A Secure Image Steganography Based on DCT Domain

Qi Gui
Lab of Images Communication
Chongqing Communication Institute
Chongqing, 400035, P.R.China.
86-23-68759665
guiqi2003@sina.com

Sen Bai
Lab of Images Communication
Chongqing Communication Institute
Chongqing, 400035, P.R.China.
86-23-68760819
baisenchina@tom.com

Jing Sun
Lab of Signal and Information Processing
Chongqing Communication Institute
Chongqing, 400035, P.R.China.
86-23-68760924
masktml@265.com

ABSTRACT
Information hiding is an information security technology of secretly embedding information into digital multimedia such as image, video and audio signals without changing the perceptual quality of the cover-data. In this paper, we propose a high embedding capacity steganographic method in still image based on transform domain. With this method we embed the information in the transform domain after decorrelating the image in the spatial domain. The decorrelation processing results in a significant increase in the number of transform coefficients that can be used to embed the secret information into. Experimental results show that the proposed method can not only preserve good stego-image quality, but also have a good performance in resisting to chi-square analysis method, information quantity estimation method, RS analysis method and Jeremiah's histogram analysis method.

Categories and Subject Descriptors
K.6.m [**Management of Computing and Information Systems**]: Miscellaneous – *Security*. I.4.m [**Image Processing and Computer Vision**]: Miscellaneous

General Terms
Algorithms, Design, Performance, Security

Keywords
Information hiding, steganography, steganalysis, image decorrelation, Discrete Cosine Transform (DCT)

1. INTRODUCTION
Information hiding is a novel and rapidly evolutive technique that is different from the Encryption and the cryptography but is still in some connection with them. Taking the sense redundancy of human's sense organ and the redundancy of multimedia digital signal itself, information hiding technique embeds the information into the host signal, which can be undetectable and also do not weaken the visual imperceptibility of the host signal [1]. The two major branches of information hiding are steganography and watermark. The object of communication in watermark is the host signal, with the embedded correlative message providing copyright protection. And steganography aims to protect the secret message hided within a biggest one in such a way that others can not discern the presence or contents of the hidden message. The main purpose of watermark is the robustness of the method, the undetectability and the capacity. Steganography, as different from watermark, has the most important requirement of algorithmic undetectability, the capacity and robustness following.

Steganography also differs from the cryptography, which does not conceal the communication itself but only transforms the secret data by some algorithms into unknown signs or scrambled codes in order to prevent eavesdroppers understanding the content. But it will attract the attention of a possible attacker, and the communication may be attacked consequently. Steganography, on the other hand, improves the security of secret information and also the reliability of transmission [2] by embedding secret information into the common digital signal. In steganography the cover-media can be various digital media , considering the increasingly wide use of digital image in the internet and human life daily, the steganographic method taking the image as the cover-media has attracted much more attention than other digital forms. So far there are lots of steganographic techniques that based on the digital image. LSB (Least Significant Bit) steganography is a typical but also simple information hiding technique [3-5] which replaces the lowest bit of image to hide the secret information. There are many tools that using the LSB method to embed, such as Steganos, S-Tools and Hide4PGP [6]. And then some improved LSB algorithms have been brought forward in order to increase the hiding capacity and better stego-image quality, such as steganography based on the HVS (Human Visual System) [7] and the BPCS (Bit Plane Complexity Segmentation) [8]. But simple LSB embedding is vulnerable to some attacks [9-11] because of the change of image statistical feature. Then more new algorithms have been proposed to strengthen the system security. Lisa M. Marvel suggests that we should embed the information transformed to be Gauss noise into the uncompressed cover-image [12]. And another effective algorithm which makes a simple bit exchange on the DCT coefficient matrix to embed secret infomation is proposed by Faisal Alturki [13]. And he also has proved that the modification of cover-image is similar to be added the Gauss noise. Along with the development of steganographic technique, the steganalytic detection techniques have been improved correspondingly. Jeremiah J. Harmsen proposes a new steganalysis method with the

Infoscale2007, June 6-8, 2007, Suzhou, China.

assumption that the embedding process is adding noise to image which leads the same effect with using lowpass on the histogram of the image. So the energy of the stego-image's histogram is low than that of the cover-image's histogram. Basing on this point, he brings forward a classified method to distinguish the stego-image and cover-image.

In this paper, we propose a high embedding capacity steganographic method. With this method we embed the information in the DCT domain, and increase the capacity by decorrelating the cover-image. Experimental results show that in the proposed method the capacity can be $MN-64$ where M presents the length of cover-image and N presents the width respectively, and have a good performance in resisting to some steganalysis methods proposed in [9,11,14,15]. The rest of this paper is organized as follows. Firstly, we will summarize the theory of image decorrelation and the typical steganalysis method. Secondly we will describe the proposed method in detail. In section 4 the simulated results are given. Finally we conclude in section 5.

2. THE KEY IDEA

2.1 Image Decorrelation

It is well known that most natural images are consist of low frequency signals [16], i.e., most of the signal energy and significant components are contained in the low frequency coefficients. Image transforms, such as the DCT, concentrate the image energy into a relatively small number of coefficients called DC (Direct Current) coefficient. Therefore, if we try to embed the information directly into an image in the transform domain, there may not be enough coefficients to be embedded all of the desired information into. Furthermore, embedding the information directly into the transformed image will reduce the security of the system as the data embedding rate increases.

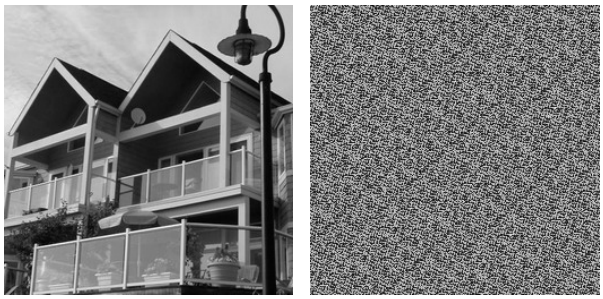
Image decorrelation or whiten is to scramble image using some method to decrease the correlation of inter-pixel, i.e., making the image look like white noise to the viewer. This process can be denoted as follows.

$$I'(n_1,n_2)=S(I(n_1,n_2),K)$$

Where I denotes the natural image. The $I(n_1,n_2)$ is the pixel value at point (n_1,n_2). The operator S represents some scramble method, i.e., whiten or decorrelation which be used to the image. Correspondingly, the variable K is the key of scramble operation and it can be public key or private key. The I' is the whitened image.

Whitening an image has a great impact on its power spectrum in the transform domain [17], because it spreads the original signal energy uniformly over all frequency bands. From a communication theory prospective, if we model the cover-image as a channel, then the process of whitening the cover-image results in an increase in the data transmission bandwidth, which results in an increase in the data embedding capacity. So, this process can increase the number of the mid and high frequency coefficients, i.e., AC (Alternating Current) coefficient that can be used to embed information in the DCT domain. For example, we choose the gray-scale image Lena and an image at random from the CBIR [18] database called Rand1 image to be the cover-image. In this experiment we scramble the cover-image by the Arnold transformation [19] to gain the whitened image and choose the iterative number 90 as the key K. The result as shown in Figure 1.

a) Cover-image Lena and whitened Lena



b) Cover-image Rand1 and whitened Rand1

Figure 1. Cover-image and whitened image

Then we divide the two images into blocks of no overlapping and size of 8×8, and we transform each block with DCT. Table 1 and table 2 include two rounded coefficient matrixes after DCT respectively. Comparing the two matrixes, we can see that the AC coefficient value is generally heightened while the DC coefficient value is reducing. So, we can conclude that the image energy distributes uniformly over all frequency bands and almost every coefficient can be used to be embedded secret information into, i.e., the hiding capacity of cover-image has been improved greatly.

Table 1. Comparing DCT vector of cover-image Lena with whitened Lena

a) DCT vector of cover-image Lena

1266	3	-1	3	3	-3	-2	3
8	6	-5	4	0	5	-7	7
6	-3	2	-3	5	0	-1	0
-2	-2	3	1	-4	-1	-1	2
-1	1	0	0	0	0	0	0
-2	1	-3	-2	2	1	0	0
-1	-2	2	2	1	-1	0	1
0	2	1	-3	-1	0	0	-1

b) DCT vector of whitened Lena

552	-2	50	23	35	17	67	-37
85	-65	41	-34	30	-17	92	-16
85	-11	94	73	97	25	98	-131
31	-32	16	45	9	-23	-43	-97
89	2	122	73	58	9	-16	-36

54	-30	-20	42	-9	24	55	-18
107	76	32	-40	31	12	65	4
87	42	-4	-20	-42	-17	107	27

Table 2. Comparing DCT vector of cover-image Rand1 with whitened Rand1

a) DCT vector of cover-image Rand1

1666	-16	2	0	-1	0	-1	1
19	4	-4	-3	-2	2	-1	0
6	-3	2	-1	0	0	-1	0
-10	3	3	-1	1	-1	0	-1
-7	8	-2	-2	4	-1	1	0
1	-2	-3	-2	2	-3	1	0
6	-5	-1	0	0	-1	0	1
5	-3	3	1	-1	1	0	1

b) DCT vector of whitened Rand1

999	14	-9	-93	150	-9	164	75
10	48	-96	-4	-77	83	-99	4
-68	97	15	50	-24	-20	-180	-111
75	-48	-40	50	-138	92	-40	-47
-69	22	129	-12	-37	25	-162	18
-59	6	-53	-177	7	-67	-67	9
-59	-8	55	-38	21	42	-44	-35
41	-31	-27	-35	-22	28	-63	-5

2.2 Analysis of Typical Steganography Algorithm

To improve the algorithm security, we need to analyze the feature of the existing typically steganographic method and steganalysis method at first. The LSB replacement method, as well as its improved methods such as BPCS, has an advantage of high capacity and the better visual imperceptibility etc. Because the spatial domain steganography will change the statistical feature of image histogram, so it is vulnerable to some attacks [9, 10] such as chi-square analysis attack [11], information quantity estimation method [15] and RS analysis attack [9] etc. In addition, it also can not keep high security that transforming secret information into Gaussian white noise. There are two reasons to explain it. First, the Gaussian white noise is different from the device noise added during the image transmission and capturing process. Second, the noise is independent with the image itself. A novel steganalysis method has been proposed by Jeremiah [14], which can effectively attack the additive noise modelable steganography. From the viewpoint of Jeremiah's steganalysis method, the additive noise introduced to image acts as a lowpass filter on the HCF (Histogram Characteristic Function). This filtering causes the histogram bins to "bleed" together. Futhermore, the Gaussian noise adding method is only the one of the additive noise modelable steganography, so it also can not resist to the Jeremiah's steganalysis.

From the analysis above, we can see that the statistical features in the bit-planes should not be changed much after embedding for a high performance steganographic method. In addition, we also cannot directly apply simple Gaussian noise adding method. But, we still think that the additive noise modelable steganography has a perfect performance on the condition that the noise just should be the content-dependent noise. To sum up the above analysis, we present a DCT-based steganagraphic method, which take advantages of the correlation of the DCT coefficients in the same position of the adjacent image blocks. To embed message, we quantize the difference between the coefficients instead of the coefficients themselves. Thus the distortion spreads to the adjacent image blocks. Because quantized noise is produced by both of the DCT coefficients of the adjacent blocks, the magnitude of the noise is different according to different image contents. It means that the quantized-noise is not independent of the image contents. So our method cannot be considered as additive noise steganography model in which the additive noise must be independent of the image. This can help our method resist Jeremiah's steganalysis. On the other hand, the quantized noise is scattered in different bit-planes after taking the inverse block DCT. Thus the randomicity of the bit-planes is kept the same as that in the natural images, which makes χ^2 analysis method, RS analysis attack and information quantity estimation method failed.

3. THE HIDING ALGORITHM

Let I be the gray-scale cover-image of size $M \times N$. Without loss of generality, $M = 8 \times k_1$, $N = 8 \times k_2$, k_1, $k_2 \in Z^+$. We first whiten image I and then divide it into blocks of no overlapping and size of 8×8. Then we apply 8×8 DCT transform to each blocks. Let B_m and B_{m+1} be the adjacent DCT block in every row or column, $m = 2k_3 + 1$, $k_3 \in \overline{Z^-}$, where $\overline{Z^-}$ denotes non-negative integer, $2k_3 + 1$ denotes odd number and $2k_3$ denotes even number respectively. Let RB_m and RB_{m+1} be the rounded DCT coefficients of the block B_m and B_{m+1} respectively, $RB_m(i, j)$ and $RB_{m+1}(i, j)$ be the value of adjacent blocks at point (i, j), $1 \le i, j \le 8$. The difference of the DCT coefficients of adjacent DCT blocks in the same position is calculated as follows.

$$d_m(i, j) = RB_{m+1}(i, j) - RB_m(i, j)$$

Let Q be the quantized coefficient and it represents the information embedding intensity, $RB'_m(i, j)$ and $RB'_{m+1}(i, j)$ denote the DCT coefficients of adjacent DCT blocks in the same position after embedding, similarly.

$$d'_m(i, j) = RB'_{m+1}(i, j) - RB'_m(i, j)$$

Let $\left\lfloor \frac{d_m(i, j)}{Q} \right\rfloor = s$, where $\lfloor \bullet \rfloor$ represents the floor function.

The specific process of embedding method as follows.

To embed a "1" and $s = 2k_3 + 1$ or embed a "0" and $s = 2k_3$, we get the new DCT coefficients $RB'_m(i, j)$ and $RB'_{m+1}(i, j)$ using these following formulas.

$$RB'_m(i, j) = RB_m(i, j) - \left(\frac{s \times Q - d_m(i, j)}{2}\right)$$

$$RB'_{m+1}(i, j) = RB_{m+1}(i, j) + \left(\frac{s \times Q - d_m(i, j)}{2}\right)$$

Similarly, to embed a "1" and $s = 2k_3$ or embed a "0" and $s = 2k_3 + 1$, we have.

$$RB'_m(i,j) = RB_m(i,j) - (\frac{(s+1)\times Q - d_m(i,j)}{2})$$

$$RB'_{m+1}(i,j) = RB_{m+1}(i,j) + (\frac{(s+1)\times Q - d_m(i,j)}{2})$$

In addition, we present the embedding capacity as follows.

$MN/4$, if k_1 and k_2 are even.

$(M-8)(N/4-2)$, if k_1 and k_2 are odd.

$M(N/4-2)$, if k_1 is even and k_2 is odd.

$N(M/4-2)$, if k_1 is odd and k_2 is even.

To increase the capacity, we can use the adjacent blocks repeatedly to be embedded into, i.e., we embed information after comparing the first block with the second block, and then we use the second block again to compare with the third block to embed. Then the capacity of image will be $MN-64$.

The extracting process is straightforward. Similar with the embedding process, the stego-image is partitioned into no overlapping blocks of size 8×8. Next, the block DCT is used, and each difference of the DCT coefficients in the same position of the adjacent blocks is calculated. Then each difference value is divided by Q. The process is following.

If $\mathrm{mod}(\left\lfloor \frac{d'_m(i,j)}{Q} \right\rfloor, 2) = 1$, then extracted "1";

If $\mathrm{mod}(\left\lfloor \frac{d'_m(i,j)}{Q} \right\rfloor, 2) = 0$, then extracted "0".

Where, the function mod $(\bullet)$ represents the mod operation.

4. EXPERIMENTAL RESULTS

4.1 The Visual Imperceptibility

In this section we present an example to illustrate the imperceptibility of proposed method. We choose the popular gray-scale image Lena of size 256×256, and an image at random from CBIR called Rand2 which is cropped to size of 256×256 as cover-image. Thinking about the choice of the quantized coefficient Q, if we choose a larger one, the image will be degraded greatly. Contrarily, choosing a smaller one leads the embedded information to be more vulnerable. And because of emerging the decimal in the process of DCT transform, some error will be produced during the rounding process. So, the Q should not be too small. Table 3 shows the PSNR (Peek Signal and Noise Ratio) of stego-image Lena and Rand2 with different Q.

Table 3. The PSNR with different Q

a) Lena image

Q	4	6	8	10	12
PSNR	45.0403	42.1728	39.9367	38.1423	36.6012

b) Rand2 image

Q	4	6	8	10	12
PSNR	45.6178	42.7652	40.5536	38.7521	37.2169

Furthermore, the HVS does not find any change of stego-image with PSNR is greater than 38*dB* [20]. So, in order to keep the better quality of stego-image and the stronger ability of anti-steganalysis, we select the value of Q is 6 in our experiment. Figure 2 shows the cover-image and the stego-image embedded with the payload 16.384*kbits*. The PSNR value between the stego-image with the cover-image is 42.1728*dB* and 42.7652*dB* respectively.

a) Lena image

b) Rand2 image

Figure 2. Comparing cover-image with stego-image

4.2 The Algorithm Security

The purpose of steganography is to protect the embedded secret information and then keeping a secure communication process. Taking a suspicious image, we can not detect whether it is embedded with secret information just by vision. Then we need the statistical character of image to judge. The secret communication process is failure if the very existence of hidden communication is doubted. So the demand on undetectability is much serious. In the following, we will analysis our algorithm's security with four steganalysis methods.

4.2.1 χ^2 (chi-square) Analysis Method [11]

LSB steganography, in which the lowest bit plane of an image is used to convey the secret information, has long been known to steganographers. The method either changes the pixel value or leaves them unchanged depending on the corresponding pixel value of the secret bit and the image's LSB. This process can be described as follows.

Embedding "0": $2j \to 2j$, $2j+1 \to 2j$

Embedding "1": $2j \to 2j+1$, $2j+1 \to 2j+1$

Where $2j$ denotes the pixel value of an image, $j \in \{0,1,2,\mathrm{L}\ 128\}$.

The secret information will be encrypted before embedding, and can be regarded as normally distributed bit stream. So the chance of value is 0 or 1 are even distribution. We define h_i is the quantity of pixels with the value equal to i, i.e., the histogram of image, $i \in \{0,1,2,\mathrm{L}\ 255\}$. If the LSB of image is replaced by the secret information entirely, then the value of h_{2i} and h_{2i+1} will be close. So, we can analyze the histogram feature to detect the secret message.

The experiment chooses standard Lena as cover-image and its partial histogram is shown by Figure 3. Figure 4 and Figure 5 are the partial histogram of stego-image using LSB method and proposed method respectively. The x-axes depicts the value of image pixels, and the y-axes depicts the number of pixels.

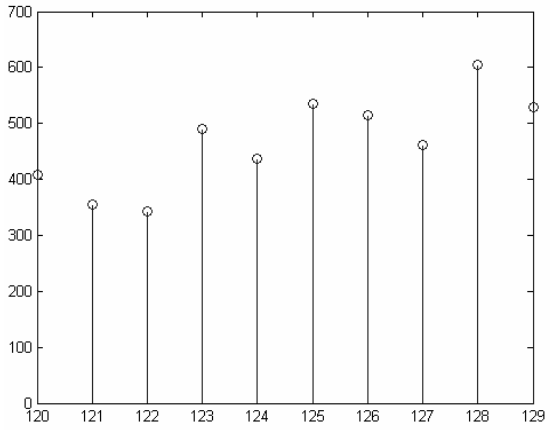


Figure 3. Partial histogram of cover-image

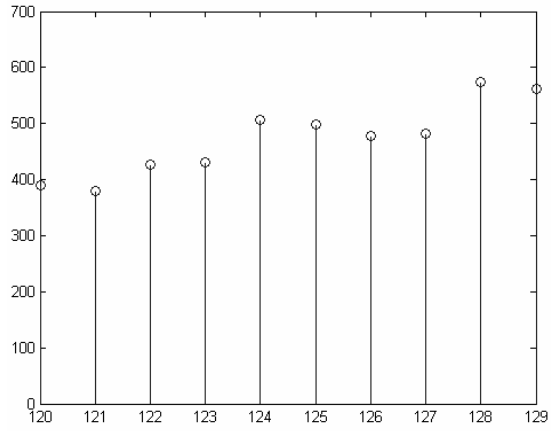


Figure 4. Partial histogram of stego-image using LSB method

As can be seen from the three graphs above, the difference between h_{2i} and h_{2i+1} such as h_{122} and h_{123} is obvious in cover-image but almost nonexistent in stego-image using LSB method. In figure 5, we can find that the difference between h_{122} and h_{123} is also clear after embedding secret information using the proposed method. So, the proposed method is security against the χ^2 analysis.

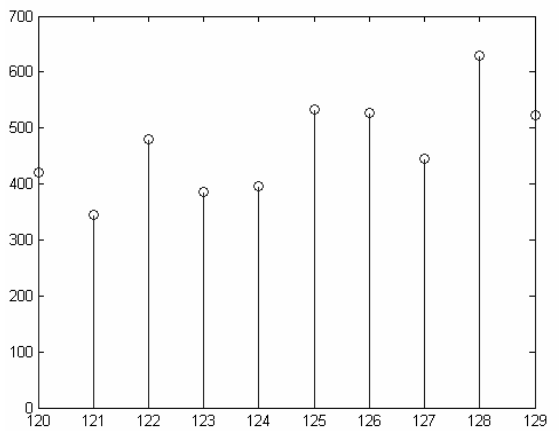


Figure 5. Partial histogram of stego-image using proposed method

If we don't embed information into all LSB of image but randomly choose bits to embed, furthermore the analyzer can not find the exact position where the secret embedded, then the χ^2 analysis can not work. Figure 6 shows the partial histogram of stego-image that is randomly embedded with the length of secret message is 50 percent of maximum hiding capacity according to the cover-image using LSB method.

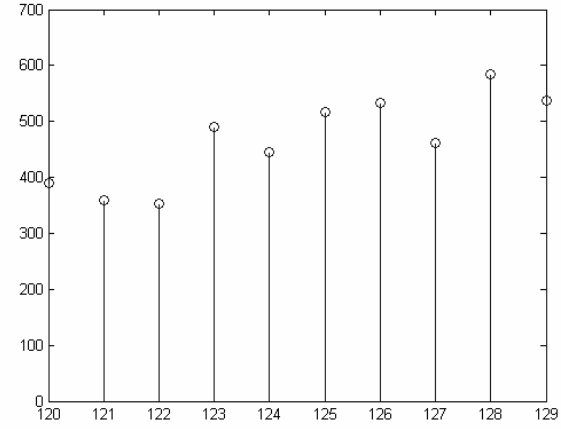


Figure 6. Partial histogram of stego-image using LSB method

As shown in Figure 6, the difference between h_{122} and h_{123} is also existing, we can not detect the existence of secret information. That also proves the limitation of χ^2 analysis method.

4.2.2 Information Quantity Estimation Method [15]

The information quantity estimation method is more effective than χ^2 analysis. It not only detects the steganography with less embedded quantity but also can estimate the length of embedded information. In this paper we only use it to detect secret message, and the capacity estimate is not mentioned. The specific detection process as follows.

Through the analysis with LSB steganography, we have

$$E(h_{2i+1} - h_{2i}) = (1-\alpha)(f_{2i+1} - f_{2i}) \quad (1)$$

$$E(h_{2i+2}-h_{2i+1})=(f_{2i+2}-f_{2i+1})+\frac{1}{2}\alpha(f_{2i+3}-f_{2i+2}+f_{2i+1}-f_{2i}) \qquad (2)$$

Where h_i and f_i are the histogram in cover-image and stego-image respectively, $i\in\{0,1,2,\mathrm{L}\ 255\}$. The $E(\bullet)$ represents the mathematic expectation and the α denotes the embedding intensity.

Comparing equation (1) with equation (2), we can seen that the h_{2i+1} and h_{2i} are equal to each other gradually with the augment of embedding intensity α . But at the same time, the h_{2i+2} and h_{2i+1} not always be equality in the process, even the difference between them may become larger with the augment of embedding intensity α .

So, hold an ambiguous image to detect, define

$$\begin{cases} F_1=\sum_i |h_{2i+1}-h_{2i}| \\ F_2=\sum_i |h_{2i+2}-h_{2i+1}| \end{cases}$$

We can conclude that if an image is unsteganographic, then the value of F_1 and F_2 should be very close. Contrarily, the value of F_1 must be reduced with augment of α while the value of F_2 does not always decrease, even if F_2 is reduced, the speed of decreasing is much less than that of F_1 . So, if the value F_2 is obviously bigger than F_1 , we can consider that the image is steganographic.

Figure 7 is the statistical feature of F_1 and F_2 using the LSB method.

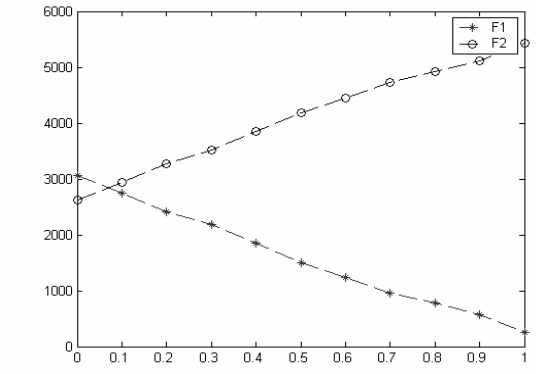


Figure 7. The statistical feature of F_1 and F_2 using LSB method

In the diagram, the x-axes depicts the embedding intensity α , and the y-axes depicts the sum of the adjacent pixel's difference absolute value. In figure 7, we can clearly find the different between F_1 and F_2 , i.e., this analysis method can easily detect the LSB steganography. Seen from figure 8, the curve of F_1 and F_2 is approximate linear distribution with the change of α and the value of them are very close. So, this perfectly illustrates that our

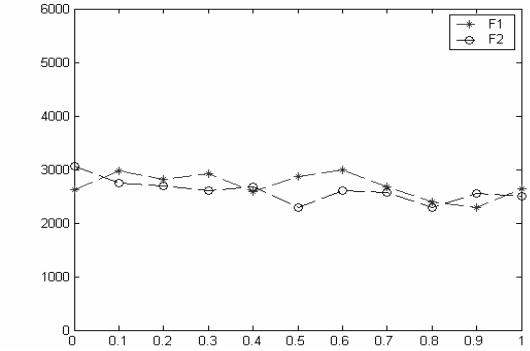


Figure 8. The statistical characteristic of F_1 and F_2 using our proposed method

method can resist to the information quantity estimation method.

4.2.3 RS (Regular-Singular) Analysis Method [9]

The χ^2 analysis method and the information quantity estimation method exploits the histogram feature of image to detect the existence of secret information, however, the RS steganalysis utilizes the spatial correlation of image to perform.

Given an image block (supposing is 8 gray-scale), we use Zigzag scan method to transform it into a one-dimensional vector. The spatial correlation (or discrimination function) of image block can be expressed as follows.

$$f(x_1,x_2,\mathrm{L}\ ,x_n)=\sum_{i=1}^{n-1}|x_i-x_{i+1}|$$

Where $x_1,x_2,\mathrm{L}\ ,x_n$ are pixel values in the image blocks.

We define F_1 , F_{-1} , F_0 are the invertible operations, where F_1 represents the shift between x_{2i} and x_{2i+1} , i.e., the permutation $F_1:0\leftrightarrow 1,2\leftrightarrow 3,\mathrm{L}\ ,254\leftrightarrow 255$, F_{-1} denotes the change between x_{2i-1} and x_{2i} , i.e., $F_{-1}:-1\leftrightarrow 0,1\leftrightarrow 2,\mathrm{L}\ ,254\leftrightarrow 255$, similarly, we also define F_0 as the unchanged function, $F_0:x_i\leftrightarrow x_i$.

We apply the invertible functions to image blocks.

$$F(G)=(F_{M(1)}(x_1),F_{M(2)}(x_2),\mathrm{L}\ ,F_{M(n)}(x_n))$$

Where $M(1),M(2),\mathrm{L}\ ,M(n)$ can be assigned with 1, 0 or -1, G represents the image block.

The purpose of the $F(G)$ is perturbing the pixel values in an invertible way by some small amount, thus simulating the act of invertible noise adding is necessary. This process is the same with LSB steganographiy. In typical images, adding a small amount of noise (for example, flipping by a small amount) will lead to an increase in the discrimination function f rather than a decrease. So

If $f(F(G))>f(G)$, then G is regular;

If $f(F(G))<f(G)$, then G is singular.

We denote the number of regular blocks and singular blocks using the invertible operation F_1 as R_M and S_M respectively. Similarly, we get R_{-M} and S_{-M} by exploiting the function F_{-1}.

Thus, if the image is unsteganographic, the total number of regular blocks will be larger than the total number of singular blocks, i.e., $R_M > S_M$ and $R_{-M} > S_{-M}$. Similarly, the expected value of R_M equals that of R_{-M}, and the same is true for S_M and S_{-M}.

Figure 9 is shown the curve of R_M, S_M, R_{-M}, S_{-M} with the different embedding intensity using our proposed method. As we can see from the diagram, the stego-image seemingly do not contain any secret information because the curve is same with that in the analysis above.

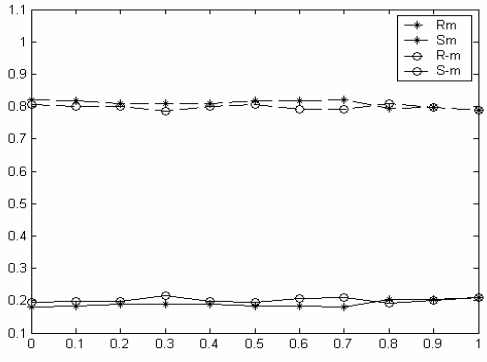


Figure.9 The statistical feature of R_M, S_M, R_{-M}, S_{-M} using our proposed method

According to RS steganalysis, if more and more LSB are replaced with secret data, then the variety in the percentages of R_M and R_{-M}, S_M and S_{-M} in the diagram can be expressed by a curve model like Figure 10.

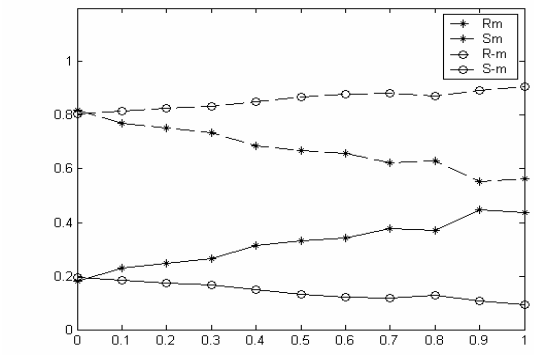


Figure.10 The statistical feature of R_M, S_M, R_{-M}, S_{-M} using LSB method

4.2.4 Jeremiah's Histogram Attack [14]

Jeremiah has proposed a steganalytic method. He based his attack on the hypothesis that the secret information can be seen as an additive model to image and it is independent with image. Thus, the histogram of stego-image is a convolution of the noise PMF (Probability Mass Function) and the histogram of cover-image. In the transform domain this convolution is viewed as a multiplication of the HCF[1] (Histogram Characteristic Function) and the NCF (Noise Characteristic Function). Let $h_s[n]$ be the stego-image histogram, $h_c[n]$ be the cover-image histogram and $f_\Delta[n]$ be the PMF, we have.

$$h_s[n] = h_c[n] * f_\Delta[n]$$

Where $f_\Delta[n] \cong p(x_s - x_c = n)$, x_s is the pixel value of the stego-image, and x_c is the pixel value of the cover-image. Generally speaking, $f_\Delta[n]$ is the probability that a pixel will be altered by n.

Because the DFT of noise has lowpass feature, so, the additive noise modelable steganography is equivalent to a lowpass filter processing on the cover-image histogram which is quantified by a decrease in the HCF COM (Center of Mass). As follows.

$$C(H_s[k]) \cong \frac{\sum k|H_s[k]|}{\sum |H_s[k]|}, k = (0,1,\mathrm{L}\ \frac{N}{2} - 1) \quad (3)$$

$$C(H_c[k]) \cong \frac{\sum k|H_c[k]|}{\sum |H_c[k]|}, k = (0,1,\mathrm{L}\ \frac{N}{2} - 1) \quad (4)$$

And we have $C(H_s[k]) \le C(H_c[k])$.

The equation (3) and the equation (4) is the COM of stego-image and cover-image respectively. The $H_s[k]$ is the DFT of stego-image, similarly, the $H_c[k]$ is the DFT of cover-image. The N is the DFT length.

According to the conclusion above, to test the security of proposed method, 48 images captured from the CBIR database are used and we change these images into 8 bit gray-scale images. Calculating the COM of every image, we exploit two methods to embed the secret information.

1) Embedding the additive noise to image's LSB, the experiment result is shown in Figure 11.

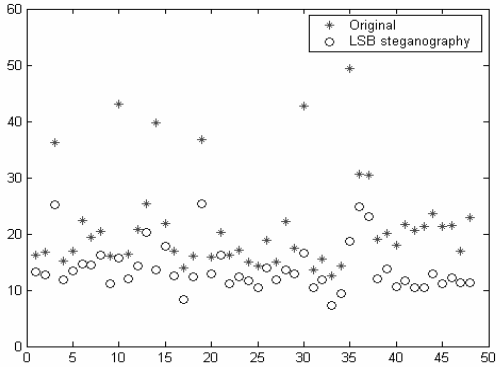


Figure.11 The COM distribution of stego-image using LSB method and cover-image

[1] The HCF is the DFT of image's histogram. Similarly, the NCF is the DFT of noise's histogram.

2) Using proposed method to embed, as shown in Figure 12.

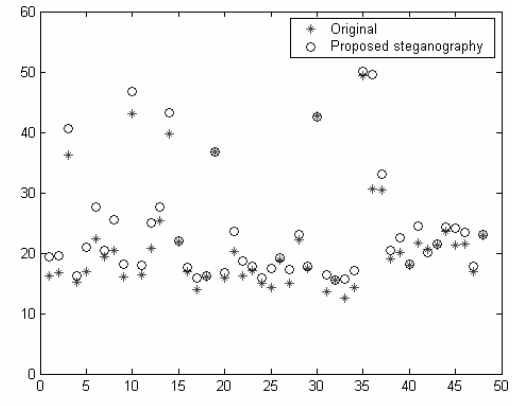


Figure.12 The COM distribution of stego-image using proposed method and cover-image

In Figure 11, we can see that Jeremiah's attack can effectively distinguish the LSB stego-images from cover-images because the circle sign is below the star one. But as is shown in Figure 12, Jeremiah's method could not distinguish between cover-images and stego-images using proposed method. Comparing Figure 11 and Figure 12, we can conclude that our steganographic method is secure to Jeremiah's steganalysis.

5. CONCLUSIONS

This paper proposes an effective image steganographic algorithm based on DCT and decorrelation. This method have a high data rate by whitening the cover-image which results in an increase in the transform coefficients that can be used for data embedding. Then we quantize the DCT coefficients in the same position of the adjacent image blocks to embed secret information. This process keeps a high correlation between cover-image and secret bit, which can enhance the proposed method's performance of anti-steganalysis. Lots of experimental results demonstrate that the proposed method not only can preserve good image quality, but also can resist some typical steganalysis algorithm. The method also can be used to color image.

6. ACKNOWLEDGMENTS

This work is supported by Natural Science Foundation of Chongqing # CSTC, 2005BB2208 and 2005BB2210.

7. REFERENCES

[1] Sen, B., Yu, Z. H., and Hua, L. W. et al. Steganography of Telecommunication Information. National Defense Industry Press, Beijing, 2005.

[2] Katzenbeisser, S., and Petitcolas, F. A. P. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Boston, 2000.

[3] Bender, W., Gruhl, D., and Morimoto, N. et al. Techniques for Data Hiding. IBM System Journal, 1996, 35(3,4): 313-336.

[4] Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G. Information Hiding-A Survey. In Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Information, 1999, 87(7): 1062-1078.

[5] Hartung, F., and Kutter, M. Multimedia Watermarking Techniques. In Proceedings of the IEEE: Special Issue on Identification and Protection of Multimedia Information, 1999, 87(7): 1079-1107.

[6] Steganographic software: http://www.jjtc.com /Steganography/toolmatrix.htm.

[7] Yeuan, K. L., and Ling, H. C. An Adaptive Image Steganographic Model Based on Minimum-Error Lsb Replacement. In Proceedings of The Ninth National Conference on Information Security, Taichung, Taiwan. May 14-15, 1999: 8-15.

[8] Kawaguchi, E., and Eason, R. O. Principle and Application of BPCS-Steganography. In Proceedings of SPIE: Multimedia Systems and Applications, 1998, 3528: 464-472.

[9] Fridrich, J., Du, R. and Goljan, M. Detecting LSB Steganography in Color and Grey-Scale Images. Magazine of IEEE Multimedia Special Issue on Security, October, 2001: 22-28.

[10] Fridrich, J., Du, R. and Long, M. Steganalysis of LSB Encoding in Color Image. In Proceeding of IEEE International Conference on Multimedia and Expo, Piscataway, 2000.

[11] Westfeld, A., and Pfitzmann, A. Attacks on Steganographic Systems. Lecture Notes in Computer Science, 1999, 1768: 61-76.

[12] Lisa, M. M., Charles, T. R., and Charles, G. B. Hidding Information in Images. International Conference on Image Processing, 1998, 2: 396-398.

[13] Faisal, A., and Russell, M. A Novel Approach for Increasing Security and Data Embedding Capacity in Images for Data Hiding Applications. International Conference on Information Technology: Coding and Computing, 2001: 228-233.

[14] Harmsen, J. J., and Pearlman, W. A. Steganalysis of Additive Noise Modelable Information Hiding. In Proceeding of SPIE: Electronic Imaging, Santa Clara, January, 2003: 21-24.

[15] Zhong, S. W., Peng, X. Z., and Wen, K. Z. Digital Steganography and Steganalysis. Tsinghua University Press, Beijing, 2005.

[16] Jain, A. Fundamentals of Digital Image Processing. Prentice Hall, Englewood Cliffs, NJ, 1989.

[17] Depovere, G., Kalker, T., and Linnartz, J. P. Improved watermark detection using filtering before correlation. In Proceeding of IEEE International Conference of Image Processing, October, 1998, 1: 430-434.

[18] CBIR Image Database, University of Washington. http://www.cs.washington.edu/research/imagedatabase/groundtruth/.

[19] Arnold, V. I., Avez, A. Ergodic Problems of Classical Mechanics. Mathematical Physics Monograph Series. W A Benjamin, Inc., New York, 1968.

[20] Petitcolas, F. A. P., and Anderson, R. J. Evaluation of Copyright Marking Systems. In Proceeding of IEEE Multimedia Systems. Italy, Florence, 1999: 574-579.