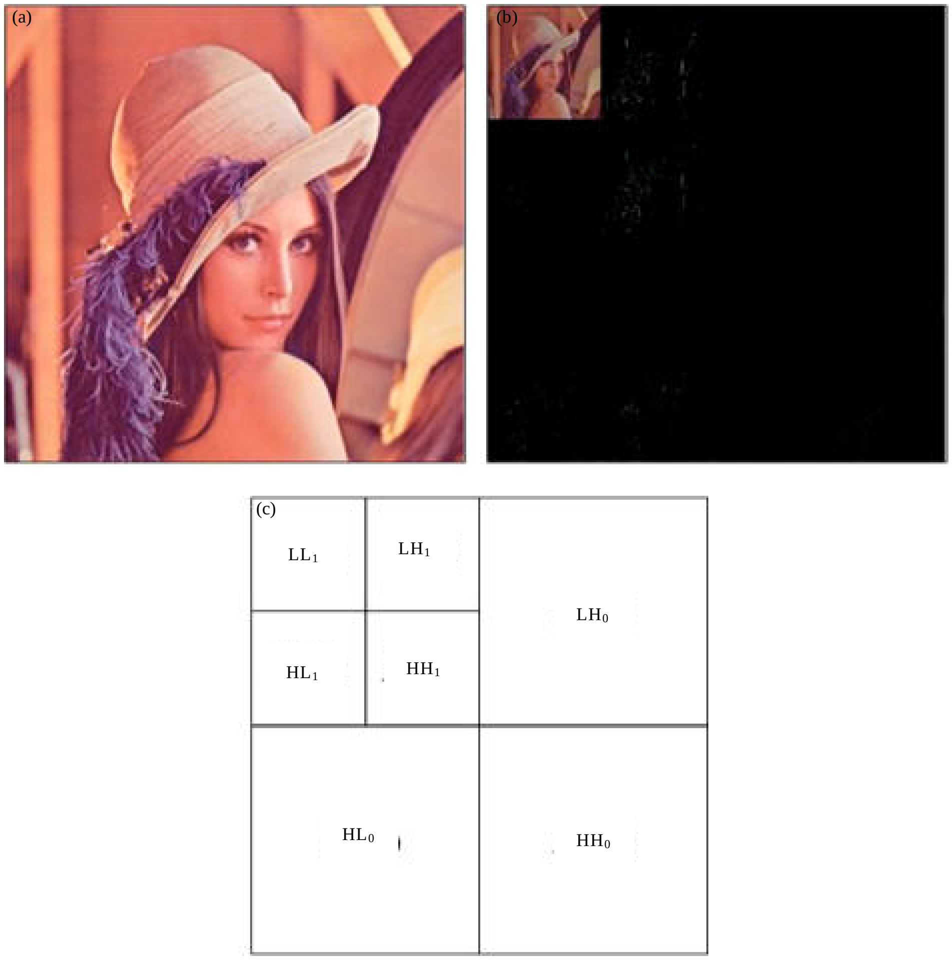

Fig. 1(a-c): First-order CL multi-wavelet transform

combined to produce image C which has the same color characteristics of A and structural shape of B. The biggest advantage of color transfer theory based on lαβ color space is to eliminate the correlation between each color component of RGB. Equation 1 is the color transfer theory proposed by Marcus and Pierce (1994).

$$\Gamma^* = \frac{\sigma\Gamma_c}{\sigma\Gamma_s}\left(\Gamma_s - \bar{\Gamma}_s\right) + \bar{\Gamma}_c \tag{1}$$

where, Γ is for space component of l, α and β, respectively. $\bar{\Gamma}_c$ and $\sigma\Gamma_c$ are separately for mean and standard deviation of l, α and β in color image A. $\bar{\Gamma}_s$ and $\sigma\Gamma_s$ are separately for mean and standard deviation of l, α and β in structure image B.

Using the color transfer equation of color transfer theory, generate the embedding rule to modify the data units in order to embed information:

- **Rule 1:** Figure 2 shows the chosen of image A and B. 2×2 pixel module in space domain is the basic embedding unit. A_1 and A_2 compose color image A. B_1 and B_2 compose structure image B
- **Rule 2:** Is for luminosity. Figure 3 indicates that l is of the greatest weight in visibility influence compared with α and β

Based on the weight of lαβ, only modify the α and β component. The modify rules are showed in Eq. 2:

$$\begin{aligned} \alpha'_C &= \frac{\sigma\alpha_A}{\sigma\alpha_B}(\alpha_{B2} - \overline{\alpha_B}) + \overline{\alpha_A} \\ \beta'_C &= \frac{\sigma\beta_A}{\sigma\beta_B}(\beta_{B2} - \overline{\beta_B}) + \overline{\beta_A} \end{aligned} \tag{2}$$

Every basic unit can be embedded with two bits information. The embedding positions are α bit and β bit

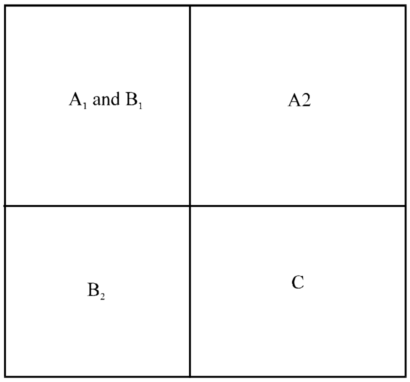

Fig. 2: Chosen of image A and image B

Table 1. Embedding rule

Modified bit	Embedding information 00	01	10	11
α_C	√	√	α'_C	α'_C
β_C	√	β'_C	√	β'_C

of C pixel. "√" is for no change and the others represent modifying them to the data in Table 1 shown.

INFORMATION HIDING SCHEME

CL-CTT Information hiding scheme has seven steps. Figure 4 shows general process:

Step 1: Transform the cover image with first-order CL multi-wavelet and the four sub-images with lαβ color space. Extract α and β sub-images and denoted by LL^{α}_2, LH^{α}_2, HL^{α}_2, HH^{α}_2 and LL^{β}_2, LH^{β}_2, HL^{β}_2, HH^{β}_2

Step 2: Code LH2 and HL2 with row traversal method in 2×2 pixel module based on the rule shown on Eq. 3. Where $\Delta_\beta = |\beta_C-\beta'_C|$, $\Delta_\alpha = |\alpha_C-\alpha'_C|$. β_C and α_C are separately for the value of α component and β component in C pixel. α'_C and β'_C are separately for the value of α and β after Eq. 2 calculated. Coding definition is as follows Eq. 1 Based on the embedding rule (Table 1), there is no change when coding is 00. So, the priority of 00 is the highest. Modify the components both α and β when coding is 11. So, the priority of 11 is the lowest. There is no need to code 00 and 11, Eq. 2 Code LH_2 and HL_2 and denoted separately by $C_{LH} = t'_1, t'_2,\ldots, t'_k$, $t'_i\in\{01, 10\}$ and $C_{LH} = t''_1, t''_2,\ldots, t''_k$, $t''_i\in\{01, 10\}$, Eq. 3 Get the final coding of units LH_2 and HL_2 from C_{LH} and C_{HL} and denoted by $C_{LH} = t'_1, t''_2, t'_1, t''_2,\ldots, t'_k, t''_k, t'_i, t''_i,\in\{01, 10\}$:

$$C = \begin{cases} 01, & \Delta_\beta \le \Delta_\alpha \\ 10, & \Delta_\beta > \Delta_\alpha \end{cases} \tag{3}$$

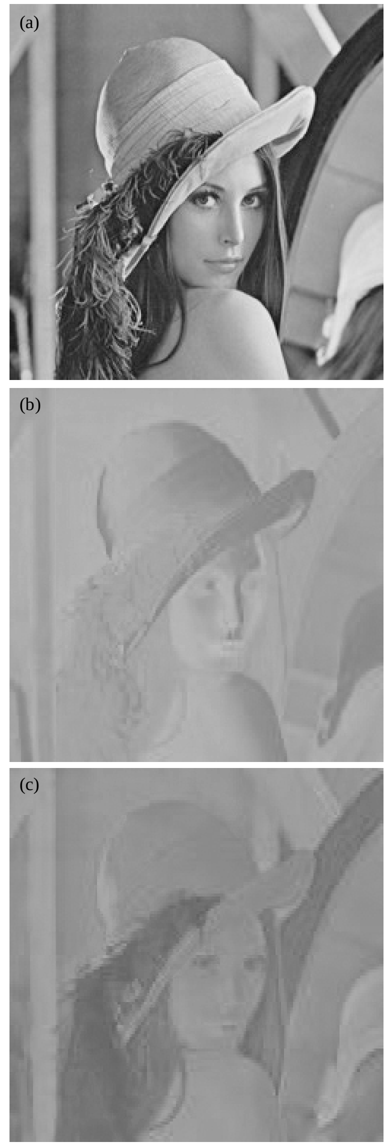

Fig. 3(a-c): lαβ transform of sub-image (a) l component, (b) α component and (c) β component

Step 3: Use Logistic mapping of Chaotic map algorithm to optimize information, as defined in Eq. 4. Suppose the bit series scrambled according to μ and x_k is

$$C^x_{IN} = b^x_1, b^x_2,\ldots, b^x_{n-1}, b^x_n\in\{00, 01, 10, 11\};$$
$$X_{k+1} = \mu x_k(1-x_k),\ x_k\in(0, 1) \tag{4}$$

Step 4: In order to optimize the sequence of embedded bits with genetics algorithm, suppose F as the amount of the same bit value in matched positions between C^x_{IN} and C. Optimize x_k using

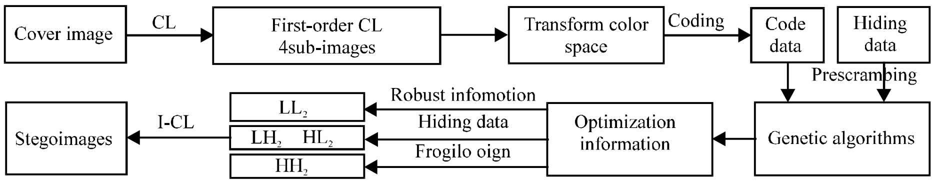

Fig. 4: Embedding process for CL-CTT

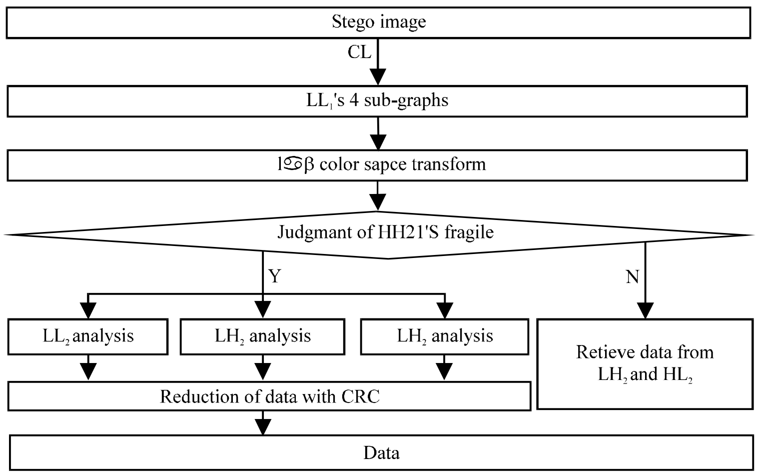

Fig. 5: Process for extracting information

genetic algorithm to maximize F. The optimization model based on CL-CTT is Eq. 5. Where $\bar{\oplus}$ is for the XOR. Get the optimal solution y by genetic algorithms optimization:

$$F(y) = \operatorname{Max}F(x_k) = \operatorname{Max}\sum(t_n \bar{\oplus} b_n^x) \tag{5}$$

Step 5: Put y into C^x_{IN} to obtain the optimal embedded bit $C^y_{IN} = b^y_1, b^y_2, \ldots, b^y_{n-1}, b^y_n$. Embed C^y_{IN} alternately into LH_2 and HL_2 with RAID4 row traversal based on Table 1 listed. Eight bits is the basic data unit of RAID4

Step 6: LL_2 is the most robust region in four CL first-order sub-images. The CL-CTT embeds the cyclic redundancy check (CRC) of RAID4 (recorded as R^L), the optimization scrambling parameters y and μ in LL_2

Step 7: HH_2 is the most vulnerable region in four sub-images. Embedding the CRC of RAID4 (recorded as R^H) in HH2. Receiver can judge quickly by comparing R^H and R^L whether the stego image is attacked

Extracting Information: Extracting information is divided into five steps as shown in Fig. 5:

Step 1: Transform the stego image with first-order CL to obtain four sub-images (LL_2, LH_2, HL_2 and HH_2)

Step 2: Transform the 4 sub-images with l$\alpha\beta$ color space transformation and extract α, β sub-images

Step 3: Draw the y¡¢μ and R^L from LL_2 and R^H from HH_2

Step 4: It can be indicated that the stego image has not been attacked if $R^L = R^H$. Then receiver can extract information from LH_2 and HL_2 by parameters *y*. It can be indicated that the stego image is attacked if $R^L \ne R^H$

Step 5: Extracting information from of LH_2 and HL_2 by using *y* and R^L

SAFETY PERFORMANCE ANALYSIS

Concerning robustness, It can be improved by proposing strategy based on features of first-order CL energy distribution and embedding information in LH_2 and HL_2 with RAID4; Concerning invisibility, firstly, based on the weak relativity of l$\alpha\beta$ color space, there is no need to consider the change of other dimensionality components when modify random components; Secondly, because 2×2 pixel module is the embedding basic unit, the final image is the communal area in 2×2 pixel module, the embedding measure can reach 25% and reduce the span of color transfer; Finally, only change α and β component and use chaotic map and genetic algorithm to reduce the change of cover image. Concerning sensitivity, use the feature of CL energy distribution and contrast CRC of RAID4 between LL_2 robustness and fragile sign module. CL-CTT has excellent sensitivity of image processing.

SIMULATION EXPERIMENT

Simulation environment is MATLAB 7.0.0.19920. Cover image is Lena (256×256) (Fig. 6a). Stego image is binary image baboon (64×64) (Fig. 6b). Figure 6c shows stego image based on CL-CTT. PSNR = 35.2823 and indicates that it is of better invisibility.

Table 2 shows invisibility of CL-CTT increases by 19.40% averagely when embedding rate is 25% compared with LSB, DCT and DWT and some developed algorithm.

Define texture evaluation and modification rate of binary image (n×n pixels) separately in Eq. 6 and 7. Where $n = N/2^k$, $k\in\{1, 2,..., \log_2(N-1)\}$. f'(i, j) and f'(i, j) are separately for the pixel at (i, j) of normal and extraction image with n×n pixels:

$$w = \frac{n\times n}{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j)\,\overline{\oplus}\, f(i\pm 1, j\pm 1)} \tag{6}$$

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

Comparison experiments between CL-CTT and LSB, DCT and DWT are as follows. Robustness test algorithm (RTV) is defined in Eq. 8 and k = 4. Information extraction is the most preserved when RTV = 100:

$$Q = w\times p \tag{8}$$

Figure 7a shows image under the JPEG2000 57% compression and image rebuilt (RTV = 56.0631). Figure 7b shows the RTV of every algorithm under JPEG2000 compression from 0-100%.

Figure 8a shows image under the cutting 20% and image rebuilt (RTV = 88.8639). Figure 8b shows the RTV of every algorithm under cutting processing from 0-100%.

Figure 9a shows image under the rotation 110.5° and image rebuilt (RTV = 11.2268). Figure 9b shows the RTV of every algorithm under rotation processing from 0-180°.

Figure 10a shows image under the mean filter [3, 3] and image rebuilt. Figure 10b shows image under the wiener2 filter [3, 3] and image rebuilt. Table 3 lists the RTV of CL-CTT and other algorithm.

Figure 11a shows image under the Gaussian noise (μ = 0, σ2 = 0.003) and image rebuilt. Figure 11b shows image under the 'salt and pepper' noise (d = 0.15) and image rebuilt. Table 3 lists the RTV of CL-CTT and other algorithm.

Experiment show that CL-CTT algorithm is robust against JPEG2000 below 72%, cutting below 47%, rotation below 75°, common filtering and adding noise. And show that RTV of CL-CTT increase by 40.02, 28.65,

Table 2: Invisibility comparison based on PSNR

Scheme	CL-CTT	LSB	DCT	DWT	DWT and DCT	DWT and LSB
PSNR	35.2823	25.1258	29.1547	30.0952	31.1124	32.2590

Table 3. RTV comparison results of filtering and noise

	Information hiding algorithm			
Attacks	CL-CTT	LSB	DCT	DWT
[3, 3] mean filter/wiener2 filter	62.44/58.54	30.58/40.25	50.21/43.26	66.26/57.32
Gaussian/'salt and pepper' noise	71.45/32.76	20.15/21.01	60.26/40.21	66.22/29.26

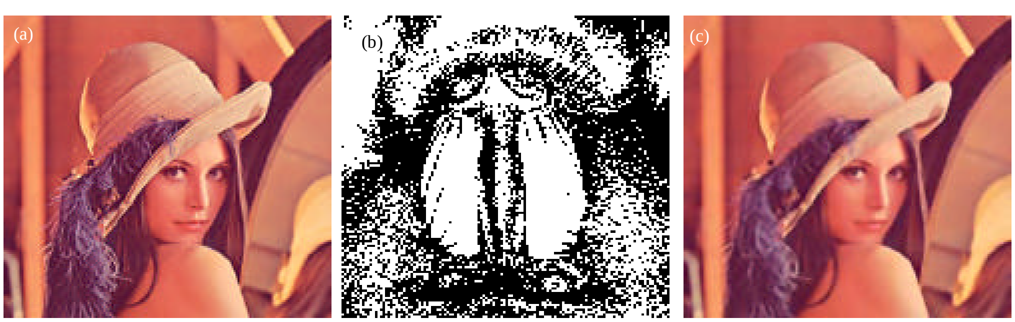

Fig. 6(a-c): Invisibility experiment (a) Cover image, (b) Hiding information and (c) Stego image

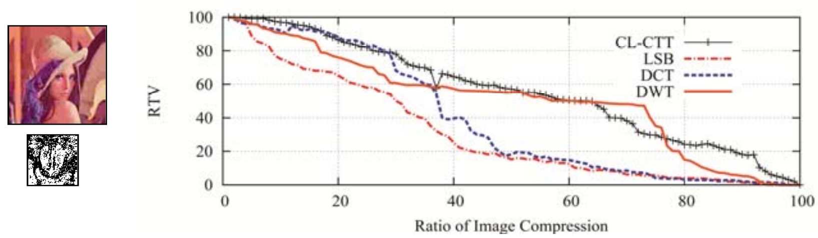

Fig. 7(a-b): JPEG2000 compression experiment (a) JPEG2000 (57%) and (b) RTV results under JPEG2000 compression from 0-100%

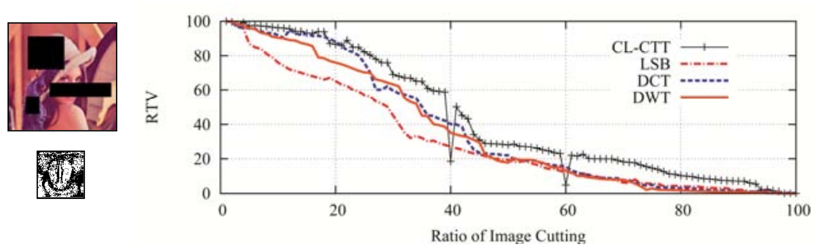

Fig. 8(a-b): Cutting processing experiment (a) Cutting (20%) and (b) RTV results under Cutting from 0-100%

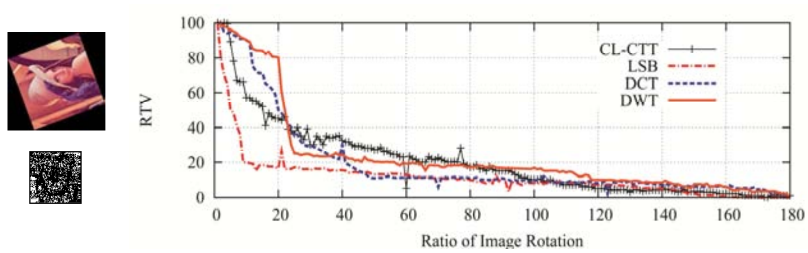

Fig. 9(a-b): Rotation processing experiment (a) Rotation (110.5°) and (b) RTV results under rotation from 0-180°

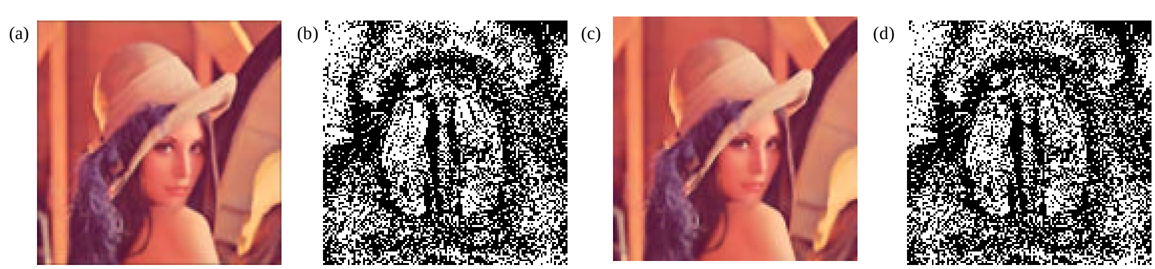

Fig. 10(a-b): Filter processing experiment (a) mean filter [3, 3] and (b) wiener2 filter [3, 3]

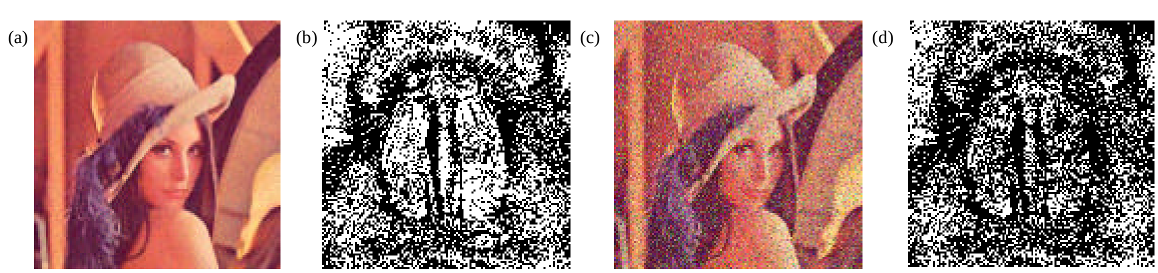

Fig. 11(a-b): Noise processing experiment (a) Gaussian noise and (b) 'salt and pepper' noise

Table 4: Detectable rate of attacks

Processing	JPEG2000 (%)	Cutting (%)	Rotation (%)	Filtering (%)	Gaussian (%)	'Salt and pepper' (%)
Detectable rate	89.22	87.01	99.29	96.97	93.05	98.63

19.99, 24.97 and 28.60% separately compared with LSB, DCT and DWT being under attacks such as JPEG2000 compression, cutting, rotation, filter and noise.

Sensitivity to image attacks is the peculiar characteristic in CL-CTT. Comparing CRC of LL2 and HH2 indicates CL-CTT has excellent sensitivity to image processing. Table 4 lists the detectable rate when JPEG2000 compression ratio is 5%, random cutting ratio is 5%, rotation ratio is 1°, [3, 3] median filter, Gaussian (μ = 0, $\sigma 2$ = 0.003) and 'salt and pepper'(d = 0.05). The average of detectable rate is 94.03%.

ACKNOWLEDGMENTS

Our research was funded by many Projects and the names and numbers of these Projects are as follows (1) Basic Research Project of Shaanxi Province Natural Science Foundation (Grant No. 2013JM8018), (2) The National Natural Science Foundation of China (Grant No. 61303041), (3) The Special Fund for Basic Scientific Research of Central Colleges of Chang'an University (Grant No. 2013G1241118 and 2013G2241020), (4) Xi'an Science and Technology Project (Grant No. CXY1318), (5) Jilin Province Association for International Exchange of Personnel Project (Grant No. 2012-7-102-2), (6) National IOT Project Major Demonstration Projects (Grant No. 2012-364-208-205 and 2012-364-812-105), (7) The State 863 Project (Grant No. 2012AA112312) and (8) The Ministry of Transport of the People's Republic of China Project (Grant No. 2012-364-208-600, 2012-364-208-200 and 201231849A70). 9. The Fund from Xi'an Red Sun Company (Grant No. XARESUN2013090101).

CONCLUSION

In conclusion, Simulation results show that due to the combination of CL multi-wavelet and color transfer and induction of chaotic map, genetic algorithm and RAID4, CL-CTT satisfies information hiding and also meets the basic security needs of secret information transmission for communication system. The future work is focus on choosing image A and B, embedded module, robustness parameters l and key data in LL_2.

REFERENCES

Chui, C.K. and J.A. Lian, 1996. A study of orthonormal multi-wavelets. Applied Numer. Math., 20: 273-298.

Deb, K., A. Pratap, S. Agarwal and T. Meyarivan, 2002. A fast and elitist multiobjective genetic algorithm: NSGA-II. IEEE Trans. Evol. Comput., 6: 182-197.

Lai, I.J. and W.H. Tsai, 2011. Secret-fragment-visible mosaic image-a new computer art and its application to information hiding. IEEE Trans. Inform. Forensics Security, 6: 936-945.

Li, Z., Z. Jing, X. Yang and S. Sun, 2005. Color transfer based remote sensing image fusion using non-separable wavelet frame transform. Pattern Recognition Lett., 26: 2006-2014.

Marcus, R.T. and P.E. Pierce, 1994. An analysis of the first surface correction for the color matching of organic coatings from the viewpoint of radiative transfer theory. Prog. Org. Coat., 23: 239-264.

Ye, G., 2010. Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recognit. Lett., 31: 347-354.

Yuan, S., S.X. Yao, Y.H. Xin and M.T. Liu, 2011. Information hiding based on the optical interference principle. Opt. Commun., 284: 5078-5083.