International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.265-274
http://dx.doi.org/10.14257/ijsia.2016.10.9.25

An Image Spatial Domain Steganography Algorithm with High Payload, Commendable Perceptual Quality and High Statistical Un-detectability

Hao Huang* and Zhiping Zhou

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

Abstract

The Octonary PVD algorithm is the method that simultaneously achieves three contradicting objectives, high payload, commendable perceptual quality and high statistical un-detectability. However, the Octonary PVD algorithm has a major defect that it does not embed the secret data in the optimum locations because it does not consider the use of different pixel groups will have different effects on the statistical un-detectability and payload of the stego image in the process of embedding. In view of the above problem, an improved steganography is proposed. An improved objective function which is used by the PSO module is defined at first in this proposed method. Then, an improved data hiding scheme is proposed. The proposed algorithm is an improved method based on the Octonary PVD algorithm, and the improved objective function which be used by the PSO module is set in such a way that both perceptual quality and statistical un-detectability are considered. This proposed algorithm has high statistical un-detectability and high payload with commendable visual quality. An extensive experimental evaluation has demonstrated the excellent performance of the proposed algorithm compared with other existing image spatial domain steganography algorithms.

Keywords*: image steganography; adaptive data hiding; high capacity; statistical un-detectability*

1. Introduction

With the rapid development of digital media technology, more and more attention has been paid to the steganography scheme based on digital media. Digital image is one of the most widely used digital media. The development of the steganography algorithm based on digital image is very fast. The image steganography algorithm is divided into two categories, which are spatial domain steganography and transform domain steganography. 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.

Least Significant Bit (LSB) substitution [1] is one categories of the image spatial domain steganography algorithm. The LSB substitution is the most common algorithm. The secret data is embedded in the fixed length LSB of each pixel. However, this method can be easily detected by many reported steganalytic techniques such as the regular/singular groups (RS) analysis [2], sample pair analysis (SPA) analysis [3] and the weighted stego (WS) analysis [4]. The Least Significant Bit Matching (LSBM) method is an improved one of LSB. The cover pixel value is incremented or decremented by ± 1, at

* Corresponding author

ISSN: 1738-9976 IJSIA

random. Thus, the LSBM algorithm is also called embedding scheme. The common methods that used to detect LSB substitution are ineffective detecting the LSBM. Many steganalytic techniques (*e.g.*, [5-7]) have been proposed to detect the LSBM.

Pixel Value Differencing (PVD) scheme [8] is another categories of the image spatial domain steganography algorithm. The number of secret bits that should be embedded is determined based on the difference value between two neighbor pixels in PVD scheme. Larger the difference, more secret information should be embedded. In order to further improve the perceptual quality of the stego image, Hong [9] proposed a method based on the Human Vision System (HVS). Chang [10] proposed an inspired method which uses tri-way pixel-value differencing (TPVD). This algorithm can effectively improve the payload of secret information in the premise of keeping the visual quality of the image containing no obvious change.

Most of the existing image spatial domain steganography algorithms have a common point, that is, a pseudo random sequence is employed, which decides the order in which the pixels are selected to embed the secret data. The selection of the pseudo random sequence is independent of the content of the cover image. According to the paper [11], most steganography algorithms which employ a pseudo random sequence use some smooth regions to hide the secret data in the condition that the sharp edge regions are not fully utilized. Thus, this defect can reduce the perceptual quality and statistical un-detectability of the stego image. Aiming at this defect, the Octonary PVD (OPVD) method [11] was proposed. Firstly, each pixel with all of its neighbors in all eight directions is used as a group in the OPVD algorithm. Then, edge regions are identified according to the pixel difference of each pixel group. Finally, the maximum payload is determined according to the range table. The defect of the OPVD algorithm is that the standard for the edge region identification is too loose. The use of different pixel groups will have different effects on the statistical un-detectability and payload of the stego image in the process of embedding. However, the OPVD method does not consider this. A spatial domain based image steganography algorithm using Particle Swarm Optimization (PSO) was proposed in paper [12]. In this algorithm, the cover image is divided into equal sized image blocks at first. Secondly, according to the length of the secret data that need to be embedded, the secret information of equal length is determined to be embedded in each block. Then, PSO is used to find the optimal embedding position in each image block. Finally, these secret data are embedded in the optimal embedding position using the operation of optimal pixel intensity quantization. The defect of the algorithm is that some image block may be smooth region. The equal embedded operation of the original algorithm can reduce the visual quality and the statistical un-detectability of the stego image.

This paper mainly focuses on the defect that the paper [11] fails to embed the secret data in the optimal location. Combined with the PSO method, an improved steganography scheme based on OPVD is proposed in this paper. Compared with other existing image spatial domain steganography algorithms, the proposed scheme has higher statistical un-detectability, commendable perceptual quality and high payload through an extensive experiments evaluation.

2. Proposed Steganography Scheme

The purpose of this paper is to find optimum locations adaptively in the cover image to hide the secret data. Under the condition of maintaining the visual quality of stego image, higher statistical un-detectability and payload are the advantages of the proposed algorithm. The following subsections discuss the improved objective function and the scheme for secret data hiding.

2.1. Improved Objective Function

The objective function which be used by the PSO module is set in such a way that both perceptual quality and statistical un-detectability are acceptable. The perceptual quality of the stego image is calculated using Structural Similarity Index (SSIM) [12] which is defined as follows:

$$\mathrm{SSIM}(x,y)=\frac{(2\hat{x}\hat{y}+c_1)(2\sigma_{xy}+c_2)}{(\hat{x}^2+\hat{y}^2+1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{1}$$

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 [12].

The statistical un-detectability of the stego image is calculated based on the HOLMES strategy [13]. The second-order residuals along the horizontal is computed by the formula $r_{xy}^{(2)}=P_{(x-1,y)}-2P_{(x,y)}+P_{(x+1,y)}$. In the same way, the second-order residuals along the vertical, diagonal and minor diagonal direction are as follows:

$$\begin{cases} r_{xy}^{v}=P_{(x,y-1)}-2P_{(x,y)}+P_{(x,y+1)} \\ r_{xy}^{d}=P_{(x-1,y-1)}-2P_{(x,y)}+P_{(x+1,y+1)} \\ r_{xy}^{m}=P_{(x-1,y+1)}-2P_{(x,y)}+P_{(x+1,y-1)} \end{cases} \tag{2}$$

The truncated function is represented by $trunc_T(g)$. And the symbol T is the threshold.

$$trunc_T(x)=\begin{cases} T & ,if \quad x>T \\ -T & ,if \quad x<-T \\ x & ,else \end{cases} \tag{3}$$

The horizontal co-occurrence matrix of order 3 is defined as follows:

$$C_{d_1,d_2,d_3}^{h}(R)=\Pr(r_{xy}=d_1\wedge r_{x,y+1}=d_2\wedge r_{x,y+2}=d_3) \tag{4}$$

The co-occurrence matrixes of the other three directions are defined analogically. $d_1,d_2,d_3\in[-T,\mathrm{K},T]$.

Thus, the statistical un-detectability of the stego image is calculated as follows:

$$D(\boldsymbol{X},\boldsymbol{Y})=\sum_{d_1,d_2,d_3=-T}^{T}\left[\omega(d_1,d_2,d_3)\left|C_{\boldsymbol{X}}^{k}(R)-C_{\boldsymbol{Y}}^{k}(R)\right|\right] \tag{5}$$

The $k\in\{h,v,d,m\}$. The form of the following weight function $\omega(d_1,d_2,d_3)$ comes from the literature [14]:

$$\omega(d_1,d_2,d_3)=\frac{1}{\left[\sqrt{d_1^2+d_2^2+d_2^3}+\sigma\right]^{\gamma}} \tag{6}$$

where $\sigma,\gamma>0$ are parameters that should be determined in order to minimize the detectability. These parameters are set to $\sigma=1,\gamma=1$ [14].

The $D(\boldsymbol{X},\boldsymbol{Y})$ represents the embedding distortion function. The bigger the $D(\boldsymbol{X},\boldsymbol{Y})$ value is, the lower the statistical un-detectability is. The aim of the proposed algorithm is to minimize $D(\boldsymbol{X},\boldsymbol{Y})$ and to maximize the SSIM index between the cover and the stego images. Thus, the objective function F minimized by PSO is defined as follows:

$$F = \gamma(1-\mathrm{SSIM}(f, f')) + (1-\gamma)D(x, y) \quad (7)$$

where γ is a weighting constant which has been calculated experimentally. f and f' are corresponding blocks in original and stego images.

2.2. Data Hiding Algorithm

The detailed principle of PSO can refer to the paper [15, 16]. The pseudo code of the proposed steganography algorithm is defined as follows:

Step 1. Read cover image I and secret image data array W, $len \leftarrow \mathrm{length}(W)$

Step 2. Dividing cover image into sub-blocks:

- Cover image I is divided into a number of 3×3 non-overlapping ceil-blocks, namely, $CB_l, l = 1,\ldots,r$. The maximum payload of each ceil-block is computed according to Table 1, namely, C_l. $C_l \in \{24,25,\ldots,55,56\}$.

- Dividing these ceil-blocks that have same payload into a same sub-block according to the order of the small to large, namely, $SB_i, i = 1,2,\ldots,33$. The total payload of the sub-block SB_i is a_i, $i = 1,2,\ldots,33$.

Step 3. $j \leftarrow 33$

While $(len > a_j)$

{

Embedding the secret information which have the length of a_j into the sub-block SB_j using the embedding method of Step 5

$len \leftarrow len - a_j$

$j \leftarrow j - 1$

}

Step 4. Using PSO:

$m \leftarrow \lfloor len/(j+23) \rfloor$, $n \leftarrow len \bmod (j+23)$

Initialize constants: *ns* (number of particles), *iters* (maximum no. of iterations), *iw* (inertia weight factor), c_1 and c_2 (cognitive and social acceleration factors), r_1 and r_2 (random numbers in the range $(0,1)$)

- If $(n = 0)$ then

{

Set the dimensionality of each particle equal to the value of m. Then, find the optimal particle by using the PSO method in sub-block SB_j. Thus, the optimum locations could be obtained. }

- If $(n \neq 0)$ then

{

Find one part of the optimum locations l_1 by performing the operation that is same as the above operation which $n = 0$.

Find the other part of the optimum locations l_2 from the residual elements of sub-block SB_j by performing the operation that is almost same as the above operation which $n = 0$ except the dimensionality of each particle is 1. }

Step 5. Embedding secret data: These secret data are embedded in the optimal embedding position using the method that proposed in paper [11]. In addition, the secret data is embedded in each pixel pair of each ceil-block according to the sequence of the payload from large to small.

Step 6. Return stego image I'.

Table 1. Range Table

Range [lower upper]	Hiding Capacity in Bits
[0 7]	3
[8 15]	3
[16 31]	4
[32 63]	5
[64 127]	6
[128 255]	7

3. Experiments

All images that have been used in this experiment are from BOSSbase 1.01. This 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 pixels. The superior performance of the proposed algorithm is demonstrated by two aspects: commendable image perceptual quality and good statistical un-detectability. In the first category, eight standard images such as Lena, Baboon, Airplane, *et al.* were used as covers. There were 20 different random bit streams were 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. 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].

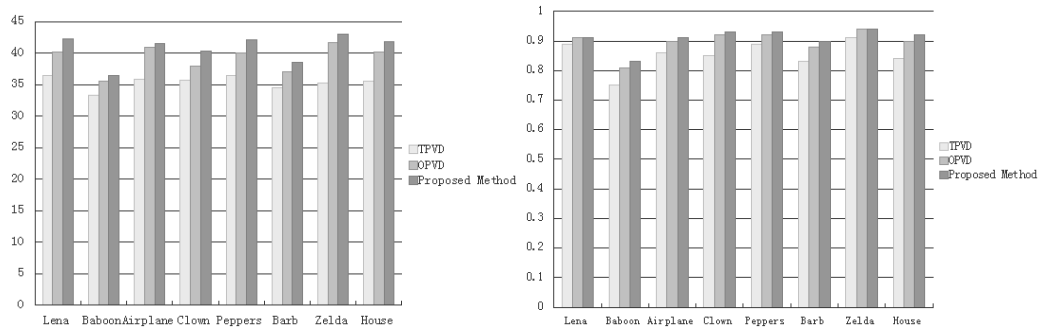
3.1. The Perceptual Quality Analysis

The objective quantitative measures used for comparison of stego image quality are Peak Signal Noise Ratio (PSNR) and Structural Similarity Index (SSIM). Tables 2 shows the experimental results on 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 clearly seen that the proposed method can maintained the commendable image perceptual quality. This conclusion is further illustrated by graphs in Figure 1.

Table 2. Values of the PSNR and SSIM Obtained by Various Edge-based Steganography Algorithms

Cover-images	TPVD		OPVD		Proposed method	
(512×512)	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	36.4217	0.89	40.2103	0.91	42.3571	0.91
Baboon	33.3547	0.75	35.5124	0.81	36.4120	0.83
Airplane	35.8177	0.86	40.9111	0.90	41.5684	0.91

Clown	35.7301	0.85	38.0213	0.92	40.4212	0.93
Peppers	36.5146	0.89	40.0730	0.92	42.1251	0.93
Barb	34.4628	0.83	37.1023	0.88	38.5207	0.90
Zelda	35.2327	0.91	41.6924	0.94	43.0183	0.94
House	35.5074	0.84	40.2418	0.90	41.8455	0.92



(a) (b)

Figure 1. Comparative (a) PSNR and (b)SSIM Values obtained by TPVD, OPVD and the Proposed Method

3.2. The Statistical un-detectability Analysis

The minimal average decision error is one of the most classical accuracy measure in the statistical un-detectability analysis [13,14]. Thus, the chosen accuracy measure in this paper is the minimal average decision error, defined as follows:

$$P_E = \min \frac{1}{2}(P_{F_p} + P_{F_n}) \tag{8}$$

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

- PVD Steganalysis

There is a specific feature set come from Vajiheh Sabeti *et al.* [17] has been used to compare the statistical un-detectability of the proposed algorithm with TPVD and OPVD. The experimental results are shown in Figure 2.

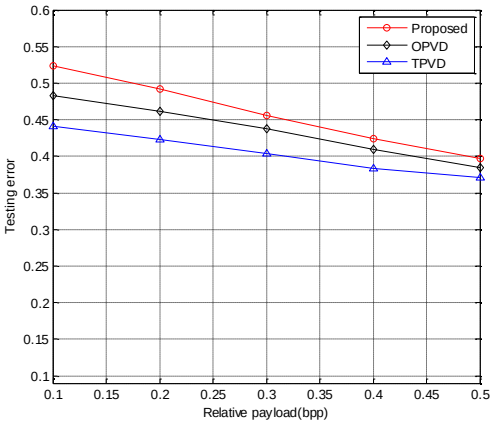
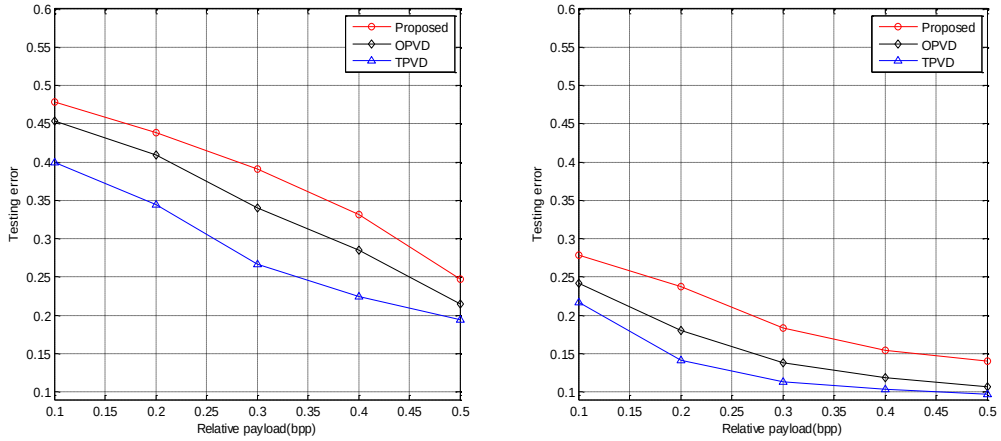


Figure 2. Results of Steganalysis by Vajiheh Sabeti *et al.* 21-D Feature Set

It can be clearly seen from Figure 2 that the proposed method have a better statistical un-detectability to the PVD steganalysis method that based on the Vajiheh Sabeti et al. 21-D Feature Set compared with the OPVD method and the TPVD method. The lower the relative load is, the more obvious the superiority is. This PVD steganalysis method is ineffective in detecting the proposed method when the relative payload is less than 18%. It can also be observed that OPVD had higher values than TPVD. This phenomenon is consistent with the view in literature [11], *i.e.*, OPVD is the method that simultaneously achieving the three contradicting objectives such as high payload, commendable perceptual quality and high statistical un-detectability.

- Universal Steganalysis

There are two feature sets such as Geetha-48D [18] and HOLMES [13] have been employed to compare the statistical un-detectability of the proposed algorithm with TPVD and OPVD. The experimental results are shown in Figure 3. In HOLMES strategy, the quantized MINMAX feature has been used in this paper.



(a) (b)

Figure 3. (a) Results of Steganalysis by Geetha-48D; (b) Results of Steganalysis by the quantized MINMAX Feature

It can be noted that the proposed algorithm withstand many steganalytic systems better than the OPVD method and the TPVD method. The lower the relative load is, the more obvious the superiority is. It can be observed that from Figure 3 (a) that the testing error of the proposed algorithm is 48% when the relative payload is 10%, which is close to that of a random guessing. However, compared with Figure 2 and Figure 3 (a), it can be clearly seen from Figure 3 (b) that these three steganography algorithm can not effectively resist the detection of the steganalysis method based on the quantitative MINMAX features. The reason of this phenomenon is that these three steganography algorithms are belong to the edge based schemes.

4. Conclusion

Based on the OPVD algorithm, an improved steganography algorithm using PSO is proposed in this paper. This proposed algorithm can find the optimum locations adaptively in the cover image to hide the secret data using the PSO method. Since the improved objective function which be used by the PSO module is set in such a way that both perceptual quality and statistical un-detectability are considered. In addition, since the proposed algorithm is an improved method based on the OPVD, this proposed algorithm is a high payload image steganography scheme. This proposed algorithm has

high statistical un-detectability and high payload with commendable visual quality. But in the process of establishing the objective function of PSO, only considering the characteristics of the statistical un-detectability is not enough. In addition, because the pixel point search in the image space is a discrete problem, the PSO method may not have a good better performance than the ant colony algorithm, which provides a new way of image steganography.

Acknowledgments

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

References

[1] C. C. Chang, M. H. Lin and Y. C. Hu, "A fast and secure image hiding scheme based on LSB substitution", International Journal of Pattern Recognition and Artificial Intelligence, vol. 4, no. 16, **(2002)**, pp. 399-416.
[2] 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, **(2001)** October 27-30; Ottawa, Canada
[3] S. Dumitrescu, X. Wu, Z. Wang. Detection of LSB steganography via sample pair analysis. Signal Processing, IEEE Transactions on 7, 51 **(2003)**, pp. 1995-2007.
[4] J. Fridrich, 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
[5] Y. Q. Shi, D. Zou and W. Chen, "Image steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network", Proceedings of 2005 IEEE International Conference on Multimedia and Expo, Amsterdam, Netherlands, **(2005)** July 4.
[6] M. Goljan, J. Fridrich and T. Holotyak, "New blind steganalysis and its implications", Proceedings of International Society for Optics and Photonics, in Electronic Imaging 2006, 607201-607201-13; San Jose, CA, **(2006)** January.
[7] T. Pevný, P. Bas and J. Fridrich, "Steganalysis by subtractive pixel adjacency matrix", Information Forensics and Security, IEEE Transactions on, vol. 2, no. 5, **(2010)**, pp. 215-224.
[8] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing. Pattern Recognition Letters", vol. 9, no. 24, **(2003)**, pp. 1613-1626.
[9] W. Hong, "Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique", Information Sciences, vol. 221, **(2013)**, pp. 473-489.
[10] K.. C. Chang, C. P. Chang and P. S. Huang, "A novel image steganographic method using tri-way pixel-value differencing", Journal of multimedia, vol. 2, no. 3, **(2008)**, pp. 37-44.
[11] C. Balasubramanian, S. Selvakumar and S. Geetha, "High payload image steganography with reduced distortion using octonary pixel pairing scheme", Multimedia Tools and Applications, vol. 3, no. 73, **(2014)**, pp. 2223-2245.
[12] P. Bedi, R. Bansal and P. Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance", Computers & Electrical Engineering, vol. 2, no. 39, **(2013)**, pp. 640-654.
[13] 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, pp. 102-117.
[14] 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, pp. 161-177.
[15] A. P. Engelbrecht, "Fundamentals of computational swarm intelligence", John Wiley & Sons, Hoboken, **(2006)**.
[16] A. P. Engelbrecht, "Computational intelligence: an introduction", John Wiley & Sons, Hoboken **(2007)**.
[17] V. Sabeti, S. Samavi and M. Mahdavi, "Steganalysis of embedding in difference of image pixel pairs by neural network", International Journal of Information Security, vol. 1, no. 1, **(2009)**, pp. 17-26.
[18] S. Geetha, S. S. S. Sindhu and N. Kamaraj, "Passive steganalysis based on higher order image statistics of curvelet transform", International Journal of Automation and Computing, vol. 4, no. 7, **(2010)**, pp. 531-542.

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.