Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/070518

A Confidential Communication-Oriented Information Hiding Algorithm based on GHM multi-wavelet and DCT

Zhang Tao[1,*], *Mu Dejun*[2] *and Ren Shuai*[3]

[1] School of Electronic and Control Engineering, Chang'an University, Xi'an 710064, China
[2] College of Automation, Northwestern Polytechnical University, Xi'an 710062, China
[3] School of Information Engineering, Chang'an University, Xi'an 710064, China

Received: 11 Jan. 2013, Revised: 14 May. 2013, Accepted: 15 May. 2013
Published online: 1 Sep. 2013

Abstract: Structure and energy properties of carrier are considered as the most important factors to information hiding performance. This paper develops a new method to analyze energy and structure characteristics of digital images in order to preprocess the carriers. We adopt GHM multi-wavelet transformation to decompose the cover image into sub-images with different energy level. Then we obtain the embedding regions which are expressed as numerical range by discrete cosine transform. We embed data with different robustness in different regions. Then we get the stego image which is rarely changed in energy and structure properties compared with the original cover image. Experimental results indicate that the invisibility and robustness can be increased separately by 26.87% and 19.25% averagely, and the ability against steganalysis such as RS and Higher Order Statistics based on wavelet coefficients can be improved. Moreover, our algorithm has excellent sensitivity of image processing.

Keywords: Information hiding, GHM multi-wavelet transform, discrete cosine transform, carrier preprocessing, genetic algorithm.

1 Introduction

Information hiding is an important approach to secure confidential information transformation. A good information hiding scheme should have reliable performance, such as invisibility, robustness, sensitivity and anti-steganalysis. And performance improvement of information hiding scheme is the most favorite research topic. Currently, most of the schemes have not achieved the above performances at the same time. Schemes based on space domain are good at invisibility, but can not satisfy robustness and anti-steganalysis at the same time [1–3]. The schemes based on transform domain are good at robustness, however, most algorithms are poor in anti-steganalysis [4–6]. According to our previous studies [7], we know that operand-based methods, whether they are space domain- or transform domain-based, don't consider the energy and structure properties of carriers. Although the property analyze of carriers determines the performance of information hiding algorithms.

This paper proposes a preprocessing method based on GHM multi-wavelet transforms and discrete cosine transform (DCT) to analyze the energy and structure properties of digital image carriers. Taking advantage of the GHM in energy analyze and DCT in structure analyze, we embed secret information with minimal change in energy and structure of carriers. In particular, GHM multi-wavelet transform can process multi-transformation at the same time, and satisfy compact support and symmetry of the image processing.

2 Information hiding algorithm design

Embedding region:In the 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 GHM transform [8] provides a flexible information hiding strategy. Figure 1 shows GHM transform to Lena image. Energy ratio of four First-order GHM Multi-wavelet Transform sub-images is approximately as Table 1 [9].

After GHM multi-wavelet transforms, the most energy not only concentrated in the first-order sub-image (LL_1), and also energy distribution of four components is

[*] Corresponding author e-mail: zt904@foxmail.com

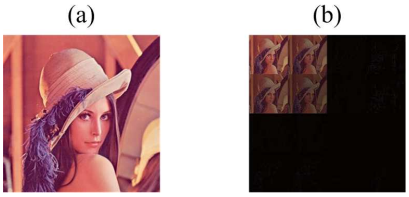
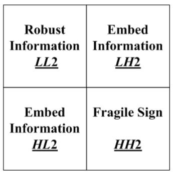


Fig. 1 First-order GHM multi-wavelet transform.

Table 1 Energy distribution of first-order GHM multi-wavelet

first-order image	LL_2	LH_2	HL_2	HH_2
97.31%	44.76%	21,80%	22.24%	11.20%



Robust Information *LL2*	Embed Information *LH2*
Embed Information *HL2*	Fragile Sign *HH2*

Fig. 2 Embedded region strategy.

similar to 4.5:2.2:2.2:1.1. Based on the energy distribution of GHM, generation of GHM-DCT embedding region can be divided into four steps:

Step1. Transform the cover image with first-order GHM multi-wavelet to obtain four sub-images such as LL_2, LH_2, HL_2 and HH_2. Embed robust parameters in LL_2. And embed secret information in LH_2 and HL_2, fragile sign in HH_2, as shown in Figure 2.

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

Step3. LH_2 and HL_2 ($N \times N$) will also be carried on DCT. Choose the interval distribution $[0,(N^2/2)-1]$ of DCT coefficient as embedding region in LH_2 and HL_2.

Step4. Decomposed HH_2 into $l\alpha\beta$ color component and transform the β component into gray image. Bit plane decompose to the gray image. The Bit Plane 0 is the embedding region in HH_2.

Generation of GHM-DCT embedding rules can be divided into four steps:

Rule1. Even and odd coefficients of DCT separately represent as 0 and 1.

Rule2. Embed information into LH_2 and HL_2 with RAID4 (Eight bits is the basic data unit of RAID4).

Rule3. Embed information into LL_2 following a sequential order $[(N^2/4) - 1, N^2 - 1]$, and embed information into LH_2 and HL_2 following a sequential order $[0,(N^2/2)-1]$.

Rule4. Embed information into HH_2 by line traversal order.

Information hiding scheme based on GHM Multi-wavelet and DCT can be divided into seven steps:

Step1. Transform the cover image with first-order GHM 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 $0 \leq m \leq N^2/2$.$CLL_1^{(3)} = x_1^{(3)}, x_2^{(3)}, \cdots, x_n^{(3)}$ and $0 \leq n \leq N^2/2$. The final analysis result denoted as C:

$$\begin{aligned} &C = (x_1, x_2, \cdots, x_i) \\ &= \left(x_1^{(2)}, x_2^{(2)}, \cdots, x_m^{(2)}, x_1^{(3)}, x_2^{(3)}, \cdots, x_n^{(3)}\right) \end{aligned} \tag{1}$$

Step3. Use Chebyshev map [10] of chaotic map algorithm to optimize information, as defined in Equation (2). 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 Equation (3), in which $C_{IN}^x = \left(b_1^x, b_2^x, \ldots b_{m+n-1}^x, b_{m+n}^x\right)$.

$$\begin{cases} 1\ , -1 \leq x_{k+1} < \eta \\ 0\ ,\ \ \eta \leq x_{k+1} \leq 1 \end{cases} , x_{k+1} = \cos\left(\mu \mathrm{arc} cos(x_k)\right) \tag{2}$$

$$C_{IN}^x = C_{pre} \oplus C_h \tag{3}$$

Step4. In order to optimize the sequence of embedded bits with genetics algorithm [11], suppose F as the amount of the same bit value in matched positions between C_{IN}^x and C. The optimization model based on GHM-DCT is Equation (4). Get the optimal solution x_n', η' and μ' by genetic algorithms optimization.

Step5. Bring x_n', η' and μ' into Equation (2) and (3) to get optimization embedded bits $C_{IN}^y = b_1^y, b_2^y, \ldots b_{n-1}^y, b_n^y$. Embed C_{IN}^x into DCT coefficients of LH_2 and HL_2 between 0 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 RAID4, 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.

Extracting information:Extracting information is divided into four steps:

Step1. Transform the cover image with first-order GHM 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

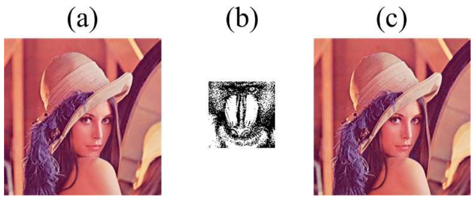


Fig. 3 Hiding and result of GHM-DCT.

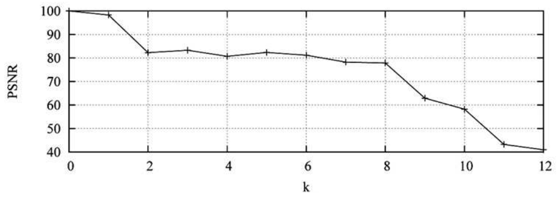


Fig. 4 Experiment of embedding dense and corresponding Invisibility.

data from LH_2 and HL_2 component, 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. Draw the check code of RAID4 from LL_2 component and use them to process C'' and get final secret information.

3 Simulation experiment

Simulation environment of the algorithm is Matlab7.0.0.19920. Cover image is Lena (256×256) as shown in Figure.3 (a). Stego image is binary image Baboon (64×64) as shown in Figure.3 (b).

Invisibility Experiment. Fig.3(c) shows stego image based on GHM-DCT. PSNR value equals 36.8921. It shows that this method is of better invisibility.

Invisibility is determined by Information content. Embed information in 400 images randomly. 2^k is used to denote bit quantity ($0 \leq 2^k \leq 4096$). Fig. 4 shows the PSNR of different embedding quantity. The experimental results indicated that when $k \leq 12$, it is of better invisibility ($PSNR \geq 40.325$).

Robustness Experiment. Define texture evaluation and modification rate of binary image ($N \times N$ pixels) separately in Equation (4) and (5).

$$w = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \oplus f(i+\mu, j \pm \eta)}{2n^2} \tag{4}$$

$$p = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \oplus f'(i,j)}{n^2} \tag{5}$$

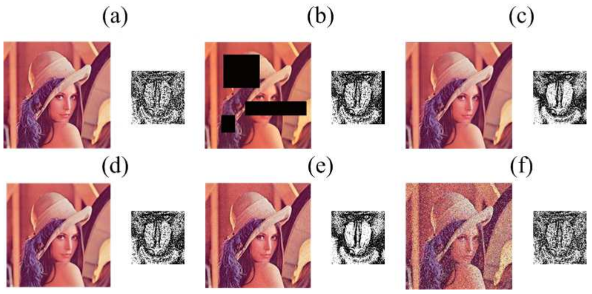


Fig. 5 Results of robustness experiment.

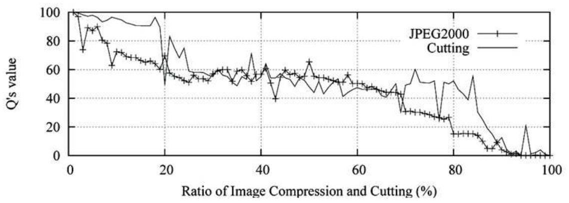


Fig. 6 JPEG2000 and cutting experiment.

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 Equation (6). Q is robustness test value and $Q \in [0,1]$. In the following experiments, $\mu = \eta = 1$. Expand Q 100 times to accommodate judgment habit.

$$Q = w\,(1-p) \tag{6}$$

Figure 5 shows the result of different attacks such as JPEG2000 compression, cutting, filtering and noise.

Images are vulnerable to compression and cutting attacks, Figure 6 shows the Q' value corresponding to ratio of these attacks.

According to experiment, embedded information can be identified when Q reach about 30. Figure 5 and Figure 6 show that GHM-DCT is robust against JPEG2000 compression below 73%, cutting below 85%, common filtering and adding noise.

Experiment of ability against steganalysis. Higher order statistics detection algorithm based on wavelet coefficients (HOSWC) is a general detection algorithm [12]. Use the algorithms above-mentioned to analyze the performance of GHM-DCT. Experiment results are shown in Figure 7.

Experimental results of detection analysis to GHM-DCT using the High-order statistics detection based on wavelet coefficient (HOSWC) are shown in Figure 7. 100 random stego-images, we cant find one or even more threshold values. Using these detection methods, we obtain maximum detectable rate are respectively 3.91% and 3.64% which are very low.

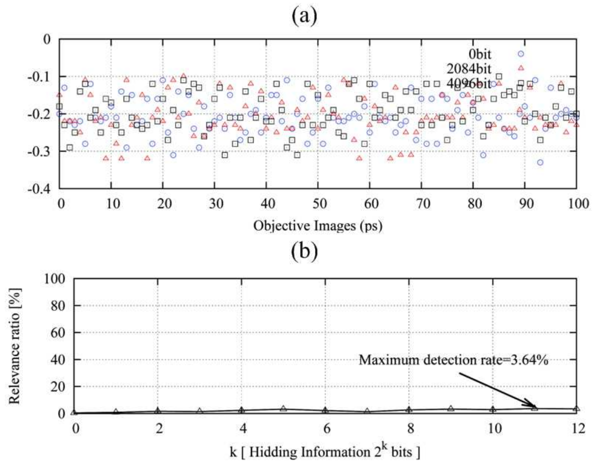


Fig. 7 Steganalysis experiment result of HOSWC to GHM-DCT.

Table 2 Detectable rate of attacks

JPEG2000	Cut	Filter	Gauss	saltpepper
99.25%	98.19%	99.57%	98.43%	99.85%

Table 3 Invisibility comparison based on PSNR

Algorithm	GHM-DCT	DWT-DCT	DWT-LSB
PSNR	36.8921	35.3270	935.9501

Experiments show the algorithm can resist these steganalysis.

Experiment of sensitivity to image attacks. Sensitivity to image attacks is the peculiar characteristic in GHM-DCT. Comparing R^L with R^H indicates the algorithm has excellent sensitivity of image processing. TABLE 2 lists the detectable rate when JPEG2000 compression ratio is 5%, random cutting ratio is 5%, [3,3] median filter, Gaussian ($\mu = 0$, $\sigma^2 = 0.003$) and salt and pepper($d = 0.15$). The average of detectable rate is 98.86%.

Experiment of invisibility comparison. According to PSNR, GHM-DCT has advantages in invisibility compared with DWT-DCT and DCT-LSB. Table 3 shows that invisibility increases by 3.51% averagely when embedding rate is 25%.

Experiment of robustness comparison. Figure 8, Figure 9 and Table 4 show robustness comparison results when embedding rate is 25% based on RTV.

The Q's value of GHM-DCT in JPEG2000 compression is 44.3492. DWT-DCT is 32.9980, and DCT-LSB is 42.6989. Indicate GHM-DCT is better robustness at JPEG2000. The Q's value of GHM-DCT in cutting is 57.3453. DWT-DCT is 33.7810, and DCT-LSB is 31.0311. Indicate GHM-DCT is better robustness at cutting. TABLE 4 show that GHM-DCT have better performance in robustness under filter and noise except compared with salt and peppe noise of DWT-DCT.

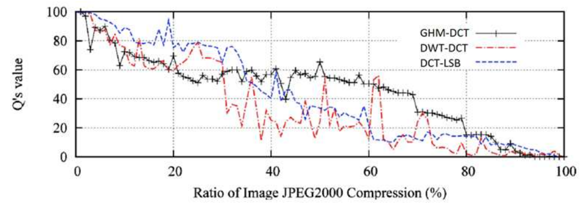


Fig. 8 Compression comparison.

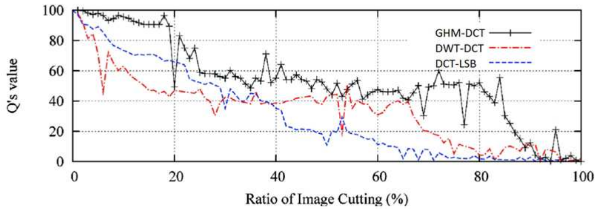


Fig. 9 Cutting comparison.

Table 4 RTV comparison of filtering and noise

Attacks	GHM-DCT	DWT-DCT	DWT-LSB
median filter	62.01	45.33	60.11
wiener2 filter	59.36	58.74	49.60
Gaussi	67.79	46.90	60.14
saltpepper	54.30	53.48	42.15

4 Conclusions

Propose an Information hiding scheme based on GHM and DCT. Take advantage of the energy distribution ratios in the four sub-images after first-order GHM 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 97.31% 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 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 LH_2 according to robustness rule of DCT hiding are. The statistical properties of Chebyshev traverse and zero mean white noise are consistent [11], which is of good distribution and hiding characteristics to improve anti-steganalysis. Decompose HH_2 according to l 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.

5 Acknowledgments

The authors would like to thank the reviewers for their detailed refereeing and constructive comments, which have helped in improving the quality of this paper. The study was supported by the National 863 plans projects, the Ministry of Transport of the People's Republic of CHINA projects, the Jilin Association for International Exchange of Personnel projects, and the Special Fund for Basic Scientific Research of Central Colleges, Chang?an University. The Grant Numbers are respectively 2012AA112312, 2012-364-208-600 and 201231849A70, 2012-7-102-2 and CHD2011TD009.

References

[1] D. Abed, N. Mustafa, Int. J. Adv. Comput. Technol., **2**, 140 (2010).
[2] L. Anuradha, K. Achana, International Conference on Advances in Computing, Communication and Control, **364**, (2011).
[3] X. Sun, Inf. Technol. J., **9**, 460 (2010).
[4] A. Cheddad, J. Condella, K. Currana, Sig. Proc., **90**, 727 (2010).
[5] L. Li, H. Xu, C. Chang, Y. Ma, J. Syst. Soft., **84**, 923 (2011).
[6] W. Lu, W. Sun, H. Lu, Comput. Electr. Eng., **35**, 183 (2009).
[7] Z. Tao, M. De-jun, R. Shuai, Appl. Math. Inf. Sci., **6**, 253 (2011).
[8] Z. Tao, M. De-jun, R. Shuai, Int. J. Digit. Content Technol. Appl., **5**, 210 (2011).
[9] H. Zhuo-jun, M. Zheng-ming, J. Image Graphics, **12**, 1198 (2001).
[10] D. E. Goldberg, Addison Wesley Publishing Company, PISCATAWAY, **237**, (2007).
[11] F. Hany, L. Siwei, IEEE Workshop on Statistical Analysis in Computer Vision,**94**, (2003).
[12] C. Dongming, C. Yunpeng, Adv. Inf. Sci. and Serv. Sci., **3**, 364 (2011).

Zhang Tao obtained her PhD from Northwestern Polytechnical University of China in 2012. She is a lecture in School of Electronic and Control Engineering in Chang'an University. She has been engaged in Information hiding and Network security for 8 years. She published 20 scientific research articles in international publications and 1 are cited by SCI, 6 are cited by EI.She has carried out 4 tasks to study a plan in all, won patent 1.

Mu Dejun obtained the Ph.D. degree in control theory and control engineering from Northwestern Polytechnical University, Xi'an, Shaanxi, China, in 1994. He is currently a Professor with the School of Automation, Northwestern Polytechnical University, China. His current research interests include control theories and information security, including basic theories and technologies in network information security, application specific chips for information security, and network control systems.

Ren Shuai obtained his PhD from Northwestern Polytechnical University of China in 2009. He is a lecture in School of Information Engineering in Chang'an University. He has been engaged in Information hiding and Network security for 7 years. He published 23 scientific research articles in international publications and 2 are cited by SCI, 7 are cited by EI. He has carried out 5 tasks to study a plan in all, won patent 2. During the last yearhe has written or co-edited for 5 textbooks.