Fundamenta Informaticae 118 (2012) 281–289
DOI 10.3233/FI-2012-714
IOS Press

A Novel Steganographic Method with Four-Pixel Differencing and Modulus Function

Xin Liao*, Qiao-yan Wen, Ze-li Zhao
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications
Beijing, 100876, China
liaoxinbupt@gmail.com

Jie Zhang
School of Science
Beijing University of Posts and Telecommunications
Beijing, 100876, China

Abstract. To improve the stego-image quality and provide a larger embedding capacity, a novel steganographic method based on four-pixel differencing and modulus function is presented. We process a block of four neighboring pixels, and form three two-pixel groups to record the information of secret data. In each group, the difference value between two pixels is exploited to estimate how many secret bits will be embedded. Two pixels will be adjusted so that the sum of the remainders of them is equal to secret data. In order to extract the secret data exactly, four pixel values in a block are adjusted synchronously by using modulus function. An optimization problem is formulated to minimize the embedding distortion. A theoretical proof is given to ensure the solvability of the problem. The experimental results show the proposed method not only has a larger embedding capacity but also provides better stego-image quality.

Keywords: Steganography; Pixel-value differencing; Four-pixel differencing; Modulus function

*Address for correspondence: State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

1. Introduction

Steganography is the art and science of secret communication, which is known as the prisoners' problem formulated by Simmons [9, 5]. A steganographic scheme thus communicates secret messages under the cover of innocence objects by slightly modifying the cover in such a way that an intended recipient cannot detect the existence of secret messages [1, 8, 12].

Least significant bit (LSB) substitution, the most common and well-known steganographic method, embeds secret messages by replacing the fixed length LSBs of pixels with secret messages directly [2]. Many optimized LSB methods have been proposed to improve this work [13, 10, 3]. According to the characteristics of human visual system, changing in smooth areas is more sensitive than changing in edge areas. Not all pixels in a cover image can tolerate equal amount of changes without causing noticeable distortion. Thus, several adaptive methods based on pixel-value differencing (PVD) have been proposed [14, 4, 15, 7, 11, 17]. In 2003, Wu and Tsai presented a novel steganographic method to embed secret data, where the number of bits to be embedded in a pixel is decided by the difference value between two neighboring pixels [14]. In 2004, Chang and Tseng utilized the difference value between the pixel and its upper and left side pixels to determine how many secret bits should be embedded [4]. In 2005, Wu et al. combined pixel-value differencing and LSB substitution[15], and Park et al. proposed a new steganographic method based on the difference value between two pixels adjacent to the target pixel [7]. In 2008, Wang et al. presented a steganographic method that utilizes the remainders of two consecutive pixels to record the information of secret data [11]. Yang et al. proposed an adaptive steganographic method using the difference value of two consecutive pixels to distinguish between edge areas and smooth areas. All pixels are embedded by the k-bit modified LSB substitution, where k is decided by the range which the difference value belongs to [17].

However, most of the previous works did not consider the features of edge sufficiently. Because they processed a block of at most two pixels at a time, the embedding capacity is limited. To overcome this problem, in 2008, Liu et al. [6] proposed two generalizations of pixel-value differencing for data hiding, and extended the 2-pixel block to the n-pixel block. In each block, $n - 1$ difference values are calculated between consecutive pixels, and more difference values are classified to embed secret data. In 2010, Yang et al. [16] proposed a novel steganographic method using four-pixel differencing and pixel-value shifting operations. These two methods can provide the larger embedding capacities, but the stego-image qualities are not very good.

In this paper, in order to provide better stego-image quality, a novel steganographic method for digital images with four-pixel differencing and modulus function is presented. We process a block of four neighboring pixels, forming three two-pixel groups. In each group, the difference value between two pixels is exploited to estimate how many secret bits will be embedded. Two pixel values will be adjusted so that the sum of the remainders of them is equal to secret data. To extract secret data exactly, four pixel values in a block are adjusted synchronously by using modulus function. An optimization problem is formulated to minimize the embedding distortion. A theoretical proof is given to ensure the solvability of the problem. Experimental results show the proposed method not only has a larger embedding capacity but also provides better stego-image quality.

The remainder of this paper is organized as follows. Yang et al.'s method [16] is briefly reviewed in the next section. In Section 3, the embedding and extracting algorithms of our proposed method is presented in detail. In Section 4, the experimental results and analyses are presented. Conclusions are drawn in the last section.

2. Literature Review

In this section we will describe Yang et al.'s method, and use the similar notations as that in Ref. [16]. First, a gray-value cover image is partitioned into non-overlapping blocks of four neighboring pixels, $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j+1}$, $p_{i+1,j}$. p_0 is assigned to the pixel with the smallest gray value, and others are renamed as p_1, p_2, and p_3 in a clockwise sequence. If there is more than one pixel with the smallest value in the block, p_0 is assigned following the priority order of $p_{i,j}, p_{i,j+1}, p_{i+1,j+1}, p_{i+1,j}$. Thus, their corresponding values g_0, g_1, g_2 and g_3 satisfy $g_0 \leq g_1, g_2, g_3$. Then three two-pixel groups (g_0, g_1), (g_0, g_2), and (g_0, g_3) are formed. For each group, we execute the traditional pixel-value differencing method. All possible difference values $d_i = g_i - g_0 (i = 1, 2, 3)$ range from 0 to 255. A range table R are designed, consisting of 13 contiguous sub-ranges $R_k (k = 1, 2, 3, \cdots, 13)$. Each sub-range R_k has its lower and upper bound values l_k and u_k. The width $w_k = u_k - l_k + 1$ is designed to be a power of 2. The sub-ranges of R_k are set to $R_1 = [0, 0]$, $R_2 = [1, 8]$, $R_3 = [9, 16]$, $R_4 = [17, 32]$, $R_5 = [33, 64]$, $R_6 = [65, 128]$, $R_7 = [129, 192]$, $R_8 = [193, 224]$, $R_9 = [225, 240]$, $R_{10} = [241, 248]$, $R_{11} = [249, 252]$, and $R_{12} = [253, 254]$, $R_{13} = [255, 255]$.

For each four-pixel block, the embedding algorithm is described as follows.

Step 1: Calculate the difference value d_i of each two-pixel group by $d_i = g_i - g_0, i = 1, 2, 3$.

Step 2: Find the optimal sub-range R_{k_i} of d_i such that $d_i \in [l_{k_i}, u_{k_i}]$. The number of secret bits t_i that can be embedded in each group is calculated by $t_i = \log_2(w_{k_i})$.

Step 3: Read t_i bits from the binary secret data stream and transform t_i into decimal value $b_i (i = 1, 2, 3)$.

Step 4: Calculate the new difference value d'_i by $d'_i = l_{k_i} + b_i, i = 1, 2, 3$.

Step 5: The secret data can be embedded by modifying the pixel values g_0, g_1, g_2 and g_3 as follows:

$$g'_0 = g_0, \quad g'_i = g_i + d'_i, \quad i = 1, 2, 3.$$

Step 6: This step is called "pixel-value shifting", that is, increase or decrease all the four pixel values synchronously. The final pixel values $\hat{g}_0$, $\hat{g}_1$, $\hat{g}_2$ and $\hat{g}_3$ satisfy

Condition 1: $\hat{g}_0 - g'_0 = \hat{g}_1 - g'_1 = \hat{g}_2 - g'_2 = \hat{g}_3 - g'_3$.

Condition 2: $0 \leq \hat{g}_0, \hat{g}_1, \hat{g}_2, \hat{g}_3 \leq 255$.

Condition 3: The value of $\sum_{i=0}^{3} (\hat{g}_i - g_i)^2$ is minimized.

After replacing (g_0, g_1, g_2, g_3) by $(\hat{g}_0, \hat{g}_1, \hat{g}_2, \hat{g}_3)$, secret data have been embedded.

For example, suppose we have a block with four neighboring pixel values (151,155,158,154). The smallest pixel value is 151, and three groups are $(g_0, g_1) = (151, 155)$, $(g_0, g_2) = (151, 158)$ and $(g_0, g_3) = (151, 154)$. $d_1 = 4, d_2 = 7, d_3 = 3$, all of them belong to $R_2 = [1, 8]$. 3 bits of secret data will be embedded in each group. Assume the secret data are 101100111, we obtain the new difference values $d'_1 = 6, d'_2 = 5, d'_3 = 8$. The pixel values are modified to $g'_0 = 151$, $g'_1 = 157$, $g'_2 = 156$, and $g'_3 = 159$. After executing the "pixel-value shifting", the final pixel values are $\hat{g}_0 = 150$, $\hat{g}_1 = 156$, $\hat{g}_2 = 155$ and $\hat{g}_3 = 158$.

In the extracting algorithm, we can quickly extract the secret data without the original image. Partition the stego image into four-pixel blocks, which is identical with the embedding algorithm. For each block, determine which pixel has the smallest value and form three two-pixel groups. Calculate three difference values d'_i and find the optimal sub-range R_{k_i}. Subtract l_{k_i} from d'_i and obtain $b_i = d'_i - l_{k_i}$. At last, transform the decimal value b_i into the binary secret data stream with length of t_i $(i = 1, 2, 3)$.

3. The proposed method

In this section, a novel steganographic method using four-pixel differencing and modulus function is proposed. The embedding and extracting algorithms are presented in the following subsections.

3.1. The embedding algorithm

Some designs are the same as Yang et al.'s method in Section 2. For the four neighboring pixels $p_{i,j}$, $p_{i,j+1}$, $p_{i+1,j+1}$, $p_{i+1,j}$, p_0 is assigned to the pixel with the smallest gray value, and others are renamed as p_1, p_2, and p_3 in a clockwise sequence. Their corresponding values g_0, g_1, g_2, g_3 satisfy the condition $g_0 \leq g_1, g_2, g_3$. Form three two-pixel groups (g_0, g_1), (g_0, g_2), and (g_0, g_3) with their difference values $d_i = g_i - g_0 (i = 1, 2, 3)$. A range table R is consisted of 13 contiguous sub-ranges $R_k (k = 1, 2, 3, \cdots, 13)$, which has its lower and upper bound values l_k and u_k. The width $w_k = u_k - l_k + 1$ is a power of 2.

For each four-pixel block, the embedding algorithm is described as follows.

Step 1: Calculate the difference value d_i of each two-pixel group by

$$d_i = g_i - g_0, i = 1, 2, 3 \tag{1}$$

Step 2: Find the optimal sub-range R_{k_i} of d_i such that

$$d_i \in [l_{k_i}, u_{k_i}], i = 1, 2, 3 \tag{2}$$

The number of secret bits t_i that can be embedded in each group is calculated by

$$t_i = \log_2(w_{k_i}), i = 1, 2, 3 \tag{3}$$

Step 3: Read t_i bits from the binary secret data stream and transform t_i into decimal value $b_i (i = 1, 2, 3)$.

Step 4: In each group, the sum of the remainders of two pixels will be equal to secret data, that is to say, $g'_i + g'_0$ is congruent to b_i (modulo 2^{t_i}). Four pixel values are modified synchronously to ensure extraction exactly, i.e., guarantee the same sub-range that the difference value of each group belongs to before and after embedding. Note that there would be more than one choice. To minimize the embedding distortion, an optimization problem with two constraints is formulated as follows.

$$\begin{array}{ll} \min\limits_{0 \leq g'_i \leq 255} & \sum\limits_{i=0}^{3} (g'_i - g_i)^2 \\ \text{s.t.} & g'_i - g'_0 = d'_i \in [l_{k_i}, u_{k_i}], i = 1, 2, 3 \\ & (g'_i + g'_0) = b_i \bmod 2^{t_i}, i = 1, 2, 3 \end{array} \tag{4}$$

After replacing (g_0, g_1, g_2, g_3) by (g'_0, g'_1, g'_2, g'_3), secret data have been embedded.

Theorem 3.1. There exists at least one choice (g'_0, g'_1, g'_2, g'_3) such that:

1. $g'_i - g'_0 = d'_i \in [l_{k_i}, u_{k_i}]$.
2. $(g'_i + g'_0) = b_i \bmod 2^{t_i}$.
3. $0 \leq g'_0, g'_i \leq 255$.

where $i = 1, 2, 3$.

Proof:
Suppose $g'_0 = g_0$, without loss of generality, we only justify that under the above conditions g'_1 exists. The cases of g'_2 and g'_3 can be analyzed in the same way. Then, there exists at least one choice (g'_0, g'_1, g'_2, g'_3) such that the former conditions hold.

According to Condition 1, we know that g'_1 should satisfy $g'_0 + l_{k_1} \leq g'_1 \leq g'_0 + u_{k_1}$, thus $2g'_0 + l_{k_1} \leq g'_0 + g'_1 \leq 2g'_0 + u_{k_1}$. Note that the width is $(2g'_0 + u_{k_1}) - (2g'_0 + l_{k_1}) + 1 = u_{k_1} - l_{k_1} + 1 = w_{k_1} = 2^{t_1}$. Thus, for every integer $b_1 \in [0, 2^{t_1} - 1]$, we have $g'_1 = q_1 \times 2^{t_1} + b_1 - g'_0$, $q_1 \in \mathbf{Z}$, satisfying $(g'_1 + g'_0) = b_1 \bmod 2^{t_1}$. Obviously, there exists at least one integer q_1 such that $g'_1 = q_1 \times 2^{t_1} + b_1 - g'_0 \in [0, 255]$. Therefore, the pixel value g'_1 satisfies the above conditions. □

Theorem 3.1 states that there exists at least one choice such that these constraints hold in Eq. (4). Then, there exist the best one in the finite choices, with the smallest embedding distortion. Thus, the optimization problem is solvable.

For example, suppose we have a block with four neighboring pixel values (149,154,155,150). The smallest pixel value is 149, and three groups are $(g_0, g_1) = (149, 154)$, $(g_0, g_2) = (149, 155)$ and $(g_0, g_3) = (149, 150)$. $d_1 = 5, d_2 = 6, d_3 = 1$, all of them belong to $R_2 = [1, 8]$. 3 bits of secret data will be embedded in each group. Assume the secret data are 010111111, we obtain the final pixel values $g'_0 = 150$, $g'_1 = 156$, $g'_2 = 153$ and $g'_3 = 153$.

3.2. The extracting algorithm

The following steps are executed to extract the secret data.

Step 1: Partition the stego image into four-pixel blocks, and each block forms three two-pixel groups. The process is identical with the embedding algorithm.

Step 2: For each two-pixel group, calculate the difference value d'_i by $d'_i = g'_i - g'_0, i = 1, 2, 3$. Find the optimal sub-range R_{k_i} of d'_i, and calculate the number of secret bits t_i that can be extracted from this group.

Step 3: Calculate the sum of the remainders of two pixels in each group (g'_0, g'_i) by

$$(g'_i + g'_0) = b_i \bmod 2^{t_i}, i = 1, 2, 3 \tag{5}$$

Transform the decimal value b_i into the binary secret data stream with length of $t_i (i = 1, 2, 3)$.

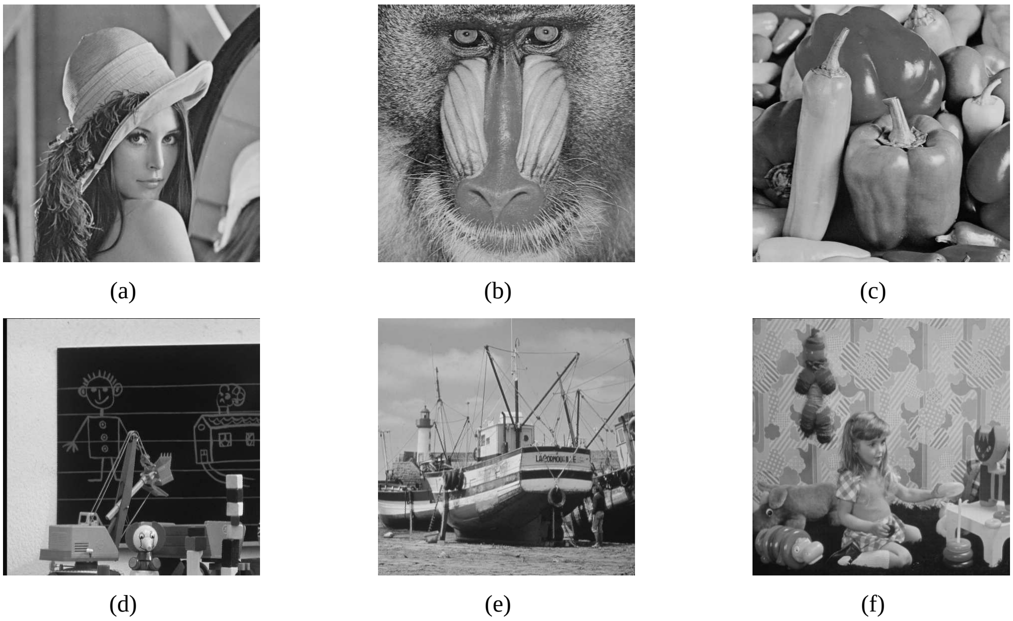


Fig. 1 Six cover images with size 512×512: (a) Lena (b) Baboon (c) Peppers (d) Toys (e) Boat (f) Girl

For instance, we extract the embedding example (150,156,153,153), which is shown in the above subsection. For three groups (150,156), (150,153), (150,153), $d_1 = 6$, $d_2 = 3$, $d_3 = 3$. All the embedding capacities are 3 bits. $b_1 = (150 + 156) \bmod 2^3 = 2$, $b_2 = (150 + 153) \bmod 2^3 = 7$, $b_3 = (150 + 153) \bmod 2^3 = 7$. At last, transform the decimal value b_i into the binary secret data stream with length of 3, and obtain the secret data 010111111.

4. Experimental results

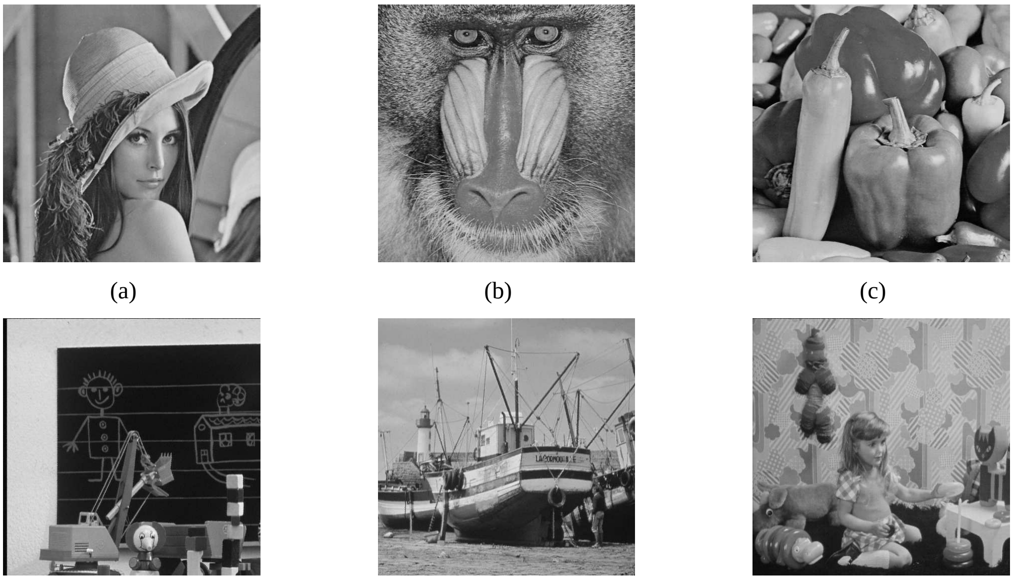
Ten grayscale images with size 512×512 are used in the experiments as cover images, and six of them are shown in Fig. 1. A series of pseudo-random numbers as the secret bit streams are embedded into the cover images. The embedding capacities (in bits) and the PSNR values are average values of the results executed by random bit streams 100 times. The peak signal to noise ratio (PSNR) is utilized to evaluate the quality of the stego image. For an $M \times N$ grayscale image, the PSNR value is defined as follows:

$$PSNR = 10 \times \log_{10} \frac{255 \times 255 \times M \times N}{\sum\limits_{i=1}^{M} \sum\limits_{j=1}^{N} (p_{i,j} - q_{i,j})^2} \, (dB) \tag{6}$$

where $p_{i,j}$ and $q_{i,j}$ denote the pixel values in row i and column j of the cover image and stego image, respectively.

Stego images created by our proposed method are shown in Fig. 2. It is shown that the embedding distortions are imperceptible to human vision.

Table 1 shows the comparisons of the results between Liu et al.'s [6] and ours in terms of embedding capacity and PSNR value, where Liu et al.'s method adopts 4-pixel horizontal and 2×2 square block



(a) (b) (c)

(d) (e) (f)

Fig. 2 Six stego images: (a) Lena (embedded 561740 bits, PSNR=41.20 dB) (b) Baboon (embedded 691735 bits, PSNR=35.65 dB) (c) Peppers (embedded 562249 bits, PSNR=41.30 dB) (d) Toys (embedded 577003 bits, PSNR=40.16 dB) (e) Boat (embedded 596989 bits, PSNR=39.26 dB) (f) Girl (embedded 565000 bits, PSNR=41.52 dB)

arrangements. It is shown that our method provides both larger embedding capacity and better stego-image quality.

Table 1. Comparisons of the results between Liu et al.'s [6] and ours

	4-pixel horizontal		2×2 square		Ours	
Covers	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Lena	524811	38.93	530882	38.43	561740	41.18
Baboon	676167	31.90	640096	33.59	691735	35.61
Peppers	538008	38.45	530617	38.55	562249	41.28
Toys	541933	37.36	547122	37.42	577003	40.17
Boat	552654	37.60	565089	36.70	596989	39.29
Girl	525680	38.95	535563	38.86	565000	41.54
Gold	560643	38.26	553124	38.34	584926	41.01
Zelda	513542	39.41	527212	39.42	554039	42.39
Barb	598164	35.53	613006	34.39	646062	37.08
Tiffany	514301	39.18	523518	38.62	556213	41.51
Average	554590	37.56	556623	37.43	589596	40.11

Table 2 shows the comparisons of the results between Yang et al.'s [16] and ours in terms of embedding capacity, PSNR value and the number of bit changes (i.e., the number of different pixels between cover image and stego image). The statistics show that the PSNR values given by our method are increased by about 3 dB when concealing with the same embedding capacity. The numbers of bit changes

Table 2. Comparisons of the results between Yang et al.'s [16] and ours

	Yang et al.			Ours		
Covers	Capacity	PSNR	Number	Capacity	PSNR	Number
Lena	561740	38.24	217727	561740	41.18	208443
Baboon	691735	32.24	229813	691735	35.61	224461
Peppers	562249	38.42	217224	562249	41.28	208441
Toys	577003	37.20	218811	577003	40.17	210283
Boat	596989	36.17	221509	596989	39.29	212992
Girl	565000	38.71	218500	565000	41.54	209335
Gold	584926	38.06	219227	584926	41.01	211574
Zelda	554039	39.79	216571	554039	42.39	207551
Barb	646063	33.75	225661	646062	37.08	218833
Tiffany	556213	38.72	216100	556213	41.51	206746
Average	589596	37.13	220114	589596	40.11	211866

given by our method are decreased by about 3.75%. Therefore, the proposed steganographic method performs better than Yang et al.'s.

5. Conclusions

In this paper, we have proposed a novel steganographic method based on four-pixel differencing and modulus function. We use four-pixel block to form three two-pixel groups. In each group, the difference value between two pixels is exploited to estimate how many secret bits will be embedded into the group. The sum of the remainders of two pixels in each group is utilized to record the information of secret data. Four pixel values in a block are adjusted synchronously by using modulus function. An optimization problem is formulated, so as to minimize the embedding distortion. The theorem presented in Section 3 is of theoretical importance, because the solvability of the optimization problem is validated explicitly. The experimental results show that the proposed method provides a larger embedding capacity and better stego-image quality.

Acknowledgments

This work is supported by National Natural Science Foundation of China (Grant Nos. 60903152, 61003286, 61170270, 61100203, 61121061), the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01, BUPT2011RC0505, 2011PTB-00-29, 2011RCZJ15).

References

[1] Anderson, R., Petitcolas, F.: On the limits of steganography, 16, may. 1998, ISSN 0733-8716.

[2] Bender, W., Gruhl, D., Morimoto, N., Lu, A.: Techniques for data hiding, *IBM Systems Journal*, **35**(3.4), 1996, 313 –336, ISSN 0018-8670.

[3] Chan, C.-K., Cheng, L. M.: Hiding data in images by simple LSB substitution, *Pattern Recognition*, **37**(3), 2004, 469 – 474, ISSN 0031-3203.

[4] Chang, C.-C., Tseng, H.-W.: A steganographic method for digital images using side match, *Pattern Recognition Letters*, **25**(12), 2004, 1431 – 1437, ISSN 0167-8655.

[5] Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: *Digital Watermarking and Steganography*, Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2007, ISBN 0123725852, 9780123725851.

[6] Liu, J.-C., Shih, M.-H.: Generalizations of pixel-value differencing steganography for data hiding in images, *Fundam. Inf.*, **83**(3), 2008, 319–335, ISSN 0169-2968.

[7] Park, Y.-R., Kang, H.-H., Shin, S.-U., Kwon, K.-R.: A Steganographic Scheme in Digital Images Using Information of Neighboring Pixels, *Advances in Natural Computation* (L. Wang, K. Chen, Y. S. Ong, Eds.), 3612, Springer Berlin / Heidelberg, 2005.

[8] Petitcolas, F., Anderson, R., Kuhn, M.: Information hiding-a survey, *Proceedings of the IEEE*, **87**(7), jul. 1999, 1062 –1078, ISSN 0018-9219.

[9] Simmons, G. J.: The Prisoners' Problem and the Subliminal Channel, *CRYPTO*, 1983.

[10] Thien, C.-C., Lin, J.-C.: A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, *Pattern Recognition*, **36**(12), 2003, 2875 – 2881, ISSN 0031-3203.

[11] Wang, C.-M., Wu, N.-I., Tsai, C.-S., Hwang, M.-S.: A high quality steganographic method with pixel-value differencing and modulus function, *Journal of Systems and Software*, **81**(1), 2008, 150 – 158, ISSN 0164-1212.

[12] Wang, H., Wang, S.: Cyber warfare: steganography vs. steganalysis, *Commun. ACM*, **47**(10), 2004, 76–82, ISSN 0001-0782.

[13] Wang, R.-Z., Lin, C.-F., Lin, J.-C.: Image hiding by optimal LSB substitution and genetic algorithm, *Pattern Recognition*, **34**(3), 2001, 671 – 683, ISSN 0031-3203.

[14] Wu, D.-C., Tsai, W.-H.: A steganographic method for images by pixel-value differencing, *Pattern Recognition Letters*, **24**(9-10), 2003, 1613 – 1626, ISSN 0167-8655.

[15] Wu, H.-C., Wu, N.-I., Tsai, C.-S., Hwang, M.-S.: Image steganographic scheme based on pixel-value differencing and LSB replacement methods, *Vision, Image and Signal Processing, IEE Proceedings -*, **152**(5), oct. 2005, 611 – 615, ISSN 1350-245X.

[16] Yang, C.-H., Wang, S.-J., Weng, C.-Y.: Capacity-Raising Steganography Using Multi-Pixel Differencing and Pixel-Value Shifting Operations, *Fundam. Inf.*, **98**(2-3), 2010, 321–336, ISSN 0169-2968.

[17] Yang, C.-H., Weng, C.-Y., Wang, S.-J., Sun, H.-M.: Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems, *Information Forensics and Security, IEEE Transactions on*, **3**(3), sep. 2008, 488 –497, ISSN 1556-6013.