Journal of Computer Science

Original Research Paper

A High Quality Steganography Method with Twenty Five-Pixel Value Differencing

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

[1]*Department of Mathematics, School of Computer Science,*
Bina Nusantara University, Jakarta, Indonesia 11480, Indonesia
[1,2]*Department of Computer Science, BINUS Graduate Program-Doctor of Computer Science,*
Bina Nusantara University, Jakarta, Indonesia 11480, Indonesia

Article history
Received: 19-06-2019
Revised: 16-10-2019
Accepted: 29-10-2019

Corresponding Author:
Rojali
Department of Mathematics,
School of Computer Science,
Bina Nusantara University,
Jakarta, Indonesia 11480,
Indonesia
Email: rojali@binus.edu

Abstract: The fundamental objectives of image steganography algorithm are to simultaneously achieve high payload or embedding capacity, good visual imperceptibility and security. This paper presents a new approach to improve the embedding capacity and provide an imperceptible visual quality, a novel steganography method based on algorithm twenty five pixel value differencing and modified interval table (TFPVD). The cover image is made into 5×5 blocks that don't overlap and TFPVD method with modified interval is used to embed and extract secret information. The results showed that the proposed TFPVD steganography algorithm has a higher steganographic capacity, which is 1,764 times that of the PBVD algorithm.

Keywords: Pixel Value Differencing, TFPVD, Imperceptibility, Steganography

Introduction

New trends and rapid advances in the field of information technology have been very developed to communicate in the digital world can be done very quickly via the internet. Through the internet digital media distribution is sent, the information sent is vulnerable to malicious attacks, unauthorized access, forgery, plagiarism, etc.

One method for securing confidential information is to use steganography. Some of the goals of steganography are to increase the capacity of hidden bits, provide good visual imperceptibility and ensure safety of steganalysis. The most widely used security parameters of steganography are RS analysis where it will be very difficult to find information in the media that is sent.

Wu and Tsai (2003) proposed a novel steganography method that uses the difference Pixel Value Differencing (PVD) between two pixel that embeds bits into pairs that have large PVD values, such as those found in edge areas. A Modified version of PVD steganography was presented by (Zhang and Wang, 2004) which removed the step effects by varying the lower and upper bounds of sub range using a pseudorandom parameter. Wang *et al.* (2008) uses modulus function beside two pixel value differencing, propose methods to avoid the problem of boundary values, where values are below or above the pixel values they should. Using tri-way pixel-value differencing introduced by (Chang *et al.*, 2008) Steganography uses four pixel value differencing and Modified LSB substitution to improve way to avoid these step effects (Liao *et al*., 2011; 2012). To increase capacity and improve visual perception, (Khodaei and Faez, 2012) using PVD and LSB Subtitution, the proposed method is safe against RS detection attacks and steganalysis detectors using SPAM

The features (Sabokdast and Mohammadi, 2013) using the smallest modified bit and the modulus function with the pixel difference-value technique to increase the bit capacity. Number of pixel difference using seven pixel proposed by (Pradhan *et al*., 2016). An Improved Image Steganography Algorithm based on PVD (Bhuiyan *et al*., 2018) embedding data only to less intensity pixel difference areas or regions. Yu *et al.* (2019) From dynamic parameters using a modular function used to optimize the amplitude value of pixels that have been modified (PBVD). Confidential information is embedded into the cover image directly both with the LSB or PVD approach. By using the secret key selection the data embed approach is decided (Prasad and Pal, 2019). The proposed scheme is to increase embedding capacity use Twenty Five Pixel difference and modified range table.

DOI: 10.3844/jcssp.2019.1538.1545

Research Method

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 (Liao *et al*., 2011) Before the first insertion process is done, the cover image is partitioned into non-overlapping blocks of two adjacent pixels, for example p_0 and p_1. The value d_i is calculated for each block of adjacent pixel pairs, i.e., $d_i = p_0 - p_1$ and find the level of di form the range table define in Fig. 1. This table is divided into n regions of R_k (k = 1,2, ..., n) the value of each region 2 to the power of n. The number of bits obtained in the R_k region is $m = \log2 (w_k)$, where w_k is the width of the k-th region. So, m is the number of bits embedded in the region of R_k. The b_i symbol is a decimal form of confidential information.

Twenty Five-Pixel Value Differencing

To achieve maximum message capacity, pixels are divided into 5×5 pixel blocks, The point (x, y) or P_{13} is the center, so the other point is reduced by the point (x, y) in Fig. 2. This section will explain the insertion and extraction algorithm.

Interval standard	Lower-upper	0-7	8-15	16-31	32-63	64-127	128-255
	Hiding bits	3	3	4	5	6	7
Propose interval	Lower-upper	0-15		16-47	48-63	64-127	128-255
	Hiding bits	4		5	4	6	7

Fig. 1: Range table R, lower and upper bound

(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-1)
(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)

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)

Fig. 2: Original block in (x, y) and *P*; (a) Original block in (x, y); (b) Original block in *P*

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 block. The secret message is inserted in the twenty four pixel-pair difference. The next step is the embedding process as follows:

1. The pixel which is the center of the image is assumed to be P_{13}. The 24-neighboring central pixel P_{13} are denoted by P_i where i = 1, 2,…25
2. Calculate the difference between the central pixels P_{13} and P_i, where i = 1, 2,..25:

$$d_i = P_{13} - P_i$$

3. From the table, calculate the difference in range to get the upper (u) and lower (l) limits. Compute w, $w = l-u+1$ and n the number of bits embedded, $n = \log2(w)$
4. According value n, convert n value to decimal b, compute d_i' :

$$d_i' = \begin{cases} l+b & if\ d_i \ge 0 \\ -(l+b) & if\ d_i < 0 \end{cases} \quad (1)$$

5. Compute P_i' with 24 iteration is calculated as:

$$\left(p_{13_i}', p_i'\right) = \begin{cases} \left[\left\lceil p_{13} + \left\lfloor \frac{m_i}{2} \right\rfloor \right\rceil, p_i - \left\lfloor \frac{m_i}{2} \right\rfloor \right] & if\ d_i\ is\ odd \\ \left[\left\lceil p_{13} + \left\lfloor \frac{m_i}{2} \right\rfloor \right\rceil, p_i - \left\lfloor \frac{m_i}{2} \right\rfloor \right] & if\ d_i\ is\ even \end{cases} \quad (2)$$

$d_i'' = p_{13} - p_{13_i}'$, Where, i = 1,2,..25

6. According to step 5 compute p_i' where, i = 1,2,..25:

$$p_i' = \begin{cases} p_i - \left\lceil \frac{m_i}{2} \right\rceil + d_i'' & if\ d_i\ is\ odd \\ p_i - \left\lceil \frac{m_i}{2} \right\rceil + d_i'' & if\ d_i\ is\ even \end{cases} \quad (3)$$

p_i' is pixel stego image after embedded the message. For example, there is a pixel block of images with twenty-five pixels value P_1 until P_{25} (124,133,133,130,133,185,182,183,180,159,158,182,199 ,18,4,171,158,183,193,183,182,202,180,167,172,183). 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 determine l dan 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 base on Equation (2) (P_1' = 117, P_{13_1}' = 205), (P_2' = 117, P_{13_2}' = 217), (P_3' = 116, P_{13_3}' = 217) until $\left(P_{25}' = 182, P_{13_{25}}' = 200\right)$. The final pixel value according to Equation 3 P_1' = 111, P_2' = 97, P_3' = 98, P_{25}' = 181.

Extraction Algorithm

Stego received images divided into several 5×5 blocks of non-intersecting pixels are the same way of the embedding process. The middle Pixel P_{13}' is taken from a stego image.

Whereas the extraction process is as follows:

- The middle pixel as central pixel P_{13}'. The 24-neighboring central pixel P_{13}' are denoted by P_i where i = 1, 2, …25
- Compute the difference value di between the central pixel P_{13}' and P_i', where i = 1, 2,..25:

$$d_i = P_{13}' - P_i'$$

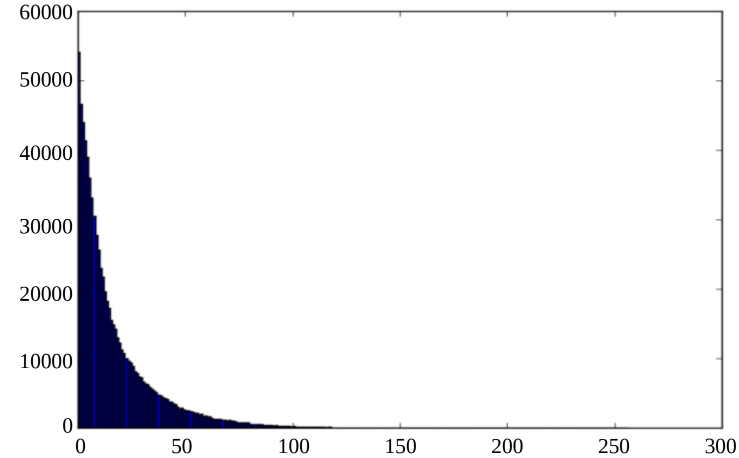
- From the table in Fig. 1, determine the R_k value based on the d_i value obtained in step 2. Compute w, $w = l-u+1$ and n the number of bits embedded, $n^* = \log2(w)$
- According value n_i^*, compute b and number of embedded is convert to b_i^* binary with length n^*:

$$b_i^* = \begin{cases} d_i' - l_i & if\ d_i' \ge 0 \\ -(d_i' + l_i) & if\ d_i' < 0 \end{cases} \quad (4)$$

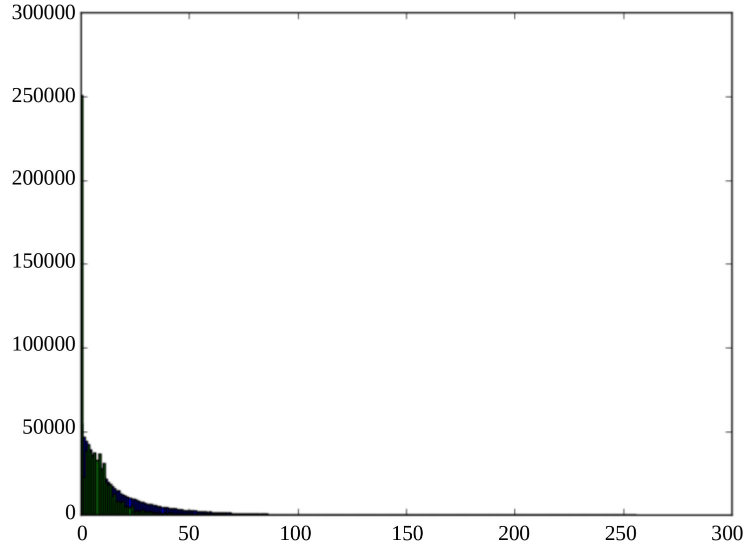
For example, the stego image file steps 1 to 3 are the same as those done in the process of the embedding process obtained d_1' = 88, l_1 = 64, n_1^* = 6; d_2' = 102, l_2 = 64, n_2^* = 6; d_3' = 101, l_3 = 64, n_3^* = 6 until d_{23}' = 18, l_{25} = 16, n_{25}^* = 6. According to Equation 4 obtained b_1^* = 24, b_2^* = 38, b_3^* = 37, b_{25}^* = 2 and final secret message convert b_i^* to binary along n_i^*.

Result

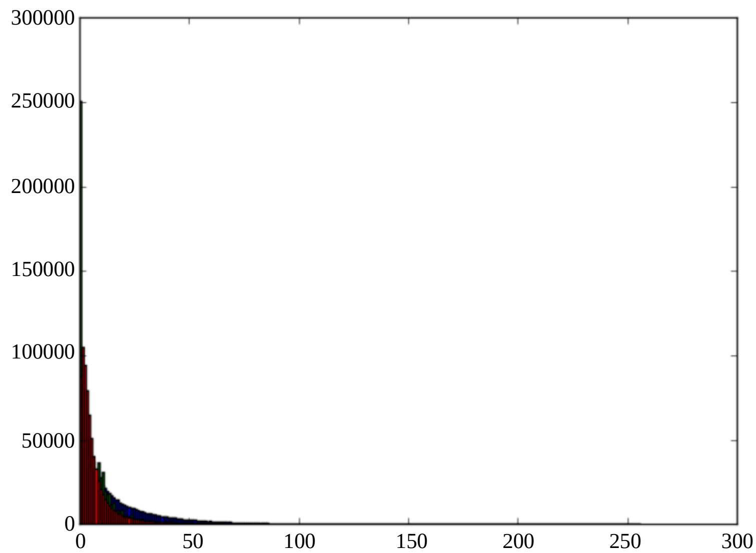
This stage is a simulation part of the proposed method, the width and length of the test image is 512×512 unit of madril, peppers, lena, house, tiffany, tank and airplane. Figure 4. is a cover image used to evaluate the PSNR value and bit capacity.


60000
50000
40000
30000
20000
10000
0
0
50
100
150
200
250
300

(a)

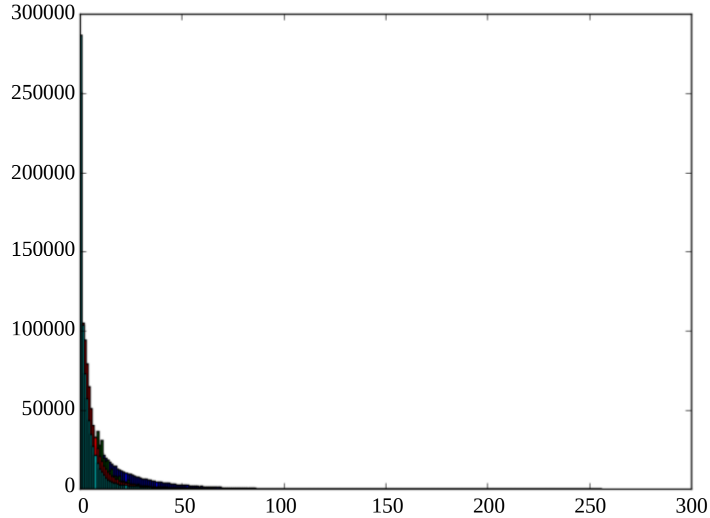

300000
250000
200000
150000
100000
50000
0
0
50
100
150
200
250
300

(b)

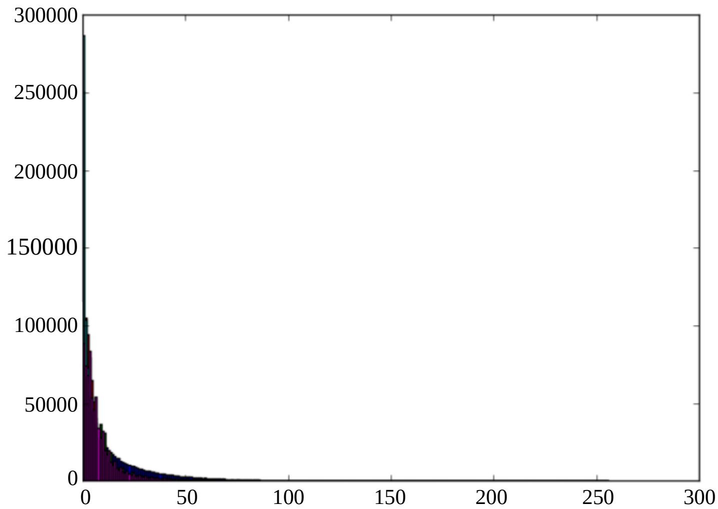

300000
250000
200000
150000
100000
50000
0
0
50
100
150
200
250
300

(c)

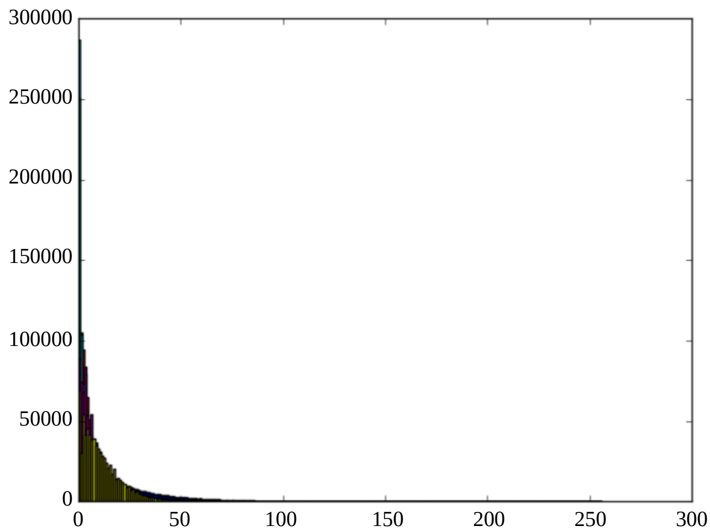
DOI: 10.3844/jcssp.2019.1538.1545



(d)

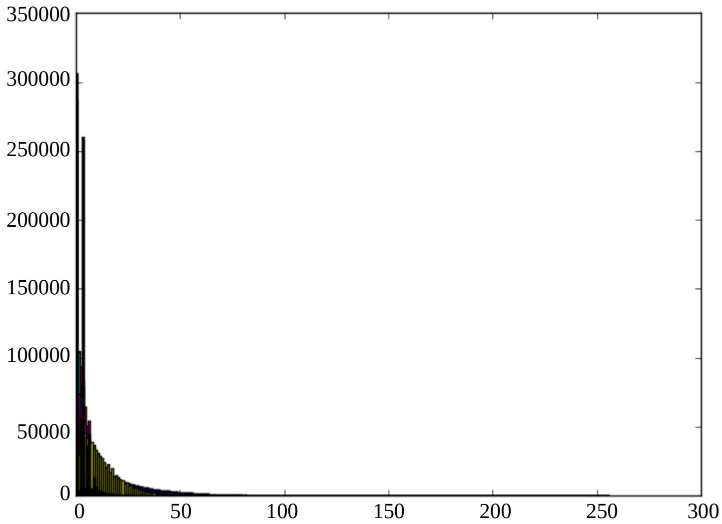


(e)



(f)

DOI: 10.3844/jcssp.2019.1538.1545



(g)

Fig. 3: Distribution of pixel differences per block (a) Madril (b) Peppers (c) Lena (d) House (e) Tiffany (f) Tank (g) Airplane

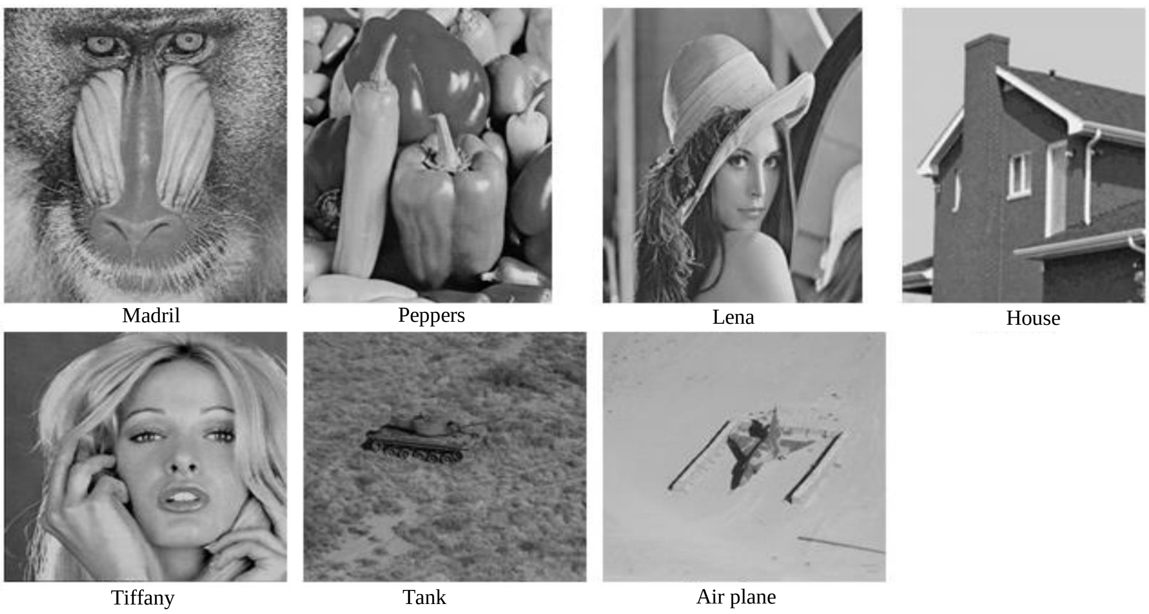


Fig. 4: Cover image for testing

From the cover image and stego image M×N, calculate PSNR using the following formula:

$$PSNR = 10 \bullet \log_{10}\left(\frac{255^2}{MSE}\right) dB \quad (5)$$

The mean square error value is obtained using a formula:

$$MSE = \frac{1}{M \bullet N}\sum_{i=1}^{M}\sum_{j=1}^{N}\left(x_{ij} - y_{ij}\right)^2 \quad (6)$$

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.

Based on Fig. 3, the y axis is the number of pixels, the x axis is pixel the pixel range distribution is grouped at a value of 0 to 50 for all types of images. In the stage of analyzing the spread of the differences of each pixel as the distribution of pixel ranges clustered at the values of 0 to 50 for all types of images. Interval changes above the value of 50 were not too significant for the number of bits to insert.

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

Cover image 512×512	Interval standard		Propose method	
	Capacity (bit)	PSNR (db)	Capacity (bit)	PSNR (db)
Madril	896,283	34.03	1,092,023	31.46
Peppers	799,683	36.23	1,035,204	31.58
Lena	800,996	36.57	1,034,057	32.06
House	778,732	36.87	1,018,308	31.44
Tiffany	812,840	36.37	1,042,386	32.04
Tank	829,824	35.78	1,064,396	31.78
Airplane	764,963	37.68	1,008,712	31.85
Average	811,903		1,042,155	

Table 2: Comparison of the result PBVD with TFPVD

Cover Image	PBVD	TFPVD interval standard	TFPVD propose interval
512×512	Capacity (bits)	Capacity (bits)	Capacity (bits)
Madril	670845	896283	1092023
Peppers	565442	799683	1035204
Lena	570592	800996	1034057
Airplane	556425	764963	1008712
Average	590826	815481	1042499

The comparison of interval standard with propose method in embedding capacity and PSNR are shown in Table 1. For all image storage capacity increases, even though the psnr value decreases but is still at the fair value limit in the naked eye, it is rather difficult to distinguish the difference between the two image cover images and stego image. According to Fig. 3, the highest percentage increase in the airplane image is 24.16% (764,964 to 1,042,155 bits) while the lowest percentage increase in the Madril image is 17.92% (896,283 to 1,092,023 bits) with an average increase of 22.13%.

Table 2 show the experiment comparison result of the embedded capacity of TFPVD algorithm with the PBVD algorithm capacity. The results showed that the proposed TFPVD steganography algorithm has a higher steganographic capacity, which is 1,764 times that of the PBVD algorithm.

Conclusion

In this paper, we have proposed a novel steganography method in spatial domain based on Twenty Five-Pixel Value Differencing (TFPVD). The cover image is made into non-overlapping 5×5 blocks, producing 24 pixel pairs for all possible pixel pairs. Experiment comparison result of the embedded capacity of TFPVD algorithm with the PBVD algorithm capacity. The results showed that the proposed TFPVD steganography algorithm has a higher steganographic capacity, which is 1,764 times that of the PBVD algorithm.

Acknowledgement

This research is supported by Doctoral of Computer Science, Bina Nusantara University.

Author's Contributions

Rojali: Lead research project, program development, do computer experiments, analyze data and write papers.

Ford Lumban Gaol: Supervising research projects, the supervisor designs the application, data analysis review, paper writing, final paper review.

Edi Abdurachman: Supervising research projects, supervising the design of the experiment, data analysis review, paper writing, final paper review.

Benfano Soewito: Supervising research projects, research methodology design advisors, data analysis advisors, final paper reviews.

Ethics

The author states that this paper has never been published and there are no ethical issues in writing.

Conflict of Interest Declaration

The author states that there is no conflict of interests regarding the publication of this paper.

References

Bhuiyan, S.S.N., N.A. Malek and O.O. Khalifa, 2018. An improved image steganography algorithm based on PVD. Indonesian J. Electrical Eng. Comput. Sci., 10: 569-577. DOI: 10.11591/ijeecs.v10.i2.

Chang, K.C., C.P. Chang, P.S Huang and T.M. Tu, 2008. A novel image steganographic method using tri way pixel-value differencing. J. Multimedia, 3: 37-44. DOI: 10.4304/jmm.3.2.37-44

Khodaei, M. and K. Faez, 2012. New adaptive steganographic method using least significant bit substitution and pixel differencing. IET Image Process., 6: 677-86. DOI: 10.1049/iet-ipr.2011.0059

Liao, X., Q. Wen and J. Zhang, 2011. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. J. Visual Commu. Image Represent., 22: 1-8. DOI: 10.1016/j.jvcir.2010.08.007

Liao, X., Q.Y. Wen, Z.L. Zhao and J. Zhang, 2012. A novel steganographic method with four-pixel differencing and modulus function. Fundamenta Informat. 118: 281-289. DOI: 10.3233/FI-2012-714

Pradhan, K., R.K. Sekhar and G. Swain, 2016. Digital image steganography based on seven way pixel value differencing. Ind. J. Sci. Technol., 9: 37-37. DOI: 10.17485/ijst/2016/v9i37/88557

Prasad, S. and A.K. Pal, 2019. Logistic Map-Based Image Steganography Scheme using Combined LSB and PVD for Security Enhancement. In: Emerging Technologies in Data Mining and Information Security, Abraham, A., P. Dutta, J. Mandal, A. Bhattacharya and S. Dutta (Eds.), Springer, Singapore, ISBN-10: 978-981-13-1500-8, pp: 203-214.

Sabokdast, M. and M. Mohammadi, 2013. A steganographic method for images with modulus function and modified LSB replacement based on PVD. Proceedings of the 5th Conference on Information and Knowledge Technology, May 28-30, IEEE Xplore Press, Shiraz, Iran, pp: 121-6. DOI: 10.1109/IKT.2013.6620050

Wang, C.M., N.I. Wu, C.S. Tsai and M.S. Hwanget, 2008. A high quality steganographic method with pixel-value differencing and modulus function. J. Syst. Softw., 81: 150-158. DOI: 10.1016/j.jss.2007.01.049

Wu, D.C. and W.H. Tsai, 2003. A steganographic method for images by pixel-value differencing. Patt. Recogn. Lett., 24: 1636-26. DOI: 10.1016/S0167-8655(02)00402-6

Yu, Y., Z. Ru, L. Jianyi, Y. Wang and F. Huang, 2019. An image steganography algorithm based on pixel block difference and variable modulus function. Proceeding of the 14th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Nov. 26-28, Springer, Sendai, Japan, pp: 36-43. DOI: 10.1007/978-3-030-03748-2_5

Zhang, X and S. Wang, 2004. Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recognit. Letters. 25: 331-339. DOI: 10.1016/j.patrec.2003.10.014