BLOCK BASED DATA HIDING METHOD FOR IMAGES

***Türker TUNCER** [*1], **Yasin SÖNMEZ** [2],*

[*1]Fırat University, Technology Faculty, Digital Forensics Engineering, Elazığ, Turkey

[2]Dicle University, Technical Sciences Vocational School, Diyarbakır, Turkey

[*] Corresponding author; E-mail: tuncer.turker@gmail.com

In this article, a new block based data hiding method is presented. The proposed data hiding method uses non-overlapping blocks and this method consists of block type determination, data hiding and data extraction functions. The most significant bit of the secret data determines the block type. If the most significant bit of the secret data is 1, the block type is the odd, otherwise the block type is even. The other bits of secret data determine index of abnormal pixel. We use ±1 operator to set abnormal pixel and pre-processing in this paper. To extract secret data, we use index of abnormal pixel and block type. Capacity, execution time and visual quality parameters are used for measuring performance of the proposed method. Experimental results show that the proposed method is a successful data hiding method and that the proposed data hiding method can be used in methods such as image authentication, fragile watermarking etc.

Key words*: Block based data hiding; image processing; information security.*

1. Introduction

Nowadays, multimedia data transformations and digital communication techniques have been widely used. Multimedia consists of texts, images, audios and videos. Multimedias have been used in e-learning, web conference, peer to peer communication, televisions, social media applications, mobile applications, biomedical engineering etc. Because of the high usage of multimedia, many multimedia editing tools have been developed. Owing to these tools, multimedia can be easily modified and this situation causes a lot of information security problems. To provide information security of the multimedia, data hiding and multimedia authentication methods have been widely used. Data hiding is divided into two sub categories which are steganography and digital watermarking. The chiefly aim of the steganography is to obtain a secure data transmission channel by using multimedia or others. Steganography does not associate secret message with cover object, it only intends privacy of the secret message. The main purpose of digital watermarking is to associate the multimedia with the watermark (watermark uses for copyright protection. Users can select it or it can be automatically generated by using an algorithm). Digital watermarking techniques have been commonly used to copyright protection and multimedia authentication. The watermarking techniques are active authentication methods [1-6]. The watermarking techniques use spatial, frequency, compressed and encrypted domains to image authentication and copyright protection [7].

Digital watermarking techniques are widely used for image authentication but not all of the watermarking methods can be used as an image authentication method. The data hiding methods for images consist of 5 components. These are cover image, secret data, data hiding algorithm, stego image and data extraction algorithm. The cover image is an original image which is used for host media. Secret data is embedded into cover image by using data hiding algorithm. LSBR (Least Significant Bits Replacement), QIM (Quantization Index Modulation), HS (Histogram Shifting), CRT (Chinese Remainder Theorem). etc. are widely used data hiding algorithms in the literature. Stego image carries secret data. Receivers use data extraction algorithm to extracting secret data from stego images [8-15].

In this paper, a novel block based data hiding is presented. The characteristics of the presented method is given below.

- This method can use variable size of blocks.
- The proposed method has high visual quality because of this method used ±1 operator for data hiding.
- The capacity of the block based data hiding method is depended on size of blocks.
- The secret data and data hiding map determine to hidden pixel.

The rest of this article is organized as follows. Section 2 describes the proposed block based data hiding method, Section 3 demonstrates experimental results and Section 4 presented conclusions and recommendations.

2. The Proposed Block based Data Hiding Method

In this article, a novel block based data hiding method is presented. The proposed block based data hiding method consists of data hiding and data extraction phases. In the data-hiding phase, the block type and data hiding pixels are determined by using secret data. In the data extraction phase, firstly the block type is determined. Then, the abnormal pixel is detected. The location of the abnormal pixel is expressed as index value. Secret data is calculated by using MSB (Most Significant Bit) of secret data and index value. The steps of the proposed block based data hiding algorithm are given below.

Step 1: Load cover image.

Step 2: Divide blocks into the cover image.

Step 3: Calculate MSB of secret data.

$$MSB(SD) = \left\lfloor \frac{SD}{m * n} \right\rfloor \tag{1}$$

SD is secret data, m is width of block, MSB refers most significant bit and n is height of the block.

Step 4: Modify pixel values in the blocks according to MSB of the secret data. Eq. 2. Describes this modifying.

$$p_{i,j} = \begin{cases} SI_{i,j} = SI_{i,j} - 1, MSB(SD) = 0 \text{ } and \text{ } p_{i,j} \text{ } (mod \text{ } 2) = 1 \\ SI_{i,j} = SI_{i,j} + 1, MSB(SD) = 1 \text{ } and \text{ } p_{i,j} \text{ } (mod \text{ } 2) = 0 \end{cases} \tag{2}$$

p is cover image and SI is stego image.

In step 4, the whole of the pixel values of the blocks are modified.

Step 5: Calculate MSB eliminated secret data and this value used as index of the abnormal pixel. Eq 3-6. are used to select and modify data hiding index.

$$index = SD_{k,l} - MSB(SD_{k,l}) * m * n \qquad (3)$$

$$row = \left\lfloor \frac{index}{b} \right\rfloor \qquad (4)$$

$$col = index \ (mod\ b) \qquad (5)$$

After determined row and col, the data hiding process is applied by using ±1 operator.

$$SI_{m+row,n+col} = \begin{cases} MSB(SD_{k,l}) = 0, & p_{m+row,n+col} + 1 \\ MSB(SD_{k,l}) = 1, & p_{m+row,n+col} - 1 \end{cases} \qquad (6)$$

Step 6: Repeat step 3-5 until size of secret data.

Data extraction steps of the proposed method is depended on counters, counter of even and counter of odd are used to determine block type and abnormal pixel. We use these counters for calculating secret data. Steps of the proposed data extraction algorithm are given below.

Step 1: Load stego image.
Step 2: Block dividing.
Step 3: If counter even is m*n-1and counter odd is 1 then MSB(SD) is 1, otherwise MSB(SD) is 0. To calculate counters, algorithm 1 is used.

Algorithm 1: Pseudo code of the calculating counters.

```
Input: Stego block (sb) which size of m x n.
Output: counter even which is c_even and counter odd which is c_odd.

c_even=0;
c_odd=0;
for i=1 to m do
    for j=1 to n do
        if sb(i,j) (mod 2)=0 then
            c_even=c_even+1;
        else
            c_odd=c_odd+1;
        endif
    endfor
endfor
```

We use counter even and counter odd to calculate MSB.
Step 4: Determine abnormal pixel to calculate index. Algorithm 2 is used to calculate index.

Algorithm 2: Pseudo code of the calculating index.

Input: Stego block (sb) which size of m x n and SD.

Output: index

```
counter=0;
for i=1 to m do
    for j=1 to n do
        if MSB(SD)=1 then
            if sb(i,j) (mod 2)=0 then
                index=counter;
                break;
            endif
            counter=counter+1;
        else
            if sb(i,j) (mod 2)=1 then
                index=counter;
                break;
            endif
            counter=counter+1;
        endif
    endfor
endfor
```

Step 5: Use Eq. 7. to calculate secret data.

$$SD = MSB * m * n + index \tag{7}$$

Step 6: Repeat steps 3-5 until size of secret data.
Block diagram of the block based data hiding algorithm is shown in Fig. 1.

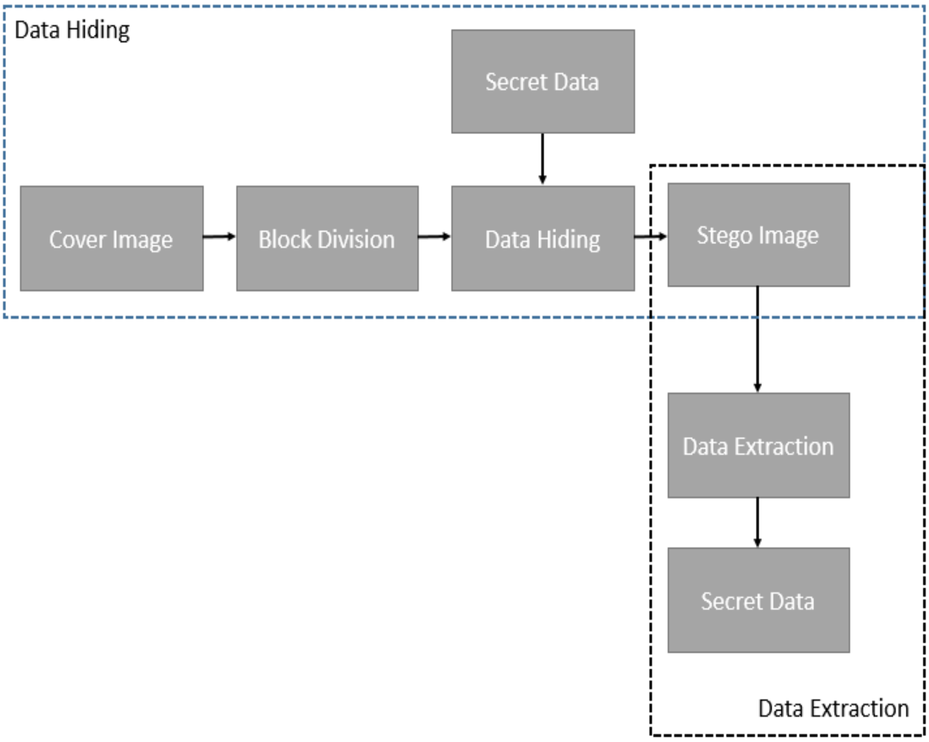


Fig. 1. Block diagram of the block based data hiding method for images.

The following example is given to better understand the proposed block based data hiding method. Example: 3 x 3 size of non-overlapping blocks are used in this example. In this situation, the range of secret data is [0,3 x 3 x 2-1]. For example, if 14 is embedded into block which is shown in Fig. 2., the steps which are given below should be performed.

87	132	134
92	110	143
118	95	99

(a)

0	1	2
3	4	5
6	7	8

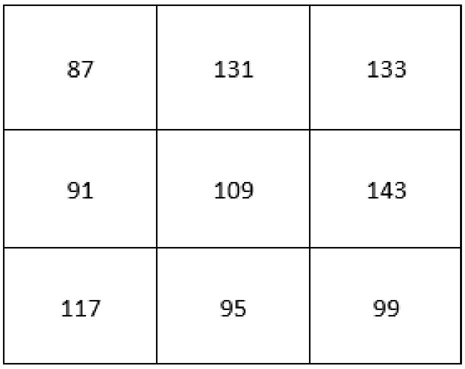
(b)

Fig. 2. Sample block and data hiding map (a) 3 x 3 size of sample image block (b) data hiding map.

Step 1: We determine MSB of the secret data that is 14. To determine this, Eq.1 is used.

$$MSB(14) = \left\lfloor \frac{14}{3*3} \right\rfloor = 1$$

Step 2: MSB(14)=1. For this reason, convert the whole of the pixels of block to odd by using -1 operator. The preprocessed block is given in Fig. 3.



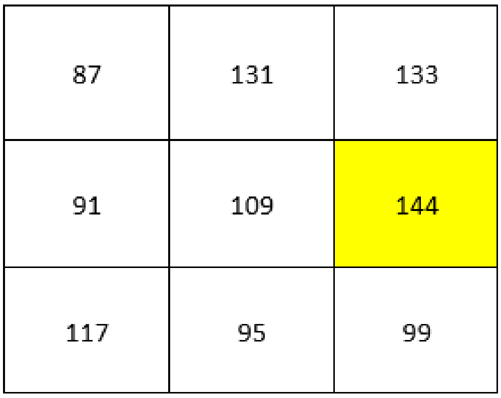
87	131	133
91	109	143
117	95	99

Fig. 3. Pre-processed block.

Step 3: Calculate index value of the secret data.

$$index = 14 - 1 * 3 * 3 = 5$$

Step 4: Modify pixel by using map and +1 operator. The stego block is shown in Fig. 4.



87	131	133
91	109	144
117	95	99

Fig. 4. Stego block.

To data extraction by using stego block, we use steps which are given below.

Step 1: Calculate counter even and counter odd by using Algorithm 1.

Step 2: If c_even is 8 and c_odd is 1 then MSB is 0, otherwise MSB is 1. In this example c_odd is 8 and c_even is 1. Thus MSB is 1.

Step 3: Calculate index by using Algorithm 2.

Step 4: Calculate secret data by using Eq. 7.

$$SD = 1 * 3 * 3 + 5 = 14$$

3. Experimental Results

In this section, the performance of the proposed block based data hiding method was evaluated by using capacity, execution time and visual quality criterias. To obtain experiments of the proposed method, the general test images, which are shown in Fig. 5. are used.

Fig. 5. The general test images.

Capacity: The capacity of the proposed method depends on the used block size. For example, when 3-bit data is embedded into 2 x 2 size of blocks, 5-bit data can be hidden in 4 x 4 size of blocks. General capacity formula of the proposed method is described in Eq. 8.

$$Capacity = \lfloor W/m \rfloor \lfloor H/n \rfloor \lfloor \log_2(mn) \rfloor \qquad (8)$$

For instance, if we use 1 x 2 or 2 x 1 size of non-overlapping blocks, the capacity is obtained 1 bpp (bit per pixel). If we use 2 x 2 size of non-overlapping blocks, the capacity is 0.75 bpp. If we use 3 x 3 size of non-overlapping blocks, the capacity is 0.44 bpp. If we use 4 x 4 size of non-overlapping blocks, the capacity is 0.3125 bpp.

Execution Time: One of the most frequently used performance evaluation criteria to measure the success of a data hiding method is the execution time. The proposed block-based data hiding method is programmed by using Matlab 2013a on Windows 10 operating system with Intel i5-4300U processor and 4 GB RAM. Obtained data hiding time and data extraction timelines are shown in Table 1.

Table 1. Data hiding and data extraction times of the proposed method with various size of blocks and various size of image.

	HT	ET	HT	ET	HT	ET	HT	ET	HT	ET	HT	ET
256 x 256	0.0183	0.1725	0.0123	0.1174	0.0094	0.0775	0.0082	0.0579	0.0068	0.0524	0.0058	0.0384
512 x 512	0.0755	0.7732	0.0514	0.4984	0.0425	0.3112	0.0369	0.2398	0.0294	0.1927	0.0239	0.1661
256 x 256 x 3	0.0640	0.6200	0.0395	0.3455	0.0284	0.2288	0.0248	0.1973	0.0231	0.1341	0.0183	0.1258
512 x 512 x 3	0.2740	2.0496	0.1988	1.4628	0.1270	0.9840	0.1088	0.6938	0.0854	0.5040	0.0728	0.4676

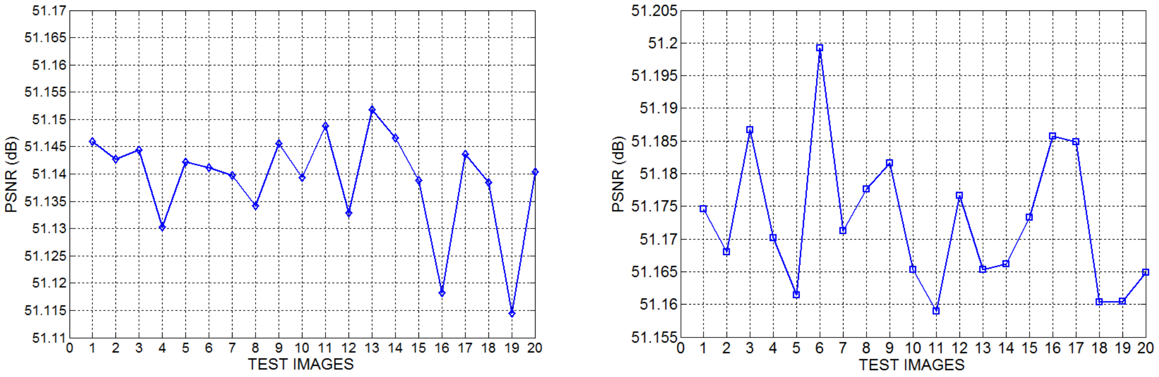
HT is data hiding time and ET is data extraction time.

Visual Quality: One of the most important evaluation parameters is visual quality. To measure visual quality, Mean Square Error (MSE) and Peak Signal to-Noise Ratio (PSNR) are used [16-18]. The equations of MSE and PSNR are given Eq. 9 and Eq. 10.

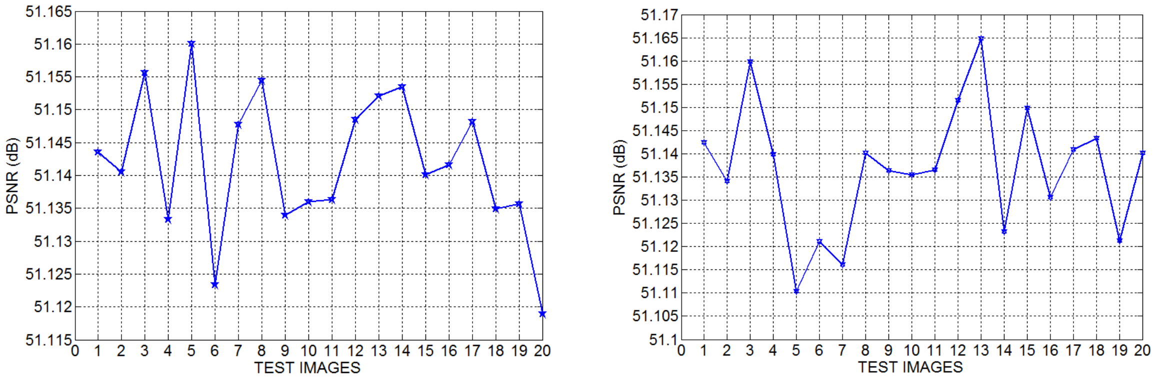
$$MSE = \frac{1}{WH}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(p_{i,j} - SI_{i,j}\right)^2 \quad (9)$$

$$PSNR = 10\log_{10}\frac{Max(p_{i,j}^2)}{MSE} \quad (10)$$

PSNR is generally used evaluation parameter of visual quality in the literature. The obtained PSNR values of the 20 test images with 2 x 2, 3 x 3, 4 x 4 and 8 x 8 size of blocks are shown in Fig. 6.



(a) (b)



(c) (d)

Fig. 6. PSNR values of the proposed block based data hiding method with different size of blocks (a) 2 x 2 (b) 3 x 3 (c) 4 x 4 (d) 8 x 8.

In this article, ±1 operator is used to data hiding and thus the theoretical worst PSNR value is $10\log_{10}(255^2/1)=48.13$. Range of the PSNR values of the proposed block based data hiding method is [48.13, ∞**)**. The average PSNR value of the used test images is 51.1476.

In order to compare of the proposed method to other method in view of visual quality, Lin and Tsai's [19] method, Yang et al.'s [20] method, Chang et al.'s [21] method, Eslami and Ahmadabadi's [22] method, Wu and Lin's [22] method were utilized. The obtained comparison results were shown in Table 2.

Table 2. Comparison of PSNR values of the proposed method with other methods.

	Lin and Tsai's method [30]	Yang et. al.'s method [31]	Chang et. al.'s method [32]	Eslami and Ahmadabadi's method [33]	Wu and Lin's 1. Scheme [34]	Wu and Lin's 2. Scheme [34]	The proposed method
Lena	43.82	46.11	42.28	47.59	51.10	51.15	51.18
Baboon	43.81	46.14	42.31	47.55	51.10	51.15	51.17
Peppers	43.78	46.14	42.30	47.53	51.10	51.12	51.17
Barbara	43.77	46.12	42.30	47.51	51.12	51.14	51.16
Tiffany	43.80	46.11	42.29	47.50	51.13	51.15	51.17
Airplane	43.81	46.10	42.27	47.52	51.14	51.14	51.17
House	43.79	46.15	42.24	47.52	51.10	51.13	51.16

Table 2 clearly showed that, the proposed method has superior visual quality than others.

4. Conclusions and recommendations

A novel block based data hiding method is presented in this paper. The proposed block based data hiding method consists of block division, pre-processing, data hiding and data extraction sections. Variable size of non-overlapping blocks are used to obtain experiments. Firstly, cover image is divided into non-overlapping blocks. Type of block is determined according to secret data. MSB and index value are used for data hiding. In the data extraction section, firstly, block division is processed and type of block is determined. The index of different (abnormal) pixel is determined. Secret data is calculated by using MSB and index of different pixel. In the experimental result, capacity, execution time and visual quality is used. The experimental results showed that, the proposed block based data hiding method is successfully resulted. The presented data hiding method is fragile data hiding method. The help of the proposed method can obtain the fragile watermarking method for image authentication.

In the future works, the proposed method will be used as fragile watermarking and image authentication method. Chaotic maps will be used to create data hiding map.

References

[1] Ma, X., Pan, Z., Hu, S., Wang, L., Reversible data hiding scheme for VQ indices based on modified locally adaptive coding and double-layer embedding strategy, J. Vis. Commun. Image R., (2015), 28, 60–70.

[2] Furon, T., A survey of watermarking security, *International workshop on digital watermarking, Lecture notes on computer science*, (2005), Vol. 3710, Springer, 201–215.

[3] Fridrich, J., Steganography in digital media: Principles, algorithms, and applications, *Cambridge University Press*, 2005.

[4] Yang, C.H., Lin, Y.C., Fractal curves to improve the reversible data embedding for VQ-indexes based on locally adaptive coding, *J. Vis. Commun. Image Represent*. , (2010), 21 (4), 334–342..

[5] Bhat, V., Sengupta, I., Das, A., An adaptive audio watermarking based on the singular value decomposition in the wavelet domain, *Digital Signal Processing*, (2010), 20, 1547–155.

[6] Daemen, J., Rijmen, V., The Design of Rijndael: AES-the Advanced Encryption Standard, *Springer*, 2002.

[7] Said, A., Pearlman, W.A., A new, fast, and efficient image codec based on set partitioning in hierarchical trees, *IEEE Trans Circuits Syst Video Technol*, (1996), 6, 243–250.

[8] Shropshire, J., Warkentin, M., Sharma, S., Personality, attitudes, and intentions: Predicting initial adoption of information security behavior, *Computers & Security*, (2015), Volume 49, 177-191.

[9] Dogan, S., A reversible data hiding scheme based on graph neigbourhood degree, Journal of Experimental & Theoretical Artifical Intelligence, (2017), 29 (4), 741-753.

[10] Chen, B., Design and analysis of digital watermarking, information embedding, and data hiding systems, Ph.D. dissertation, MIT, Cambridge, MA, June 2000.

[11] Celik, M.U., Sharma, G., Tekalp, A.M., Sable, E., Lossless generalized-LSB data embedding, *IEEE Trans. Image Process*. (2005), 14 (2), 253–266.

[12] Lin, Y. K., A data hiding scheme based upon DCT coefficient modification, *Computer Standards & Interfaces*, (2014), Volume 36, Issue 5, 855-862.

[13] Liu, Y., Zhao, J., A new video watermarking algorithm based on 1D DFT and Radon transform, *Signal Processing*, (2010), Volume 90, Issue 2, 626-639.

[14] Lee, S. H., DWT based coding DNA watermarking for DNA copyright protection, *Information Sciences*, (2014), 273, 263-286,.

[15] Vaishnavi, D., Subashini, T.S., Robust and Invisible Image Watermarking in RGB Color Space Using SVD, *Procedia Computer Science*, 2015, Volume 46, 1770-1777.

[16] Tanchenko, A., Visual-PSNR measure of image quality, *J. Vis. Commun*. Image R., (2014), 25,874–878.

[17] A-Eldayem, M. M., A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine, *Egyptian Informatics Journal*, (2013), 14,1–13.

[18] Wang, C. C., Chang, Y. F., Chang, C. C., Jan, J. K., Lin, C. C., A high capacity data hiding scheme for binary images based on block patterns, *The Journal of Systems and Software*, (2014), 93, 152–162.

[19] Lin, C.C., Tsai, W.H., Secret image sharing with steganography and authentication, Journal of System and Software, (2004), 73: 405-414.

[20] Yang, C.N., Chen, T.S., Yu, K.H., Wang C.C., Improvements of image sharing with steganography and authentication, Journal of System and Software, (2007), 80, 1070-1076.

[21] Chang, C.C., Hsieh, Y.P., Lin, C.H., Sharing secrets in stego images with authentication. Pattern Recognition, (2008), 41 (10), 3130-3137.

[22] Eslami, Z., Ahmadabadi, J.Z., Secret image sharing with authentication-chaining and dynamic embedding, Journal of System and Software, (2011), 84, 803-809.

[23] Wu, W.-C., Lin, Z.-W., SVD-based self-embedding image authentication scheme using quick response code features, Journal of Visual Communication and Image Representation, (2016), 38, 18-28.