BULGARIAN ACADEMY OF SCIENCES

CYBERNETICS AND INFORMATION TECHNOLOGIES • Volume **22**, No 2
Sofia • 2022 Print ISSN: 1311-9702; Online ISSN: 1314-4081
DOI: 10.2478/cait-2022-0022

Optimization of Cross Diagonal Pixel Value Differencing and Modulus Function Steganography Using Edge Area Block Patterns

Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Pulung Nurtantio Andono, Abdul Syukur, Purwanto

Faculty of Computer Science, Dian Nuswantoro University, Indonesia
E-mails: srustad@dsn.dinus.ac.id moses@dsn.dinus.ac.id pulung@dsn.dinus.ac.id abah.syukur01@dsn.dinus.ac.id purwanto@dsn.dinus.ac.id

***Abstract*:** *The existence of a trade-off between embedding capacity and imperceptibility is a challenge to improve the quality of steganographic images. This research proposes to cross diagonal embedding Pixel Value Differencing* (*PVD*) *and Modulus Function* (*MF*) *techniques using edge area patterns to improve embedding capacity and imperceptibility simultaneously. At the same time still, maintain a good quality of security. By implementing them into 14 public datasets, the proposed techniques are proven to increase both capacity and imperceptibility. The cross diagonal embedding PVD is responsible for increasing the embedding capacity reaching an average value of 3.18 bits per pixel* (*bpp*), *and at the same time, the implementation of edge area block patterns-based embedding is a solution of improving imperceptibility toward an average value of PSNR above 40 dB and that of SSIM above 0.98. Aside from its success in increasing the embedding capacity and the imperceptibility, the proposed techniques remain resistant to RS attacks.*

***Keywords*:** *Pixel value differencing, modulus function, image steganography, edge detection, enhanced payload capacity.*

1. Introduction

Steganography is one of the sciences to secure messages by hiding them in the container media. Messages are generally in the form of text or image data converted into binary data. This binary data is then embedded into the container media using a certain algorithm to camouflage the message on the container media [1]. The embedding algorithm constitutes two domains: spatial and frequency domains [2-4]. In steganography, the spatial domain is more popular than its frequency counterpart is. This is because the spatial domain steganography has good imperceptibility, while it also provides large embedding capacity [4-6]. The frequency domain is mostly used in watermarking, which requires more robust aspects of the watermark so that it is not easily damaged when manipulated. The spatial domain is more fragile, and the message will fail to be extracted if the container media is manipulated, but this is not

a problem in steganography. Because, in principle, steganography has the main goal of securing the message so that it cannot be read by unauthorized people[5-7].

Some of the popular algorithms in the spatial domain steganography are the Least Significant Bit (LSB), Pixel Value Differencing (PVD), modulus function, etc. The LSB is the most popular among those algorithms, but the traditional LSB is very easy to guess and extract the message content [8, 9]. Therefore, the LSB is still being developed today, where several aspects such as imperceptibility, capacity, and security are being improved. Some of the developments of the LSB method include the application of edge detection [6, 9-11], inversion or bit flipping [5, 12, 13], adaptive pattern [5, 14, 15], and its combination with cryptography [16-19]. The development of the LSB method using edge detection has several advantages, one of which is an increase of capacity and imperceptibility, because the edge area can be embedded with more bits than the smooth area. However, by default, the LSB is not superior in the Structural Similarity Index Measuring (SSIM) tool. It produces a more coarse histogram when a message with a large capacity is embedded [20]. A relatively new method is PVD which has been developed based on the principle of edge detection and the difference in the values of neighbouring pixels [21]. Compared to the LSB, the PVD method excels in embedding capacity, producing stego histogram more similar to the original image, and resulting in a better SSIM value. The PVD method is continuously being developed until now [22-24], and one of the reasons is that it is superior in terms of security due to its being more resistant to attacks based on Regular Singular (RS) analysis [20, 21, 25]. In research [22], the PVD is done with an adaptive pattern based on horizontal and vertical edges to improve stego image quality. This adaptive method significantly improves quality, capacity, and security. Research [23] tests pattern embedding on PVD, namely vertical, horizontal and diagonal neighbours. The test results show that the vertical neighbours provide the best embedding quality but with the lowest embedding capacity, while the diagonal neighbours give the opposite result, and the horizontal neighbours give results in between. This makes the basis for proposing a directional-based adaptive PVD technique. The latest research [24] propose a PVD technique combined with the Modulus Function (MF) to increase capacity, imperceptibility, and security. The research successfully has increased capacity ranging from 3.0 to 3.3 bpp, imperceptibility with PSNR values close to 40dB and SSIM in the range 0.97 to 0.98, and security with very good analytical RS values.

The PVD Algorithm has determined the embedding range according to the difference in neighbouring pixel values, and this is similar to the embedding concept which distinguishes the embedded bit size in the edge area and smooth area [26, 27]. Suppose the initial embedding can be done in the image area that has the most edge areas. In that case, the embedding will be more optimal, especially for embedding with a smaller capacity than the maximum. Based on these hypotheses, this research proposes techniques that improve steganographic methods' performance [24]. Namely increasing the embedding capacity that is not necessarily followed by a decrease of imperceptibility. The trick is to pre-process the image by dividing the image into several parts, then measuring the number of edge areas, and the part with the most edge areas will be embedded first. The cross diagonal PVD is incorporated

in the proposed techniques because it increases the maximum embedding capacity [23].

2. Literature review

2.1. Combination of Pixel Value Differencing (PVD) and Modulus Function (MF)

The MF has been combined with the PVD method to improve the quality of the stego image [24, 28-30]. By combining MF and PVD, it has been proven that the embedded message capacity can be improved on imperceptibility and security that still are maintained properly. The capacity building usually ranges from 10 to 50 percent, but in the case of [24], the combination of PVD and MF increase capacity up to two times of that reported by [25] as a pioneer of PVD. Research [24] also adopted the FOBP method in research [31], and as a result, PSNR and SSIM values with maximum embedding capacity can approach 40dB and around 0.97, respectively. The implementation of edge area patterns as described in section 3, is regarded as a part of the contribution to enhancing the effectiveness and efficiency of the existing method [24].

2.2. Directional pixel value differencing

The PVD that has been first introduced by [25] is a breakthrough in improving the spatial domain steganography, competing with the LSB method that has already been very popular. The PVD works by dividing image into very small blocks, where each block consists of two pixels. These blocks are formed in a horizontal direction from left to right, up and down. From two pixels that are side by side, the difference in pixel values is calculated to determine the number of bits that can be entered, so it is said that the message embedding is adaptive, unlike LSB, which by default embeds one message bit so that if the message size is one-eighth of the image (for grey cover image) it will be embedded evenly across all image pixels [20]. This is inspired by the theory that the edge area of the image has a higher tolerance for change than the smooth area. The edge area is a part of the image that generally has a higher pixel difference between adjacent pixels. In further research conducted by [23] which aims to develop and analyse the PVD method, it is proven that the direction of a PVD block influences the results of the stego image. Blocks that are formed horizontally, vertically, and diagonally produce different imperceptibility and capacity values due to the difference in the correlation of adjacent pixels.

The vertical block is superior in the imperceptibility aspect but has the smallest capacity; the diagonal block has the most superior capacity, but has the lowest imperceptibility, while the horizontal block is in between of the vertical and diagonal. However, further analysis indicates that the imperceptibility value is slightly lower in the diagonal direction due to the higher number of message bits embedded, and this is indeed a reasonable trade-off in steganography, and an optimization of imperceptibility with a larger capacity is still a search. Fig. 1 shows the three PVD directions selected for embedding: horizontal, vertical, and diagonal. Because the diagonal direction is commonly associated with low pixel value correlation, it provides more spaces for embedding [23].

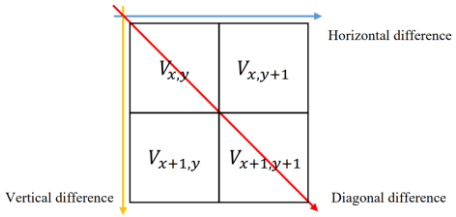

Fig. 1. Blok pixel difference directions

2.3. Edge detection based steganography

Research of edge detection for steganography has been widely carried out and most of the studies combine it with LSB as the simplest method. Researches [6, 32-35] aim to get more edge areas suitable to accommodate a larger number of bits while maintaining imperceptibility and security qualities. However, because the LSB method is the basis of the embedding process, even though it has been combined with edge detection, the security level is not as strong as PVD based on RS analysis. The research method [36] has some characteristics similar to edge detection implementations. This similarity is in the way of embedding, the image is divided into 4×4 non-overlapping blocks, and then these blocks are divided into three categories, namely smooth, less complex, and highly complex. For efficiency, the number of message bits to be embedded differs for each category. More detailed observation reveals that for a 512×512 grayscale image with a hiding capacity ranging from 140,130 to 234,737, its PSNR value is 27.23 dB to 34.19 dB, which is indeed not very satisfactory. However, this method inspires the idea of dividing image into smaller areas in order to provide the best order of embedding as proposed in this paper.

3. Proposed method

This research aims to improve the performance of the combination of PVD and MF methods [24], that is to incorporate a pre-processing based on edge detection [5, 36] and modified diagonal embedding as mentioned in [23]. In the pre-processing stage, the image with a size of 512×512 is divided into 16 blocks; each has a size of 128×128 and does not overlap. The number of edge areas is calculated for each block, and cross embedding direction technique of a modified diagonal embedding is implemented, started from the block with the highest number of edge areas.

The following is a step by step of the proposed embedding method.

Step 1. Read the image; divide it into sixteen equal blocks (Fig. 2). For example, for an image size of 512×512, each block size is 128×128.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Fig. 2. Image divided into sixteen blocks

Step 2. Perform Canny edge detection, then calculate the number of edge areas for each block, and then store it in a matrix (nE) along with the block address.

Step 3. Sort the nE matrix based on the number of edge areas in descending order (from the one with the largest number of edge areas to the smallest). Fig. 3 is an illustration of Steps 2 and 3. Then save the matrix for extraction.

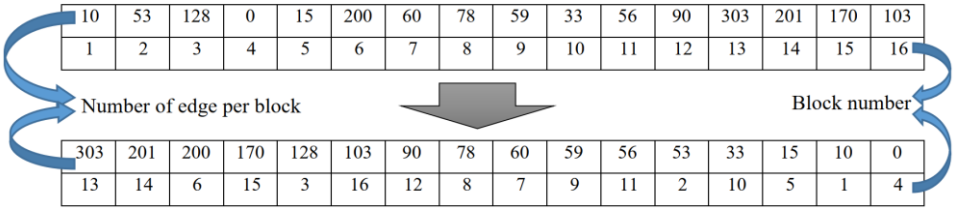

Fig. 3. Example of nE matrix before and after the sorting

Step 4. Read the secret message and convert it into binary form.

Step 5. Embed a message into blocks in the order of matrix nE. For example, in Fig. 3, the 13th block is the first to be embedded, followed by 14th, 6th, until last block.

Step 6. Take a sub-block of four pixels, i.e., $V_{x,y}, V_{x,y+1}, V_{x+1,y}$ and $V_{x+1,y+1}$, (see Fig. 1), where the variables x and y are the coordinates of the pixel V.

Step 7. Find the difference value (diff) of pair pixels ($V_{x,y}$ and $V_{x+1,y+1}$) with

$$\text{diff} = \left|V_{x,y} - V_{x+1,y+1}\right|. \tag{1}$$

Step 8. Find the remainder (r_1, r_2) of the first pixel and the second pixel using

$$(r_1, r_2) = \begin{cases} \left(V_{x,y} \bmod 8,\ V_{x+1,y+1} \bmod 8\right) & \text{if diff} \in R_1, \\ \left(V_{x,y} \bmod 16,\ V_{x+1,y+1} \bmod 16\right) & \text{if diff} \in R_2, \end{cases} \tag{2}$$

where R_1 and R_2, respectively, correspond to diff in the range of 0 to 15 and 16 to 255.

Step 9. Take the message bits (nb) of three bits for each of pair pixel if the diff is in R_1 or take four bits for each of pair pixel if the diff is in R_2.

Step 10. Convert the corresponding message bit (nb) to decimal (d_1) for first pixel ($V_{x,y}$), and d_2 for the second pixel ($V_{x+1,y+1}$). Calculate the difference value of x_1, x_2, y_1, and y_2 using

$$\begin{aligned} x_1 = r_1 - d_1, y_1 = r_2 - d_2, \\ x_2 = d_1 - r_1, y_2 = d_2 - r_2. \end{aligned} \tag{3}$$

Step 11. Obtain the modified pair pixels value ($V'_{x,y}$ and $V'_{x+1,y+1}$) using

$$V'_{x,y} = \begin{cases} V_{x,y} & \text{if } r_1 = d_1, \\ V_{x,y} - x_1 & \text{if } r_1 < d_1 \text{ and } |x_1| < 2^{\text{nb}-1}, \\ V_{x,y} + x_2 & \text{if } r_1 > d_1 \text{ and } |x_2| < 2^{\text{nb}-1}, \\ V_{x,y} - z_1 & \text{if } r_1 < d_1 \text{ and } |x_1| \geq 2^{\text{nb}-1}, \\ V_{x,y} + z_2 & \text{if } r_1 > d_1 \text{ and } |x_2| \geq 2^{\text{nb}-1}, \end{cases} \tag{4}$$

$$V'_{x+1,y+1} = \begin{cases} V_{x+1,y+1} & \text{if } r_2 = d_2, \\ V_{x+1,y+1} - y_1 & \text{if } r_2 < d_2 \text{ and } |y_1| < 2^{nb-1}, \\ V_{x+1,y+1} + y_2 & \text{if } r_2 > d_2 \text{ and } |y_2| < 2^{nb-1}, \\ V_{x+1,y+1} - zz_1 & \text{if } r_2 < d_2 \text{ and } |y_1| \geq 2^{nb-1}, \\ V_{x+1,y+1} + zz_2 & \text{if } r_2 > d_2 \text{ and } |y_2| \geq 2^{nb-1}, \end{cases} \tag{5}$$

where $z_1 = 2^{nb} + x_1$, $z_2 = 2^{nb} + x_2$, $zz_1 = 2^{nb} + y_1$, $zz_2 = 2^{nb} + y_2$.

Step 12. Calculate the new difference value of $\text{diff}' = \left|V'_{x,y} - V'_{x+1,y+1}\right|$. Use the next equation if $\text{diff} \in R_1$ to get stego-pixel pair $V^*_{x,y}$ and $V^*_{x+1,y+1}$,

$$\left(V^*_{x,y}, V^*_{x+1,y+1}\right) = \begin{cases} (V'_{x,y}, V'_{x+1,y+1}) & \text{if } \text{diff}' \in R_1, \\ (V'_{x,y} - 2^{nb}, V'_{x+1,y+1} + 2^{nb}) & \text{if } \text{diff}' \in R_2 \text{ and } V'_{x,y} \geq V'_{x+1,y+1}, \\ (V'_{x,y} + 2^{nb}, V'_{x+1,y+1} - 2^{nb}) & \text{if } \text{diff}' \in R_2 \text{ and } V'_{x,y} < V'_{x+1,y+1}, \end{cases} \tag{6}$$

or the next equation if $\text{diff} \in R_2$:

$$\left(V^*_{x,y}, V^*_{x+1,y+1}\right) = \begin{cases} (V'_{x,y}, V'_{x+1,y+1}), & \text{if } \text{diff}' \in R_2, \\ (V'_{x,y} + 2^{nb}, V'_{x+1,y+1} - 2^{nb}) & \text{if } \text{diff}' \in R_1 \text{ and } V'_{x,y} \geq V'_{x+1,y+1}, \\ (V'_{x,y} - 2^{nb}, V'_{x+1,y+1} + 2^{nb}) & \text{if } \text{diff}' \in R_1 \text{ and } V'_{x,y} < V'_{x+1,y+1}. \end{cases} \tag{7}$$

Step 13. In the case of FOBP use the next equation:

$$(V^*_{x,y}, V^*_{x+1,y+1}) = \begin{cases} \left(V^*_{x,y} + 2^{nb}, V^*_{x+1,y+1} + 2^{nb}\right) & \text{if } V^*_{x,y} \text{ or } V^*_{x+1,y+1} < 0, \\ \left(V^*_{x,y} - 2^{nb}, V^*_{x+1,y+1} - 2^{nb}\right) & \text{if } V^*_{x,y} \text{ or } V^*_{x+1,y+1} > 255. \end{cases} \tag{8}$$

Step 14. Repeat Steps 7-13 for the crossing pair ($V_{x+1,y}$, $V_{x,y+1}$), and continue until one sub-block has been completely embedded.

Step 15. Repeat Steps 7-14 for another subblock until the entire block is embedded.

Step 16. Repeat Steps 6-15 for other blocks, based on the order of the nE matrix, until all message bits are embedded and a stego image is obtained.

Fig. 4 illustrates the stages of the embedding process from Stage 1 to Stage 16.

The next is an extraction process as explained in ten steps.

Step 1. Read the stego image, then divide the image into 16 equal blocks, and next, read the nE matrix as the extraction key.

Step 2. Read the blocks according to the sorted nE matrix.

Step 3. Take a sub-block of pixels, i.e., $V^*_{x,y}, V^*_{x+1,y}, V^*_{x,y+1}$ and $V^*_{x+1,y+1}$.

Step 4. Take a pair of pixels diagonally $(V^*_{x,y}, V^*_{x+1,y+1})$ then find the difference value

$$\text{diff}^* = \left|V^*_{x,y} - V^*_{x+1,y+1}\right|. \tag{9}$$

Step 5. Get the remainder (r_3, r_4) using

$$(r_3, r_4) = \begin{cases} \left(V^*_{x,y} \bmod 8, V^*_{x+1} \bmod 16\right) & \text{if } \text{diff}^* \in R_1, \\ \left(V^*_{x,y} \bmod 16, V^*_{x+1} \bmod 16\right) & \text{if } \text{diff}^* \in R_2. \end{cases} \tag{10}$$

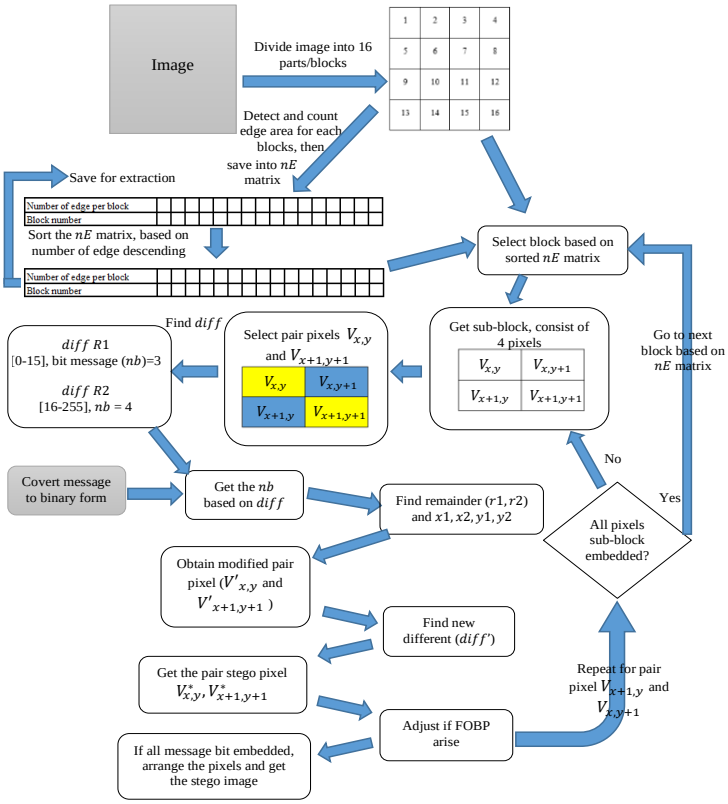

Fig. 4. Proposed embedding procedure

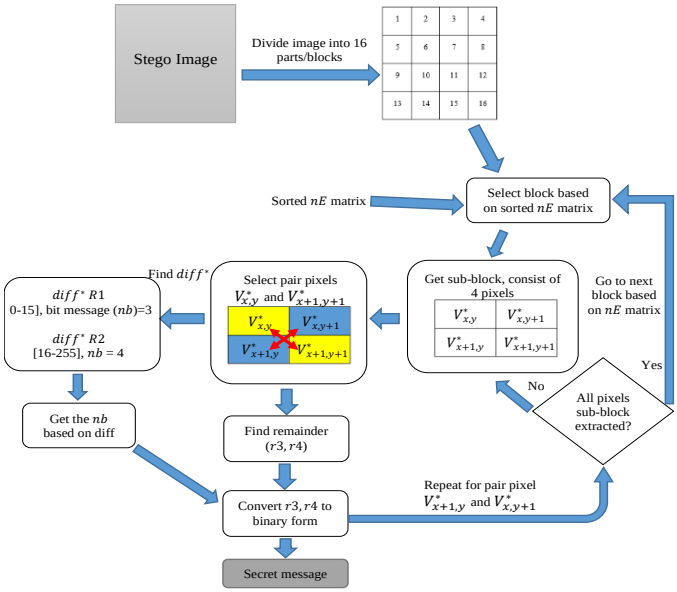

Fig. 5. Proposed extracting procedure

Step 6. Convert the remainder (r_3, r_4) into binary form, three bits for $\text{diff}^* \in R_1$ and four bits for $\text{diff}^* \in R_2$.

Step 7. Perform Steps 5-7 for pair pixels $\left(V^*_{x,y+1}, V^*_{x+1,y}\right)$.

Step 8. Perform Steps 4-8 for the next sub-block.

Step 9. Repeat Steps 4-8 for the next block based on the nE matrix until all messages are extracted.

Step 10. Concatenate the message bits into a secret message and the extraction is complete.

The extraction procedure is illustrated in a diagram as presented in Fig. 5.

4. Results and analysis

The proposed techniques are implemented with the aid of the MATLAB R2015a application, using a laptop that has AMD A12-9720P Radeon R7 specifications, 12 compute cores 4C + 8G 2.70 GHz, 8.00 GB RAM (7.39 GB usable). The cover images are of the standard grayscale presented in Fig. 6, while the secret message is a text generated from the lipsum.com web page.

Fig. 6. Cover image

The stego image imperceptibility is determined by two measuring instruments. They are Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Matrix (SSIM). The PSNR serves to determine the amount of noise that occurs in the stego image, by comparing the stego and the cover images, according to

$$\text{PSNR} = 10\log 10\left(\frac{\max\times\max}{\frac{1}{m\times n}\sum_{x=1}^{m}\sum_{y=1}^{n}(C_{(x,y)}-S_{(x,y)})^2}\right), \tag{11}$$

where m and n are the width and height of the image, x and y are the pixel coordinates, C is the cover image, and S is the stego image, max is maximum pixel intensity.

The greater the PSNR value, the better the quality of the stego image is. Different from PSNR, SSIM is an imperceptibility measurement tool that has several parameters of contrast, luminance, and structure, and its calculation obeys the next equation:

$$\text{SSIM}(C,S) = l(C,S)c(C,S')s(C,S). \tag{12}$$

where l is luminance, c is contrast, and s is structure, which satisfy Equation (13), (14) and (15), respectively,

$$l(C,S') = \frac{2\mu_C\mu_S+C_1}{\mu_C^2+\mu_S^2+C_1}, \tag{13}$$

$$c(C,S') = \frac{2\sigma_C\sigma_S+C_2}{\sigma_C^2+\sigma_S^2+C_2}, \tag{14}$$

$$s(C,S) = \frac{\sigma_{CS}+C_3}{\sigma_C\sigma_S+C_3}, \tag{15}$$

$$\mu_C = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n}C_{xy}}{mno}, \tag{16}$$

$$\sigma_C^2 = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n}(i_{xy}-\mu_C)^2}{mn}, \tag{17}$$

$$\sigma_{CS} = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n}(C_{xy}-\mu_c)(S_{xy}-\mu_S)}{mn}, \tag{18}$$

$$\mu_S = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n}S_{xy}}{mn}, \tag{19}$$

$$\sigma_S^2 = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n}(S_{xy}-\mu_S)^2}{mn}, \tag{20}$$

$$\sigma_{SC} = \frac{\sum_{x=1}^{m}\sum_{y=1}^{n}(S_{xy}-\mu_S)(C_{xy}-\mu_C)}{mn}. \tag{21}$$

The imperceptibility is better as the SSIM value is close to 1, and worse as it is close to 0. While the PSNR is more sensitive to noise caused by the embedded message, the SSIM is close to the principle of Human Visual System (HVS) in recognising the similarity of the histogram between the stego and the original

messages. The increase of PSNR value is not necessarily followed by that of SSIM, and vice versa, but the increase of both PSNR and SSIM at the same time certainly indicate a better quality of imperceptibility [20]. The results of the imperceptibility and capacity measurements of the proposed techniques for 14 datasets are presented in Table 1.

Table 1 shows that each cover image has different characteristic of edge area pattern and accordingly has different block order in embedding the secret message. The edge area pattern based and cross diagonal embedding successfully reach an average maximum capacity of 3.18 bpp with an average PSNR value above 40 dB and an average SSIM above 0.97. These values indicate that the imperceptibility quality is very good at a very large embedding level. The capacity in bpp can be calculated using

$$\text{bpp} = \frac{\text{total bits number embedded}}{\text{number of image pixels in all channels}}. \tag{22}$$

Table 1. Imperceptibility and capacity

Image	PSNR	SSIM	Max capacity (bpp)	Block order
Baboon	38.3274	0.9841	3.44	14, 16, 12, 8, 10, 1, 4, 5, 2, 6, 3, 15, 7, 13, 9, 11
Barbara	39.8651	0.9783	3.27	3, 7, 4, 9, 5, 1, 8, 13, 16, 12, 14, 15, 10, 6, 2, 11
Bee	41.3650	0.9711	3.11	5, 9, 13, 7, 8, 12, 6, 14, 10, 4, 11, 1, 15, 3, 16, 2
Boat	40.0405	0.9766	3.19	3, 14, 4, 16, 7, 15, 13, 12, 11, 8, 10, 1, 9, 5, 6, 2
Cat	39.3986	0.9692	3.20	8, 1, 15, 2, 13, 14, 3, 10, 4, 7, 11, 12, 9, 6, 5, 16
F16	41.2520	0.9733	3.13	12, 16, 15, 10, 9, 3, 11, 2, 8, 4, 6, 1, 5, 13, 7, 14
House	39.8932	0.9760	3.22	1, 6, 2, 5, 10, 9, 8, 3, 7, 15, 11, 12, 14, 13, 16, 4
Lena	41.3364	0.9743	3.11	14, 10, 7, 6, 12, 8, 3, 13, 11, 2, 1, 4, 16, 15, 5, 9
Living room	39.6393	0.9772	3.23	5, 14, 1, 16, 12, 10, 13, 2, 8, 9, 4, 7, 6, 15, 11, 3
Peppers	41.4316	0.9751	3.10	4, 11, 15, 13, 8, 5, 9, 12, 16, 7, 2, 6, 14, 1, 3, 10
Sailboat	39.8568	0.9773	3.21	1, 2, 5, 4, 6, 14, 8, 11, 12, 16, 9, 10, 15, 7, 3, 13
Tank	40.5682	0.9730	3.13	4, 8, 3, 5, 15, 16, 12, 10, 7, 13, 9, 6, 2, 11, 14, 1
Vegetable	40.3172	0.9782	3.14	14, 2, 12, 6, 5, 8, 9, 16, 1, 4, 13, 15, 11, 7, 3, 10
Zelda	41.9007	0.9734	3.06	6, 11, 8, 2, 7, 4, 3, 10, 15, 16, 12, 1, 5, 9, 14, 13
Average	40.3709	0.9755	3.18	

Table 2 presents values of the PSNR, SSIM and embedding capacity of the proposed techniques compared to that of the two related methods, namely [31] and [24], for the same datasets. In various steganographic studies, it is common knowledge that there is a trade-off between imperceptibility and capacity [3, 4], where an increase of capacity causes imperceptibility to decrease and vice versa. Table 2 shows that the results of the proposed techniques are superior to that of the previous method [31] for the three measuring parameters. With better values of SSIM and capacity, they result in a very significant increase of PSNR to reach 38.33-41.90 dB compared to 35.58-35.72 dB. In this case, the proposed techniques are said to be more efficient and imperceptible. In comparison to the previous method [24], the use

of edge area patterns in embedding a secret message as proposed in this study is proven to yield an increase of PSNR values for all cover images, SSIM values for almost all images except Lena, and capacity values for nearly all images but Barbara and Peppers. The fact that the imperceptibility-capacity trade-offs are observed for some cover images indicates that the two methods are competitive. However, the proposed techniques still give the average values of PSNR, SSIM and capacity that are relatively higher than the method [24] does. In general, this research successfully improves the performance of the existing methods. The Cross embedding technique on diagonal PVD of lower adjacent pixel value correlation explains the increasing capacity [23]. Still, the imperceptibility quality will start to decrease if the embedded message reaches maximum embedding capacity.

Table 2. Comparison with existing method

Image	The method in [31]			The method in [24] (PVDMF2)			The method in [9] (x=5, y=4, z=3)			Proposed techniques		
	PSNR	SSIM	Capacity (bpp)	PSNR	SSIM	Capacity (bpp)	PSNR	SSIM	Capacity (bpp)	PSNR	SSIM	Capacity (bpp)
Baboon	35.69	0.96	3.00	36.68	0.98	3.03	33.24	0.96	3.21	38.33	0.98	3.44
Barbara	35.69	0.96	3.00	37.69	0.97	3.30	34.15	0.96	3.10	39.87	0.98	3.27
Boat	35.72	0.97	3.00	38.43	0.97	3.15	33.63	0.96	3.18	40.04	0.98	3.19
Cat	35.58	0.96	3.00	38.08	0.97	3.14	33.88	0.96	3.15	39.40	0.97	3.20
Lena	35.70	0.96	3.00	39.34	0.98	3.09	34.31	0.97	3.10	41.34	0.97	3.11
Living room	35.69	0.97	3.00	38.58	0.98	3.15	33.75	0.96	3.17	39.64	0.98	3.23
Peppers	35.70	0.97	3.00	36.51	0.98	3.34	34.38	0.97	3.09	41.43	0.98	3.10
Tank	35.70	0.97	3.00	39.31	0.97	3.07	34.45	0.97	3.02	40.57	0.97	3.13
Zelda	35.70	0.97	3.00	40.25	0.97	3.04	34.32	0.97	3.09	41.90	0.97	3.06
Average	35.69	0.97	3.00	38.32	0.97	3.15	34.01	0.96	3.12	40.28	0.98	3.19

Security testing is also carried out using RS Analysis to detect the presence or absence of messages embedded in an image [5, 37]. In the RS analysis, it is stated that messages will be detected through two measures, namely the number of regular (R) and singular (S) groups, each of which is given a positive mask ($R_{\mathrm{m}}, S_{\mathrm{m}}$) and negative mask ($R_{-\mathrm{m}}, S_{-\mathrm{m}}$). Where the mask value used in the research is 0110. The plot of R and S values indicate a safe embedding if $R_{\mathrm{m}} \approx R_{-\mathrm{m}} > S_{\mathrm{m}} \approx S_{-\mathrm{m}}$ and $R_{-\mathrm{m}} - S_{-\mathrm{m}} > \mathrm{R}_{\mathrm{m}} - S_{\mathrm{m}}$.

Fig. 7 presents plots of RS values for Barbara, F16, Lena and Peppers to represent the same plot of RS values of all cover images. All plots show that RS values meet the requirements of $R_{\mathrm{m}} \approx R_{-\mathrm{m}} > S_{\mathrm{m}} \approx S_{-\mathrm{m}}$ and $R_{-\mathrm{m}} - S_{-\mathrm{m}} > R_{\mathrm{m}} - S_{\mathrm{m}}$. Therefore, the proposed techniques work very well in terms of security because it is resistant to RS attacks.

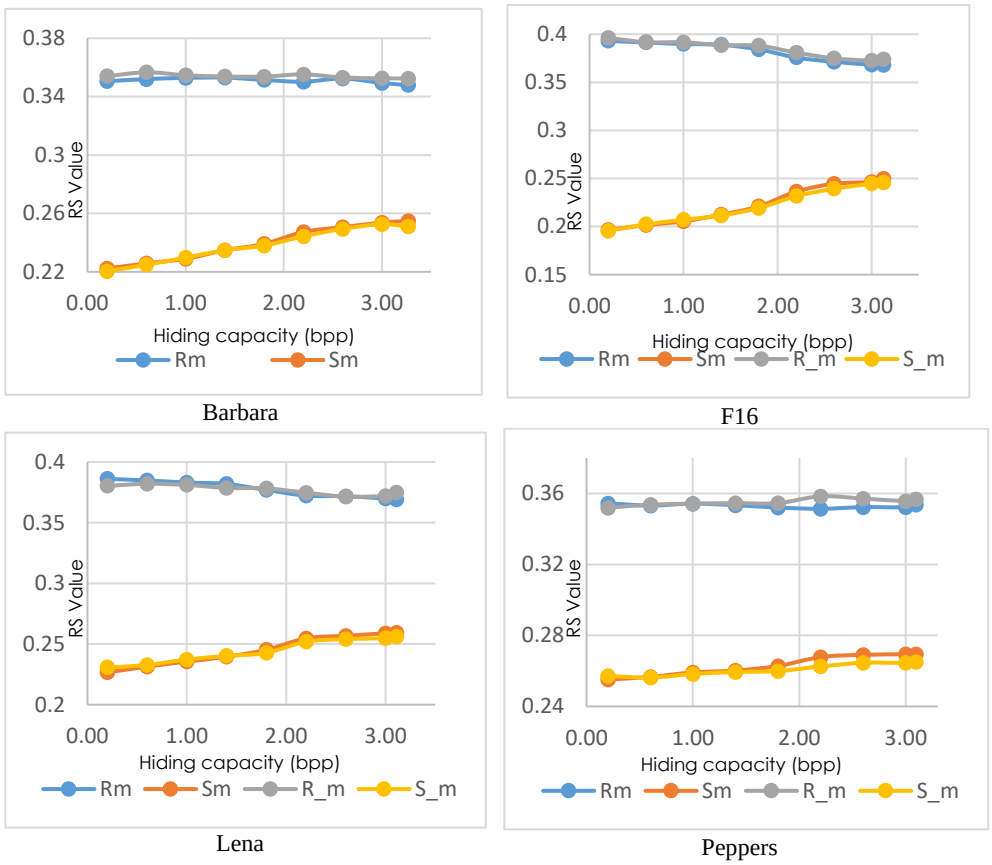

Fig. 7. Plots of RS values for Barbara, F16, Lena and Peppers

In the last stage, an extraction test is also carried out, where the embedded message of the stego image should ideally be successfully extracted perfectly. To measure the effectiveness of the extraction process, Bit Error Rate (BER), as in Equation (23) is used as a measuring tool. BER is used to find out how big the number of bit errors in the extraction process is, and the ideal BER value is 0, which means that there are no error bits in the extraction process. The extraction process results are managed to get a value of BER=0,

$$\text{BER} = \sum_{i=1}^{n} m_i \oplus m'_i, \tag{23}$$

where n is the number of message bits, i is the message bit index, m is the original message, and m' is the message extraction.

5. Conclusion

As there is a trade-off between imperceptibility and embedding capacity in implementing a steganographic method, this research does an optimization by combining cross diagonal PVD and modulus function, using edge area patterns to

improve both the imperceptibility and embedding capacity simultaneously. While the cross diagonal PVD and MF are meant to increase payloads since they are associated with lower pixel value correlation, the use of edge area patterns in embedding secret messages is essential for this process to work efficiently to yield better imperceptibility. Compared to the existing method, the proposed techniques are successfully improving the average value of PSNR to reach 40.28 (from 38.32 dB), that of SSIM to become 0.98 (from 0.97), and that of embedding capacity to be 3.19 (from 3.15 bpp). Based on the average values of PSNR, SSIM and capacity for all images, cross embedding technique on diagonal PVD using edge area patterns, is proven to be suitable in increasing both the imperceptibility and capacity simultaneously while still maintaining its resistance to RS attacks.

References

1. Darwis, D., A. Junaidi, D. A. Shofiana. Wamiliana: A New Digital Image Steganography Based on Center Embedded Pixel Positioning. – Cybernetics and Information Technologies, Vol. **21**, 2021, No 2, pp. 89-104.
2. Cheddad, A., J. Condell, K. Curran, P. Mc Kevitt. Digital Image Steganography: Survey and Analysis of Current Methods. – Signal Processing, Elsevier, 2010.
3. Hussain, M., A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, K.-H. Jung. Image Steganography in Spatial Domain: A Survey. – Signal Process. Image Commun., Vol. **65**, 2018, pp. 46-66.
   https://doi.org/10.1016/j.image.2018.03.012
4. Kadhim, I. J., P. Premaratne, P. J. Vial, B. Halloran. Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research. – Neurocomputing, Vol. **335**, 2019, pp. 299-326.
   https://doi.org/10.1016/j.neucom.2018.06.075
5. Rustad, S., D. R. I. M. Setiadi, A. Syukur, P. N. Andono. Inverted LSB Image Steganography Using Adaptive Pattern to Improve Imperceptibility. – J. King Saud Univ., Comput. Inf. Sci., 2021.
   https://doi.org/10.1016/j.jksuci.2020.12.017
6. Setiadi, D. R. I. M. Improved Payload Capacity in LSB Image Steganography Uses Dilated Hybrid Edge Detection. – J. King Saud Univ., Comput. Inf. Sci., 2019.
   https://doi.org/10.1016/j.jksuci.2019.12.007
7. Wang, Y., M. Tang, Z. Wang. High-Capacity Adaptive Steganography Based on LSB and Hamming Code. – Optik (Stuttg), Vol. **213**, 2020, 164685.
   https://doi.org/10.1016/j.ijleo.2020.164685
8. Pradhan, A., K. R. Sekhar, G. Swain. Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edges in Six-Pixel Blocks. – Secur. Commun. Networks., Vol. **2017**, 2017.
   https://doi.org/10.1155/2017/1924618
9. Setiadi, D. R. I. M., J. Jumanto. An Enhanced LSB-Image Steganography Using the Hybrid Canny-Sobel Edge Detection. – Cybernetics and Information Technologies, Vol. **18**, 2018, No 2, pp. 74-88.
10. Bai, J., C.-C. Chang, T.-S. Nguyen, C. Zhu, Y. Liu. A High Payload Steganographic Algorithm Based on Edge Detection. – Displays, Vol. **46**, 2017, pp. 42-51.
11. Mukherjee, S., G. Sanyal. Edge Based Image Steganography with Variable Threshold. – Multimed. Tools Appl., Vol. **78**, 2019, pp. 16363-16388.
12. Nashat, D., L. Mamdouh. An Efficient Steganographic Technique for Hiding Data. – J. Egypt. Math. Soc., Vol. **27**, 2019, 57.
13. Sahu, A. K., G. Swain, E. S. Babu. Digital Image Steganography Using Bit Flipping. – Cybernetics and Information Technologies, Vol. **18**, 2018, No 1, pp. 69-80.

14. M u h a m m a d, K., J. A h m a d, N. U. R e h m a n, Z. J a n, M. S a j j a d. CISSKA-LSB: Color Image Steganography Using Stego Key-Directed Adaptive LSB Substitution Method. – Multimed. Tools Appl., Vol. **76**, 2017, pp. 8597-8626.
15. H a m e e d, M. A., M. H a s s a b a l l a h, S. A l y, A. I. A w a d. An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient and PVD-LSB Techniques. – IEEE Access., Vol. **7**, 2019, pp. 185189-185204.
16. P a k, C., J. K i m, K. A n, C. K i m, K. K i m, C. P a k. A Novel Color Image LSB Steganography Using Improved 1D Chaotic Map. Multimed. – Tools Appl., Vol. **79**, 2020, pp. 1409-1425.
17. S h a r a f i, J., Y. K h e d m a t i, M. M. S h a b a n i. Image Steganography Based on a New Hybrid Chaos Map and Discrete Transforms. – Optik, Vol. **226**, 2021, 165492.
https://doi.org/10.1016/j.ijleo.2020.165492
18. S a r i, C. A., G. A r d i a n s y a h, D. R. I. M. S e t i a d i, E. H. R a c h m a w a n t o. An Improved Security and Message Capacity Using AES and Huffman Coding on Image Steganography. – TELKOMNIKA (Telecommunication Comput. Electron. Control), Vol. **17**, 2018, pp. 2400-2409
19. A s t u t i, Y. P., D. R. I. M. S e t i a d i, E. H. R a c h m a w a n t o, C. A. S a r i. Simple and Secure Image Steganography Using LSB and Triple XOR Operation on MSB. – In: Proc. of International Conference on Information and Communications Technology, ICOIACT'18, Yogyakarta, 2018.
20. S e t i a d i, D. R. I. M. PSNR vs. SSIM: Imperceptibility Quality Assessment for Image Steganography. Multimed. – Tools Appl., Vol. **80**, 2021, pp. 8423-8444.
21. S w a i n, G. Digital Image Steganography Using Eight-Directional PVD against RS Analysis and PDH Analysis. – Adv. Multimed., Vol. **2018**, 2018.
22. S w a i n, G. Adaptive Pixel Value Differencing Steganography Using Both Vertical and Horizontal Edges. – Multimed. Tools Appl., Vol. **75**, 2016, pp. 13541-13556.
https://doi.org/10.1007/s11042-015-2937-2
23. A b d e l H a m e e d, M., S. A l y, M. H a s s a b a l l a h. An Efficient Data Hiding Method Based on Adaptive Directional Pixel Value Differencing (ADPVD). – Multimed. Tools Appl., Vol. **77**, 2018, pp. 14705-14723.
https://doi.org/10.1007/s11042-017-5056-4
24. S a h u, A. K., G. S w a i n. An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function. – Wirel. Pers. Commun., Vol. **108**, 2019, pp. 159-174.
https://doi.org/10.1007/s11277-019-06393-z
25. W u, D.-C., W.-H. T s a i. A Steganographic Method for Images by Pixel-Value Differencing. – Pattern Recognit. Lett., Vol. **24**, 2003, pp. 1613-1626.
https://doi.org/10.1016/S0167-8655(02)00402-6
26. S w a i n, G. Two New Steganography Techniques Based on Quotient Value Differencing with Addition-Subtraction Logic and PVD with Modulus Function. – Optik (Stuttg)., Vol. **180**, 2019, pp. 807-823.
https://doi.org/10.1016/j.ijleo.2018.11.015
27. L i n, W. B., T. H. L a i, C. L. C h o u. Chi-Square-Based Steganalysis Method against Modified Pixel-Value Differencing Steganography. – Arab. J. Sci. Eng., Vol. **469**. 2021, No 46, pp. 8525-8533.
https://doi.org/10.1007/S13369-021-05554-2
28. S h e n, S., L. H u a n g, Q. T i a n. A Novel Data Hiding for Color Images Based on Pixel Value Difference and Modulus Function. – Multimed. Tools Appl., Vol. **74**, 2015, pp. 707-728.
https://doi.org/10.1007/s11042-014-2016-0
29. L i, Z., Y. H e. Steganography with Pixel-Value Differencing and Modulus Function Based on PSO. – J. Inf. Secur. Appl., Vol. **43**, 2018, pp. 47-52.
https://doi.org/10.1016/j.jisa.2018.10.006
30. W a n g, Z., J. Z h a n g, X. L i a o, Q. W e n. Data Embedding Based on Pixel Value Differencing and Modulus Function Using Indeterminate Equation. – J. China Univ. Posts Telecommun., Vol. **22**, 2015, pp. 95-100.
https://doi.org/10.1016/S1005-8885(15)60631-8

31. J u n g, K. H. High-Capacity Data Hiding Scheme Based on Exploiting Modification Direction and Modulo Operation. – Adv. Sci. Lett., Vol. **22**, 2016, pp. 2471-2474.
https://doi.org/10.1166/asl.2016.7805
32. G a u r a v, K., U. G h a n e k a r. Image Steganography Based on Canny Edge Detection, Dilation Operator and Hybrid Coding. – J. Inf. Secur. Appl., Vol. **41**, 2018, pp. 41-51.
https://doi.org/10.1016/j.jisa.2018.05.001
33. C h e n, W.-J., C.-C. C h a n g, T. H. N. L e. High Payload Steganography Mechanism Using Hybrid Edge Detector. – Expert Syst. Appl., Vol. **37**, 2010, pp. 3292-3301.
https://doi.org/10.1016/j.eswa.2009.09.050
34. A l-D m o u r, H., A. A l-A n i. A Steganography Embedding Method Based on Edge Identification and XOR Coding. – Expert Syst. Appl., Vol. **46**, 2016, pp. 293-306.
https://doi.org/10.1016/j.eswa.2015.10.024
35. I o a n n i d o u, A., S. T. H a l k i d i s, G. S t e p h a n i d e s. A Novel Technique for Image Steganography Based on a High Payload Method and Edge Detection. – Expert Syst. Appl., Vol. **39**, 2012, pp. 11517-11524.
https://doi.org/10.1016/j.eswa.2012.02.106
36. K u m a r, R., D. S. K i m, K. H. J u n g. Enhanced AMBTC Based Data Hiding Method Using Hamming Distance and Pixel Value Differencing. – J. Inf. Secur. Appl., Vol. **47**, 2019, pp. 94-103.
https://doi.org/10.1016/j.jisa.2019.04.007
37. F r i d r i c h, J., M. G o l j a n, R. D u. Detecting LSB Steganography in Color and Gray-Scale Images. – IEEE Multimed., Vol. **8**, 2001, pp. 22-28.
https://doi.org/10.1109/93.959097

Received: 23.11.2021; Second Version: 01.04.2022; Accepted: 18.04.2022