Applied Mathematics & Information Sciences
An International Journal

Study of Reversible Information Hiding Scheme Based on GHM and ASA

Shuai REN[1] , *Tao ZHANG*[2] *and Dejun MU*[3]

[1] School of Information Engineering, Chang'an University, Xi'an 710064, CHINA
[2] School of Electronic and Control Engineering, Chang'an University, Xi'an 710064, CHINA
[3] College of Automation, Northwestern Polytechnical University, Xi'an 710072, CHINA

Received: Jul 8, 2011; Revised Oct. 4, 2011; Accepted Oct. 6, 2011
Published online: 1 May 2012

Abstract: Information hiding based on digital images is still the mainstream now. In this paper, using first-order transformation of GHM multi-wavelet, carrier image is decomposed into four components of lowest resolution sub-image. These four components are processed by ASA (Annulus Sector Analysis) to obtain embedding areas. Information hiding follows two rules: First, satisfies four components energy distributed feature of GHM multi-wavelet first-order sub-images. That means embedding robust parameters LL_1 in, embedding pre-hiding information by RAID4 method in LH_1 and HL_1 , embedding fragile identifier HH_1 in. Second, use two or more annulus to embed data symmetrically. Moreover, using Logistic chaotic map and genetic algorithm to adjust sequence of embedded data and LSB is checked by MSB. Experimental results show that the invisibility of this scheme is of 3.65% average increase and excellent perception to distortion. Robustness is improved by 11.06% at least. This scheme has a good robustness against, cutting, mean and medium filteringespecially can completely resist rotation.

Keywords: Information Hiding (IH), GHM (Geronimo Hardin Massopust) multi-wavelet transform, ASA (Annulus Sector Analysis), Logistic chaotic map, Bit-plane decomposition, RAID4.

1. Introduction

Information hiding is of high-quality invisibility to secure confidential communication with public carrier. But attackers always destroy confidential communication by physical attacks without analysis. So, robustness of information hiding is of vital importance. Most of the literatures don't have good robustness against attacks such as solve rotation, cutting, mean and medium filtering, and few resist against them at the same time [1-4]. Multi-wavelet technologies have boosted in information hiding technical field and more and more researchers emphasis on its applications [5-7]. Furthermore, embedding pre-hiding information based on annular can obviously resist against rotation. This paper focuses on information hiding algorithm based on GHM multi-wavelet and annulus sector analysis (ASA). Energy distributed feature of components obtained by GHM multi-wavelet transformation can well satisfy invisibility and robustness at the same time. Moreover, the most important features such as annulus sector analysis to carrier, averaging sector's pixel value and using two or more annular to embed data symmetrically can solve robustness against rotation, cutting, mean and medium filtering with good performance. The overview of this scheme is organized as follows: (1) put carrier image into GHM first-order transformation to obtain four sub-images; (2) determine width of annulus and angle of sector; (3) divide the four sub-images into annulus sectors; (4) analysis data from annulus sectors of carrier image; (5) selection usable annulus sectors by texture and matching discriminant function; (6) embed pre-hiding information in usable annulus sectors.

2. GHM multi-wavelet transformation

Multi-wavelet transform is a new concept in wavelet transform system [8]. It adds smoothness, compact sup-port, symmetry and orthogonality based on time domain and frequency domain of single wavelet local characteristic [9].

* Corresponding author: Shuai REN, e-mail: maxwellren@qq.com

Compared with scalar wavelet, Multi-wavelet transform which is indicated by multi-dimensional vector function has several scaling and wavelet functions. GHM multi-wavelet transform [10], which 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 GHM multi-wavelet first-order transformation to $Lena$ image. Figure 1(a) is $Lena$ Normal image. Figure 1(b) is $Lena$ first-order image. It illustrates that energy ratio LL_1:LH_1:HL_1:HH_1 of four sub-images is about 4.5:2.2:2.2:1.1.

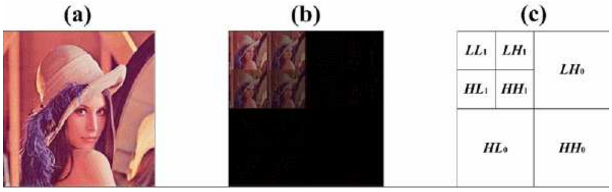

Figure 1 First-order GHM multi-wavelet transform.

3. Annulus Sector Analysis

Annulus sector analysis is a new digital image analytic method, it includes three key steps: first, determine width of analytic annulus; second, determine angle of annulus sector; third, analyze annulus data. This algorithm embeds pre-hiding information by modification of annulus sector analysis data. Examples for writing definition, lemma, theorem, corollary, example, remark.

Determine analytic annulus and sector. We make the assumption that carrier image is square, D presents side length. Annulus sector analysis rules are as follows. Figure 2 shows the definition of analytic annulus, Figure2(a) shows the annulus width and Figure2(b) shows the annulus division line and attribution.

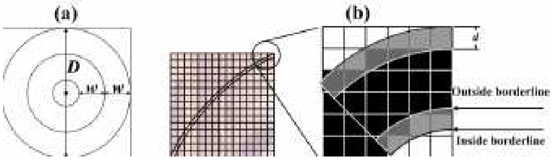

Figure 2 Annulus analysis.

Rule 1: The outer-most annulus inscribes square of carrier image. Annulus is denoted as R_j ,in which j gradually increasing from the outside to inside;

Rule 2: w annulus width

Rule 3: Width of annulus division line equals to width of one;

Rule 4: Following the rule named inside borderline of division line crossing, which means pixels crossed by inner boundary of division line belongs to the annulus. Figure 2(b) shows detailed schematic diagram after annulus division, two division lines divide carrier image into three regions. One region is an annulus (represented by black), the others are two white regions;

Rule 5: Determine sector angle α. Obtain sectors, shown in Figure 3(a). In which, r_{1i} represents the ith sector of annulus R_1;

Rule 6: Take the average value of all pixels in the sector as the sector value. Obtain one-dimensional array as the annulus analytic value by traversing the sectors clockwise from 12 o'clock direction. Shown in figure 3(b), the analytic value of annulus R_1 is [r_{11}, r_{12}, r_{13}, r_{14}, r_{15}, r_{16}, r_{17}, r_{18}], when α=45°.

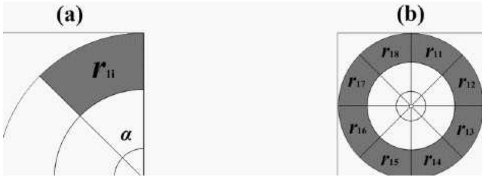

Figure 3 Sector division and analysis.

Selection of usable analytic annulus. According to basic requirements of information hiding technology such as invisibility, capacity, robustness and anti-steganalysis ability, usability of analytic annulus is determined by texture complexity and data matching rate. There are two steps of usable analytic annulus selection

Step 1: Texture complexity judgment. The analytic value of annulus is denoted as $R = (r_n | n = 1, 2, \cdots, 2\pi/\alpha)$. Texture complexity discriminant function is Eq. (1).

$$q = \frac{\left(\sum_{n=2}^{2\pi/\alpha} r_n - r_{n-1}\right) + \left(r_1 - r_{2\pi/\alpha}\right)}{2\pi/\alpha} \tag{1}$$

In which, q is the annulus complexity and is inversely with sector angle α. Step 2: Matching rate judgment. The core idea is optimization and matching between scrambled pre-hiding information and analytic data. If matching rate is too low, then give up the annulus. Achieve optimal adjustment by genetic algorithm [11]. Set $C = (c_1, c_2, \cdots c_n) \in (0, 1)$ to be pre-hiding information $C = (c_1, c_2, \cdots c_n) \in (0, 1)$. C is scrambled as $C'(x, y) = (c'_1, c'_2, \cdots c'_n) \in (0, 1)$. And $T = (t_1, t_2, \cdots t_n)$ is data of carrier image, $T' = (t'_1, t'_2, \cdots t'_n) \in (0, 1)$ is analytic data by embedding rules mentioned in 2.1. F denotes bits number with

Security level	Parameters
High	$w\alpha/D < 1.0 \times 10^{-3}$
Medium	$1.0 \times 10^{-3} < w\alpha\big/D < 6.8 \times 10^{-3}$
Low	$6.8 \times 10^{-3} < w\alpha\big/D < 8.9 \times 10^{-3}$

Table 1 Parameters under different communication requirement

Security level	*q*	*f*	*G*
High	$[0.86, 1]$	$[0.63, 1]$	$[6, 10]$
Medium	$[0.57, 0.86]$	$[0.30, 0.63]$	$[4, 6]$
Low	$[0.34, 0.57]$	$[0.10, 0.30]$	$[1, 4]$

Table 2 Parameters under Different Security Levels

same value between C' and T'. Optimal adjustment maximizes F. Definition of F is shown as:

$$F = Max\sum\left(t'_n\bar{\oplus}c'_n\right) \tag{2}$$

Maximum matching rate is rate of bits not required to modify, which is calculated by Eq. (3):

$$f = F/n \tag{3}$$

4. Information Hiding Scheme

Information hiding rules is the kernel of our scheme, which includes hiding region selection and data modification methods. There are seven rules in this scheme:

Rule 1: Annulus sector analysis based on first-order sub-images after GHM multi-wavelet transformation such as LL_1, *LH*$_1$, *HL*$_1$ and *HH*$_1$;

Rule 2: Table 1 shows analysis parameters setting under different communication requirement (measured by robustness and invisibility). Carry LL_1, *LH*$_1$, *HL*$_1$ and *HH*$_1$ into annulus sector analysis and denote the obtained sector as S_{ijk}, *i*=1,2,3,4 respectively correspond to LL_1, *LH*$_1$, *HL*$_1$ and *HH*$_1$; j denotes annulus serial number, and $j \in Z$, $1 \leq j \leq D/2w$. k denotes number of sectors divided from 12 o'clock direction, and $k \in Z$, $1 \leq k \leq 2\pi/\alpha$.

Rule 3: Extract usable annulus sectors according to selection steps. Table 2 shows parameters corresponding to different security levels:

Rule 4: Hide information after selection of usable annulus sectors according to the following rules: (1) Symmetry principle: Embed same information in symmetrical sectors of the same annulus. As shown in Figure 4, symmetrical sectors represented with the same letter A carry the information; (2) Double or more annulus: Information embedded in the outer-most annulus should be embedded in at least another one annulus which is interval from the outer-most annulus. As shown in Figure 4, region A and region B carry the same information. Annulus R_3 in Figure 4 is usable, and if R_3 is unusable but R_4 is usable, then we embed the same information with R_1 in R_4. Annulus number embedded the same information is represented as G, G=2,3,...; (3) Determination of starting position: the first t (shown as region C in Figure 4) sectors from 12 o'clock direction are embedded initial information identifier which can judge the starting position of annulus data.

LL$_1$	*LH*$_1$	*HL*$_1$	*HH*$_1$
Robustness data	Pre-hiding data		Fragile identifier

Table 3 Embedding in Different Regions According to Data Characteristic

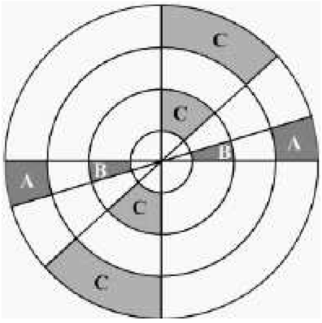

Figure 4 Information Hiding Sector Rules.

Rule 5: Table 3 shows embedding data with different characteristic corresponding to regions with different characteristics.

Specific strategies are as follows: (1) LL_1 is robustness data unit, so we embed analysis parameters such as D, w, α, t and $Hash$ value of pre-hiding information in LL_1; (2) Embed pre-hiding information in LH_1 and HL_1 by RAID4 method; (3) Embed Hash value of pre-hiding information in HH_1. Embedding data with different characteristic according to region energy can satisfy robustness and excellent perception to distortion.

Rule 6: Modify all pixels' value to the average value of themselves in all annulus sectors;

Rule 7: In all sectors, embed data by Combination Bit Plane strategy [12] , shown in Figure 5. Steps are as follows: (1) Bit Plane 0 of every sector is regarded as information hiding plane, Bit Plane 3 is auxiliary plane and Bit Plane 7MSBis datum plane; (2) C_7 is the binary data of Bit Plane 7, and Bit Plane 3 is modified by Eq. (4) when hiding information C_I:

$$C_3 = C_7 \oplus C_I \tag{4}$$

Rule 8: Pre-hiding information is optimized by $Logistic$ chaotic map before matching rate judgment, and $Logistic$ chaotic map id defined as follows:

$$x_{k+1} = \mu x_k \left(1 - x_k\right),\ x_k \in (0, 1) \tag{5}$$

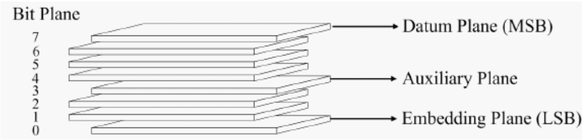

Figure 5 Combination Bit Plane Embedding Strategy.

Pre-hiding information is scrambled according to x_k. We obtain binary sequence E by Eq. (5), where $E = (e_1, e_2, \cdots e_n) \in (0, 1)$. We scramble pre-hiding information as Eq. (6):

$$C' = (c'_1, c'_2, \cdots c'_n) = C \oplus E \tag{6}$$

where C is pre-hiding information and is scrambled pre-hiding information.

5. Information Hiding and Extraction

Our scheme is blind, and extraction is inverse process of information hiding. Information hiding is divided into 5 steps. The flow chart of information hiding is shown as Figure 6:

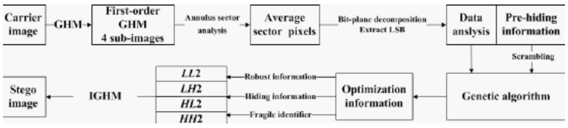

Figure 6 Information Hiding Flow Chart.

Information extraction is divided into 5 steps. The flow chart of information extraction is shown as Figure 7:

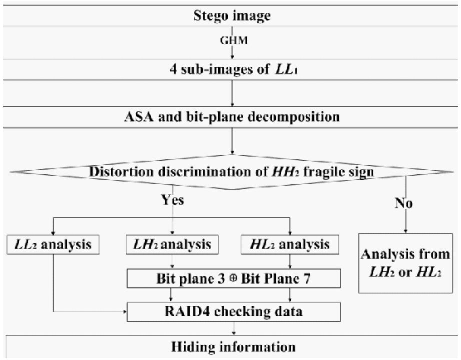

Figure 7 Information Extraction Flow Chart.

6. Simulation Experiment.

Simulation environment of this scheme is Matlab7.0.0.19920. Cover image is $Lena$ (256×256) as shown in Figure 8(a). Stego image is binary image Baboon (64×64) as shown in Figure 8 (b).

Figure 8 Hiding and result of GHM-ASA.

Scheme performance analysis. We analyze the invisibility, robustness, sensitivity and anti-steganalysis of our scheme by experiments and related measure standards.

Invisibility analysis experiment. The following two properties ensure invisibility of this scheme: (1) LSB and part of Bit Plane 3 are the modified position in this scheme and invisibility is the greatest advantage of information hiding based on LSB; (2) By $Logistic$ chaotic map scrambling, texture complexity and matching rate judgment, we can lessen modification to carrier image in the greatest degree. Figure 8 (c) shows stego image obtained by this scheme when D=256, w=4, α=5°, f, q and G are on medium level of security. PSNR value equals 36.7686. It shows that this method is of better invisibility.

Robustness analysis experiment. This scheme is robust because of the following four properties: (1) We propose different embedding strategies based on energy distribution characteristics of GHM sub-images. Moreover, hiding information in LH_1 and HL_1 by RAID4 method; (2) We embed information along the annulus, so it is robust against rotation. We embed information symmetrically, so receivers can extract hiding information with 100% integrity under regular cutting less than 50%. (3) Considering Bit Plane7 and Bit Plane 3 as auxiliary embedding planes, robustness of LSB is improved by 3 levels; (4) Averaging all pixels of sector before embedding is in fact a mean filtering operation. By filtering theory [10], this algorithm is of excellent robustness against mean and medium filtering when satisfied invisibility. There are at least two same pixels in most sectors, so extract all pixels of a sector. By comparison all pixel values, take the value of most pixels as the final extracted value.

Define texture evaluation and modification rate of binary image ($n \times n$ pixels) separately in (7) and (8).

$$w = \frac{\sum_{i=0}^{n-1} \sum_{j=0}^{n-1} f(i,j) \oplus f(i+\mu, j \pm \eta)}{2n^2} \tag{7}$$

$$p = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \oplus f'(i,j)}{n^2} \tag{8}$$

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 Eq. (9). 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.

$$Q = w\,(1-p) \tag{9}$$

Figure 9 shows the result of different attacks such as JPEG2000 compression (58% and Q=56.01), cutting (50% and Q=100), rotation (110.5° and Q=98.34), median filtering ([3,3] and Q=90.31), mean filtering ([3,3] and Q=92.62) and wiener2 filtering ([3,3] and Q=86.48), where operated object is stego image Figure 8 (c).

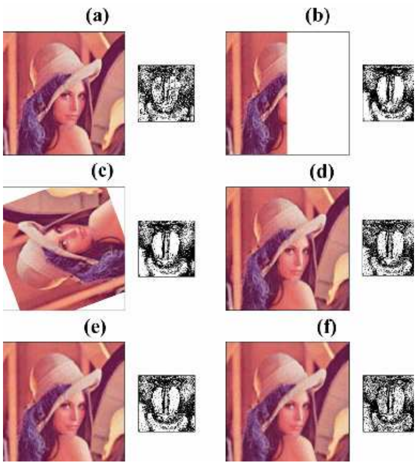

Figure 9 Results of Robustness Experiment.

Images are vulnerable to compression and cutting attacks, Figure 10 shows the robustness test value results corresponding to ratio of these attacks. Rotation is a fatal attack to images. Robustness results corresponding to different attack degrees are shown in Figure 11.

According to experiment data, embedded information can be identified when robustness test value reach about 45. Figure 10 and Figure 11 show that this algorithm is robust against JPEG2000 compression below 67%, cutting below 86%, rotation below 100%.

Sensitivity analysis to image attacks. The following two properties ensure distortion sensitivity of this scheme: (1) We embed $Hash$ value of hiding information in both LL_1 and HH_1 based on energy distribution characteristics of GHM sub-images. Judge distortion by comparison of $Hash$ value; (2) Embed same information in sectors of the same annulus. Compare data in symmetrical sectors to judge distortion.

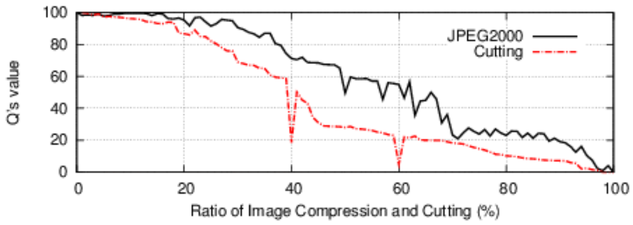

Figure 10 JPEG2000 and Cutting Experiment.

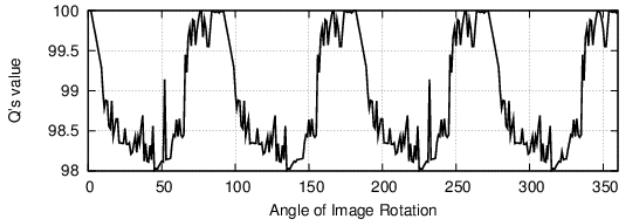

Figure 11 Rotation Experiment.

Experiments show that the false negative rate of distortion is 0 by comparison of $Hash$ value in LL_1 and HH_1, or comparison of data in symmetrical sectors. In practical application, normal noise in communication will be mistaken for malicious tampering due to high sensitivity of this scheme. So this scheme is of high false positive rate. And we can reduce false positive rate by modification threshold. We judge distortion by experimental results based on comparison of symmetric data. If different rate of symmetric data below 7%, we regard it as normal noise.

Anti-steganalysis ability analysis experiment. This scheme can resist steganalysis because of the following four properties: (1) Most recent steganalysis strategies are invalid to multi-wavelet transformation; (2) By $Logistic$ chaotic [13] map scrambling, texture complexity and matching rate judgment, we can improve against steganalysis ability.

RS statistics analysis [12] is an efficient detection method. We can effectively detect hidden information by comparison of R_m and R_{-m}, S_m and S_{-m} in RS algorithm. High-order statistics detection algorithm based on wavelet coefficient ($HOSWC$) is an universal detection algorithm. Experimental results of detection analysis to GHM-ASA using the above two algorithms are shown in Figure 12 and Figure 13 when D=256, w=4, α=5°, f and q are on low level of security. Figure 12(a) shows the result of RS. Figure 12(b) shows the Steganalysis detection rate of RS to GHM-ASA. Figure 13(a) shows the result of $HOSWC$. Figure 13(b) shows the Steganalysis detection rate of HOSWC to GHM-ASA.

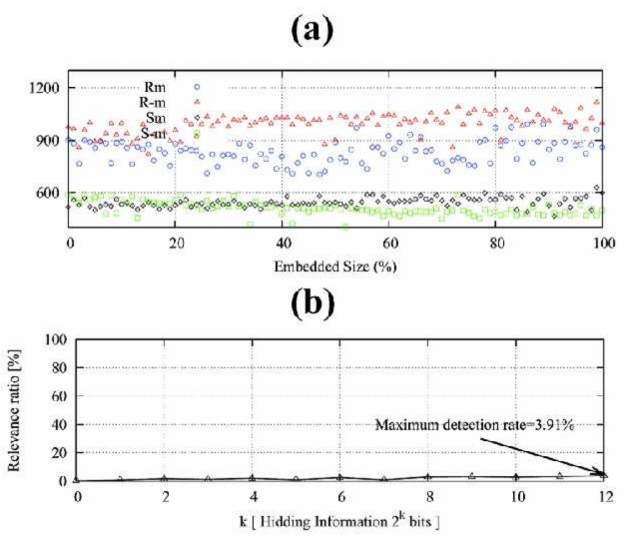

Figure 12 Experiment result of RS.

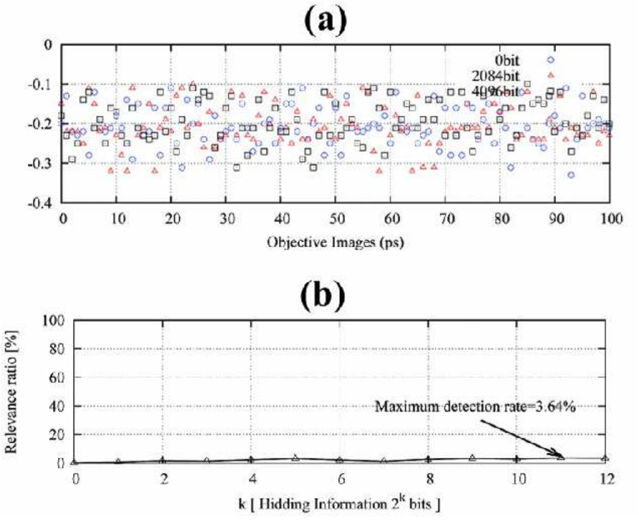

Figure 13 Experiment result of HOSWC.

Based on the initial deviation (approximately equal to 168) of RS, we know that the maximum difference between R_m and R_{-m} is 362 and the maximum difference between is 357. And embedding rate doesn't have a there is no positive affect on difference. In HOSWC, 100 random stego-images, we can't find one or even more threshold values. Using these detection methods, we obtain maximum detectable rate are respectively 3.91

Performance comparison with other schemes. Information hiding schemes based on LSB, DCT or DWT are obviously poor in robustness and anti-steganalysis [12]. Bringing GHM multi-wavelet technology into information hiding is a significant contribution to this field. Comparisons between our scheme and other scheme based on GHM are as follows [9, 14-15]:

GHM-ASA	GHM-CT	GHM-CMVS	GP-GHM
36.7686	34.1954	35.6794	36.5501

Table 4 Invisibility Comparison based on PSNR

Invisibility comparison. According to PSNR, GHM-ASA has advantages in invisibility compared with other schemes based on GHM. Table 4 shows that invisibility increases by 3.65% averagely when embedding rate is 25%.

Experiments of robustness comparison. Figure 14-16 and Table 5 show robustness comparison results when the embedding rate is 25% based on Robustness test algorithm.

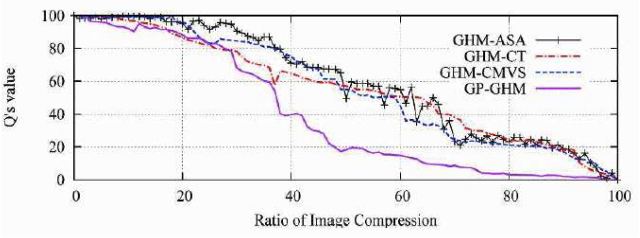

Figure 14 Compression Comparison.

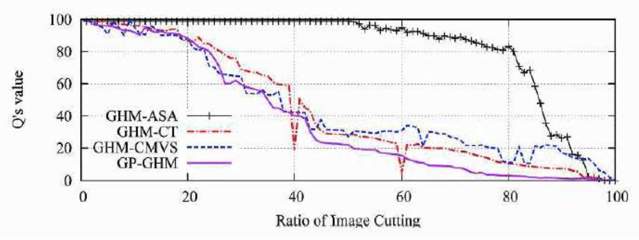

Figure 15 Cutting Comparison.

The experiment results show that robustness test value of GHM-ASA increases by 27.36% and one time compared with GHM-CT, GHM-CMVS and GP-GHM under attacks of JPEG2000 and random cutting.

The experiment results show that robustness test value of GHM-ASA increases by four times compared with GHM-CT, GHM-CMVS and GP-GHM under attacks of rotation.

The experiment results show that Robustness test values of GHM-ASA increase by 16.44%, 29.83% and 11.06% averagely compared with GHM-CT, GHM-CMVS and GP-GHM in under attacks such as [3,3] median filter, [3,3] mean filter and [3,3] wiener2 filter.

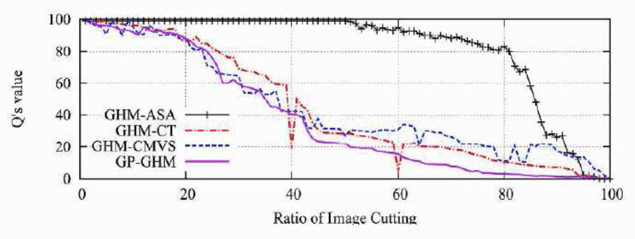

Figure 16 Rotation Comparison.

Scheme	[3,3] Median	[3,3] Mean	[3,3] Wiener
GHM-ASA	70.53	71.64	58.36
GHM-CT	60.23	57.82	57.48
GHM-CMVS	55.18	40.56	42.41
GP-GHM	63.31	67.16	57.76

Table 5 Robustness Test Values Comparison of Filtering and Noise

Comparison index	GHM-ASA	GHM-CT
FPR	98.63%	92.02%
FNR	99.13%	97.23%
	GHM-CMVS	GP-GHM
FPR	95.28%	96.93%
FNR	98.03%	98.95%

Table 6 Anti-steganalysis comparison based on false positive rate and false negative rate

To sum up, the experiment results show that GHM-ASA is of better performance in robustness against image attacks such as JPEG2000 (below 67%), cutting (below 86%), rotation (below 100%), common filtering.

Sensitivity comparison. Sensitivity to distortion of this scheme is almost 100% and obviously better than other schemes.

Anti-steganalysis comparison. Use RS statistics analysis and HOSWC to detect GHM-CT, GHM-CMVS and GP-GHM. Embedding percentage in experiment is 25%, selected carrier images are 200 random images. False positive rate (fpr) and false negative rate (fnr) of these three schemes are shown in Table 6.

False positive rate and false negative rate of our scheme are much higher than others. It illustrates that this scheme is of excellent anti-steganalysis ability.

7. Conclusion

We propose an information hiding scheme using image energy feature after GHM multi-wavelet transformation and spatial feature after ASA. Our scheme is robust against cutting, rotation and filtering and is of better invisibility. Need to note that, the carrier images in our scheme are digital, so annulus is relative. Annulus analysis is difficult point in experiment. In practical application, we consider to fix size of annulus and divide annulus sectors by papery or electronic reference cards that senders and recipients possess. Anti-steganalysis experiments should be improved in the future because anti- steganalysis has great relationship with carrier images, embedding information quantity and structure.

Acknowledgement

The project was supported by the Special Fund for Basic Scienti?c Research of Central Colleges, Chang'an University. The Grant Number is CHD2011JC074.

References

[1] P. Tsaia, Y.C. Hub and H.L. Yeha, Sign. Process. **89**, 1911 (2009).
[2] A. Cheddad, J. Condella, K. Currana and P.M. Kevitt, Sign. Process. **90**, 727 (2010).
[3] Z.X. Yin, C.C. Chang and Y.P. Zhang, J. Syst. Software **83**, 2073 (2010).
[4] C.C. Lin, Comput. Stand. Inter. **33**, 477 (2011).
[5] L. Ghouti, A. Bouridane, M.K. Ibrahim and S. Boussakta, Sig. Process. IEEE Trans. **54**, 1519 (2006).
[6] P. Kumsawat, K. Attakitmongcol and A. Srikaew, LNCS **5376**, 155 (2008).
[7] N.S. Liu, G.H. Yang, D.H. Guo and L.L. Cheng, Proc. International Conference on Intelligent Information Hiding and Multimedia Signal Processing 994 (2008).
[8] J.S. Geronimo, D.P. Hardin and P.R. Massopust, J. Approx. Theory **78**, 373 (1994).
[9] S. Ren, D.J. Mu ,T. Zhang and W. Hu, Chinese Optoelectron. Lett. **5**, 454 (2009).
[10] S. Ren, D.J. Mu ,T. Zhang, W. Hu and D.G. Zhang, Journal of Northwestern Polytechnical University **28**, 264 (2010).
[11] M.B. Aryanezhada and M. Hemati, Appl. Math. Comput. **199**, 186 (2008).
[12] S. Ren, D.J. Mu, T. Zhang and W. Hu, Proc. International Conference on Artificial Intelligence and Computational Intelligence 345 (2009).
[13] Q.C. Qian, Z.Q. Chen and Z.Z. Yuan, Int. J. Innov. Comput. I. **6**, 313 (2010).
[14] T. Zhang, D.J. Mu and S. Ren, Int. J. Digit. Con.t Tech. Appl. **5**, 210 (2011).
[15] S. Ren, D.J. Mu, T. Zhang and W. Hu, Proc. International Conference on Computational Intelligence and Software Engineering, 1 (2009).

Shuai REN 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.

Tao ZHANG 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. He has carried out 4 tasks to study a plan in all, won patent 1.

Dejun MU 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.