International Journal of Security and Its Applications
Vol. 10, No. 7 (2016) pp.83-92
http://dx.doi.org/10.14257/ijsia.2016.10.7.08

An Image Steganography Algorithm based on the Quantitative Features of Higher Order Local Model

Hao Huang* and Zhiping Zhou

Engineering Research Center of Internet of Things Technology Applications Ministry of Education, Wuxi, 214122, China.
huanghao1928jn@163.com

Abstract

HUGO is the content-based adaptive steganography method for spatial images which can approximately preserve the joint statistic of differences between up to four neighboring pixels in four different directions. But the steganalysis method based on the higher order local model can fail HUGO. In view of the above problem, an improved steganography is proposed. Firstly, by analyzing the higher order local model, the distortion function is defined based on the quantitative MINMAX features. Then, combined with the theoretical framework of the Gibbs construction in steganography, the improved image steganography algorithm is proposed. The experimental results show that the proposed algorithm can not only resist the detection of the steganalysis method based on the quantitative MINMAX features , but also resist the detection of the steganalysis method based on the hybrid quantitative MINMAX features.

Keywords*: information hiding; digital steganography; image steganography; security*

1. Introduction

Compared with many steganography algorithms in the transform domain, most of the spatial domain steganography algorithms have the following advantages, *i.e.*, the embedding method is more simple and the embedding capacity is much larger. Therefore, researches on the spatial domain steganography algorithms are very extensive. These spatial domain steganography algorithms can be broadly divided into two categories. One is the traditional spatial domain techniques which adopt fixed means to embed secrets in the whole cover image without considering the correlation of cover image. The other is the content-based adaptive steganography.

The traditional spatial domain techniques focus on the visual imperceptivity. The most common algorithm is called LSB (Least Significant Bit substitution). The secret data is embedded in the fixed length LSB of each pixel. The LSBM (Least Significant Bit Matching) method is an improved one of LSB. The embedding scheme of the LSBM algorithm is ± 1 embedding scheme. The cover pixel value is incremented or decremented by 1, at random. Then, an improved method which is called the $\pm K$ method is proposed based on this method.

Along with the development of image steganography technology, people gradually realize that the security criteria *i.e.*, visual imperceptivity is not enough. LSB and the above different LSB extension methods can be detected by many steganalytic methods, such as the RS analysis [1], SPA analysis [2] and WS analysis [3]. Statistical undetectability which is the security criteria of steganography algorithms has caused the attention of researchers. The method called MPSteg-color method is a heuristic algorithm [4]. The cover image is decomposed into a group of redundant units based on the content of the image. Then the secret data is embedded in the coefficients of the various

* Corresponding author

ISSN: 1738-9976 IJSIA

redundant units. The EA (Edge Adaptive) Algorithm method is another heuristic algorithm [5]. According to the content of the image, the cover image is divided into the edge region, the smooth region and the texture region. Then, the secret data is embedded into the edge region. There are still many content-based adaptive steganography algorithms. But most of them are the same as those above-mentioned algorithms which only consider the low dimensional statistical features and do not consider the high dimensional statistical features. Most of the existing steganalysis algorithms have good results for the analysis of steganography algorithms based on the low dimensional models. However, because the number of training samples is limited and the calculation is too complex, the steganography algorithms based on the high dimensional models can not be effectively detected. Therefore, the design of the content-based adaptive steganography algorithms using the high dimensional models is a better idea [6]. HUGO (Highly Undetectable steGO) [6] is a spatial steganography algorithm in which the high dimensional model is used. Based on the SPAM (subtractive pixel adjacency matrix), the cost of each pixel is computed. Then the distortion function is constructed. Finally, the secret data is embedded by using the STC (syndrome-trellis codes) [7] coding algorithm. HUGO can effectively preserve the joint statistic of first-order differences between up to four neighboring pixels in four different directions. Filler et al. proposed a theoretical framework which permitted us to consider spatially dependent embedding changes [8]. A heuristic algorithm was proposed which is called HUGO-BD (Bounding Distortion) based on the distortion function that is allowed to be arbitrary. Li *et. al.*, analyzed the influence of different embedding schemes [9]. Then, an improved HUGO steganography algorithm was proposed based on three embedding rules. There are many other similar content based adaptive steganography algorithms. However, considering these high dimensional statistical features is not enough to protect the statistical undetectability. Fridrich *et. al.*, proposed a newly steganalysis method based on HOLMES (Higher-Order Local Model Estimators of Steganographic changes) which can effectively analyze the steganographic algorithm HUGO [10,11]. It is a great threat to the steganography algorithms which strives to maintain a high dimensional feature vector. Therefore, a spatial steganography method which can resist the detection of the newly steganalysis method based on HOLMES should be proposed to break the dilemma of the research on the spatial steganography algorithms.

2. Proposed Image Hiding Scheme

The design idea of the steganography algorithm HUGO is as follows. Firstly, the steganalysis method based on the SPAM features is analyzed. Then, a distortion function is constructed based on the SPAM features. Finally, HUGO is proposed. In this paper, the design of the proposed scheme is similar to the design of HUGO. First of all, the HOLMES Strategy is analyzed. Secondly, an improved distortion function is constructed based on the quantized MINMAX feature vector. At last, combined with the theoretical framework of the Gibbs construction, the improved image hiding scheme is proposed.

2.1. The HOLMES Strategy

The HOLMES strategy mainly presents two types of feature combinations with better performance. One is the quantized MINMAX feature vector which only contains the same order pixel residuals of the higher-order local models. The other is the hybrid quantized MINMAX feature vectors which contain different order pixel residuals of the higher-order local models.

The second-order residuals along the horizontal is computed by the formula $r_{ij}^{(2)} = x_{i,j-1} - 2x_{ij} + x_{i,j+1}$. In the same way, the second-order residuals along the vertical, diagonal and minor diagonal direction are defined as follows:

$$r_{ij}^{v} = x_{i-1,j} - 2x_{ij} + x_{i+1,j}, \tag{1}$$

$$r_{ij}^{d} = x_{i-1,j-1} - 2x_{ij} + x_{i+1,j+1}, \tag{2}$$

$$r_{ij}^{m} = x_{i-1,j+1} - 2x_{ij} + x_{i+1,j-1} \tag{3}$$

Then, the MIN and MAX residuals can be formed:

$$r_{ij}^{MIN} = trunc_{T}(\min\{r_{ij}^{h}, r_{ij}^{v}, r_{ij}^{d}, r_{ij}^{m}\}), \tag{4}$$

$$r_{ij}^{MAX} = trunc_{T}(\max\{r_{ij}^{h}, r_{ij}^{v}, r_{ij}^{d}, r_{ij}^{m}\}) \tag{5}$$

The truncated function is represented as $trunc_{T}(\mathrm{g})$. And the symbol T is the threshold.

$$trunc_{T}(x) = \begin{cases} T & ,\text{if} \quad x > T \\ -T & ,\text{if} \quad x < \text{-}T \\ x & ,\text{else} \end{cases} \tag{6}$$

In order to reduce the dimensions of the feature, a scalar quantizer is used as follows.

$$Q_{q}(x) = \mathrm{floor}\left(\frac{r_{ij}}{q}\right) \tag{7}$$

At last, the famous quantized MINMAX feature vector is obtained:

$$\mathbf{F}^{\mathrm{QUANT,q}} = (C^{\mathrm{h}}(Q_{q}(\mathbf{R}^{\mathrm{MIN}})) + C^{\mathrm{v}}(Q_{q}(\mathbf{R}^{\mathrm{MIN}})), C^{\mathrm{h}}(Q_{q}(\mathbf{R}^{\mathrm{MAX}})) + C^{\mathrm{v}}(Q_{q}(\mathbf{R}^{\mathrm{MAX}}))) \tag{8}$$

The horizontal co-occurrence matrix of order m is defined as follows:

$$C^{h}_{d_1 \mathrm{L}\, d_m}(\mathbf{R}) = \Pr(r_{ij} = d_1 \wedge \mathrm{L} \wedge r_{i,j+m-1} = d_m), d_1, \mathrm{K}, \mathrm{d}_m \in [-T, \mathrm{K}, T] \tag{9}$$

The co-occurrence matrixes of the other three directions are defined analogically. The order m of the quantized MINMAX feature vector is 3.

In this paper, an improved distortion function is defined according to the quantized MINMAX feature vector. Then, an improved steganography method is proposed which can effectively preserve the statistic of the quantized MINMAX feature vector. Since the hybrid quantized MINMAX feature vectors consist of multiple quantized MINMAX features, this proposed method can also resists the attacks from the steganalysis algorithm which is based on the hybrid quantized MINMAX feature vectors.

2.2. Improved Embedding Distortion Function

For the image content adaptive steganography algorithms, the purpose of constructing an embedding distortion model is to maintain a certain statistical property by minimizing the embedding distortion.

In this paper, we first give the following definitions:

$$C(\mathbf{R}^{\mathrm{MIN}}) = C^{\mathrm{h}}(Q_{q}(\mathbf{R}^{\mathrm{MIN}})) + C^{\mathrm{v}}(Q_{q}(\mathbf{R}^{\mathrm{MIN}})), \tag{10}$$

$$C(\mathbf{R}^{\mathrm{MAX}}) = C^{\mathrm{h}}(Q_{q}(\mathbf{R}^{\mathrm{MAX}})) + C^{\mathrm{v}}(Q_{q}(\mathbf{R}^{\mathrm{MAX}})), \tag{11}$$

Then, the quantized MINMAX feature vector can be written as follows:

$$\mathbf{F}^{\mathrm{QUANT,q}} = (C(\mathbf{R}^{\mathrm{MIN}}), C(\mathbf{R}^{\mathrm{MAX}})) \tag{12}$$

In order to highlight the more sensitive part of the co-occurrence matrix for steganalysis, the improved embedding distortion function is designed by combining with the weighted function as follows:

$$D(\mathbf{X},\mathbf{Y}) = \sum_{d_1,d_2,d_3=-T}^{T} [\omega(d_1,d_2,d_3)\left|C^{\mathbf{X}}(\mathbf{R}^{\mathrm{MIN}}) - C^{\mathbf{Y}}(\mathbf{R}^{\mathrm{MIN}})\right| + \omega(d_1,d_2,d_3)\left|C^{\mathbf{X}}(\mathbf{R}^{\mathrm{MAX}}) - C^{\mathbf{Y}}(\mathbf{R}^{\mathrm{MAX}})\right|] \quad (13)$$

The form of the following weight function $\omega(d_1,d_2,d_3)$ comes from the literature [6]

$$\omega(d_1,d_2,d_3) = \frac{1}{[\sqrt{d_1^2+d_2^2+d_3^2}+\sigma]^{\gamma}} \quad (14)$$

where $\sigma,\gamma > 0$ are parameters that should be determined in order to minimize the detectability. These parameters are set reasonably in the following Section 3.1.

2.3. Improved Steganography Algorithm

Combining the above improved embedding distortion function with the theoretical framework of the Gibbs construction, a conclusion can be obtained that the neighborhood system [8] here is formed by 7×7 neighborhoods , thus the cover image can be divided into 16 square sub-lattices in which embedding was carried out independently.

The costs of embedding change are defined as

$$\rho_{i,j} = D(\mathbf{X},\mathbf{Y}^{i,j}), \quad (15)$$

where $\mathbf{Y}^{i,j}$ is the stego image obtained by embedding secret data in the (i,j) th pixel of cover image $\mathbf{X}$.

The proposed steganography algorithm is as follows:

(1) The cost of embedding change about each pixel in each sub-lattice is calculated separately based on the improved embedding distortion function proposed in Section 3.1;

(2) Suppose there are m bits of secret data needing to be embedded in the cover image. Then each sub-lattice should be embedded $m/16$ bits of secret data. Therefore, the general embedding distortion about each sub-lattice is calculated by minimizing the detectability;

(3) The general embedding distortion can be obtained according to the embedding distortion of each sub-lattice.

(4) Finally, the secret data should be optimally embedded based on the theory of the Gibbs sampling.

3. Experiments

All images used in this experiment are from BOSSbase 1.01. The image library contains 10000 pieces of gray image originally acquired by different digital cameras in the RAW format. All images are processed to the same size of 512×512 pixels. The superior performance of the proposed algorithm is demonstrated by two aspects: comparison of stego image quality and classification results based on different features. In the first category, eight standard images such as Lena, Baboon, Airplane, et.al are used as covers. There are 20 different random bit streams used as secrets. In the second category, there are 4000 images which are randomly selected from the image library as the experimental images. Then, these 4000 experimental images are divided into a training set of 2000 images and a testing set of 2000 images. Finally, the training set and

the testing set respectively choose 1000 images as the cover image. In order to accurately compare the proposed method with HUGO-BD [8], HUGO-AVG-FILTR [9] and S-UNIWARD-AVG-FILTR [9], these four methods are combined with the binary ± 1 steganography algorithm. The secret data is respectively embedded in each cover image with the relative payload sequence [0.1, 0.2, 0.3, 0.4, 0.5]. Four kinds of complete training samples and testing samples can be obtained. In addition, the Ensemble Classifier proposed by literature [10] can be better suitable for high dimensional image steganalysis compared with Support Vector Machine. In order to prove the superiority of the proposed steganography algorithm, this paper adopts the Ensemble Classifier proposed in literature [10].

3.1. Initialization of Parameters

The following parameters need to be initialized before embedding secret data in the proposed algorithm: the threshold of the truncated function T , the quantitative order q and the parameters of the weight function σ and γ .

According to the above improved steganography algorithm proposed in section 2.3, we can draw two conclusions as follows: (a) when the parameter $T = 30$, the steganalysis model has more than 10^6 features; (b) when the parameter $T = 90$, the steganalysis model has more than 10^7 features. However, the classification error rate has no obvious change, no matter $T = 30$ or $T = 90$ for the steganalysis algorithm based on the HOLMES. Since the increase of feature dimensions may cause the increase of time in the process of embedding secret data spend, thus we choose $T = 30$ in this paper.

Table 1. Value of MMD(lower is better) Plotted against Parameters σ and γ

		γ			
		2^{-1}	2^0	2^1	2^2
σ	10^{-2}	0.000605	0.000356	0.000856	0.000254
	10^{-1}	0.000527	0.000281	0.000237	0.000203
	10^0	0.000109	0.000053	0.000017	0.000058
	10^1	0.001533	0.000036	0.000023	0.000103

In order to choose suitable parameters σ and γ of the weight function, a grid optimization method is used in this paper where $(\sigma,\gamma) \in \{(10^k, 2^j) \mid k \in \{-2, \mathrm{L}\ ,1\}, j \in \{-1, \mathrm{L}\ ,2\}\}$. Then, the relative payload is fixed to 0.2bpp in order to reduce the complexity of the grid optimization method. The undetectability is evaluated by Maximum Mean Discrepancy [12]. The experimental results of the grid optimization method are shown in Table 1. All values keep six digits after the decimal point.

Obviously, when $\sigma = 1, \gamma = 2$, the corresponding MMD is the minimum. Therefore, we should set $\sigma = 1, \gamma = 2$. According to the literature [10,11], when the quantitative order $q = 2$, the performance of the steganalysis algorithm based on the quantized MINMAX feature vector is the best compared with other values of the quantitative order. Since the proposed algorithm mainly focus on defeating this steganalysis algorithm in this paper, the quantitative order q is set $q = 2$.

Because the classifier used in this paper is proposed in literature [10], the corresponding parameters should set to the optimal parameters.

3.2. Comparison of Stego Image Quality

The objective quantitative measures used for the comparison of stego image quality are as follows:

The Peak Signal Noise Ratio (PSNR) is defined as:

$$\text{PSNR}=10\times\log_{10}\left\{\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}255^2\Big/\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-I'(i,j)]^2\right\} \tag{16}$$

where $I(i,j)$ and $I'(i,j)$ are corresponding pixel intensities of the original and stego images respectively.

The Structural Similarity Index (SSIM) [13] is defined as:

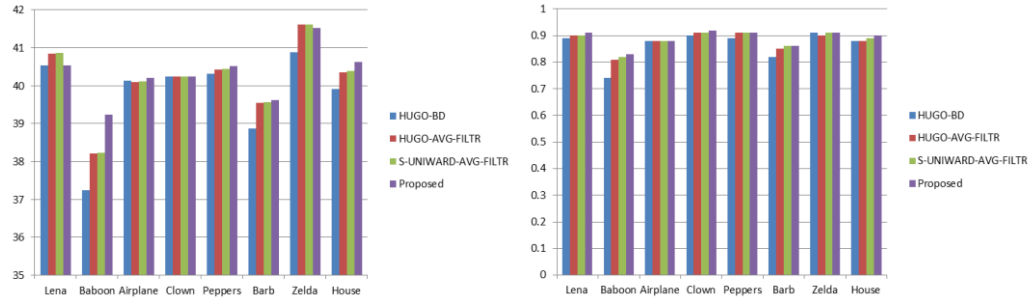
$$\text{SSIM}(x,y)=(2\hat{x}\hat{y}+c_1)(2\sigma_{xy}+c_2)\big/(\hat{x}^2+\hat{y}^2+1)(\sigma_x^2+\sigma_y^2+c_2) \tag{17}$$

where x and y are corresponding original and stego images. $\hat{x}$ and $\hat{y}$ are the corresponding averages of x and y respectively. σ_x^2 and σ_y^2 are the corresponding variances of x and y, σ_{xy} is the covariance of x and y. c_1 and c_2 are appropriate constants and are set refer to literature [13].

Table 2. Values of the Quality Measure PSNR and SSIM Obtained by Various Content based Adaptive Steganography Algorithms

Cover-images	HUGO-BD		HUGO-AVG-FILTR		S-UNIWARD-FILTR		Proposed method	
(512×512)	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	40.5364	0.89	40.8522	0.90	40.8615	0.90	40.5267	0.91
Baboon	37.2358	0.74	38.2123	0.81	38.2251	0.82	39.2301	0.83
Airplane	40.1284	0.88	40.1023	0.88	40.1093	0.88	40.2110	0.88
Clown	40.2351	0.90	40.2454	0.91	40.2481	0.91	40.2356	0.92
Peppers	40.3157	0.89	40.4211	0.91	40.4351	0.91	40.5133	0.91
Barb	38.8615	0.82	39.5412	0.85	39.5564	0.86	39.6124	0.86
Zelda	40.8741	0.91	41.6124	0.90	41.6210	0.91	41.5234	0.91
House	39.9211	0.88	40.3518	0.88	40.3818	0.89	40.6232	0.90

Tables 2 shows the experimental results of these eight standard images comparing PSNR and SSIM by various content-based adaptive steganography algorithms. PSNRs and SSIMs are the average results. It can be seen that the proposed algorithm can maintain the quality of stego images compared with the other content-based adaptive steganography method. This conclusion is further illustrated by graphs in Figure 1.



(a) (b)

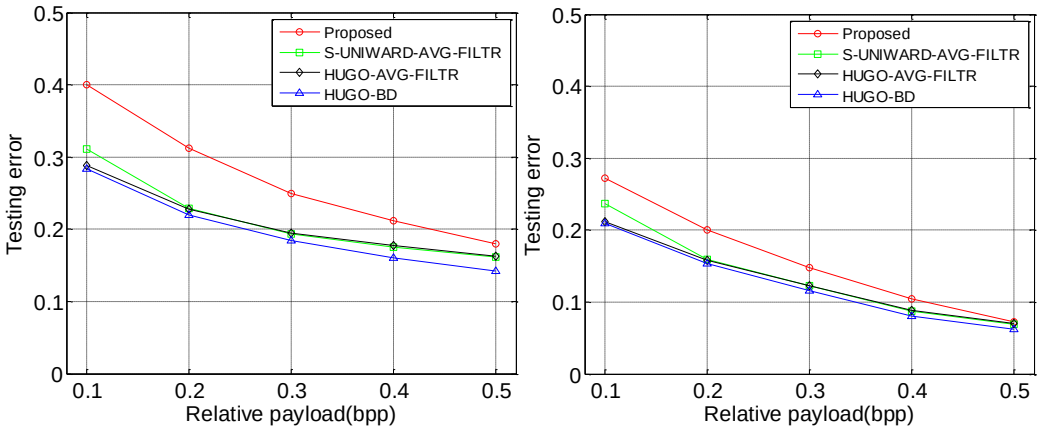
Figure 1. Comparative (a) PSNR and (b) SSIM Values Obtained by HUGO-BD, HUGO-AVG-FILTR, S-UNIWARD-AVG-FILTR and the Proposed Method

3.3. Classification Results based on Different Features

The chosen accuracy measure in this paper is the minimal average decision error, defined as follows:

$$P_{\mathrm{E}} = \min \frac{1}{2}(P_{\mathrm{F_p}} + P_{\mathrm{F}_n}) \ , \tag{18}$$

where $P_{\mathrm{F_p}}$ stands for the probability of false alarm and $P_{\mathrm{F_n}}$ stands for the probability of missed detection.



(a) (b)

Figure 2. (a) Classification Results based on Quantization MINMAX Feature Classifier

(b) Classification results based on hybrid quantization MINMAX feature classifier.

Since there are two types of quantitative feature set proposed in literature [10] to detect HUGO. In order to highlight the advantages of the improved steganography algorithm proposed in this paper, HUGO-BD, HUGO-AVG-FILTR, S-UNIWARD-AVG-FILTR and the proposed method need to be respectively detected by the classifier based on the quantitative MINMAX feature and the classifier based on the hybrid quantitative MINMAX feature .The experimental results are shown in Figure 2.

The embedding distortion model of HUGO-BD, HUGO-AVG-FILTR and S-UNIWARD-AVG-FILTR are not additive. Thus, these three algorithms can embed secret data better than HUGO because of considering spatially dependent embedding changes.

It can be seen obviously from Figure 2 (a) that, compared with those algorithms proposed in literature [8] and literature [9], the proposed algorithm can better resist the attack from the steganalysis method based on the quantitative MINMAX feature. The lower the relative load is, the more obvious the superiority is.

Similarly, it can be seen from Figure 2 (b) that, compared with those algorithms in literature [8] and literature [9], the proposed algorithm can better resist the attack from the steganalysis method based on the hybrid quantitative MINMAX feature. But this superiority is not as obvious as that in Figure 2 (a). The reason of this phenomenon is that the hybrid quantitative MINMAX feature not only contains the quantitative MINMAX feature, but also contains other high-order residual features. This phenomenon is also consistent with the view in literature [10], *i.e.*, the steganalysis method based on a large feature set which is a union of many diverse feature set can perform better in detecting steganography algorithms.

4. Conclusion

Based on the HOLMES strategy, an improved steganography algorithm is proposed in this paper. This algorithm is designed specifically for defeating the attacks from the steganalysis method based on the quantitative MINMAX feature. Experimental results show that the proposed method can not only effectively resist the detection of the steganalysis method based on the quantitative MINMAX feature, but also can resist the attacks from the steganalysis method based on the hybrid quantitative MINMAX feature. It provides a new research idea of designing a steganography algorithm in spatial domain for the next.

Acknowledgements

This work was supported by the Fundamental Research Funds for the Central Universities (JUSRP51510).

References

[1] J. Fridrich, M. Goljan and R. Du, "Reliable detection of LSB steganography in grayscale and color images", Proceedings of ACM, Special Session on Multimedia Security and Watermarking, Ottawa, Canada, **(2001)** October 27-30.
[2] S. Dumitrescu, X. Wu and Z. Wang, "Detection of LSB steganography via sample pair analysis", Signal Processing, IEEE Transactions on 7, vol. 51, **(2003)**, pp. 1995-2007.
[3] J. Fridrich and M. Goljan, "On estimation of secret message length in LSB steganography in spatial domain", Proceedings of International Society for Optics and Photonics, in Electronic Imaging 2004, **(2004)** June 23–34.
[4] G. Cancelli and M. Barni, "MPSteg-color: data hiding through redundant basis decomposition", Information Forensics and Security, IEEE Transactions on 3, vol. 4, **(2009)**, pp. 346-358.
[5] W. Luo, F. Huang and J. Huang, "Edge adaptive image steganography based on LSB matching revisited", Information Forensics and Security, IEEE Transactions on 2, vol. 5, **(2010)**, pp. 201-214.
[6] T. Pevný, T. Filler and P. Bas, "Using high-dimensional image models to perform highly undetectable steganography", Proceedings of Information hiding, Calgary, Canada, **(2010)** January 161-177.
[7] T. Filler, J. Judas and J. Fridrich, "Minimizing embedding impact in steganography using trellis-coded quantization", Proceedings of International Society for Optics and Photonics, in Electronic Imaging, **(2010)** February 754105-754105
[8] T. Filler and J. Fridrich, "Gibbs construction in steganography", Information Forensics and Security, IEEE Transactions on 4, vol. 5, **(2010)**, pp. 705-720.
[9] B. Li, S. Tan, M. Wang and J. W. Huang, "Investigation on cost assignment in spatial image steganography", Information Forensics and Security, IEEE Transactions on 8, vol. 9, **(2014)**, pp. 1264-1277.
[10] J. Fridrich, J. Kodovský, V. Holub and M. Goljan, "Steganalysis of content-adaptive steganography in spatial domain", Proceedings of Information Hiding, Prague, Czech Republic, **(2011)** January 102-117.
[11] J. Fridrich, J. Kodovský, V. Holub and M. Goljan, "Breaking HUGO–the process discovery", Proceedings of Information Hiding, Prague, Czech Republic, **(2011)** January 85-101.
[12] T. Pevný and J. Fridrich, "Benchmarking for steganography", Proceedings of Information Hiding, Sana Barbara, USA, **(2008)**, January 251-267.
[13] P. Bedi, R. Bansal and P. Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance", Computers & Electrical Engineering 2, vol. 39, **(2013)**, pp. 640-654.

Authors

Hao Huang, Master Degree Candidate; Institution: Engineering Research Center of Internet of Things Technology Applications Ministry of Education, jiangnan university; Address: Binhu District Road No.1800, Wuxi Jiangsu, China; Email: huanghao1928jn@163.com; Subject: image steganography algorithm, information hiding.

Zhiping Zhou, Professor; Institution: Engineering Research Center of Internet of Things Technology Applications Ministry of Education, jiangnan university; Address: Binhu District Road No.1800, Wuxi Jiangsu, China; Email: zzp@jiangnan.edu.cn; Subject: detection technique and automatic device, information security.