Image Steganography Based on Hamming Code and Edge Detection

Shuliang Sun
School of Electronics and Information Engineering, Fuqing Branch of Fujian Normal University, China

Abstract: *In this paper a novel algorithm which is based on hamming code and 2^k correction is proposed. The new method also utilizes canny edge detection and coherent bit length. Firstly, canny edge detector is applied to detect the edge of cover image and only edge pixels are selected for embedding payload. In order to enhance security, the edge pixels are scrambled. Then hamming encoding is practiced to code the secret data before embedded. Calculate coherent bit length L on the base of relevant edge pixels and replace with L bits of payload message. Finally, the method of 2^k correction is applied to achieve better imperceptibility in stego image. The experiment shows that the proposed method is more advantage in Peak Signal-to-Noise Ratio (PSNR), capacity and universal image quality index (Q) than other methods.*

Keywords: *Hamming code, 2^k correction, coherent bit length, canny edge detector.*

Received October 5, 2015; accepted March 30, 2016

1. Introduction

With the rapid development in both communication and Internet technologies, digital signal can be transmitted conveniently over the Internet. However, Internet is an open transmission medium, communication over the Internet will bring us not only convenience but also some hazards and risks. It is more and more important to protect information to communicate securely nowadays. There are two important techniques to protect secret data: cryptography and information hiding. As a kind of information hiding technology, steganography has been developed rapidly and caused widespread attention [13]. Steganography is a skill that hides the existence of secret message under the cover of a carrier signal. As a result, no one apart from the sender and intended recipient realizes there is a hidden message. The original image is called the cover image, which is used to carry secret message as a carrier signal. The secret message is embedded into cover medium. The image which has carried secret message is called the stego image. The most important features in steganographic system are embedding payload, security (imperceptibility) and robustness. A steganographic scheme with low image distortion, high payload and security is more expected. However, the three factors are inevitable conflict. Therefore, there is a compromise among them depending on different application requirements [14].

Image steganography is widely used over the internet. In order to increase safety, secret information was encoded before embedded in the cover image. Since human eyes are more sensitive to smooth areas than edge regions, secret information will be embedded in the edge pixels of cover image [3, 4].

The rest of the paper is organized as follows: The related work is displayed in section 2. Related skills are discussed in section 3. The proposed algorithms of embedding and extraction are presented in section 4. Experiments and conclusion are showed in section 5 and 6.

2. Related Works

Bassil [3] proposed an image steganography algorithm based on the canny edge detection. Secret data was hidden within boundary pixels of the cover image.

Three parameters were provided in the algorithm and three Least Significant Bits (LSBs) of every color edge pixel were replaced with bits of secret data. In Jain *et al.* [7] proposed a way to search the edges of the cover image that could be used to hide secret message. It also provided the depth view of image steganography and edge detection filter techniques. In Yu *et al*. [19] proposed a new steganography scheme which was based on the methods of just noticeable difference and contrast sensitivity function. The method of 2^k correction was also applied to get better imperceptibility. The steganography technique could provide more payloads and had better imperceptibility in [10]. In [15], a novel secure steganography method was put forward. It was based on edge detection and Huffman Encoding. Coherent bit length was also adopted to embed different bits of secret data according to the values of edge pixels values. Authors in [4, 11, 17, 20] represented a steganography technique based on Hamming Code. Secret data was encrypted with Hill cipher before embedding in the cover image [9, 12]. Other coding methods were also used in steganography technique [1, 2, 5, 8, 16].

3. Proposed Work

3.1. Hamming Code

Hamming code is proposed by Hamming [6]. It is a block code which could detect and correct error.

Especially, (7, 4) hamming code is the most widely used. Four data bits (m_1, m_2, m_3, and m_4) are encoded by adding three parity bits (p_1, p_2, and p_3) to become the codeword of length 7. Each parity check bit is created by its associated data bits. The hamming code detects errors by ensuring each parity check bit and its corresponding data bits achieve the even parity [11].

This detection procedure is called parity checking.

$$2^r - 1 \geq n \text{ or } 2^r - 1 \geq k + r \quad r \geq 2 \tag{1}$$

Where n is the length of codeword, k is the length of secret data and r is the length of parity bits.

Table 1 illustrates the relationship between parity check bits and data bits, where "√" indicates the relationship exists between parity check bits and associated data bits.

Table 1. Relationship between parity check bits and data bits.

	m_1	m_2	m_3	m_4
p_1	√	√		√
p_2	√		√	√
p_3		√	√	√

As shown in Table 1, the parity check bits can be created by using the associated date bits. The results are shown in Table 2, where "⊕" donates an Exclusive OR (XOR) operation.

$$p_1 = m_1 \oplus m_2 \oplus m_4 \tag{2}$$

$$p_2 = m_1 \oplus m_3 \oplus m_4 \tag{3}$$

$$p_3 = m_2 \oplus m_3 \oplus m_4 \tag{4}$$

Table 2. Codeword of hamming code (7, 4).

No.	codeword		No.	codeword	
	$m_1\, m_2\, m_3\, m_4$	$p_1\ p_2\ p_3$		$m_1\, m_2\, m_3\, m_4$	$p_1\ p_2\ p_3$
0	0 0 0 0	0 0 0	8	1 0 0 0	1 1 0
1	0 0 0 1	1 1 1	9	1 0 0 1	0 0 1
2	0 0 1 0	0 1 1	10	1 0 1 0	1 0 1
3	0 0 1 1	1 0 0	11	1 0 1 1	0 1 0
4	0 1 0 0	1 0 1	12	1 1 0 0	0 1 1
5	0 1 0 1	0 1 0	13	1 1 0 1	1 0 0
6	0 1 1 0	1 1 0	14	1 1 1 0	0 0 0
7	0 1 1 1	0 0 1	15	1 1 1 1	1 1 1

The way to combine data and parity together is to put the parity bits at position 2^i such as p_1, p_2, m_1, p_3, m_2, m_3, m_4.

Parity matrix H and generator matrix G are both applied in hamming code. Especially matrix G is used for encoding and matrix H is used for decoding. On the sending side, each 4-bit data will be multiplied by the matrix G and the result is modulo of 2. The codeword X will be obtained and sent through the communication channel.

$$X = M \times G \tag{5}$$

Where M = (m_1, m_2, m_3, m_4) and

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

At the destination, in order to check the encoded message of 7-bit R (data and parity) that has been received, matrix R will be multiplied by the transpose of the parity check matrix H, and the result is modulo of 2 again.

$$Z = R \times H^T \tag{6}$$

Where

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

The vector Z is composed of three bits (z_1, z_2, z_3). The vector Z will be all zeroes (0 0 0) if the message is correct during transmission. Otherwise, any change in the message will lead to flipping one or more bits of the message; then it needs an error correction process.

3.2. Coherent Bit Length L

The basic idea of embedding is to replace the LSB of the cover image with the Most Significant Bits (MSB) of the secret image. It should not undermine the visual effects of the cover image obviously after embedding. Different pixel value could be embedded different number of binary bits. Coherent bit length L determines the payload of each edge pixels (E_i). The parameter L is calculated according to the conditions given below [15]:

- If $E_i \geq 2^7$; L=4
- If $2^6 \leq E_i < 2^7$; L=3
- If $2^5 \leq E_i < 2^6$; L=2
- Else L=1

The conditions to determine L also serves as secret key to retrieve the payload at the destination.

3.3. 2^k Correction Method

A mathematic method is used to achieve better imperceptibility in stego image. In some cases there are some differences between cover pixel and stego pixel after embedding. To overcome these differences and get better vision effects, 2^k correction method is adopted [12].

The process of 2^k correction is defined as follows:

Error value (EV) = |Actual Pixel Value (APV) - Stego Pixel Value (SPV)|, parameter *k* is the number of bits which are embedded in an edge pixel value.

```
If (SPV-APV>$2^{k-1}$) & (SPV-$2^k$>=0)
      New stego pixel value = SPV -$2^k$
Else if (SPV- APV<-$2^{k-1}$) & (SPV+$2^k$<=255)
      New stego pixel value = SPV +$2^k$
Else
      New stego pixel value = SPV
```

In this way, the 2^k correction makes the new stego pixel value closer to the Actual Pixel Value (APV) without affecting the secret data.

4. The Proposed Algorithm

4.1. Data Embedding Algorithm

The flowchart of data embedding procedure is shown in Figure 1. The steps of embedding algorithm are depicted as follows:

Algorithm 1: Image_Embedding

```
Input: Cover image and secret image.
Output: Stego image.
Begin
Step 1: Read the cover image and secret image.
Step 2: Canny edge detector is executed to detect the
    boundaries of cover image.
Step 3: Scramble the edge pixels with key 1.
Step 4: Secret image is converted to 1-D bit streams.
Step 5: Scramble the 1-D bit streams with key 2.
Step 6: Calculate coherent bit length L according to the value
    of edge pixel.
Step 7: Encode bit streams using Hamming (7, 4) encoder and
    the result of the encoded data is executed exclusive OR
    (XOR) operation with the 7 bits of random value using key3.
Step 8: Binary bit streams, coherent bit length L are embedded
    into scrambling edge pixels.
Step 9: Unscramble edge pixels.
Step 10: The method of $2^k$ correction is applied to achieve
    better imperceptibility in stego image.
Step 11: New stego image is obtained.
End
```

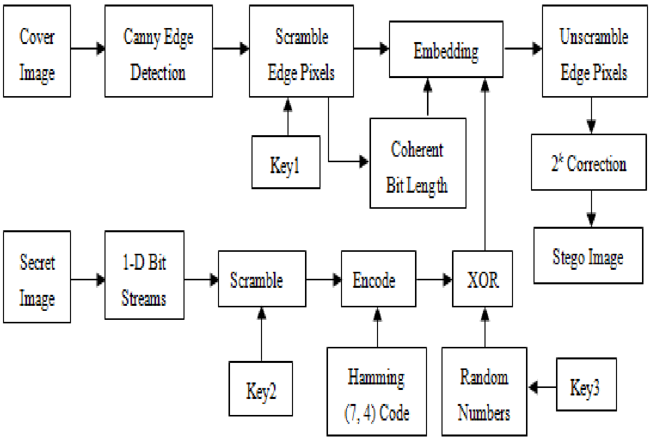

Figure 1. The block diagram of the embedding procedure.

4.2. Data Extraction Algorithm

The process of data extracting procedure is shown in Figure 2. It consists eleven parts.

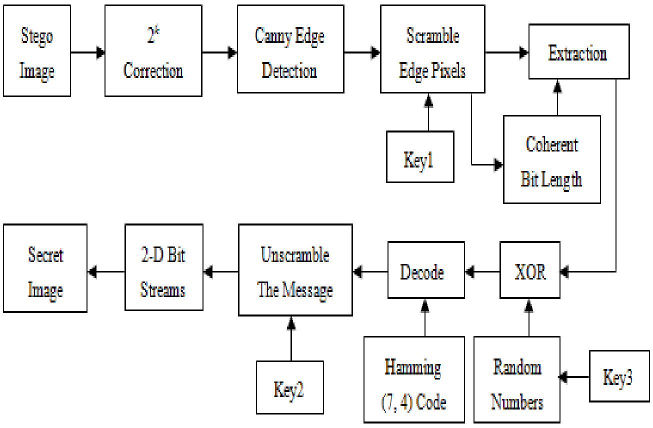

Figure 2. The block diagram of the extracting procedure.

Algorithm 2: Image_Extraction

```
Input: Stego image
Output: Secret image
Begin
Step 1: Get the stego image.
Step 2: Perform $2^k$ correction method on the stego image.
Step 3: Canny edge detector is performed to detect the edge of
stego image.
Step 4: Rearrange edge pixels with key1 and obtain original
sequence.
Step 5: Calculate the coherent bit length L.
Step 6: Extract L bits LSBs of edge pixels.
Step 7: The message is performed exclusive OR operation with
random numbers.
Step 8: Decode secret message using hamming (7, 4) decoder.
Step 9: Reposition the whole message into the original order
with key2.
Step 10: Convert the bit streams to 2-D array.
Step 11: Secret image is achieved.
End
```

Especially, key1, key2 and key3 are generated by pseudorandom number generator.

5. Experiments

In this paper, the experiment is simulated using MATLAB 10 program on Windows 7. To measure image quality of the proposed scheme, Peak Signal-to-Noise Ratio (PSNR), Universal Image Quality Index (Q) and Capacity are adopted.

To calculate PSNR, first Mean Square Errorm (MSE) is calculated using Equation (7):

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left\|I(i,j)-S(i,j)\right\|^2 \qquad (7)$$

MSE is the cumulative squared error Best wishes, original image (I) and stego image (S). M and N are the size of row and column of cover image. Thereafter PSNR value is calculated using Equation (8) in decibels. A higher value of PSNR is better because of the superiority of the signal to that of the noise.

$$PSNR = 20\log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \qquad (8)$$

Universal image quality index (Q) was developed by Wang [18]. Image distortion is often evaluated with three factors: loss of correlation, luminance distortion and contrast distortion. Traditional methods use error summation to measure image quality, but image quality measure Q is proposed by combining three factors which are employed to depict image distortion.

Q is defined as follows:

$$Q = \frac{4\sigma_{xy}\bar{x}\bar{y}}{(\sigma_x^2+\sigma_y^2)[(\bar{x})^2+(\bar{y})^2]} \qquad (9)$$

Where

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i, \quad \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \qquad (10)$$

$$\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i-\bar{x})^2, \sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i-\bar{y})^2 \qquad (11)$$

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i-\bar{x})(y_i-\bar{y}) \qquad (12)$$

$x= \{x_i \mid i =1, 2 \ldots, N\}$, $y = \{y_i \mid i =1, 2 \ldots, N\}$

Capacity means the number of bits in a cover image that can be modified without deteriorating the vision effect. The embedding capacity demands to preserve the statistical properties of the cover image. It is represented by Bits Per Pixel (BPP).

The ways of LSBs and Yu *et al*. [19] are compared with proposed method in this paper. Cover images of 512×512 gray-scale were used in the experiments. Secret image is an 8-bit grayscale image of size 128×128.

Figure 3 shows the results of applying the canny edge detection algorithm on the input image. As for the parameters, the size of the Gaussian filter is set to 1.5; the low threshold is arranged to 5, and the high threshold is appointed to 40.

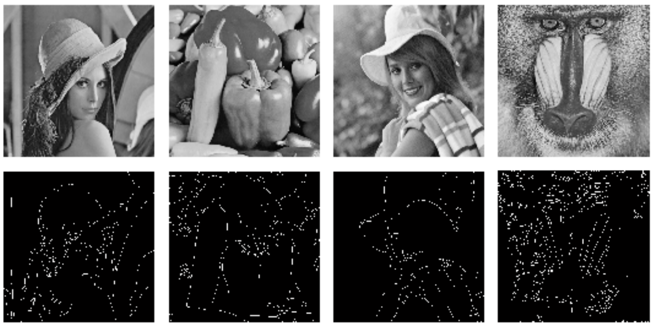

Figure 3. The cover images and edge images generated by the canny edge detector.

In this paper, secret data is only embedded in edge pixels in three methods. Though payload is smaller in this paper than with traditional methods, the values of PSNR and Q are much larger than other techniques. From Table 3, it can be concluded that the proposed technique is better than LSB-3 and Yu *et al*. [19] in three parameters.

Table 3. Comparison of Capacity, PSNR and Q.

Cover images		**LSB-3**	**Jae-Gil Yu's**	**Proposed Technique**
Lena	Capacity (bit)	36985	37348	38427
	PSNR (dB)	51.2655	55.5273	63.4807
	Q	0.9826	0.9925	0.9999
Peppers	Capacity (bit)	33205	34263	35946
	PSNR (dB)	51.6637	56.3618	63.2399
	Q	0.9874	0.9945	0.9998
Elaine	Capacity (bit)	31081	753695	35852
	PSNR (dB)	51.9693	55.8437	62.7690
	Q	0.9907	0.9953	0.9995
Baboon	Capacity (bit)	96340	102574	108074
	PSNR (dB)	47.0073	51.0359	58.3720
	Q	0.9673	0.9857	0.9984

As shown Figures 4 and 5, histogram and stego image of Baboon are displayed with LSB-3, Yu's and proposed method. It is seen that proposed technique is the best in three methods.

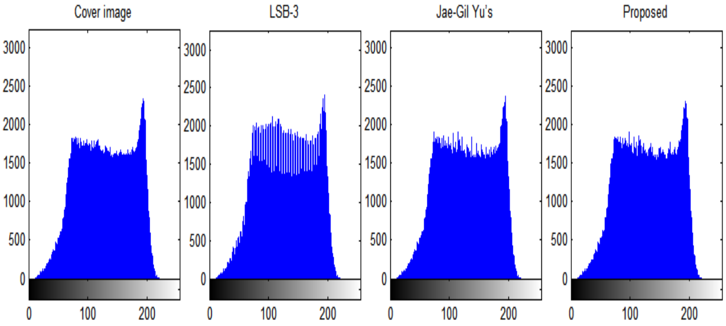

Figure 4. Comparison of histogram of baboon.

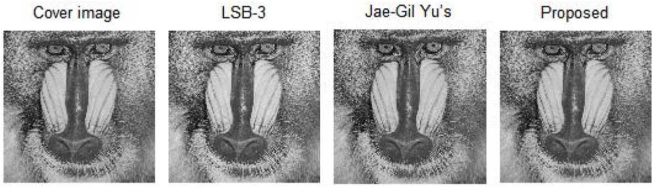

Figure 5. Comparison of stego image of baboon.

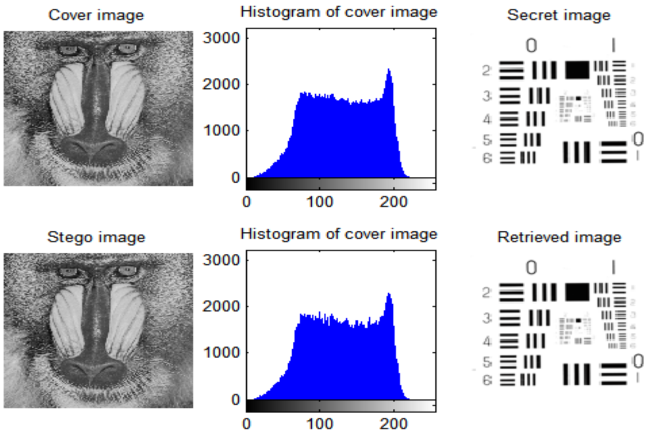

Figure 6. Stego image baboon and retrieved image.

It shows the stego image, relevant histogram and retrieved image with the proposed method in Figure 6.

Security is satisfied in proposed method. Three keys are used to embed and extract secret message.

This algorithm is considered a high visual effect due to the low modification on the host data that makes the stego image has a very good quality. The visual quality is measured by the PSNR and Q.

6. Conclusions

In this paper, the secret data is embedded in the edge of cover image only. That's because the Human Visual System (HVS) is more sensitive to slight changes in smooth areas than edge regions. At the same time, Hamming Code is applied to protect secret data. Three keys are applied to improve security. The larger edge pixel value is, the more bits it could be hidden. In order to alleviate the difference between stego image and cover image, 2^k correction technique is applied. By experiment it is found that proposed approach is better than two other methods in capacity, Q and PSNR.

Acknowledgment

This research was financially supported by the project of the Natural Science Foundation of Fujian Province, China (Grant No. 2016J05153, 2018J01788), the Outstanding Youth Scientific Research Training Program of Fujian Province of China in 2017 and the Training Program for Talents from the Fuqing Branch of Fujian Normal University of China under Grant KY2017NS07.

References

[1] Agarwal A., "Security Enhancement Scheme for Image Steganography Using S-DES Technique," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 4, pp. 164-169, 2012.

[2] Anand L., Sanket P., Sharath R., and Varun R., "A Novel Method of Data Encryption and Hiding Scheme Using VPASS Technique," *International Journal of Science and Research*, vol. 2, no. 5, pp. 293-296, 2013.

[3] Bassil Y., "Image Steganography Based on a Parameterized Canny Edge Detection Algorithm," *International Journal of Computer Applications*, vol. 64, no. 4, pp. 35-40, 2012.

[4] Chen W., Chang C., and Le T., "High Payload Steganography Mechanism Using Hybrid Edge Detector," *Expert Systems with Applications*, vol. 37, no. 4, pp. 3292-3301, 2010.

[5] Gokul M., Umeshbabu R., Vasudevan S., and Karthik D., "Hybrid Steganography Using Visual Cryptography and LSB Encryption Method," *International Journal of Computer Applications*, vol. 59, no. 14, pp. 5-8, 2012.

[6] Hamming R., "Error Detecting and Error Correcting Codes," *Bell System Technical Journal*, vol. 29, no. 2, pp. 147-160, 1950.

[7] Jain N., Meshram S., and Dubey S., "Image Steganography Using LSB and Edge Detection Technique," *International Journal of Soft Computing and Engineering*, vol. 2, no. 3, pp. 217-222, 2012.

[8] Javidi M. and Hosseinpourfard R., "Chaos Genetic Algorithm Instead Genetic Algorithm," *The International Arab Journal of Information Technology*, vol. 12, no. 2, pp. 163-168, 2015.

[9] Karthikeyan B., Chakravarthy J., and Ramasubramanian S., "Amalgamation of Scanning Paths and Modified Hill Cipher for Secure Steganography," *Australian Journal of Basic and Applied Sciences*, vol. 6, no. 7, pp. 55-61, 2012.

[10] Kaur A. and Kaur S., "Image Steganography Based on Hybrid Edge Detection and 2^k Correction Method," *International Journal of Engineering and Innovative Technology*, vol. 1, no. 2, pp. 167-170, 2012.

[11] Mstafa R. and Elleithy K., "A Highly Secure Video Steganography Using Hamming Code (7, 4)," *in Proceedings of IEEE Long Island Systems, Applications and Technology*, Farmingdale, pp. 1-6, 2014.

[12] Pavan N., Nagarjun G., Nihaar N., Gaonkar G., and Sharma P., "Image Steganography Based On Hill Cipher with Key Hiding Technique," *IOSR Journal of Computer Engineering*, vol. 11, no. 5, pp. 47-50, 2013.

[13] Sarkar A., Madhow U., and Manjunath B., "Matrix Embedding with Pseudorandom Coefficient Selection and Error Correction for Robust and Secure Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 225-239, 2010.

[14] Sharma S. and Kumari U., "A High Capacity Data-hiding Technique Using Steganography," *International Journal of Emerging Trends and Technology in Computer Science*, vol. 2, no. 3, pp. 288-292, 2013.

[15] Sun S., "A Novel Edge Based Image Steganography with 2^k Correction and Huffman Encoding," *Information Processing Letters*, vol. 116, no. 2, pp. 93-99, 2016.

[16] Vaidya A., More P., Fegade R., Bhavsar M., and Raut P., "Image Steganography Using DWT and Blowfish Algorithms," *IOSR Journal of Computer Engineering*, vol. 8, no. 6, pp. 15-19, 2013.

[17] Wang J., Chang Y., Yu C., and Yu S., "Hamming Code Based Watermarking Scheme for 3D Model Verification," *in Proceedings of International Symposium on Computer*, Tai chung, pp. 1095-1098, 2014.

[18] Wang Z., "A Universal Image Quality Index," *IEEE Signal Processing Letters*, vol. 9, no. 3, pp.

81-84, 2002.

[19] Yu J., Yoon J., Shin S., and Yoo K., "A New Image Steganography Based on 2^k Correction and Edge-Detection," *in Proceedings of the 5th International Conference on Information Technology: New Generations*, Las Vegas, pp. 563-568, 2008.

[20] Zhang Y., Jiang J., Zha Y., Zhang H., and Zhao S., "Research on Embedding Capacity and Efficiency of Information Hiding Based on Digital Images," *International Journal of Intelligence Science*, vol. 3, pp. 77-85, 2013.

Shuliang Sun graduated from Hangzhou Dianzi University, China, in 2003 and completed M.E. from Guangxi University in 2006, China. He received PhD from Tongji University in 2011, China. Currently, He is an Associate Professor at the School of Electronics and Information Engineering, Fuqing Branch of Fujian Normal University, China. His research includes Image Processing, Steganography and Pattern Recognition.