A Novel Image Steganography Using Chaotic Map and Visual Model

Peipei Liu[1] Zhongliang Zhu[1,2] Hongxia Wang[1] Tianyun Yan[1,3]

[1]School of Information Science & Technology, Southwest Jiaotong University, Chengdu 610031, China
[2]Key Lab, Southwest Institute of Electron & Telecom Techniques, Chengdu 610041, China
[3] Department of Computer, ChengDu University of Information Technology, Chengdu 610225, China

Abstract

A novel image steganography method using chaotic map and human visual model is presented in DCT domain. Firstly each 8×8 image block is performed Discrete Cosine Transform, then the location of image block that is embedded secret message is determined by the chaotic map. Finally the secret message is embedded adaptively in the usable middle frequency coefficient pairs judged by Just Noticeable Difference(JND). Simulation results show that the algorithm has a high capacity and a good invisibility, moreover it is robust for the common image processing like JPEG compression and cropping.

Keywords: Information hiding, Steganography, Chaotic map, Visual model.

1. Introduction

Information hiding is an old but interesting technology, which includes watermark and Steganography etc. Steganography is a form of covert communication in which a secret message is camouflaged within a carrier message[1]. The goal of steganography is to mask the very presence of communication, making the true message not discernible to the observer[2]. The payload and the imperceptibility are the two most important properties of a steganography system. Intrinsically, these two requirements conflict with each other. Since a high data payload introduces more artifacts into the cover image and, hence, increases the perceptibility of the hidden data. In addition, steganography must have security levels. Many image steganography methods for hiding data in still images have been proposed. To obtain higher payloads, image steganography methods based on LSB have been used[3]-[4]. Meanwhile, some studies[5]-[6] in watermark have considered the characteristics of the human visual system to obtain good imperceptibility.

In this paper, we proposed a novel large payload image steganography method in DCT domain using chaotic map and visual model. Simulation results show that the algorithm has a high capacity and a good invisibility, moreover that it is robust for the common image processing like JPEG compression and cropping.

2. Just Noticed Difference(JND)

One crucial principle in designing a steganography algorithm is to maintain the imperceptibility of the image. We would like to apply the character of human visual system to ensure the imperceptibility . In their work of image compression, Ahumada et al.[7]studied the frequency sensitivity portion of visual model, we refer to it as where a frequency threshold value is $t^f_{u,v}$ derived for each DCT basis function and in this case result in an 8×8 matrix of threshold values. Watson et al.[8] further refined this model by adding a luminance sensitivity and contrast masking component. The luminance-masked threshold $t^L_{u,v,b}$ is given by

$$t^L_{u,v,b} = t^f_{u,v}(X_{0,0,b} / \overline{X_{0,0}})^{\alpha} \quad (1)$$

where α is a constant with a suggested value of 0.649, $\overline{X_{0,0}}$ is the DC coefficient corresponding to the mean luminance display and $X_{0,0,b}$ is the DC coefficient of the DCT for block b. The contrast masking results in masking threshold $t^C_{u,v,b}$ is given by

$$t^C_{u,v,b} = Max\left[t^L_{u,v,b}, \left|X_{u,x.b}\right|^{w_{u,v}} (t^L_{u,v,b})^{1-w_{u,v}}\right] \quad (2)$$

where $w_{u,v} = 0.7$.

3. Proposed Image Steganography Algorithm

In the case of image steganography, the schemes fall into two broad categories: spatial-domain and transform-domain techniques. We embed the secret message into the DCT-domain. Firstly the carrier image I of size $M_1 \times N_1$ is decomposed into nojoint 8×8 blocks. Thus there are image blocks with $M_1/8$ rows and $N_1/8$ columns in I. Then DCT transform is performed independently for very block.

3.1. Chaos-based to determine image block location

All figures will be printed in black and white. You may use colour figures but it is your responsibility to check that they can be printed correctly in black and white. The colour version will be kept in the Atlantis Press on-line version of the proceedings (if this is agreed upon).

Chaotic map is used for our algorithm to increase the security. The most attractive feature of chaos in information hiding area is its extreme sensitivity to initial conditions and the outspreading of orbits over the entire space. These special characteristics make chaotic maps excellent candidates for information hiding[9].

Logistic map is one of the simplest chaotic maps, and described by

$$x_{k+1} = \mu x_k (1 - x_k) \tag{3}$$

where $0 \le \mu \le 4$. When $3.5699456 < \mu \le 4$, the map is in the chaotic state[10]. All the sequences generated by the logistic map are very sensitive to initial conditions, in the sense that two logistic sequences generated from different initial conditions are uncorrelated statistically. Moreover, all the orbits of the logistic map are dense in the range of the map [0, 1].

We can determine the location of image block embedded secret message into by the following method:

Step1. Regarding key K as the initial value of logistic chaotic map, substituting into the Logistic chaos mapping iteration (3), we can get 1-D real chaotic sequence $\{x_m \,|\, m = 1, 2, ..., M_1 \times N_1 / 64\}$ with the length of $M_1 \times N_1 / 64$;

Step2. According to ranking for $\{x_m\}$ from small to big it will be sequence $\{x_n \,|\, n = 1, 2, ..., M_1 \times N_1 / 64\}$, then extracting position subscript of x_n in $\{x_m\}$ in turn we can get the sequence $\{y_k \,|\, k = 1, 2, ..., M_1 \times N_1 / 64\}$;

Step3. With formula (4) we can get the sequence $\{i_k\}$ an $\{j_k\}$ with the length of $M_1 \times N_1 / 64$;

$$\begin{cases} i_k = \lfloor (y_k - 1) / (N_1 / 8) \rfloor + 1 \ ; \\ j_k = y_k \bmod (N_1 / 8) + 1 \ ; \end{cases} \tag{4}$$

Step4. Choosing map blocks by regarding (i_k, j_k) as coordinates.

The location of image blocks embedded secret message into is identified by Chaos mapping, as well chaotic sequence is with the ergodicity, so we can achieve the random distribution for the secret message and enhance robustness of algorithm for cropping operation. Meanwhile chaotic sequence is of the utmost sensitivity for the initial value, and is very precise on the key requirements while extracting secret message, thus it can ensure the secrecy of information security effectively.

3.2. The secret message embedding

Since messages inserted into the high frequencies are vulnerable to attack whereas the low frequency components are perceptually significant and alteration to the low frequency components may become visible, so secret information is embedded by adjusting the relative size of the intermediate frequency DCT coefficient in this paper.

(u,v)	0	1	2	3	4	5	6	7
0	16	11	10	16	24	40	51	61
1	12	12	14	19	26	58	60	55
2	14	13	16	24	40	57	69	56
3	14	17	22	29	51	87	80	62
4	18	22	37	56	68	109	103	77
5	24	35	55	64	81	104	113	92
6	49	64	78	87	103	121	120	101
7	72	92	95	98	112	100	103	99

Table 1: Middle Frequency Coefficients Range of DCT Domain.

The intermediate frequency coefficient's range is shown in Table1. In order to resist JPEG compression, we choose the intermediate frequency coefficient pairs whose quantization step is same as JPEG compression.

No.	(u_1, v_1)	(u_2, v_2)	Step size
1	(1,2)	(3,0)	14
2	(0,3)	(2,2)	16
3	(3,2)	(4,1)	22
4	(5,0)	(2,3)	24
5	(0,5)	(2,4)	40

Table 2: Coefficient Pairs with Equivalent Quantization Step Size.

Use of (u_1, v_1) and (u_2, v_2) as DCT coefficient's position index, the coefficient pairs of choice is shown in Table2 There are five pairs of coefficient pairs whose quantization step is the same. We use these coefficient pairs to embed the secret information.

The process of secret message insertion is as follows:

Step1. Converting 2-D secret message S to a 1-D bits stream $M = \{m_k \,|\, m_k \in \{0,1\}, k \in \{1, M_2 \times N_2\}\}$;

Step2. We can calculate JND for each DCT coefficient in the image block B_i selected by formula (1) and (2) ; we refer to group j coefficient pair in the image block B_i as $B_{ij}(u_1, v_1)$ and $B_{ij}(u_2, v_2)$; JND values

of them are defined with $J_{ij}(u_1, v_1)$ and with $J_{ij}(u_2, v_2)$ respectively;

Define $\min J_{ij} = \min\{J_{ij}(u_1, v_1), J_{ij}(u_2, v_2)\}$;

Judging method is as follows:

if $\left| B_{ij}(u_1, v_1) - B_{ij}(u_2, v_2) \right| \le \min J_{ij}$, then Coefficient pairs are available. Otherwise it is unavailable and it can not be used for embedding. This process is called as Determination of Coefficient Pair Based on JND (DCPBJ). DCPBJ disposal abandoned the coefficient pair that will seriously damage the perceived quality when embedding secret message and it can ensure that secret message is not perceptible.

Step3. We make use of relative size of DCT coefficient to code secret message; and define secret message bit as m_k, the method is as follows:

When $m_k = 0$ and $B_{ij}(u_1, v_1) > B_{ij}(u_2, v_2)$;

$$stemp = B_{ij}(u_1, v_1); B_{ij}(u_1, v_1) = B_{ij}(u_2, v_2); B_{ij}(u_2, v_2) = stemp;$$

When $m_k = 0$ and $B_{ij}(u_1, v_1) < B_{ij}(u_2, v_2)$;

$$B_{ij}(u_1, v_1) = B_{ij}(u_1, v_1); B_{ij}(u_2, v_2) = B_{ij}(u_2, v_2);$$

When $m_k = 1$ and $B_{ij}(u_1, v_1) > B_{ij}(u_2, v_2)$;

$$B_{ij}(u_1, v_1) = B_{ij}(u_1, v_1); B_{ij}(u_2, v_2) = B_{ij}(u_2, v_2);$$

When $m_k = 1$ and $B_{ij}(u_1, v_1) < B_{ij}(u_2, v_2)$;

$$stemp = B_{ij}(u_1, v_1); B_{ij}(u_1, v_1) = B_{ij}(u_2, v_2); B_{ij}(u_2, v_2) = stemp;$$

Step4. To ensure the correct extraction of secret message, this scheme uses $\min J_{ij}$ to adjust the relative size of two DCT coefficients as

$$\left| B_{ij}(u_1, v_1) - B_{ij}(u_2, v_2) \right| > \beta \cdot \min J_{ij};$$

where β is proportion factor. The adjusting method is as follows:

$$B_{ij}(u_1, v_1) = B_{ij}(u_1, v_1) - (\beta \cdot \min J_{ij} - D_{ij});$$

$$B_{ij}(u_2, v_2) = B_{ij}(u_2, v_2) + (\beta \cdot \min J_{ij} - D_{ij});$$

where $D_{ij} = \left| B_{ij}(u_1, v_1) - B_{ij}(u_2, v_2) \right|$.

Step5. Embed secret message in turn in this way then inverse DCT transform, and the image I' carrying secret message is obtained.

3.3. Extraction of the secret message

The steps of secret message extraction are as follows:

(1) We have a DCT transform by block for the original image and image embedded secret message into, and calculate the JND value of each DCT coefficient for image I;

(2) It generates chaotic sequence by key K as a chaotic sequence initial value, and identifies image block embedded the secret message into according to chaotic map;

(3) We can judge if DCT coefficient pairs are available by JND value, and if so, thus secret message bit is extracted from intermediate frequency coefficient pairs of corresponding image block in I'.
the method is as follows:

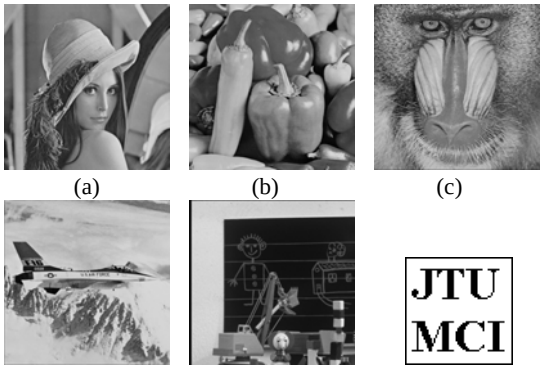
$$m'_k = \begin{cases} 0 & B'_{ij}(u_1, v_1) > B'_{ij}(u_2, v_2) \\ 1 & B'_{ij}(u_1, v_1) < B'_{ij}(u_2, v_2) \end{cases} \quad (5)$$

where m'_k is bit of the extracted secret massage. $B'_{ij}(u_1, v_1)$ and $B'_{ij}(u_2, v_2)$ are available coefficient pairs of DCT domain in I'.

(4) We can get the secret image information by transforming the one-dimensional secret message Sequence into the two-dimensional image information Sequence.

4. Simulation Results

In order to demonstrate the validity of algorithm, we introduce the experimental results. We ues the standard gray level images of size 512×512 such as 'Lena', 'Peppers', 'Baboon', 'Airplane', Toys' as carrier image. The secret message is 64×64 binary text. Thus there are totally 4096 secret message bits. In our experiments, we set $\mu = 4$ as the logistic map parameter and proportion factor β =0.85.



(a) (b) (c) (e) (f) (g)

Fig.1: The carrier images and secret message. (a) Embedding 'Lena'. (b) Embedding 'Peppers'. (c) Embedding 'Baboon'. (d) Embedding 'Airplane'. (a) Embedding 'Toys'. (a-f) with PSNR values 46.272 dB, 46.315 dB, 45.096 dB, 44.619 dB, 47.402 dB. (g) Original secret massage.

The performance of secret information extracted is evaluated by the normalized cross-correlation (*NC*) as follows[9]

$$NC = \frac{\sum_i \sum_j I(i, j) I'(i, j)}{\sum_i \sum_j [I(i, j)]^2} \quad (6)$$

Fig. 1(a)-(e) shows the carrier images embedding scret massage into, and Fig. 1(g) shows the original secret message. The images embedded secret massage into have good perceptual quality. The peak signal-to-noise ratio (PSNR) of the embedded images is high.

image	Lena	Peppers	Baboon	Airplane	Toys
DCPBJ	46.272	46.315	45.096	44.619	47.402
No CPBJ	41.602	42.657	35.443	39.314	39.311

Table 3: PSNR under DCPBJ Circumstance and Normal Circumstance (dB).

Table3 shows the PSNR values of images embedded secret massage into under DCPBJ and direct embedding secret information. From the table we can see that the algorithm using DCPBJ treatment has improved the perceptual quality of image carrying the secret message. For different images, PSNR is 44-48dB, about 4-10dB higher than those without DCPBJ process. The algorithm has more advantages for subjective observation. If they do not adopt DCPBJ, while 'Airplane' and 'Toys' images are amplified, we can see the visible artifacts in a relatively smooth and high bright Region, but the algorithm in this paper has not such a problem.

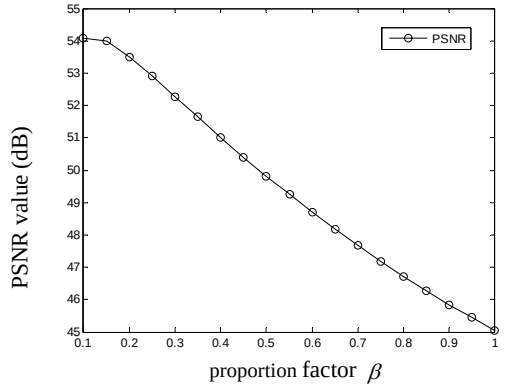


Fig.2: The PSNR value of embedded 'Lena' with different β

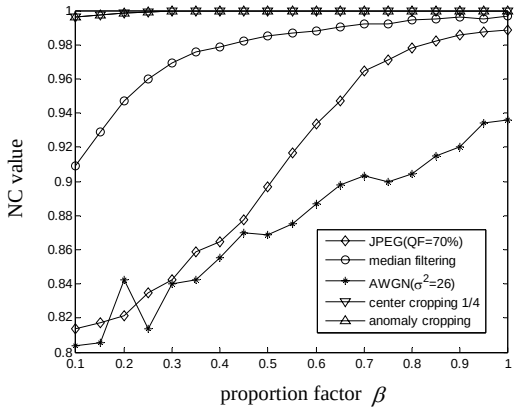


Fig.3: The *NC* value of extracted message with different β

Fig. 2 shows the relation between the PSNR value of embedding 'Lena' and proportion factor β. We can find that PSNR decreases linearly with the increase of the β. The relationship between β and PSNR is linear, and the reason is that secret information is adaptively embedded according to image content.

There is the *NC* value of 'Lena' embedded the secret message into while β value changes as shown in Fig.3. We can see that with the increase of the β, *NC* increases as well, and the robustness of information hiding systems is improved. Thus, by adjusting the value, we can get an expected compromise between the imperceptibility and robustness.

(a) (b) (c) (d) (e)

Fig.4: The secret messages extracted with *NC* values equal to 0.982, 0.994, 0.999, 0.996, 0.914. (a) Secret message extracted after JPEG compression (QF=70%) (b) Secret message extracted after median filtering. (c) Secret message extracted after centre cropping (Area=25%). (d) Secret message extracted after anomaly Cropping. (e) Secret message extracted after AWGN(σ^2 =26).

Fig.4 (a)-(e) show the extracted secret messages while JPEG compression, median filtering, cropping and AWGN for the images embedded secret massage into. Obviously, the extracted secret messages are all still recognizable.

QF	PSNR(dB)	*NC*
Q=85%	40.177	1
Q=80%	39.318	0.996
Q=75%	38.589	0.989
Q=70%	38.117	0.982
Q=65%	37.754	0.965
Q=60%	37.514	0.927

Table 4: Robustness of Resisting JPEG Compression.

Table 4 shows the correlation results after JPEG compression. Each column refers to a different quality factor *Q* where lower *Q* values correspond to greater compression. The image quality suffers significantly for *Q* values lower than 60, resulting in very visible blocking artifacts.

There are 5 groups of DCT coefficients pairs in each image block to hide information. And each of the coefficient pairs hides a bit; in other words, the most hiding capacity of each image block is five bits. Considering abandoning the available coefficient pairs, the hiding capacity of algorithm can be determined by formula (7).

$$L = \sum_{j=1}^{5} (N - E_j) = 5 \cdot N - \sum_{j=1}^{5} E_j \qquad (7)$$

Where N is the number of image blocks in carrier image, j is the ordinal number of 5 coefficient pairs in each image block. E_j is the number of the abandoned DCT coefficients pairs in the whole image and E_j is determined by the specific content of image. The results show that the Hiding capacity varies significantly depending on the particular image characteristics.

image	Lena	Peppers	Baboon	Airplane	Toys
E1	1389	1496	3012	1523	1620
E2	1263	1104	2555	1073	1193
E3	559	637	2198	698	548
E4	520	517	2070	719	792
E5	335	223	1247	402	640
L	16414	16503	9398	16065	15687
Ref[6]	2048	2048	2048	2048	2048

Table5: Payload Comparison of Different Carrier image (bit).

The hiding capacity of test images is shown in table5. For most images, the hidden capacity is about 16×10^3 bits. Only image Baboon whose texture is complex would abandon more coefficients to ensure visibility, thus hidden capacity is relatively small, but more than $1{,}024 \times 8$bit too. This shows that the hiding capacity of this algorithm is much greater than the one in reference [6]. In addition, the experimental data show that about one quarter of intermediate-frequency pairs close to the low-frequency part is not available; this validates the algorithm's validity of using DCPBJ to improve visual quality from the side face.

5. Conclusions

This paper presents a large capacity of steganography algorithm, and it can embed the secret information adaptively into the still image based on chaotic mapping and human visual characteristics. When the secret message is embedded, we can locate the image block embedded secret massage into according to chaotic sequence and guarantee the security of secret information embedded. Robust algorithms have a very good imperceptibility at the same time, which is attributed to the application of the human visual model. Simulation results show that the algorithm has a high capacity, a good invisibility, and that it is robust for the common image processing like JPEG compression and cropping etc.

Acknowledgement

This work is supported by Sichuan Youth Science & Technology Foundation of China (Grant No. 07ZQ026-004) and Southwest Jiaotong University Development Foundation (Grant No. 2006A04).

References

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, Information hiding—a survey,. *Proc. Of IEEE*, 87(7):1062-1078, 1999.

[2] K. Satish, T. Jayakar, C.Tobin, K. Madhavi and K. Murali. Chaos based spread spectrum image steganography, *IEEE Transactions on Consumer Electronics*, 50:587-590, 2004.

[3] C. K. Chan and L. M. Cheng, Hiding capacity image steganographic model, *Pattern Recognition*, 37:469-474, 2004.

[4] R. Z. Wang and Y. S. Chen, High-payload image steganography using two-way block matching,*IEEE signal processing letters*, 13(3):2045-2047, March 2006.

[5] C. I. Podilchuk, W. J. Zeng, Image-Adaptive Watermarking in the DCT Domain, *International Conference on Acoustics, Speech, and Signal Processing (ICASSP)*, 16:525-539, 1998.

[6] H. F. Ling, Z. D. Lu, F. H. Zou, and R. X. Li, An energy modulation watermarking algorithm based on Watson perceptual model, *Journal of Software*, 17(5):1126-1132, 2006.

[7] H. A. Peterson, A. J. Ahumada, Jr., and A. B. Watson, Improved detection model for DCT coefficient quantization, *Proc. Of SPIE Conference on Human Vision,Visual Processing and Digital Display*, London, 1913:191-201, 1993.

[8] A. B. Watson, DCT quantization matrices visually optimized for individual image, *Proc. Of SPIE Conference on Human Vision,Visual Processing and Digital Display*,London, 1913:202-216, 1993.

[9] H. X. Wang, H. He and K. Ding, Public watermarking based on chaotic map, *IEICE Trans. On Fundamentals*, E87-A(8):2045-2047, May 2004.

[10] D. Zhao, G. Chen and W. A. Liu, A chaos-based robust wavelet-domain watermarking algorithm, *Chaos, Solitons Fractals*, 22(10):47-54, 2004.