International Journal of Intelligence Science, **2013, 3, 77-85**
http://dx.doi.org/10.4236/ijis.2013.32009 Published Online April 2013 (http://www.scirp.org/journal/ijis)

Research on Embedding Capacity and Efficiency of Information Hiding Based on Digital Images

Yanping Zhang[1,2], Juan Jiang[1,2], Yongliang Zha[1,2], Heng Zhang[1,2], Shu Zhao[1,2*]
[1]School of Computer Science and Technology, Anhui University, Hefei, China
[2]Key Laboratory of Intelligent Computing and Signal Processing of Ministry of Education, Anhui University, Hefei, China
Email: *zhaoshuzs2002@hotmail.com

Received December 30, 2012; revised January 31, 2013; accepted February 25, 2013

ABSTRACT

Generally speaking, being an efficient information hiding scheme, what we want to achieve is high embedding capacity of the cover image and high visual quality of the stego image, high visual quality is also called embedding efficiency. This paper mainly studies on the information hiding technology based on gray-scale digital images and especially considers the improvement of embedding capacity and embedding efficiency. For the purpose of that, two algorithms for information hiding were proposed, one is called high capacity of information hiding algorithm (HCIH for short), which achieves high embedding rate, and the other is called high quality of information hiding algorithm (HQIH for short), which realizes high embedding efficiency. The simulation experiments show that our proposed algorithms achieve better performance.

Keywords: Information Hiding; Embedding Capacity; Embedding Efficiency; Security; Peak-Signal-to-Noise-Rate (PSNR)

1. Introduction

The protection of digital data, especially for confidential data, becomes more and more important. As a kind of data security technique, digital steganography has been developed rapidly and attracts a great deal of attention from both the industrial and academic communities [1-15].

Digital steganography based on images is a way of hiding the existence of secret message under the cover of a carrier signal in such a way that no one apart from the sender and intended recipient even realizes there is a hidden message. An original image, used to carry secret message as a carrier signal, is called the cover image. And an image which has carried secret message is called the stego image. By virtue of generating stego images that are perceptually identical to the cover images with small embedding distortion, the secret messages are embedded into cover images.

The desires of good steganographic schemes are high embedding efficiency and security as well as large embedding payload. A steganographic scheme with low image distortion is more secure than that with high distortion because it does not raise any suspicion of adversaries. A steganographic scheme with high payload is expected because more secret messages can be transmitted. A steganographic scheme with high security can be powerful to resist the attacks by the steganalysis. However, the three factors are irreconcilable conflict. Therefore, we often make a compromise among them depending on different application requirements. A commonly used method, called the LSB (*i.e.* least significant bits) replacement method, is a simple hiding method by modifying the LSB of cover pixels to embed secret data [3-6]. However, it is easy to be detected. To improve the embedding efficiency, the (7,4) Hamming Code method is introduced into the steganographic schemes [1,11,13-15]. The WPC (*i.e.* wet paper codes) schemes [7,13,14], not only achieving high embedding efficiency but also providing a non-shared selection channel, are also proposed. On the contrary, some other hiding methods are utilized to the steganographic schemes so as to achieve large embedding payload [2,10-12,15-18]. Specifically, the embedding payload of the scheme proposed in [11] is close to 1 bpp. And a hiding scheme called "Hamming + 1" was proposed by Zhang *et al*. [9], for the purpose of improving the embedding capacity.

For the current information hiding schemes, the improvement of the embedding capacity and the embedding efficiency is still the goal that we pursuit and the starting

[*]Corresponding author.

point that we consider as to improve the algorithms. Considering the advantages and disadvantages of the previous methods, the paper proposed two algorithms for information hiding, one is high capacity of information hiding algorithm (HCIH algorithm), and the other is high quality of information hiding algorithm (HQIH algorithm).

On the one hand, considering the performance standard of embedding capacity, we present a high capacity of information hiding algorithm (HCIH algorithm), based on the (7,4) Hamming Code and the LSB replacement method, and inspiring from the "Hamming + 1" method. The HCIH algorithm can be used to embed an email address as the secret message into an 8-bit gray-scale image, and achieves to embed twelve secret bits of the binary string of the secret message, which is converted from an email address, into a block of cover pixels of a cover image sized each time. Then we evaluate the validity of HCIH algorithm through experimental simulation. The experimental results show that our proposed HCIH algorithm achieves high embedding capacity (*i.e.* 0.75 bpp) and acceptable visual quality of the stego image, and can be used for the applications about large payload secret message transmission.

On the other hand, considering the performance standard of embedding efficiency, we present a high quality of information hiding algorithm (HQIH algorithm), by introducing wet paper codes technology, for the purpose of improving the embedding efficiency. Considering that the embedding capacity may be lower because of introducing wet paper codes technology, when the embedding operation fails first time, the HQIH algorithm may try the second embedding operation to embed again by (7,4) Hamming Code oriented wet paper codes, to assure the embedding capacity. Meanwhile, the double operation also achieves higher security. Then, we evaluate the validity of HCIH algorithm through experimental simulation. The simulation experiments show that the HQIH algorithm achieves high embedding efficiency, that is the value of PSNR [19,20] is more than 52 dB, and large embedding payload, that is the value of ER is between 0.5499 bpp and 0.8291 bpp, which can be used for different applications. Specially, our HQIH algorithm gives some degree of security by considering twofold safeguards.

In short, considering the improvement of the embedding capacity and the embedding efficiency, this paper mainly studies on the information hiding technology based on gray-scale digital images and proposes two algorithms with detailed procedures and effective simulation experiments.

2. HCIH Algorithm

On this part, considering the performance standard of embedding capacity, we present a high capacity of information hiding algorithm (HCIH algorithm), based on the (7,4) Hamming Code and the LSB replacement method, and inspiring from the "Hamming + 1" method. The HCIH algorithm can be used to embed an email address as the secret message into an 8-bit gray-scale image, and achieves to embed twelve secret bits of the binary string of the secret message, which is converted from an email address, into a block of 4 × 4 cover pixels of a cover image sized 512 × 512 each time. The date embedding phase and data extracting phase are described in the following sections 2.1 and 2.2 respectively.

2.1. The Data Embedding Phase

Step 1: Give a cover image *I* sized 512 × 512 pixels as the carrier and an email address as the secret message needed to be embedded.

Step 2: Convert the email address into binary string *S* of *l* bits by the ASCII code, denoted as $S = \{s_i | 1 \le i \le l\}$, where $s_i \in \{0,1\}$. And then divide it into non-overlapping partitions of twelve secret bits, denoted as $s_i = (s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7, s_8, s_9, s_{0A}, s_{0B})$, where $i \in \{1, 2, \cdots, Ns\}$ and *Ns* is the total number of the partitions.

Step 3: Segment the cover image *I* into 128 × 128 blocks of 4 × 4 cover pixels, denoted as

$$P_k = (p_0, p_1, p_2, p_3, p_4, p_5, p_6, p_7, p_8, p_9, p_{0A}, p_{0B}, p_{0C}, p_{0D}, p_{0E}, p_{0F}),$$

where

$$1 \le k \le 128 \times 128, p_i \in \{0,1,\cdots,255\}, i \in \{0,1,\cdots,0E,0F\}_H$$

Step 4: Embed the first three bits (s_0, s_1, s_2) of s_i into the first seven cover pixels $(p_0, p_1, p_2, p_3, p_4, p_5, p_6)$ of block P_i by the (7,4) Hamming code and the LSB replacement method. And generate the first seven stego pixels $(q_0, q_1, q_2, q_3, q_4, q_5, q_6)$ of the stego block Q^i.

Step 5: Embed the secret bits sh into the cover pixel p_{h+4}, where $h \in \{3,4,5,6,7,8,9,0A,0B\}_H$ by taking the operation in (1).

$$S_h = (e_0 + e_1 + e_2 + e_3 + e_4 + e_5 + e_6 + e_{h+4}) \bmod 2 \quad (1)$$

where e_j is the 2^{nd}-rightmost LSB of p_j, where $j = (0,1,\cdots,6)_H$ and e_{h+4} is the *1st*-rightmost LSB of p_{h+4}, where $h = (3,4,5,\cdots,0B)_H$. If (1) holds, embed S_h with p_{h+4} unchanged; If (1) does not hold, modify the value of p_{h+4} by taking the opposite of the 1st-rightmost LSB e_{h+4}, to make (1) hold. At last, we embed sh and obtain the stego pixel q_{h+4} of the stego block Q^i.

Step 6: Repeat Step 4 to Step 5 until all the secret bits are embedded and generate the stego image I'.

Figure 1 shows the block diagrams of the proposed data embedding phase.

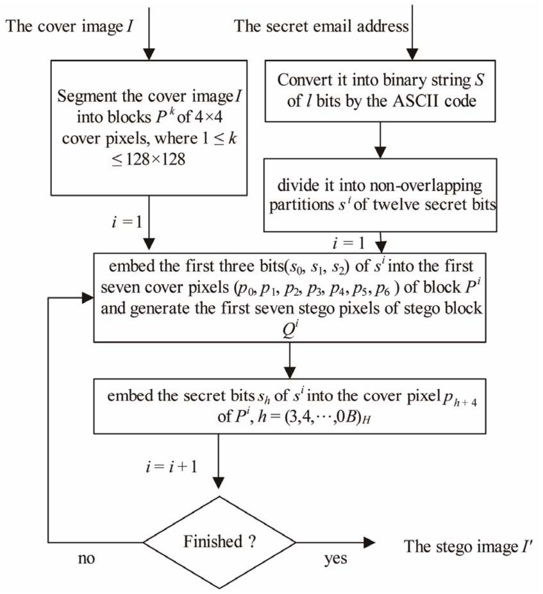

The cover image I
The secret email address
Segment the cover image I into blocks P^k of 4×4 cover pixels, where $1 \le k \le 128\times128$
Convert it into binary string S of l bits by the ASCII code
divide it into non-overlapping partitions s^i of twelve secret bits
$i=1$
$i=1$
embed the first three bits(s_0, s_1, s_2) of s^i into the first seven cover pixels ($p_0, p_1, p_2, p_3, p_4, p_5, p_6$) of block P^i and generate the first seven stego pixels of stego block Q^i
embed the secret bits s_h of s^i into the cover pixel p_{h+4} of P^i, $h=(3,4,\cdots,0B)_H$
$i=i+1$
Finished ?
no
yes
The stego image I'

Figure 1. The block diagrams about the data embedding phase of HCIH algorithm.

2.2. The Data Extracting Phase

The receiver can extract the secret message S from the received stego image I'. The detailed steps are as follows:

Step 1: Segment the stego image I' into 128 × 128 blocks of 4 × 4 stego pixels, denoted as

$$Q^k = \left(q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7, q_8, q_9, q_{0A}, q_{0B}, q_{0C}, q_{0D}, q_{0E}, q_{0F}\right),$$

where

$1 \le k \le 128\times128, q_i \in \{0,1,\cdots,255\}, i \in \{0,1,\cdots,0E,0F\}_H$.

Step 2: Extract the first three bits $\left(s_0, s_i, s_2\right)$ of s^i from the first seven stego pixels $\left(q_0, q_1, q_2, q_3, q_4, q_5, q_6\right)$ of block Q^i by (7,4) Hamming code and the LSB replacement method.

Step 3: Extract s_h from the stego pixel q_{h+4} by taking the operation in (2).

$$S_h = \left(f_0 + f_1 + f_2 + f_3 + f_4 + f_5 + f_6 + f_{h+4}\right) \bmod 2 \quad (2)$$

f_j is the 2^{nd}-rightmost LSB of $q_j, j = (0,1,\cdots,6)_H$ and f_{h+4} is the 1^{st}-rightmost LSB of q_{h+4}, $h = (3,4,5,\cdots,0B)_H$.

Step 4: Repeat Steps 2 and 3 until all the secret bits of the secret binary string are extracted.

Step 5: Convert the secret binary string into its original email address by the ASCII code.

Figure 2 shows the block diagrams of the proposed data extracting phase.

3. HQIH Algorithm

On this part, considering the performance standard of embedding efficiency, we present a high quality of information hiding algorithm (HQIH algorithm), by introducing wet paper codes technology, for the purpose of improving the embedding efficiency. Considering that the embedding capacity may be lower because of introducing wet paper codes technology, when the embedding operation fails first time, the HQIH algorithm may try the second embedding operation to embed again by (7,4) Hamming Code oriented wet paper codes, to assure the embedding capacity. Meanwhile, the double operation also achieves higher security.

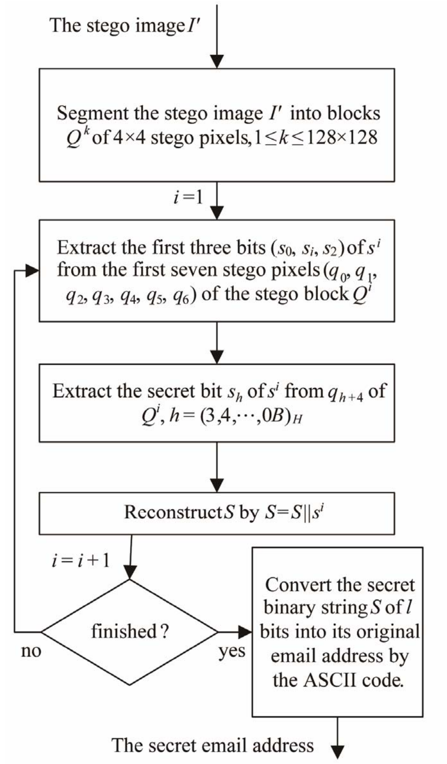

The stego image I'
Segment the stego image I' into blocks Q^k of 4×4 stego pixels, $1 \le k \le 128\times128$
$i=1$
Extract the first three bits (s_0, s_i, s_2) of s^i from the first seven stego pixels (q_0, q_1, q_2, q_3, q_4, q_5, q_6) of the stego block Q^i
Extract the secret bit s_h of s^i from q_{h+4} of Q^i, $h=(3,4,\cdots,0B)_H$
Reconstruct S by $S=S\|s^i$
$i=i+1$
finished ?
no
yes
Convert the secret binary string S of l bits into its original email address by the ASCII code.
The secret email address

Figure 2. The block diagrams about the data extracting phase of HCIH algorithm.

The main idea of the HQIH algorithm is as follows: Firstly, give an 8-bit gray-scale image as the cover image and the binary secret message need to be embedded. Secondly, segment the given cover image into non-overlapping pixel-groups, each pixel-group contains seven pixels, among which there may be some wet pixels (*i.e.* unchangeable pixels). Thirdly, after weighing the methods described above, we try to embed the first seven secret bits into the first pixel-group of seven pixels. If none of the wet pixels of the first pixel-group are modified during the embedding, the embedding operation is successful and the instruction array we have set flag $[k]=10$. If not, we try to embed the first three secret bits into the first pixel-group of seven pixels, if none of the wet pixels are altered this time, the embedding operation is successful and flag $[k]=01$, if not, flag $[k]=00$, that is, the operation of embedding secret bits into the first pixel-group fails. So we try to embed the secret bits into the next pixel-group in the same way. Until all the secret bits are embedded, we can get the stego image *I'* and the instruction array flag at last.

The date embedding phase and the data extracting phase are described in the following sections 3.1 and 3.2 respectively.

3.1. The Data Embedding Phase

A cover image *I* sized $H \times W$ pixels is given as the carrier and the binary secret message need to be embedded.

Initialization: Set an index *i* = 0, to indicate the secret bit; Set an instruction array flag $[k]$, to indicate the embedding.

Step 1: Segment the given cover image *I* sized $H \times W$ into *x* non-overlapping pixel-groups, denoted as Q^k. Each pixel-group contains seven pixels, among which there may be some wet pixels by any possibility, denoted as $\{p_j | j \in W^k\}$, W^k is one of the subsets of $\{1,2,3,4,5,6,7\}$.

Step 2: From *i*, read the first seven bits of the binary secret message *S*, denoted as $(s_1, s_2, s_3, s_4, s_5, s_6, s_7)$.

Step 3: Read one pixel-group Q^k of seven pixels, and calculate the LSB of Q^k, denoted as $C^k = (c_1, c_2, c_3, c_4, c_5, c_6, c_7)$.

Step 4: Calculate the decimal value *a* of bits $(s_3 s_5 s_6 s_7)$ and the decimal value *b* of bits $(s_1 s_2 s_4)$. If $r_a^b \oplus C^k = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, where $\oplus$ is the bit-wise exclusive-or operation, and $x_j = 0$, where $j \in W^k$, we replace C^k with r_a^b, and $\text{flag}[k] = 10, i = i + 7$, then go to Step 2; if $x_j \neq 0$, where $j \in W^k$, then go to Step 5.

Step 5: Calculate the decimal value *u* of the first three bits $(s_1 s_2 s_3)$ and compare the values between g_{u+1}^v and C^k from *v* = 0 to 15 in group G^{u+1}. If $g_{u+1}^v \oplus C^k = (x_1, x_2, x_3, x_4, x_5, x_6, x_7)$, where $\oplus$ is the bit-wise exclusive-or operation, and $x_j = 0$, where $j \in W^k$, we replace C^k with g_{u+1}^v, and $\text{flag}[k] = 01, i = i + 3$, then go to Step 2; if $x_j \neq 0$, where $j \in W^k$, $\text{flag}[k] = 00$, that is, the embedding operation fails. Go to Step 3 to try the next pixel-group Q^{k+1}.

At last, we can obtain the stego image *I'* when all the secret bits are embedded. **Figure 3** gives the block diagrams of the data embedding phase.

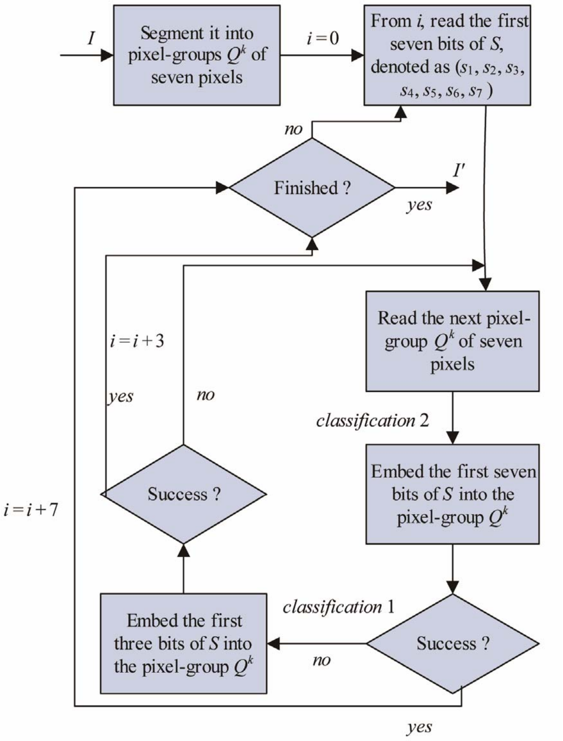

I
Segment it into pixel-groups Q^k of seven pixels
$i = 0$
From *i*, read the first seven bits of *S*, denoted as (s_1, s_2, s_3, s_4, s_5, s_6, s_7)
no
Finished ?
I'
yes
$i = i + 3$
yes
no
Read the next pixel-group Q^k of seven pixels
classification 2
Success ?
$i = i + 7$
Embed the first seven bits of *S* into the pixel-group Q^k
classification 1
Embed the first three bits of *S* into the pixel-group Q^k
no
Success ?
yes

Figure 3. The block diagrams about the data embedding phase of HQIH algorithm.

3.2. The Data Extracting Phase

The receiver can extract the secret message *S* from the received stego image *I'* *w*ith the help of the pre-shared instruction array *flag* between the sender and the receiver. The detailed steps are narrated as follows.

Step 1: Segment the received stego image *I'* sized *H* × *W* pixels into *x* non-overlapping pixel-groups, de- noted as $Q^{k'}$. Each pixel-group contains seven pixels.

Step 2: Read the next pixel-group $Q^{k'}$ of seven pixels:

If $\text{flag}[k'] = 00$, no secret bits are embedded into $Q^{k'}$, go to Step 2;

If $\text{flag}[k'] = 01$, calculate the LSB of $Q^{k'}$, denoted as $C^{k'} = (c'_1, c'_2, c'_3, c'_4, c'_5, c'_6, c'_7)$, compute $s = \left(H \times \left(C^{k'}\right)^{\mathrm{T}}\right)^{\mathrm{T}}$ and reconstruct *S* by $S = S \| s$, where || denotes the concatenation operation, then go to Step 2;

If $\text{flag}[k'] = 10$, calculate the LSB of $Q^{k'}$, denoted as $C^{k'} = (c'_1, c'_2, c'_3, c'_4, c'_5, c'_6, c'_7)$, compute $(s_1 s_2 s_4) = \left(H \times \left(C^{k'}\right)^{\mathrm{T}}\right)^{\mathrm{T}}$, and extract the next partition *s* of seven secret bits $s = (s_1, s_2, c'_3, s_4, c'_5, c'_6, c_7)$. Reconstruct *S* by $S = S \| s$, where || denotes the concatenation operation, then go to Step 2.

At last, we can extract all the secret bits and the block diagrams of the data extracting phase are shown in **Figure 4**.

4. Experimental Results and Discussions

As is well-known, high embedding efficiency and high

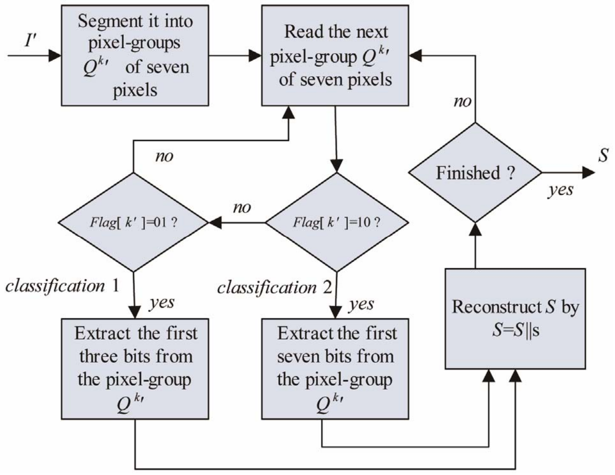

I′
Segment it into pixel-groups Q^{k′} of seven pixels
Read the next pixel-group Q^{k′} of seven pixels
no
Finished ?
S
yes
no
Flag[k′]=01 ?
no
Flag[k′]=10 ?
classification 1
yes
classification 2
yes
Extract the first three bits from the pixel-group Q^{k′}
Extract the first seven bits from the pixel-group Q^{k′}
Reconstruct S by S=S||s

Figure 4. The block diagrams about the data extracting phase of HQIH algorithm.

embedding payload are the primary goal of a good steganographic scheme. So, correspondingly, there are two important evaluation criterions to measure the performance of a steganographic scheme, one is the embedding efficiency of the stego image, and the other is the embedding payload of the cover image.

For embedding efficiency, also called embedding quality or visual quality of the stego image, in order to avoid a subjective evaluation by the human naked eyes, a well-known measurement, namely peak-signal-to-noise-r-ate (*PSNR* for short), is used to evaluate the degree of similarity between a stego image and its original image. *PSNR* is defined as following equation in (3).

$$PSNR = 10\log_{10}\frac{255^2}{MSE}\text{dB} \tag{3}$$

Here, *MSE*, being short for the mean square error, represents the difference between the stego image and its original image sized *H* × *W* pixels. The MSE is defined as in (4).

$$MSE = \frac{1}{H \times W}\sum_{i=1}^{H}\sum_{j=1}^{W}\left(I_{ij} - I'_{ij}\right)^2 \tag{4}$$

According to the visual quality evaluation, a high value of *PSNR* means that a stego image is very similar to its original image and the embedding efficiency of the steganographic scheme is high. In contrast, a low value of *PSNR* means that a stego image has visible and sensible distortion with its original image and the embedding efficiency is low. Generally speaking, if the value of *PSNR* is higher than 30 dB, it is hard to distinguish the distortion by human eyes.

For embedding payload, also called embedding capacity, we use *ER*, being short for embedding rate, to represent the percentage of the embedded secret bits in the whole pixels of the cover image. The *ER* is defined as in (5).

$$ER = \frac{N}{H \times W}\text{bpp} \tag{5}$$

Here, *N* is the total number of the embedded secret bits and *H* × *W* is the size of the carrier. According to the embedding payload evaluation, a large value of *ER* represents that the steganographic scheme has better performance in terms of the embedding payload, that is, a cover pixel in the cover image can carry more secret bits. On the contrary, a small value of *ER* represents a worse performance.

In order to evaluate the performance of HCIH algorithm, nine commonly-used gray-scale images sized 512 × 512 pixels were used to simulate the experiments as shown in **Figure 5**.

By using MATLAB 7.0 software, we simulated the procedure of the HCIH algorithm.

Figure 6 shows the visual quality of the stego images generated by the proposed method when $ER = 0.75\text{bpp}$.

Table 1 compares the results of the performance between HCIH algorithm and other methods, such as Matrix coding and the "Hamming + 1" method.

(a) Baboon (b) Barbara (c) Boats
(d) Coldhill (e) Jet (F16) (f) Lena
(g) Pepper (h) Tiffany (i) Zelda

Figure 5. The nine commonly-used gray-scale images.

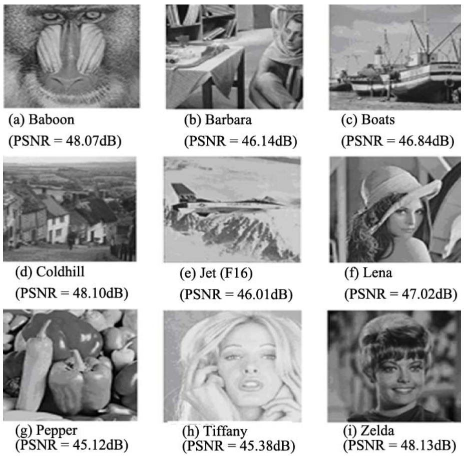

(a) Baboon (PSNR = 48.07dB) (b) Barbara (PSNR = 46.14dB) (c) Boats (PSNR = 46.84dB)
(d) Coldhill (PSNR = 48.10dB) (e) Jet (F16) (PSNR = 46.01dB) (f) Lena (PSNR = 47.02dB)
(g) Pepper (PSNR = 45.12dB) (h) Tiffany (PSNR = 45.38dB) (i) Zelda (PSNR = 48.13dB)

Figure 6. The visual quality of the stego images generated by HCIH algorithm with *ER* = 0.75 (bpp).

Table 1. The comparison results between HCIH algorithm and others.

Images	Matrix coding [21]		The "Hamming + 1" [14]		HCIH algorithm	
	PSNR	*ER*	*PSNR*	*ER*	*PSNR*	*ER*
Baboon	56.44	0.43	53.71	0.499	48.07	0.75
Barbara	54.65	0.43	48.60	0.499	46.14	0.75
Boats	54.75	0.43	49.37	0.499	46.84	0.75
Coldhill	57.02	0.43	53.73	0.499	48.10	0.75
***Jet* (*F*16)**	55.84	0.43	51.61	0.499	46.01	0.75
Lena	56.05	0.43	52.43	0.499	47.02	0.75
Pepper	54.01	0.43	47.26	0.499	45.12	0.75
Tiffany	53.98	0.43	47.46	0.499	45.38	0.75
Zelda	56.40	0.43	54.04	0.499	48.13	0.75
Average	55.46	0.43	50.91	0.499	46.77	0.75

From the **Figure 6** and the **Table 1**, we can see that the proposed method achieved high embedding capacity (0.75 bpp) with acceptable visual quality (*i.e*. the *PSNR* value is higher than 45 dB).

Figure 7 compares the embedding rate of Matrix coding, "Hamming+1" and HCIH algorithm and shows that the proposed HCIH algorithm achieves higher embedding rate, that is higher embedding capacity. **Figure 8** gives the PSNR of different stego images generated by HCIH algorithm and shows that the average value of PSNR is higher than 46 dB. According to the embedding efficiency evaluation, HCIH algorithm also achieves acceptable visual quality.

By using MATLAB 7.0 software, we simulated the procedure of the HQIH algorithm. In our simulation experiments, we chose 4 different wet rates (*i.e*. the values of *WR* is from 0.1 to 0.4) for each test image, in order to assure high accuracy of the experimental results. Meanwhile, we randomly generated 10 different wet maps for each *WR*, each map had different distribution of the wet pixels, and also generated 10 different binary strings of the same size as the different secret data. Based on the experimental data mentioned above, cyclic-cross tests were adopted. Ultimately, the average of all the values except for the maximum and the minimum was considered as the experimental results.

Table 2 in the following gives the results of the simulation experiments when *WR* is from 0.1 to 0.4. As is shown, the average value of *PSNR* is higher than 52 dB. For the visual quality evaluation, the stego image which carried the secret data is greatly similar to its original image and it is hard to distinguish the difference by human naked eyes. Thus, the HQIH algorithm of information hiding achieves higher embedding efficiency, that is, the stego image has better visual quality.

Table 2 also illustrates the results of *ER*. The values of *ER* decrease with the increase of *WR* and it can achieve 0.55 bpp at least and 0.83 bpp at most.

Figure 9 gives the embedding rate of different images with different wet rates, the value of which is from 0.1 to 0.4 and shows that the embedding rate rises with the decrease of WR. **Figure 10** compares the embedding rate of Matrix coding, "Hamming + 1", HCIH algorithm and HQIH algorithm (with *WR* = 0.1). We can find that the HQIH algorithm can achieve higher embedding capacity than others.

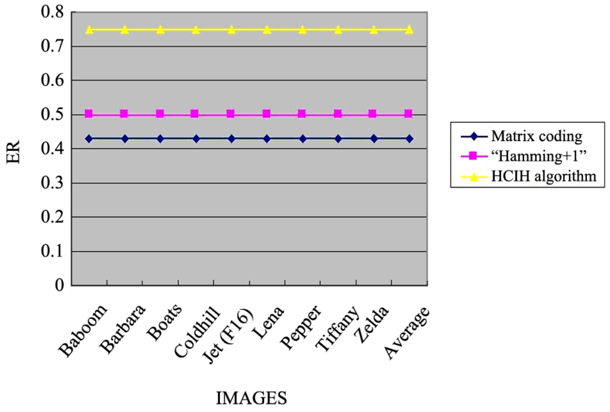


Figure 7. The embedding rate of different algorithms.

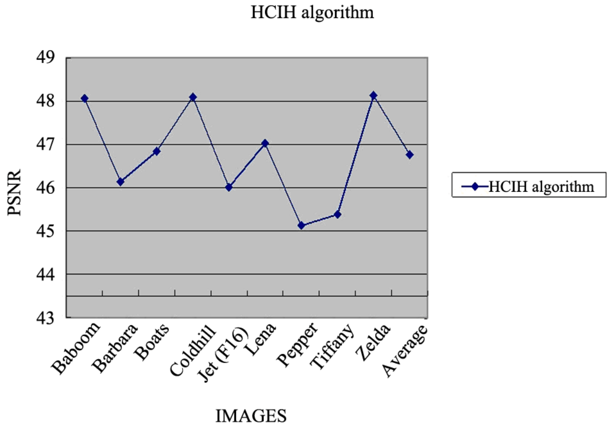


Figure 8. The PSNR of different stego images generated by HCIH algorithm.

Table 2. The results of simulation experiments of HQIH algorithm.

Images	*WR* = 0.1		*WR* = 0.2		*WR* = 0.3		*WR* = 0.4	
	PSNR	*ER*	*PSNR*	*ER*	*PSNR*	*ER*	*PSNR*	*ER*
Baboon	52.09	0.83	52.27	0.70	52.70	0.61	53.35	0.55
Barbara	52.10	0.83	52.28	0.70	52.71	0.61	53.35	0.55
Boats	52.10	0.83	52.28	0.70	52.72	0.61	53.36	0.55
Coldhill	52.09	0.83	52.29	0.70	52.70	0.61	53.34	0.55
***Jet* (*F*16)**	52.10	0.83	52.27	0.70	52.71	0.61	53.35	0.55
Lena	52.09	0.83	52.27	0.70	52.70	0.61	53.34	0.55
Pepper	52.10	0.83	52.28	0.70	52.71	0.61	53.35	0.55
Tiffany	52.10	0.83	52.27	0.70	52.71	0.61	53.35	0.55
Zelda	52.12	0.83	52.90	0.70	52.72	0.61	53.36	0.55
Average	52.10	0.83	52.28	0.70	52.71	0.61	53.35	0.55

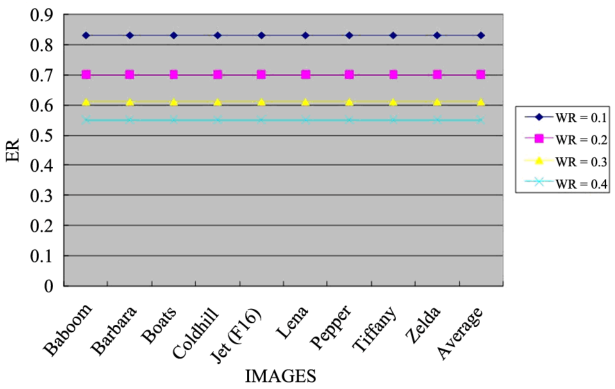


Figure 9. The embedding rate of different images with different wet rates.

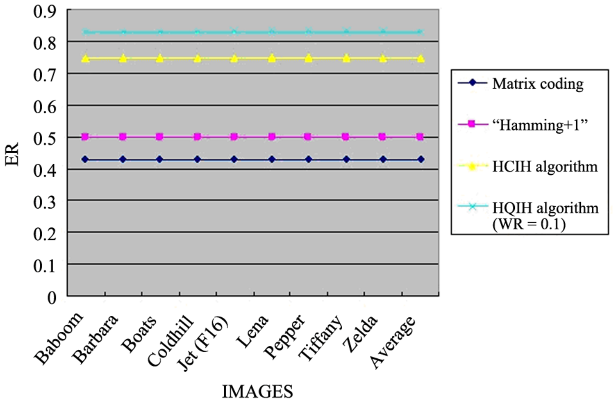


Figure 10. The embedding rate of different algorithms.

Figure 11 gives the PSNR of different images with different wet rates, the value of which is from 0.1 to 0.4 and shows that the value of PSNR rises with the increase of WR. The WR is short for Wet Rate, which refers to the share of wet pixels in an image of all the pixels of the entire image. The higher of WR, the more of wet pixel in an image, in the hidden process, wet pixels can not be modified, so the more of wet pixels, the fewer changes made in the image will have, then generated the degree of difference of the target image and the original image is relatively small, PSNR is short for the peak signal to noise ratio, which is used to measure the degree of difference between the target image and the original image, the smaller of the degree of difference, the value of PSNR is higher. *i.e.*, the value of PSNR is increased with the increase of the WR. **Figure 12** compares the PSNR between method in [6] and the HQIH algorithm. We can see that the value of PSNR is higher, comparing the method in [6]. That is, the HQIH algorithm improves the embedding efficiency obviously. Meanwhile, we also compare the PSNR between the HCIH algorithm and the HQIH algorithm in **Figure 13**.

At last, **Figure 14** gives the visual quality of the stego images generated by the HQIH algorithm with *WR* = 0.4. HCIH algorithm use the unified hidden method for each secret bit, and HQIH algorithm use the first hidden algorithm firstly in order to get a higher hiding capacity. However, the hidden opeation may fail in the first time since introduction the wet pixels. And we must use the second hidden algorithm again when the first opeation fails. So the hidden algorithm may not uniform for different secret information bit hidden. And thus the visual effect of image is irregularity. It is reflect by the fluctuate of PSNR values. But this fluctuation is relatively small, so it does not affect the effect of the algorithm.

Steganalysis is a technique to detect whether an image carries the secret messages or not [22,23]. In order to intercept and crack the secret messages, the steganalysis uses statistics tools to analyse the pixel value distribution on a suspicious image. Thus, if the stego image is generated by obviously modifying the cover pixels and corresponds to the statistic rule, then it is easier to be detected by the steganalysis. From this point of view, we choose the more appropriate method by weighing and selecting

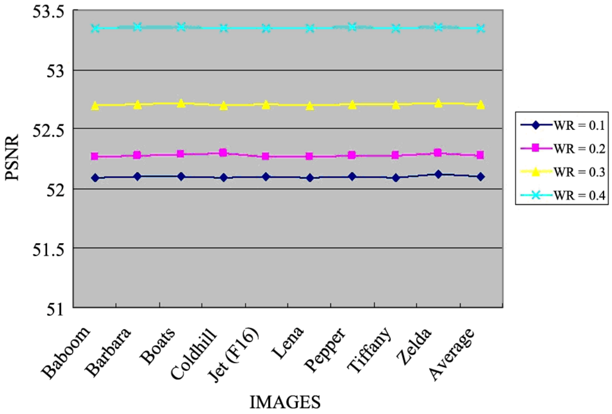


Figure 11. The PSNR of different images with different wet rates.

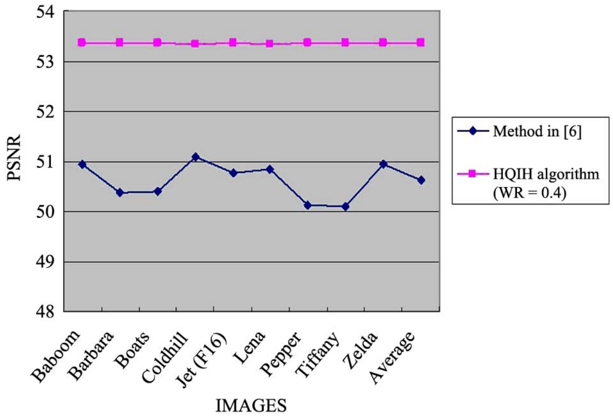


Figure 12. Comparison the PSNR of HQIH algorithm to that in [6].

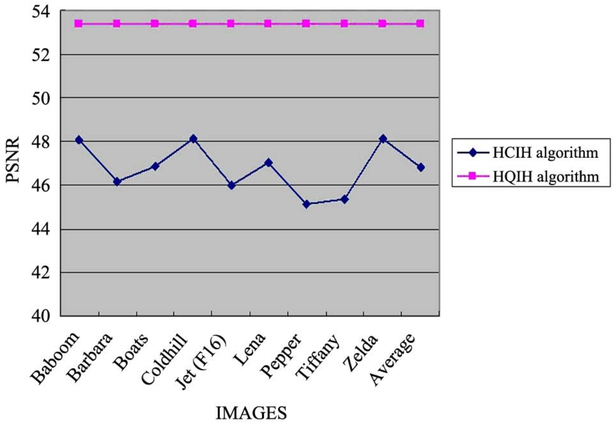
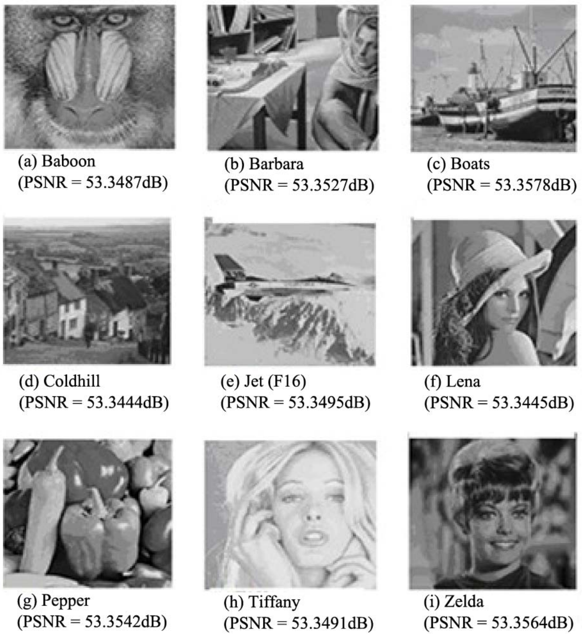


Figure 13. Comparison the PSNR of HCIH algorithm to HQIH algorithm.

in our proposed conception. It is just like to set another safeguard. And it is difficult for the attackers to aware of the secret messages. Therefore the HQIH algorithm for information hiding can achieve some degree of security compared to the related works.



(a) Baboon (PSNR = 53.3487dB)

(b) Barbara (PSNR = 53.3527dB)

(c) Boats (PSNR = 53.3578dB)

(d) Coldhill (PSNR = 53.3444dB)

(e) Jet (F16) (PSNR = 53.3495dB)

(f) Lena (PSNR = 53.3445dB)

(g) Pepper (PSNR = 53.3542dB)

(h) Tiffany (PSNR = 53.3491dB)

(i) Zelda (PSNR = 53.3564dB)

Figure 14. The visual quality of the stego images generated by HQIH algorithm with *WR* = 0.4.

5. Conclusions

Especially considering the improvement of the embedding capacity and the embedding efficiency, this paper mainly studies on the information hiding technology based on gray-scale digital images and proposes two algorithms with detailed procedures and effective experimental simulations.

Through experimental simulation, we evaluate the validity of HCIH algorithm. The experimental results show that our proposed HCIH algorithm achieves high embedding capacity (*i.e.* 0.75 bpp) and acceptable visual quality of the stego image, and can be used for the applications about large payload secret message transmission.

Through experimental simulation, we evaluate the validity of HCIH algorithm. The simulation experiments show that the HQIH algorithm achieves high embedding efficiency, that is the value of PSNR is more than 52 dB, and large embedding payload, that is the value of ER is between 0.55 bpp and 0.83 bpp, which can be used for different applications. Specially, our HQIH algorithm gives some degree of security by considering twofold safeguards.

6. Acknowledgements

This work is partially supported by National Grand Fundamental Research 973 Program of China under Grant # 2007CB311003, supported by National Natural Science Foundation of China under Grant #61073117, supported by Natural Science Foundation of Anhui Province under Grant #11040606M145, support by Provincial natural science research program of higher education institutions of Anhui province KJ2013A016, supported by Academic Innovation Research Project of Anhui University.

REFERENCES

[1] S. Dumitrescu, X. Wu and Z. Wang, "Detection of LSB Steganography via Sample Pair Analysis," *IEEE Transactions on Signal Process*, Vol. 51, 2003, pp. 355-372.

[2] A. Ker, "Improved Detection of LSB Steganography in Grayscale Images," In: J. Fridrich, Ed., *Proceedings of the Sixth International Workshop on Information Hiding*, Vol. 3200, Springer, Toronto, 2004, pp. 97-115. doi:10.1007/978-3-540-30114-1_8

[3] C. K. Chan and L. M. Cheng, "Hiding Data in Images by Simple LSB Substitution," *Pattern Recognition*, Vol. 37, No. 3, 2004, pp. 469-474. doi:10.1016/j.patcog.2003.08.007

[4] J. Mielikainen, "LSB Matching Revisited," *IEEE Signal Processing Letters*, Vol. 13, No. 5, 2006, pp. 285-287. doi:10.1109/LSP.2006.870357

[5] A. Westfeld, "F5-a Steganographic Algorithm," *Proceedings of the* 4*th International Workshop on Information Hiding*, Pittsburgh, 25-27 April 2001, pp. 289-302.

[6] C.-C. Chang, T. D. Kieu and Y.-C. Chou, "A High Payload Steganographic Scheme Based on (7,4) Hamming Code for Digital Images," *International Symposium on Electronic Commerce and Security*, Guangzhou, 3-5 August 2008, pp. 16-21.

[7] Z. X. Yin, C. C. Chang and Y. P. Zhang, "A High Embedding Efficiency Steganography Scheme for Wet Paper Codes," *Proceedings of the* 5*th International Conference on Information Assurance and Security* (*IAS* 2009), Xi'an, 18-20 August 2009, pp. 611-614. doi:10.1109/IAS.2009.93

[8] Z. X. Yin, C. C. Chang and Y. P. Zhang, "An Information Hiding Scheme Based on (7,4) Hamming Code Oriented Wet Paper Codes," *International Journal of Innovative Computing*, *Information and Control*, Vol. 6, No. 7, 2010, pp. 3121-3130.

[9] Y. P. Zhang, J. Jiang, Z. X. Yin and C. C. Xu, "A Method Embedding Email Address into Digital Images," *Proceedings of the* 5*th International Conference on Computer Science & Education* (*ICCSE* 2010), Heifei, 24-27 August 2010, pp. 346-350.

[10] J. Fridrich, M. Goljan, P. Lisonek and D. Soukal, "Writing on Wet Paper," *IEEE Transactions on Signal Processing*, Vol. 53, No. 10, Part II, 2005, pp. 3923-3935.

[11] C. C. Thien and J. C. Lin, "A Simple and High-Hiding Capacity Method for Hiding Digit-by-Digit Data in Images Based on Modulus Function," *Pattern Recognition*, Vol. 36, No. 12, 2003, pp. 2875-2881. doi:10.1016/S0031-3203(03)00221-8

[12] Y. C. Chou, C. C. Chang and K. M. Li, "A Large Payload Data Embedding Technique for Color Images," *Fundamenta Informaticae*, Vol. 88, No. 1-2, 2008, pp. 47-61.

[13] T. D. Kieu and C. C. Chang, "A High Stego-Image Quality Steganographic Scheme with Reversibility and High Payload Using Multiple Embedding Strategy," *The Journal of Systems and Software*, Vol. 82, No. 10, 2009, pp. 1743-1752. doi:10.1016/j.jss.2009.05.028

[14] W. Zhang, S. Wang and X. Zhang, "Improving Embedding Efficiency of Covering Codes for Applications in Steganography," *IEEE Communications Letters*, Vol. 11, No. 8, 2007, pp. 680-682.

[15] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," *IEEE Communications Letters*, Vol. 10, No. 113, 2006, 781-783. doi:10.1109/LCOMM.2006.060863

[16] C. C. Lin, W. L. Tai and C. C. Chang, "Multilevel Reversible Data Hiding Based on Histogram Modification of Difference Images," *Pattern Recognition*, Vol. 41, No. 12, 2008, pp. 3582-3591. doi:10.1016/j.patcog.2008.05.015

[17] Y. A. Ho, Y. K. Chan, H. C. Wu and Y. P. Chu, "High Capacity Reversible Data Hiding in Binary Images Using Pattern Substitution," *Computer Standards & Interfaces*, Vol. 31, No. 4, 2009, pp. 787-794. doi:10.1016/j.csi.2008.09.014

[18] R. Z. Wang and Y. D. Tsai, "An Image-Hiding Method with High Hiding Capacity Based on Best-Block Matching and k-Means Clustering," *Pattern Recognition*, Vol. 40, No. 2, 2007, pp. 398-409. doi:10.1016/j.patcog.2006.07.015

[19] A. Tiwari and M. Sharma, "Comparative Evaluation of Semifragile Watermarking Algorithms for Image Authentication," *Journal of Information Security*, Vol. 3, No. 3, 2012, pp. 189-195. doi:10.4236/jis.2012.33023

[20] V. H. Gaidhane, V. Singh, Y. V. Hote and M. Kumar, "New Approaches for Image Compression Using Neural Network," *Journal of Intelligent Learning Systems and Applications*, Vol. 3, No. 4, 2011, pp. 220-229. doi:10.4236/jilsa.2011.34025

[21] R. Crandall, "Some Notes on Steganography," Posted on Steganography Mailing List, 1998. http://os.inf.tu-dresden.de/west-feld/crandall.pdf

[22] J. J. Harmsen and W. A. Pearlman, "Steganalysis of Additive Noise Modelable Information Hiding," In: E. J. Delp and P. W. Wong, Eds., *Proceedings of SPIE Security Watermarking Multimedia Contents V*, Vol. 5020, San Antonio, 13 June 2003, pp. 131-142. doi:10.1117/12.476813

[23] A. D. Ker, "Quantitative Evaluation of Pairs and RS Steganalysis," In: E. J. Delp III and Pi. W. Wong, Eds., *Proceedings of SPIE—Security*, *Steganography*, *and Watermarking of Multimedia Contents VI*, *SPIE*, Vol. 5306, San Jose, 18-22 January 2004, pp. 83-97.