Hindawi Publishing Corporation
Advances in Multimedia
Volume 2015, Article ID 698492, 7 pages
http://dx.doi.org/10.1155/2015/698492

Research Article

A New Information Hiding Method Based on Improved BPCS Steganography

Shuliang Sun[1,2]

[1]*Department of Electronic and Information Engineering, Fuqing Branch of Fujian Normal University, Fuqing 350300, China*
[2]*Innovative Information Industry Research Center, Fuqing Branch of Fujian Normal University, Fuqing 350300, China*

Correspondence should be addressed to Shuliang Sun; tjussl_07@126.com

Received 31 December 2014; Revised 15 March 2015; Accepted 16 March 2015

Academic Editor: Deepu Rajan

Bit-plane complexity segmentation (BPCS) steganography is advantageous in its capacity and imperceptibility. The important step of BPCS steganography is how to locate noisy regions in a cover image exactly. The regular method, black-and-white border complexity, is a simple and easy way, but it is not always useful, especially for periodical patterns. Run-length irregularity and border noisiness are introduced in this paper to work out this problem. Canonical Cray coding (CGC) is also used to replace pure binary coding (PBC), because CGC makes use of characteristic of human vision system. Conjugation operation is applied to convert simple blocks into complex ones. In order to contradict BPCS steganalysis, improved BPCS steganography algorithm adopted different bit-planes with different complexity. The higher the bit-plane is, the smaller the complexity is. It is proven that the improved BPCS steganography is superior to BPCS steganography by experiment.

1. Introduction

Steganography is an art and science of invisible communication. It comes from Greek for covered writing and essentially means "to hide in plain sight" [1]. Embedding capacity, security (imperceptibility), and robustness are the most important three features in steganographic system. Generally speaking, there is a fundamental compromise between embedding capacity and security in information hiding scheme. Steganography methods can be divided into two categories: original (spatial) domain methods and transform domain methods. Cover image is transformed into frequency domain first, and then the secret messages are embedded in the coefficients of transformed cover image. Singh et al. [2] proposed a method to combine two techniques. One was image enhancement and the other was image steganography based on DFT. Kaur and Kochhar [3] provided a technique for image steganography based on DCT. The algorithm had good invisibility and security. A three-level DWT decomposition was done on host image and secret information was hidden in approximation coefficients of the decomposed image in [4]. The stegoimage is subjected to image processing attacks. Abu et al. [5] discussed a robust algorithm, which was based on integer Haar wavelet transform and pixel value difference. Ramezani et al. [6] gave a steganography method in contourlet domain. The optimal pixel adjustment process and genetic algorithm are also used. Alsaif and Saalih [7] presented a data hiding technique in NSCT domain. Secret data was embedded in high frequency directional band pass of contourlet transform. In spatial domain methods, the processing is applied on the image pixel values directly. Least significant bits (LSB) substitution [8] is the most well-known spatial steganographic system. Although this method is simple and easy, it is weak in robustness and compression, such as JPEG compression. Soumi et al. [9] presented a mosaic image steganography based on genetic algorithms for enhanced security. Mandal and Das [10] proposed a color image steganography method based on pixel value differencing. Secret data was hiding in the component of a pixel in a color image. Arora and Anand [11] gave an approach for image steganography using edge detection method. In their study, edges of RGB image were detected by scanning method using 3∗3 window. Since human eyes are not sensitive to tiny alterations of noisy data, it will not be noticed when the data

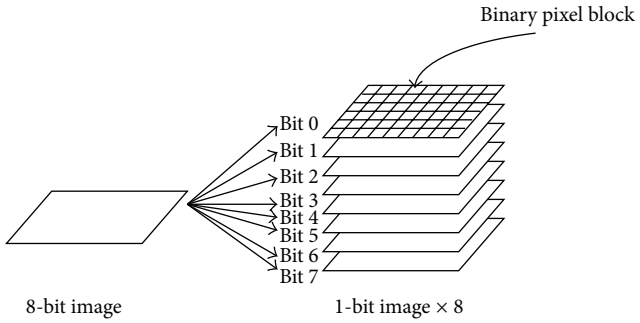


Figure 1: Binary pixel blocks on bit-planes.

in noisy regions is replaced with another noisy data. That is bit-plane complexity segmentation steganography (BPCS steganography) [12].

2. The Principle of BPCS Steganography

BPCS steganography was first put forward by Kawaguchi and Eason [13]. The basic principle is that firstly cover image is divided into "informative region" and "noise-like region." Then the secret information is hidden in noise-like blocks of cover image [14]. In LSB technique, data is hidden in the lowest bit-plane. But in BPCS technique, data is hidden in pixel blocks of all the planes, from the highest plane (most significant bit, MSB plane) to the lowest plane (LSB plane), which have noisy patterns [15]. In BPCS, a gray image consisting of n-bit pixels can be decomposed into n-binary planes. For example, $n = 8$, as shown in Figure 1.

For example, P is an n-bit gray image; here $n = 8$. Therefore = $[P_7\ P_6\ P_5\ P_4\ P_3\ P_2\ P_1\ P_0]$, where P_7 is the MSB bit-plane and P_0 is the LSB bit-plane. Each bit-plane can be segmented into "informative" region and "noise-like" region. It is simple in informative region and cannot be used for hiding information. However, it is complex in noise-like region and each noise-like region could be replaced with another noise-like pattern in BPCS. As a result, it will not change the overall quality of image after embedding. The most important step in BPCS is how to locate noisy regions in a cover image correctly. The regular method is to divide each bit-plane of the cover image into small square binary pixel blocks. The blocks are considered as noisy regions; those have complex black-and-white patterns. Often α is defined as a criterion to judge whether the block is complex or not [16]:

$$\alpha = \frac{k}{2 \times m \times (m-1)}, \tag{1}$$

where k is the total length of border in a block, m is the row or column of the block, and α is between 0 and 1. If α is higher than the given threshold value, then the block is regarded as complex.

3. Improved BPCS Steganography

The black-and-white border complexity is a simple and easy method to judge whether the blocks are complex or not. However it is not always useful. For example, the blocks that have periodical patterns, such as chessboard or stripes, are recognized as complex ones in this way. That is because, as shown in Figure 2, $\alpha_a = 1$ and $\alpha_b = 1/2$.

But these blocks cannot be used for embedding data; otherwise the cover image will deteriorate obviously. There are two new techniques to differentiate complex blocks from simple ones in this paper: run-length irregularity and border noisiness.

3.1. Run-Length Irregularity. Run-length irregularity is the histogram which consists of the run-lengths of both black-and-white pixels in a row or in a column.

Suppose that $h[i]$ is the frequency of runs of i pixels either in black or in white and n is the length of the pixel sequence; then h_s is used to measure the irregularity of a binary pixel sequence:

$$p_i = \frac{h[i]}{\sum_{j=1}^{n} h[j]},$$
$$h_s = -\sum_{i=1}^{n} h[i] \log_2 p_i. \tag{2}$$

The value of h_s is often normalized to $[0, 1]$ and denoted by $\widehat{h}_s$.

If the size of block is $n \times n$ and r_i and c_j are the ith row and jth column of a block, then the run-length irregularity β of a block is defined as follows:

$$\beta = \min\left\{\overline{\widehat{H}_s(r)}, \overline{\widehat{H}_s(c)}\right\}, \tag{3}$$

where

$$\widehat{H}_s(r) = \left\{\widehat{h}_s(r_0), \ldots, \widehat{h}_s(r_{n-1})\right\},$$
$$\widehat{H}_s(c) = \left\{\widehat{h}_s(c_0), \ldots, \widehat{h}_s(c_{n-1})\right\}. \tag{4}$$

And $\overline{X}$ is the mean of all the elements of X.

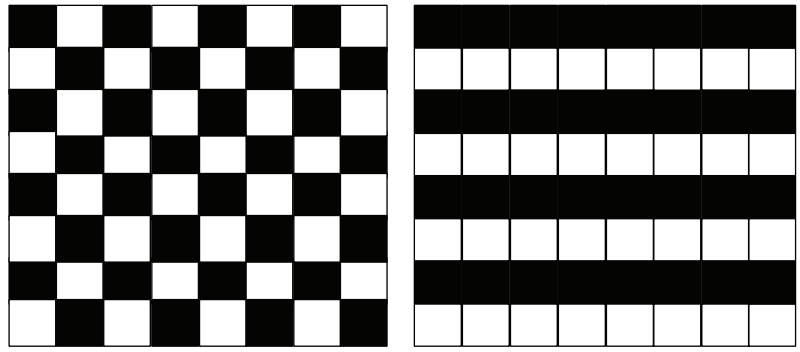
According to the definition, the smaller row and column averages are taken as the value of the run-length irregularity β. As seen in Figure 3, they are both periodic in row or column. As a result, every run-length irregularity β is 0, so they are simple and cannot be used for embedding.

The run-length irregularity β is only useful in row or column. If the block is regular in other directions, β will have nothing to do with it, as shown in Figure 3.

3.2. Border Noisiness. If data is embedded on the boundary of noisy regions and informative regions of cover image blocks, then the noisy regions will be expended. As a result, the cover image will be changed clearly.

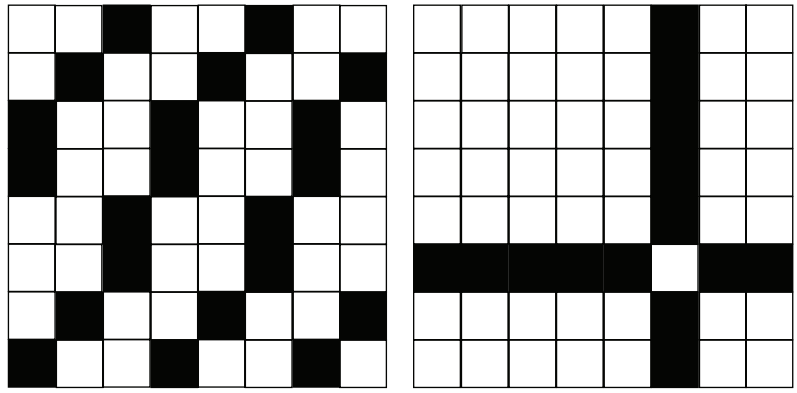
The border noisiness is based on the differences between adjacent binary pixel sequences in a block. Similarly if the block size is $n \times n$ and r_i and c_j are the ith row and jth column of a block, then the border noisiness γ of a block is defined as follows:

$$\gamma = \frac{1}{n} \min\left\{E_f[P_x(r)], E_f[P_x(c)]\right\}, \tag{5}$$



(a) Chessboard (b) Stripes

Figure 2: Blocks with large α while not complex.



(a) $\beta = 0.745$ (b) $\beta = 0.694$

Figure 3: Blocks with large β but those are not complex.

where

$$P_x(r) = \{\rho(r_0 \oplus r_1), \ldots, \rho(r_{n-2} \oplus r_{n-1})\},$$
$$P_x(c) = \{\rho(c_0 \oplus c_1), \ldots, \rho(c_{n-2} \oplus c_{n-1})\}. \quad (6)$$

$\oplus$ means bitwise exclusive OR, $\rho(x)$ is the number of ones in a binary sequence x, and

$$E_f(X) = \frac{1 - V(X)}{\max_X \{V(X)\}} \cdot \overline{X}, \quad (7)$$

where $X = \{x_0, \ldots, x_{m-1}\}$, $V(X)$ = the variance of X, and $\overline{X}$ = the average of X.

The border noisiness γ is used to check if many black-and-white pixel borders are well distributed over a block along both the horizontal and the vertical directions.

Though the blocks in Figures 3(a) and 3(b) both have large run-length irregularity β ($\beta_a = 0.745, \beta_b = 0.694$), their border noisiness γ is as little as 0.294 and 0.048, respectively. So they are not complex according to the border noisiness γ and are not suitable for embedding.

3.3. Default Threshold Values. In a word, a block B is recognized as complex only if it satisfies the following conditions:

$$\alpha(B) \geq \alpha_t, \qquad \beta(B) \geq \beta_t, \qquad \gamma(B) \geq \gamma_t. \quad (8)$$

Here, α_t, β_t, and γ_t are threshold values. Normally, the default threshold values are

$$\alpha_t^i = \begin{cases} \overline{\alpha} - i \cdot \Delta\alpha & 0 \leq i \leq 5 \\ 0 & 6 \leq i \leq 7, \end{cases}$$
$$\beta_t^i = \begin{cases} \overline{\beta} - i \cdot \Delta\beta & 0 \leq i \leq 5 \\ 0 & 6 \leq i \leq 7, \end{cases} \quad (9)$$
$$\gamma_t^i = \begin{cases} \overline{\gamma} - i \cdot \Delta\gamma & 0 \leq i \leq 5 \\ 0 & 6 \leq i \leq 7. \end{cases}$$

From the equation above, it can be concluded that the bit-plane is higher and the threshold value is larger. That is because it will raise noticeable changes for excessive embedding data in high bit-plane and will freely get enough embedding capacity in low bit-plane. There is a fact that these threshold values are default and not always optimal. They could be adjusted manually according to the actual conditions.

3.4. Canonical Gray Coding. Normally the pixel value of an image is represented by pure binary code (PBC). Canonical

Gray coding (CGC) [17] is superior to pure binary code (PBC) in BPCS steganography, because PBC will encounter "Hamming cliff," which means that a small change in pixel value will affect many bits of value [13]. CGC makes full use of characteristic of human vision system and works out this problem.

Suppose that b_i and g_i are the ith bit of the pure binary code and canonical Gray code with the same n-bit. The two codes are given by

$$b_0 b_1 \cdots b_{n-1}, \quad g_0 g_1 \cdots g_{n-1}. \tag{10}$$

The relationship between b_i and g_i is given:

$$g_i = \begin{cases} b_0 & i = 0 \\ b_{i-1} \oplus b_i & i > 0, \end{cases} \tag{11}$$

$$b_i = \begin{cases} g_0 & i = 0 \\ b_{i-1} \oplus g_i = g_0 \oplus \cdots \oplus g_i & i > 0. \end{cases}$$

Here $\oplus$ means exclusive OR operation.

It consists of informative and noise-like regions in binary image. Informative regions are simple while noise-like regions are complex. If secret information is noise-like then it is embedded in noise-like regions of the cover image directly. However, if secret data is informative then it will be conjugated firstly so as to convert it into complex pattern.

3.5. Conjugation Operation of a Binary Image. Conjugation is used to convert simple blocks into complex ones. In order to extract original data embedded in the cover image, it should record which blocks of the original data are conjugated and which are not. This information is stored in a conjugation map. It should be embedded along with the resource file as blocks. Note that the blocks of the conjugation map should be also conjugated if they are not complex enough.

If P is a binary image with size of $n \times n$ and black pixel is its foreground while white pixel is its background. W and B, respectively, represent all-white and all-black patterns. Now two checkerboard patterns W_c and B_c are put forward. In particular, W_c has a white pixel at the upper-left position, and B_c is its complement. In binary image black-and-white pixels particularly mean a logical value of 1 and 0.

Now P^* is defined as the conjugate of P which satisfies

$$P^* = P \oplus W_c. \tag{12}$$

The most important property about conjugation is

$$\alpha(P^*) = 1 - \alpha(P). \tag{13}$$

This property could transform informative pattern to complex one, so both informative and noise-like regions could be used for embedding by conjugation operation.

3.6. Statistical Analysis. Though BPCS steganography algorithm is advantageous in imperceptibility, it would change the statistic characteristics of bit-plane block complexity. Because adjacent pixels in the high bit-planes have a strong correlation, the higher the bit-plane is, the stronger the correlation is. The method of steganalysis is proposed by Zhang and Wang [17]. Suppose the following. (1) $h_0(c)$ is the complexity histogram of all the bit-plane blocks of cover image, and c is the complexity of a block, whose threshold value is $\theta \cdot C_{\max}$. (2) $h_I(c)$ is the complexity histogram of all the bit-plane blocks of secret image. If c is not as big as the threshold value $\theta \cdot C_{\max}$, the blocks should be done by conjugation first. Finally $h_s(c)$ is the complexity histogram of all the bit-plane blocks of cover image in which secret data has been embedded, and is defined as follows:

$$h_s(c) = \begin{cases} h_0(c) & c \le \theta \cdot C_{\max} \\ h_I(c) & \theta \cdot C_{\max} < c < (1-\theta) \cdot C_{\max} \\ h_I(c) + h_I(C_{\max} - c) & c \ge (1-\theta) \cdot C_{\max}. \end{cases} \tag{14}$$

From (14), it can be concluded that $h_s(c)$ is composed of three parts of complexity histograms; each of them is smooth connection, but there is a sharp jump at the joint of two adjacent histograms, such as $c = \theta \cdot C_{\max}$ and $c = (1-\theta) \cdot C_{\max}$. The way of steganalysis is shown as follows:

$$d(c) = [h(c-1) - h(c)] + [h(C_{\max} - c + 1) - h(C_{\max} - c)] \quad 0 < c < 0.5 C_{\max}. \tag{15}$$

$d(c)$ is defined to measure the discontinuity of the histogram. If there are obvious peak values which are larger than 0 in the $d(c)$, then the cover image will be considered as embedding secret information.

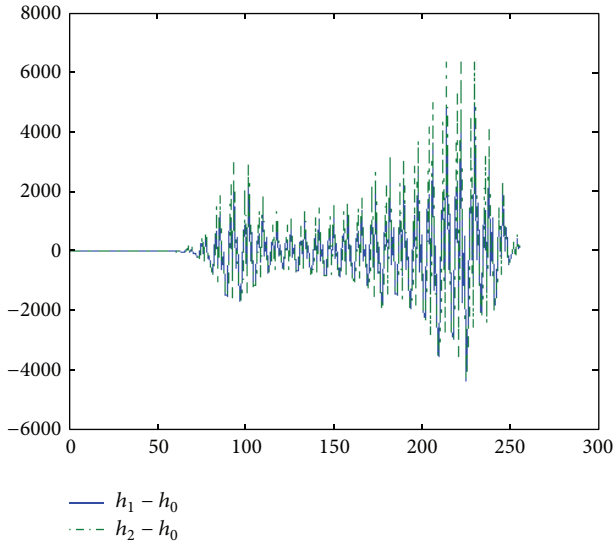


Figure 4: Two kinds of differences histograms.

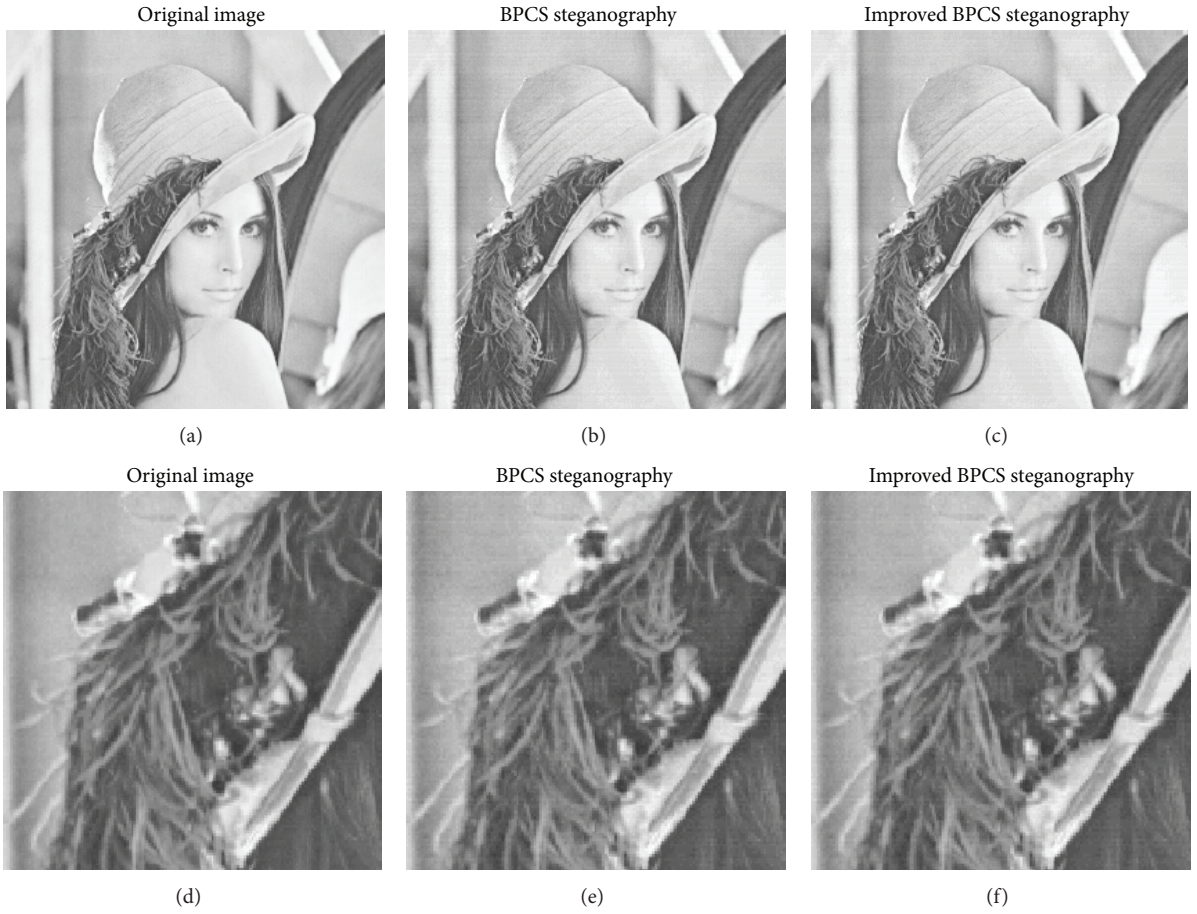


Figure 5: Comparison of BPCS and improved BPCS.

In order to resist BPCS statistical analysis, the basic principle of improved BPCS steganography algorithm adopted different bit-plane with different complexity, which the higher is, the complexity smaller is. The threshold value of bit-plane complexity is computed in the same way as in Section 3.3 (see Table 2).

4. Improved BPCS Steganography Algorithm

(1) Convert the cover image and the secret image from pure binary code (PBC) into canonical Gray code (CGC).

(2) Calculate complexity measures α, β, and γ for each block of each bit-plane of cover image and secret image.

(3) Perform conjugation operation on the "simple" or "informative" blocks of the secret image.

(4) In order to contradict statistical steganalysis, the threshold value θ is calculated.

(5) Perform embedding operation to embed secret image in cover image.

(6) Convert the embedded image from CGC to PBC.

5. Experiment

In this paper, the experiment is done with MATLAB 7. The block size is 8×8, and the peak signal-to-noise ratio (PSNR) and capacity are used to evaluate the quality of the cover image after embedding:

$$\mathrm{PSNR} = 20\log_{10} \frac{255}{\sqrt{(1/N)\sum_{i=0}^{N-1} \left(I_i' - I_i\right)^2}}. \tag{16}$$

I_i is the value of a pixel in the original image and I_i' is the value of the same pixel after embedding, respectively. N is the number of pixels.

Capacity means the number of bits that could be used for embedding.

This paper adopts three different images as samples. The size of image is 512×512.

From Table 1, it can be shown that though capacity is almost the same between BPCS and the proposed method, the PSNR value is much different. It also can be concluded that the proposed approach is better in PSNR value and capacity than existing techniques.

As shown in Figure 4, h_0, h_1, and h_2 are the histograms of original image, BPCS, and improved BPCS.

Table 1: Comparison of PSNR value and capacity with different methods.

		Image		
		Lena	Baboon	Jet
Capacity/bit	BPCS ($\alpha = 0.4$)	951783	984782	942457
	Proposed method	954140	982769	943296
	Mandal and Das [10]	145787	144916	145648
	Juneja and Sandhu [8]	561345	830546	505658
	LSB	467004	720785	463758
PSNR/db	BPCS ($\alpha = 0.4$)	42.86	40.85	41.37
	Proposed method	45.71	42.76	44.39
	Mandal and Das [10]	42.26	38.44	42.60
	Juneja and Sandhu [8]	44.59	36.36	42.50
	LSB	41.01	33.99	39.38

Table 2: Threshold values β, γ, and θ of each bit-plane.

i	0	1	2	3	4	5	6	7
β_t	0.632	0.583	0.534	0.485	0.436	0.387	0	0
γ_t	0.394	0.351	0.308	0.265	0.222	0.179	0	0
θ_i	0.562	0.448	0.334	0.220	0.106	0	0	0

The PSNR of the image obtained by BPCS (Figure 5(b)) and improved BPCS (Figure 5(c)) was 45.71 dB and 42.86 dB. Figures 5(d), 5(e), and 5(f) show the part areas of the images in Figures 5(a), 5(b) and 5(c) respectively. It can be found that there is deterioration in the image obtained by BPCS (Figure 5(e)) but not in the image obtained by improved BPCS (Figure 5(f)). The experiment also shows that improved BPCS can not only embed more data but also keep the image quality higher. In a word, improved BPCS is superior to BPCS in steganography.

6. Conclusion

It is shown that the final embedded image with the proposed method seems to be the same as the original image and locates noise-like regions in a cover image more exactly. It also shows that the algorithm in this paper can withstand statistics analysis while the way of BPCS cannot. Experiments also prove that the proposed approach is better in PSNR value and capacity than existing techniques.

In this paper, some parameters and thresholds are got by experiment. How to determine these values automatically needs to be researched in the future.

Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This research was financially supported by a grant from the National Natural Science Foundation of China (no. 61473329) and the Special Research Foundation of the Fujian Province (Grant no. JK2013062) and was also supported by Fuqing Branch of Fujian Normal University of China (Grant nos. KY2014028 and KY2014029).

References

[1] S. Channalli and A. Jadhav, "Steganography. An art of hiding data," *International Journal on Computer Science and Engineering*, vol. 1, no. 3, pp. 137–141, 2009.

[2] I. Singh, S. Khullar, and S. C. Laroiya, "DFT based image enhancement and steganography," *International Journal of Computer Science and Communication Engineering*, vol. 2, no. 1, pp. 5–7, 2013.

[3] G. Kaur and A. Kochhar, "A steganography implementation based on LSB & DCT," *International Journal for Science and Emerging Technologies with Latest Trends*, vol. 4, no. 1, pp. 35–41, 2012.

[4] T. Narasimmalou and R. A. Joseph, "Robust discrete wavelet transform based steganography," *International Journal of Power Control Signal and Computation*, vol. 4, no. 2, pp. 102–108, 2012.

[5] N. A. Abu, P. W. Adi, and O. Mohd, "Robust digital image steganography within coefficient difference on integer haar wavelet transform," *International Journal of Video & Image Processing and Network Security*, vol. 14, no. 2, pp. 1–8, 2014.

[6] H. Ramezani, F. K. Nia, and M. J. S. Zadeh, "A novel secure steganography in contourlet domain," *International Journal of Trends in Economics, Management & Technology*, vol. 2, no. 5, pp. 27–29, 2013.

[7] K. I. Alsaif and M. M. Saalih, "Text embedding based on contourlet transformation coefficients," *International Journal of Information Technology and Business Management*, vol. 12, no. 1, pp. 49–56, 2013.

[8] M. Juneja and P. S. Sandhu, "An improved LSB based steganography technique for RGB color images," *International Journal of Computer and Communication Engineering*, vol. 2, no. 4, pp. 513–517, 2013.

[9] C. G. Soumi, J. George, and J. Stephen, "Genetic algorithm based mosaic image steganography for enhanced security," *International Journal on Signal and Image Processing*, vol. 5, no. 1, pp. 15–26, 2014.

[10] J. K. Mandal and D. Das, "Colour image steganography based on pixel value differencing in spatial domain," *International Journal of Information Sciences and Techniques*, vol. 2, no. 4, 2012.

[11] S. Arora and S. Anand, "A new approach for image steganography using edge detection method," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 1, no. 3, pp. 626–629, 2013.

[12] P. R. Rudramath and M. R. Madki, "Improved BPCS steganography based novel approach for data embedding," *International Journal of Engineering and Innovative Technology*, vol. 1, no. 3, pp. 156–159, 2012.

[13] E. Kawaguchi and R. O. Eason, "Principle and applications of BPCS-steganography," in *Multimedia Systems and Applications*, vol. 3528 of *Proceedings of SPIE*, pp. 464–473, 1998.

[14] S. S. Khaire and S. L. Nalbalwar, "Review: steganography—bit plane complexity segmentation (BPCS) technique," *International Journal of Engineering, Science and Technology*, vol. 2, no. 9, pp. 4860–4868, 2010.

[15] H. Liu and H. D. Yuan, "Modified algorithm of bit-plane complexity segmentation steganography based on preprocessing," *Journal of Computer Applications*, vol. 32, no. 1, pp. 89–91, 2012.

[16] A. Al-Ataby and F. Al-Naima, "A modified high capacity image steganography technique based on wavelet transform," *The International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 358–364, 2010.

[17] X. Z. Zhang and S. Wang, "Statistical analysis against spatial BPCS steganography," *Journal of Computer-Aided Design & Computer Graphics*, vol. 17, no. 7, pp. 1625–1629, 2005.