ICIC Express Letters
Volume **13**, Number **12**, December **2019**

ICIC International ©2019 ISSN 1881-803X
pp. 1113–1119

A NOVEL STEGANOGRAPHIC METHOD WITH TWENTY FIVE PIXEL VALUE DIFFERENCING

Rojali[1], Edi Abdurachman[1], Ford Lumban Gaol[1] and Benfano Soewito[2]

[1]Computer Science Department, BINUS Graduate Program – Doctor of Computer Science
[2]Computer Science Department, BINUS Graduate Program – Master of Computer Science
Bina Nusantara University
Jl. K. H. Syahdan No. 9, Kemanggisan, Palmerah, Jakarta 11480, Indonesia
{ rojali; edia; fgaol; bsoewito }@binus.edu

Received June 2019; accepted September 2019

Abstract. *This paper presents a new approach to improve the embedding capacity and provide an imperceptible visual quality, a novel steganography method based on twenty five pixel value differencing and modified interval table. The cover image is divided into* 5×5 *non-overlapping blocks and PVD method with modified interval is used to embed and extract secret information. The experimental results show that the proposed method has a higher embedding capacity and good imperceptibility where value PNSR is above 30 dB.*

Keywords: Pixel value differencing, Twenty five pixel differencing, Embedding capacity, Imperceptibility, Steganography

1. Introduction.

In today's digital technology era, digital content can be shared quickly and easily on Internet network. With the increasingly faster and easier digital content spread, copy and digital content distribution can lead to illegal acts in Internet public. The copyright holders of digital content have paid attention to copyright protection technologies. Some experts have provided data hiding techniques to insert secrets, copyright information, or trademark into digital content to protect or secure the copyright, and they only slightly modify the original content.

There are two methods of securing data: cryptography and steganography. The difference between cryptography and steganography is that in cryptography, the media with inserted information will change, while in steganography, the media with inserted information will not have any changes. In cryptography, suspicion from the third party will arise because the media that have been inserted will be very different from the original, although the third party is not actually aware of the inserted information. Meanwhile in steganography, with naked eyes the media that has and has not been inserted with information will look the same, so it will not arouse suspicions from the third party or it will be very difficult to distinguish them. The concept of steganography has been around since Roman era, usually carried out by military to send secret messages. Messages are sent by tattooing them on the slave's scalp previously shaved; after the hair grows, the slaves are then sent to allies. To read the messages, the allies shaved the slave's head. Today, the media that carried steganography include (image, video, audio, and text) commonly used media such as image or also called as cover image. Cover image inserted with secret messages is called stego image.

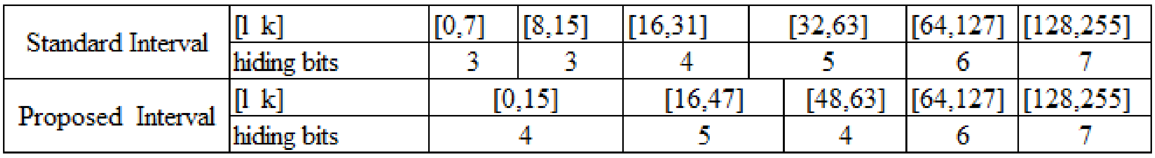
In 2003, Wu and Tsai proposed a novel steganography method that uses pixel value differencing (PVD) between two pixels that embeds bits into pairs that have large PVD values, such as those found in edge areas [1]. A modified version of PVD steganography was presented by Zhang and Wang [2], which removed the step effects by varying

DOI: 10.24507/icicel.13.12.1113

the lower and upper bounds of subrange using a pseudorandom parameter. Wang et al. in 2008 used modulus function besides two pixel value differencing, proposed method to avoid the falling-off-boundary problem [3]. Chang et al. in 2008 [4] proposed tri-way pixel-value differencing to enlarge the capacity of the hidden secret information and to provide an imperceptible stego-image for human vision. Liao et al. used four pixel value differencing and modified LSB substitution to improve ways to avoid these step effects [5,6]. To increase capacity and improve visual perception, Khodaei and Faez [7] in 2012 used four-pixel differencing and modulus function, but this method was vulnerable to attack from histogram analysis. Sabokdast and Mohammadi used modified least significant bits and the modulus function with pixel-value differencing techniques to hide much more information [8]. Number of pixel difference using seven pixel is proposed by Swain et al. in 2016 [9].

Sabeti et al. in 2010 [13] proposed steganalysis and payload estimation of embedding in pixel difference using neural network. Lee at al. in 2012 [11] used tri-way pixel value differencing to reduce the data size of secret images effectively. Tseng and Leng in 2013 [12] proposed a new quantization range table based on the perfect square number. Chen [10] proposed histogram preserving using pixel pair matching to increase the random embedding characteristic. In [14], Bhuiyan et al. proposed improved image steganography algorithm based on PVD to reduce the edge distortion. Yang et al. 2019 [16] used the modular function of dynamic parameters to optimize the amplitude of the pixel value modification (PVBD). The secret information is embedded into cover images directly either by LSB or PVD approaches. The selection of data embedding approach is decided based on a secret key by Prasad and Pal [15]. The proposed scheme is to increase embedding capacity using twenty five pixel difference and modified range table.

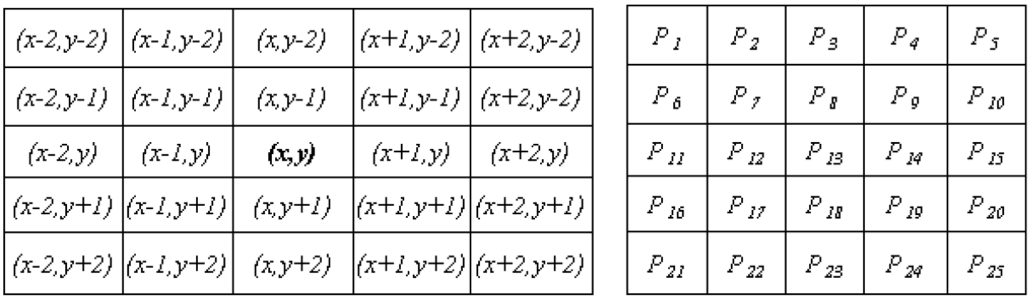
2. **Related Work – Pixel Value Differencing.** Pixel value differencing (PVD) is an information hiding algorithm that processed the pixel-difference values within non-overlapping pixels blocks to determine the bits to be embedded in host image [5]. In the first method, the cover image is partitioned into some non-overlapping blocks of two consecutive pixels, say p_0 and p_1. The difference value d_i is calculated for each block of pixel pair, $d_i = p_0 - p_1$ and find the level of d_i from the range table defined in Figure 1. This range is divided into r sub-regions R_k $(k = 1, 2, \ldots, r)$, and the width of each sub-region is power of 2. The number of bits embedding in the region of R_k is $n = \log_2(w_k)$, where w_k is the width of the k-th sub-region. So, n is the number of bits embedded in the region of R_k. The symbol b_i is the decimal form of a part of the secret information.



<table>
<tr><td rowspan="2">Standard Interval</td><td>[l k]</td><td>[0,7]</td><td>[8,15]</td><td>[16,31]</td><td colspan="2">[32,63]</td><td>[64,127]</td><td>[128,255]</td></tr>
<tr><td>hiding bits</td><td>3</td><td>3</td><td>4</td><td colspan="2">5</td><td>6</td><td>7</td></tr>
<tr><td rowspan="2">Proposed Interval</td><td>[l k]</td><td colspan="2">[0,15]</td><td colspan="2">[16,47]</td><td>[48,63]</td><td>[64,127]</td><td>[128,255]</td></tr>
<tr><td>hiding bits</td><td colspan="2">4</td><td colspan="2">5</td><td>4</td><td>6</td><td>7</td></tr>
</table>

Figure 1. Range table R, lower and upper bound

3. **The Proposed Scheme.** To achieve maximum capacity message the basic processing unit of this paper's method is 5 × 5 pixel block. The point (x, y) or P_{13} is the center, so the other point is reduced by the point (x, y) in Figure 2. This section discusses mainly the embedding and extraction algorithm.



(x-2,y-2)	(x-1,y-2)	(x,y-2)	(x+1,y-2)	(x+2,y-2)
(x-2,y-1)	(x-1,y-1)	(x,y-1)	(x+1,y-1)	(x+2,y-2)
(x-2,y)	(x-1,y)	**(x,y)**	(x+1,y)	(x+2,y)
(x-2,y+1)	(x-1,y+1)	(x,y+1)	(x+1,y+1)	(x+2,y+1)
(x-2,y+2)	(x-1,y+2)	(x,y+2)	(x+1,y+2)	(x+2,y+2)

(a) Original block in (x, y)

P_1	P_2	P_3	P_4	P_5
P_6	P_7	P_8	P_9	P_{10}
P_{11}	P_{12}	P_{13}	P_{14}	P_{15}
P_{16}	P_{17}	P_{18}	P_{19}	P_{20}
P_{21}	P_{22}	P_{23}	P_{24}	P_{25}

(b) Original block in P

FIGURE 2. Original block in (x, y) and P

3.1. **Embedding algorithm of the proposed method.** The image in this study is .png type, before insertion of each pixel is read starting from left to right and then down and so on. The proposed method divided cover image into some 5 × 5 non-overlapping pixel blocks. The secret message is inserted in the twenty four pixel-pair difference. The further steps of the embedding process are as follows.

1) The central pixel of the block is assigned as central pixel P_{13}. The 24-neighboring central pixel P_{13} is denoted by P_i where $i = 1, 2, \ldots, 25$.
2) Compute the difference value d_i between the central pixel P_{13} and P_i, where $i = 1, 2, \ldots, 25$.
$$d_i = P_{13} - P_i$$
3) From the range division table, find out range R_k to which the difference value d_i belongs. Compute w, $w = l - u + 1$ and n is the number of bits embedded, $n = \log 2(w)$.
4) According to value n, convert n value to decimal b, compute d'_i
$$d'_i = \begin{cases} l + b & \text{if } d_i \geq 0 \\ -(l + b) & \text{if } d_i < 0 \end{cases} \tag{1}$$
5) Compute P'_i with 24 iterations as:
$$(p'_{13_i}, p'_i) = \begin{cases} \left(p_{13} + \left\lfloor \frac{m_i}{2} \right\rfloor, p_i - \left\lceil \frac{m_i}{2} \right\rceil\right) & \text{if } d_i \text{ is odd} \\ \left(p_{13} + \left\lceil \frac{m_i}{2} \right\rceil, p_i - \left\lfloor \frac{m_i}{2} \right\rfloor\right) & \text{if } d_i \text{ is even} \end{cases} \tag{2}$$
$d''_i = p_{13} - p'_{13_i}$, where $i = 1, 2, \ldots, 25$.
6) According to Step 5) compute p'_i where $i = 1, 2, \ldots, 25$.
$$p'_i = \begin{cases} p_i - \left\lceil \frac{m_i}{2} \right\rceil + d''_i & \text{if } d_i \text{ is odd} \\ p_i - \left\lfloor \frac{m_i}{2} \right\rfloor + d''_i & \text{if } d_i \text{ is even} \end{cases} \tag{3}$$
p'_i is pixel stego image after embedding the message.

For example, there is an image pixel block with twenty five pixel values P_1 until P_{25} (124,133, 133, 130, 133, 185, 182, 183, 180, 159, 158, 182, 199, 184, 171, 158, 183, 193, 183,182, 202, 180, 167, 172, 183). The central pixel value is 199, and twenty four are $(P_{13}, P_1) = (199, 124)$, $(P_{13}, P_2) = (199, 133)$, $(P_{13}, P_3) = (199, 133)$ until $(P_{13}, P_{25}) = (199, 183)$. $d_1 = 75$, $d_2 = 66$, $d_3 = 66$, until $d_{25} = 16$, value d determines l and u, $l_1 = 64$ and $u_1 = 127$, $l_2 = 64$ and $u_2 = 127$ until $l_{25} = 16$ and $u_{25} = 47$. Assume the secret data are 0110001001101001. . . 00010, the embedding data are $b_1 = (011000)_2 = 24$, $b_2 = (100110)_2 = 38$ until $b_{25} = (00010)_2 = 2$. Based on Equation (1) $d'_1 = 88$, $d'_2 = 102$, $d'_3 = 101$ until $d'_{25} = 18$ and based on Equation (2) $(P'_1 = 117, P'_{13_1} = 205)$, $(P'_2 = 115, P'_{13_2} = 217)$, $(P'_3 = 116, P'_{13_3} = 217)$ until $(P'_{25} = 182, P'_{13_{25}} = 200)$. The final pixel value according to Equaton (3), $P'_1 = 111$, $P'_2 = 97$, $P'_3 = 98$, until $P'_{25} = 181$.

3.2. **Extraction algorithm.** The receive stego image is divided into some 5 × 5 non-overlapping pixel blocks which is the same manner of embedding process. The center pixel P'_{13} is selected from stego image. The steps for extraction process are as given below.

1) The central pixel of the block is assigned as central pixel P'_{13}. The 24-neighboring central pixel P'_{13} is denoted by P_i where $i = 1, 2, \ldots, 25$.
2) Compute the difference value d_i between the central pixel P'_{13} and P'_i, where $i = 1, 2, \ldots, 25$.
$$d_i = P'_{13} - P'_i$$
3) From the range division table, find out range R_k to which the difference value d_i belongs. Compute w, $w = l - u + 1$ and n is the number of bits embedded, $n^* = \log 2(w)$.
4) According to value n^*_i, compute b and number of embedded is converted to b^*_i binary with length n^*.
$$b^*_i = \begin{cases} d'_i - l_i & \text{if } d'_i \geq 0 \\ -(d'_i + l_i) & \text{if } d'_i < 0 \end{cases} \tag{4}$$

For example, the stego image file Steps 1) to 3) are the same as those done in the process of the embedding process obtained $d'_1 = 88$, $l_1 = 64$, $n^*_1 = 6$; $d'_2 = 102$, $l_2 = 64$, $n^*_2 = 6$; $d'_3 = 101$, $l_3 = 64$, $n^*_3 = 6$ until $d'_{25} = 18$, $l_{25} = 16$, $n^*_{25} = 6$. According to Equation (4) obtain $b^*_1 = 24$, $b^*_2 = 38$, $b^*_3 = 37$, until $b^*_{25} = 2$ and final secret message converts b^*_i to binary along n^*_i.

4. Experimental Result and Analysis.

This section is the simulation of the proposed method, the standard test images with sizes of 200×200 unit of Baboon, Boat, House, Jet, Lena, Peppers, Pot and Tifanny. Images were used as the experimental objects shown in Figure 3. In this paper, the proposed algorithm was evaluated by two indexes, the PSNR and Capacity.

House

Lena

Peppers

Baboon

Pot

Tiffany

Jet

Boat

FIGURE 3. Cover image for testing

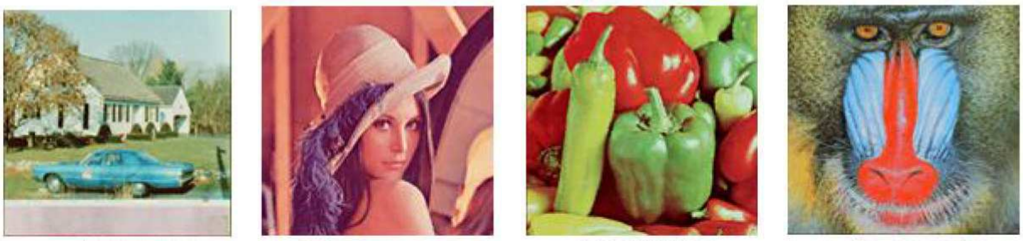
PSNR value between the cover image and stego image of size $M \times N$ is given as:
$$PSNR = 10 \cdot \log_{10}\left(\frac{255^2}{MSE}\right) dB \tag{5}$$
where the mean square error (MSE) is defined as
$$MSE = \frac{1}{M \cdot N}\sum_{i=1}^{M}\sum_{j=1}^{N}(x_{ij} - y_{ij})^2 \tag{6}$$
where M, N are horizontal and vertical pixel dimension of cover and stego image, x_{ij} and y_{ij} denote the pixel value in row i and column j of the cover image and stego image.

The comparison of interval standard with proposed method in embedding capacity and PSNR (Peak Signal Noise Ratio) is shown in Table 1. For all image storage capacity increases, even though the PSNR value decreases it is still at the fair value limit in the naked eye, it is rather difficult to distinguish the difference between the two cover images and stego images.

Table 1. Comparison of the result interval standard with proposed method

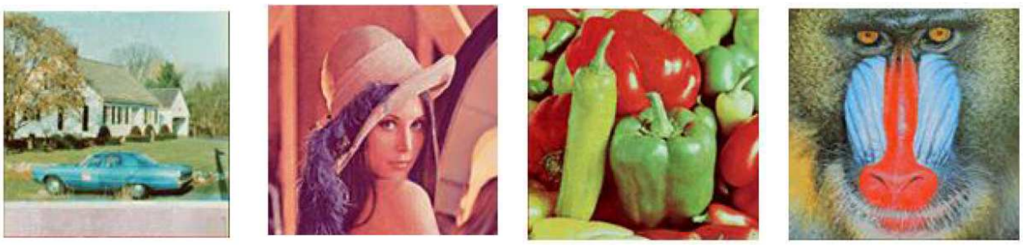
Cover Image	Interval Standard		Proposed Method	
200 × 200	Capacity (bit)	PSNR (dB)	Capacity (bit)	PSNR (dB)
House	423,687	34.22	499,009	31.68
Lena	388,847	35.21	481,640	32.15
Peppers	400,236	35.15	486,789	32.28
Baboon	441,100	33.81	501,853	31.65
Pot	376,455	35.95	477,366	32.37
Tiffany	374,612	36.04	475,207	32.38
Jet	390,875	35.15	483,708	32.22
Boat	418,288	34.56	500,825	31.93

The experimental results of our approach with interval standard and proposed standard are shown in Figures 4 and 5, respectively. From Table 1, we can see that the embedding capacity values of proposed standard are better than interval standard, but the PSNR interval standard are better than other ones. Also, the embedding capacity is increased whereas the PSNR value and the image quality are decreased. However, in all of them,



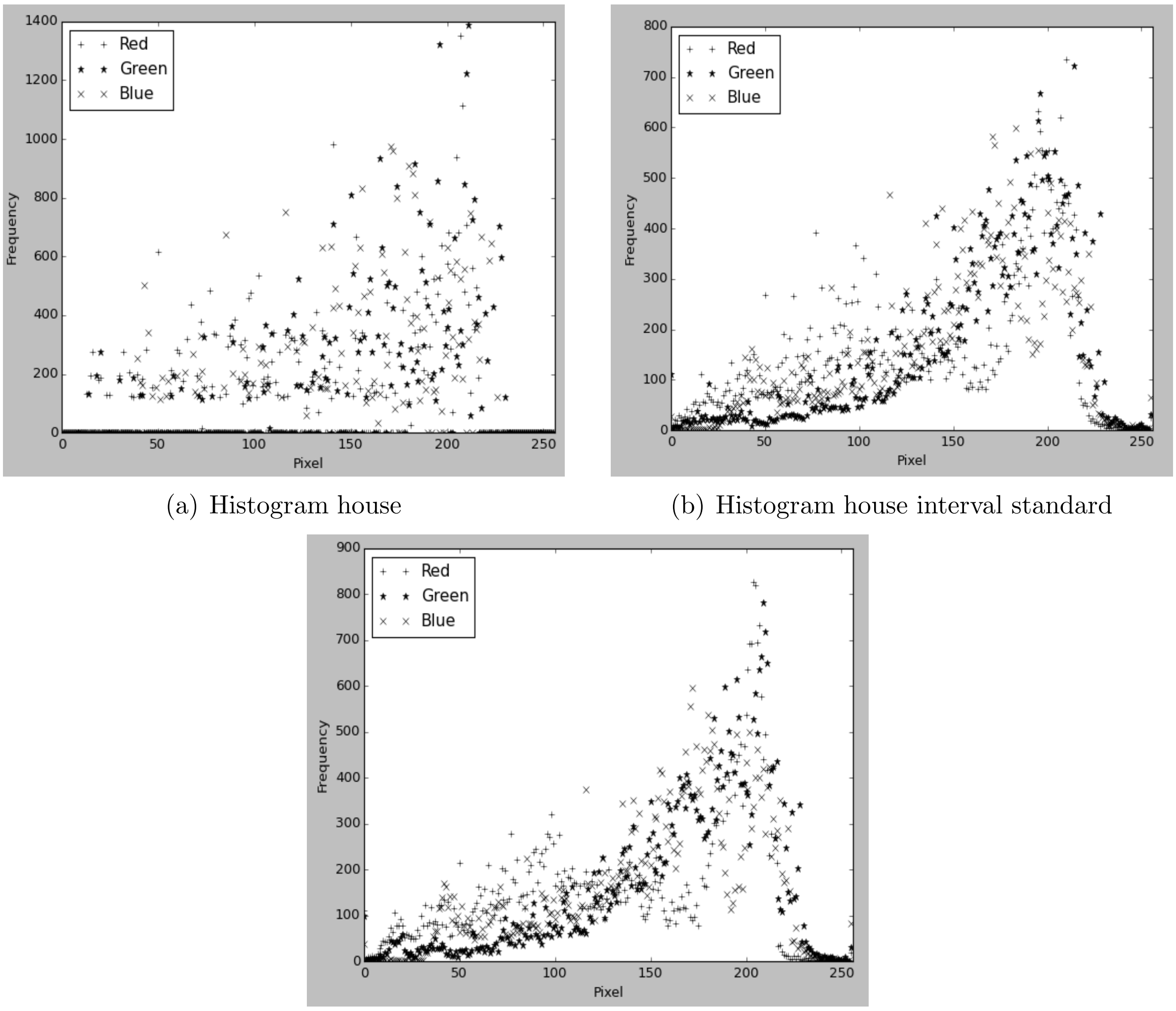
(a) House (b) Lena (c) Peppers (d) Baboon

Figure 4. Four stego images (interval standard): (a) House (embedded 423,687 bits, PSNR = 34.22 dB), (b) Lena (embedded 388,847 bits, PSNR = 35.21 dB), (c) Peppers (embedded 400,236 bits, PSNR = 35.15 dB), (d) Baboon (embedded 441,100 bits, PSNR = 33.81 dB)



(a) House (b) Lena (c) Peppers (d) Baboon

Figure 5. Four stego images (proposed method): (a) House (embedded 499,009 bits, PSNR = 31.68 dB), (b) Lena (embedded 481,640 bits, PSNR = 32.15 dB), (c) Peppers (embedded 486,789 bits, PSNR = 32.28 dB), (d) Baboon (embedded 501,853 bits, PSNR = 31.65 dB)



(a) Histogram house

(b) Histogram house interval standard

(c) Histogram house proposed method

Figure 6. Histogram of cover and stego images (House)

the PSNR values of the stego-image are above 30 dB. Thus, the distortion of stego-images is slight and indistinguishable.

In Figure 6, the histogram is leaning right where the value of pixels moves to the largest value. While the frequency of each value at pixel values tends to be more. The difference histogram of the proposed method shows the values of the stego image to be very close to the values of the cover image and is difficult to detect by the difference histogram analysis.

5. **Conclusions.** In this paper, we have proposed a novel steganographic method in spatial domain based on twenty five pixel value differencing. The cover image is partitioned into 5×5 on-overlapping blocks. It gives 24 pairs of pixels in each block in all possible directions. Experiments show that this scheme has improved the embedding capacity, stego image quality. The experimental results show that the proposed method provides larger embedding capacity and better image quality. Our proposed method majors in more significant promotions in terms of capacity and imperceptivity. There is a trade-off between embedding capacity/quality and it would sacrifice attack-resistance a little for obtaining higher embedding capacity/quality. In the future, besides the merits achieved in this paper, we will attempt to improve and modify the proposed method to achieve better PSNR.

REFERENCES

[1] D.-C. Wu and W.-H. Tsai, A steganographic method for images by pixel-value differencing, *Pattern Recognition Letters*, vol.24, nos.9-10, pp.1613-1626, 2003.

[2] X. Zhang and S. Wang, Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security, *Pattern Recognition Letters*, vol.25, no.3, pp.331-339, 2004.

[3] C.-M. Wang, N.-I Wu, C.-S. Tsai and M.-S. Hwang, A high quality steganographic method with pixel value differencing and modulus function, *The Journal of Systems and Software*, vol.81, no.1, pp.150-158, 2008.

[4] K. C. Chang, C. P. Chang, P. S. Huang and T. M. Tu, A novel image steganographic method using tri-way pixel-value differencing, *Journal of Multimedia*, vol.3, no.2, pp.37-44, 2008.

[5] X. Liao, Q. Wen and J. Zhang, A steganographic method for digital images with four-pixel differencing and modified LSB substitution, *Journal of Visual Communication and Image Representation*, vol.22, no.1, pp.1-8, 2011.

[6] X. Liao, Q. Wen, Z. Zhao and J. Zhang, A novel steganographic method with four-pixel differencing and modulus function, *Fundamenta Informaticae*, vol.118, no.3, pp.281-289, 2012.

[7] M. Khodaei and K. Faez, New adaptive steganographic method using least significant bit substitution and pixel differencing, *IET Image Process*, vol.6, no.6, pp.677-686, 2012.

[8] M. Sabokdast and M. Mohammadi, A steganographic method for images with modulus function and modified LSB replacement based on PVD, *Proc. of the 5th Conference on Information and Knowledge Technology*, Shiraz, Iran, 2013.

[9] A. Pradhan, R. S. Krovi and G. Swain, Digital image steganography based on seven way pixel value differencing, *Indian Journal of Science and Technology*, vol.9, no.37, 2016.

[10] J. Chen, A PVD-based hiding method with histogram preserving using pixel pair matching, *Signal Processing: Image Communication*, vol.29, pp.375-384, 2014.

[11] Y.-P. Lee, J.-C. Lee et al., High-payload image hiding with quality recovery using tri-way pixel-value differencing, *Information Science*, vol.191, pp.214-225, 2012.

[12] H.-W. Tseng and H.-S. Leng, A steganographic method based on pixel-value differencing and the perfect square number, *Journal of Applied Mathematics*, vol.2013, 2013.

[13] V. Sabeti, S. Samavi, M. Mahdavi and S. Shirani, Steganalysis and payload estimation of embedding in pixel difference using neural network, *Pattern Recognition*, vol.43, no.1, pp.405-415, 2010.

[14] S. S. N. Bhuiyan, N. A. Malek, O. O. Khalifa and F. D. A. Rahman, An improved image steganography algorithm based on PVD, *Indonesian Journal of Electrical Engineering and Computer Science*, vol.10, no.2, pp.569-577, 2018.

[15] S. Prasad and A. K. Pal, Logistic map-based image steganography scheme using combined LSB and PVD for security enhancement, in *Emerging Technologies in Data Mining and Information Security*, A. Abraham, P. Dutta, J. Mandal, A. Bhattacharya and S. Dutta (eds.), Singapore, Springer, https://doi.org/10.1007/978-981-13-1501-5_17, 2019.

[16] Y. Yang, R. Zhang, J. Liu, Y. Wang and F. Huang, An image steganography algorithm based on pixel block difference and variable modulus function, in *Recent Advances in Intelligent Information Hiding and Multimedia Signal Processing*, J. S. Pan, A. Ito, P. W. Tsai and L. Jain (eds.), Cham, Springer, https://doi.org/10.1007/978-3-030-03748-2_5, 2019.