Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-19059-1

Dynamic data hiding capacity enhancement for the Hybrid Near Maximum Histogram image steganography based on Multi-Pixel-Pair approach

Adnan Sondas[1] · Necla Bandirmali Erturk[2]

Received: 19 June 2023 / Revised: 4 March 2024 / Accepted: 22 March 2024

Abstract

Increasing data hiding capacity and making it difficult to detect presence of any confidential data in stego images are the key objectives in contemporary image steganography research ever-improving the embedding efficiency. With regard to these crucial and challenging points, a new Multi-Pixel-Pair (MPP)-based data hiding approach is proposed in this paper. It can dynamically increase data embedding capacity of the classical Hybrid Near Maximum Histogram (H_{NMH}) image steganography method while well-maintaining the embedding efficiency. In the proposed MPP approach, the peak value as a reference point in the histogram distribution of a cover image is obtained, and accordingly the pixel-pairs of interest where secret data is to be embedded are determined. Then, the pixels of the cover image are scanned sequentially and data hiding is performed on the relevant pixels by using the Least Significant Bit (LSB) method. In an extensive experimental study of the proposed MPP approach, it is shown that the classical H_{NMH} data hiding capacity is dynamically improved 4.74 to 37.48 times while the Peak Signal to Noise Ratio (PSNR) decreases between 6.62 and 13.75 dB, implying both a reasonable trade-off and 7.61% enhanced embedding efficiency performance. Moreover, using the well-known cover image partitioning technique, offering significant improvements in image steganography, and the proposed MPP approach together, can further extend the data hiding capacity about 7.05%.

Keywords Image steganography · H_{NMH} data hiding method · Data hiding capacity · Multi-pixel-pair

✉ Adnan Sondas
asondas@kocaeli.edu.tr

Necla Bandirmali Erturk
nerturk@bandirma.edu.tr

[1] Department of Electronics and Automation, Kocaeli University, Kocaeli, Turkey

[2] Department of Computer Engineering, Bandirma Onyedi Eylul University, Balikesir, Turkey

Published online: 23 April 2024

1 Introduction

In this paper, a new approach called Multi-Pixel-Pair (MPP) is proposed for improving the classical Hybrid Near Maximum Histogram (H_{NMH}) image steganography method known in the literature. Not only can it dynamically boost up the fixed H_{NMH} data hiding capacity but also it can in return provide a reasonably low degradation in the Peak Signal to Noise Ratio (PSNR) and maintain the embedding efficiency beyond the conventional methods.

It is very important that any type of confidential information does not fall into the hands of third parties and that only the relevant authorized people can access it. Digital data hiding (steganography) is one of the leading scientific fields with applied studies carried out for this purpose [1]. It can be essentially performed on different types of digital media (video, audio, image, etc.). Amongst the others, image steganography is the key topic, which is used to hide data in an image of different forms. It fundamentally concerns with an input cover image, confidential information and an output stego (covered) image with hidden data. A cover image refers to the original image as a carrier medium used to hide confidential data. Stego image is the resulting covered image containing the hidden data [1]. The most essential goal in image steganography is to prevent third parties from feeling or perceiving the presence of the secret message. Both increasing the data hiding capacity and making the detection of hidden data difficult by means of least changes possible on the original cover image are important development goals.

The methods presented in the image steganography field can be grouped into frequency (transform) domain and spatial (bit) domain. In the former, different transform operations such as Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) are initially applied to the pixels of a cover image whereas the pixel values of a cover image are explicitly changed in the latter to embed the secret data.

The spatial domain solutions are more favored due to their important advantages with regard to computation time and imperceptibility [2–4]. In the literature, there are many different approaches for embedding data in image files in the spatial domain. The Least Significant Bit (LSB) data hiding method is one of the most well-known techniques and stands out due to its low amount of change in the stego image and high data hiding capacity. It is simply based on replacing the LSBs of the cover image pixels with the bits of the secret data to be embedded. A very small amount of pixel change perceivable as noise occurs in the obtained stego image [5–7]. Different variations of the LSB data hiding technique have been proposed with focus on the challenging high data hiding capacity and excellent stego image quality issues [3, 4, 7, 8].

In addition to many theoretical image steganography studies in the literature, there are various professional and commercial applications in practice. When they are developed, data hiding capacity and PSNR parameters are considered as the key performance indicators in addition to the cost-effectiveness. PSNR practically reflects the similarity between the cover image and the stego image. A high PSNR result indicates that there is little change in the stego image [1]. In all of the methods proposed in image steganography, it is aimed to obtain high PSNR results and maximum embedding efficiency along with the ultimate goal of high data hiding capacity.

In many well-known research studies in the literature, different variations of the LSB method have been used to embed data into cover images [3, 4, 9–11]. A method that hides 8 bits of data in each pixel by using the LSB method was proposed in [3]. PSNR performance of the method was examined after hiding different number of bits in the color channels. In a similar study, a highly secure steganography solution was realized by combining LSB- and Pixel Value Difference (PVD)-based image steganography methods, also deploying the Advanced Encryption Standard (AES) encryption. With this hybrid approach, a reliable solution with both boosted security and high data hiding capacity that was increased by approximately 3% compared to the classical methods was introduced [9]. Another secure image steganography method based on LSB inverse transitions for color images was proposed in [10]. It was proved that if the secret data is embedded up to 1.5 bpp payload capacity, it cannot be detected; however, security vulnerabilities arise with increasing hidden data sizes. In [11], a prevailing secure data hiding method based on LSB and genetic algorithms was proposed to achieve high data hiding capacity as well as small processing times.

Another smart approach based on histogram information of a cover image for data hiding with LSB method was presented in [12]. It mainly makes use of a new algorithm in which the maximum frequency value of the image histogram is used to decide where to embed data. With its reversible data hiding approach, the values to the right of the maximum frequency value are shifted upwards and the secret data is embedded in this emptied part. In terms of performance evaluation, the PSNR results are unfavorable indeed due to the histogram shift in the method.

A method based on image histogram modification, where secret data is embedded directly on or near the maximum value by using contrast correction approaches, was proposed in [13]. The two highest histogram values are used to indicate the two brightness values next to the point where the secret data is to be embedded. This approach allows increasing the data hiding capacity such that the method is repeatedly applied on the outcome stego image created. There are two main drawbacks in this method: the image histogram is shifted and the receiver side needs to be provided with a reference information about the data embedded pixels.

The work presented in this paper has three important contributions about the proposed MPP data hiding approach. First of all, the H_{NMH} [14] image steganography method, which is known in the literature and in practice, is firmly improved by deploying the proposed MPP approach developed. It is also possible to use the MPP approach by adapting it to the other solutions based on known or future H_{NMH}-like data hiding schemes. Secondly, use of the proposed MPP approach together with the classical H_{NMH} and detailed evaluation studies have shown that it is possible to achieve increasing the data hiding capacity about 37.48 times. In addition, use of the partitioning technique for the cover image together with the proposed MPP approach can additionally increase the data hiding capacity about 7.05%. Finally, while most of the emerging approaches to increase data hiding capacity in classical image steganography methods have undesirable PSNR and embedding efficiency results, an appealing performance is obtained considering these two crucial performance metrics by using the proposed MPP approach.

Rest of the paper is organized as follows. Section 2 describes in detail the classical H_{NMH} image steganography method as well as the proposed MPP approach and the cover image segmentation technique. Section 3 presents the performance evaluation of the proposed MPP approach by means of data hiding capacity, embedding efficiency and PSNR results obtained from detailed experimental studies. The last section summarizes the MPP approach, its contributions and future directions.

2 The proposed Multi-Pixel-Pair (MPP) approach for improving data hiding capacity

In this section, the proposed MPP approach and its components are explained in detail to improve especially the data hiding capacity of the classical $\mathrm{H}_{\mathrm{NMH}}$ image steganography method [14]. First of all, the $\mathrm{H}_{\mathrm{NMH}}$ method is concisely described, followed by the data embedding/extraction algorithms and procedures of the proposed MPP approach with flow-charts. Then, the cover image partitioning technique well-known in the literature is highlighted for use in conjunction with the proposed MPP approach in order to maximize the data hiding capacity performance to the optimal level.

2.1 The classical $\mathrm{H}_{\mathrm{NMH}}$ image steganography method

The $\mathrm{H}_{\mathrm{NMH}}$ method is based on a fundamental algorithm in which hybrid use of cover image histogram distribution and LSB technique is essential [14]. It can be shortly explained that the histogram information of the cover image is used to determine pixel values of interest where secret data is to be embedded. The secret data is then hidden into the pixels of interest by using the LSB technique.

Firstly, brightness value (P) with the highest number of occurrences (vertex value) in the cover image histogram is determined. This is the key parameter in the $\mathrm{H}_{\mathrm{NMH}}$ method and also used as a reference value in the proposed MPP approach. Equation 1 is used to determine the pixels (p_g) to be used in the data hiding phase. If the brightness value of the reference value P is odd, two brightness values bigger than P, otherwise two brightness values smaller than P are used for data hiding. Than the secret data is embedded by using the LSB technique only to the pixels of interest determined through Eq. 1.

$$p_g = \begin{cases} \mathit{If\ P\ is\ even}, (P-1)\ \mathit{and}\ (P-2) \\ \mathit{If\ P\ is\ odd}, (P+1)\ \mathit{and}\ (P+2) \end{cases}, \tag{1}$$

where P is the maximum number of brightness values and p_g is the pixel values to be used for data hiding [14, 15].

In the classical $\mathrm{H}_{\mathrm{NMH}}$ method, since secret data is embedded into the pixels at different regions of the cover image, resulting pixel changes are spread throughout the stego image. Consequently, the changes are highly imperceptible thus making it difficult to perceive whether any data is hidden in the stego image.

Figure 1 shows the determination of the brightness values to be used in the data hiding process depending on whether the P value is even or odd. In the $\mathrm{H}_{\mathrm{NMH}}$ method, only one pixel-pair is used for data hiding [14, 15]. This indeed leads to inefficient utilization of the cover image, resulting in relatively low data hiding capacity. Considering this challenging weakness point, the proposed MPP approach has been developed and deployed to increase the data hiding capacity of the classical $\mathrm{H}_{\mathrm{NMH}}$ method while keeping the consequent PSNR changes relatively small.

2.2 The proposed MPP approach and its deployment for the classical $\mathrm{H}_{\mathrm{NMH}}$ method

As explained in the previous sub-section, since only one-pixel pair is used for data hiding in the $\mathrm{H}_{\mathrm{NMH}}$ method, the cover image is utilized inefficiently; therefore, the data hiding

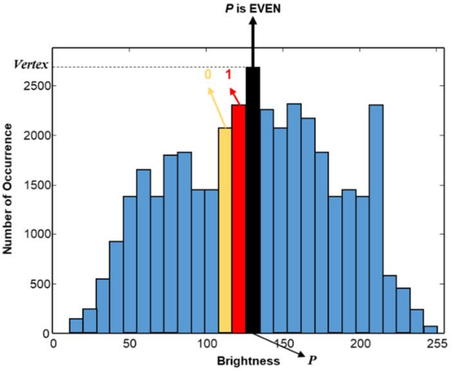


Fig. 1 Determining the brightness value of the pixels (P) to be used for data hiding in the classical $\mathrm{H_{NMH}}$ method [14]

capacity is usually low for common application types in the field. The proposed MPP approach, which aims at eliminating this key drawback and is developed for use in the $\mathrm{H_{NMH}}$ method to dynamically increase or optimize the limited data hiding capacity, is presented below.

In the proposed MPP approach, first of all, the brightness value (P) with the maximum vertex value (frequency of occurrence) in the image histogram is obtained. After that, the pixel brightness values to be used in the data hiding process are determined as defined in Eq. 2. If the P value is odd, the brightness values at its right side are used for data hiding, and if the P value is even, the brightness values at its left side are used for data hiding.

$$p_g = \begin{cases} (P-1)\ldots(P-2n) & \text{if } P \text{ is even} \\ (P+1)\ldots(P+2n) & \text{if } P \text{ is odd} \end{cases}, \tag{2}$$

where P is the maximum number of brightness values, p_g is the pixel pairs to be used for data hiding and n is the number of pixel pairs to be used.

Figure 2 shows the brightness values to be used for three pixel-pairs depending on whether the P value is even or odd. The brightness values where the secret data is to be

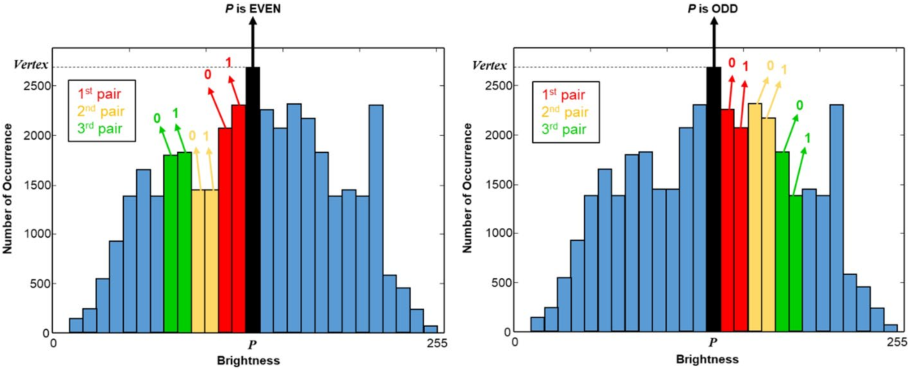


Fig. 2 Determining the brightness value of the pixels to be used for data hiding in three pixel-paired MPP approach

embedded according to the P value are determined by using the Eq. 2. When the number of pixel-pairs used for data hiding needs to be transmitted to the receiver side, it leads to various disadvantages in similar techniques as explained in the previous section. Considering this fact in the proposed MPP processes, if the maximum number of pixel-pairs is used, the pixel brightness values where the secret data to be embedded is determined according to Eq. 3, which indeed already eliminates the need to send the number of pixel-pairs to the receiver side. It consequently enables that the maximum data hiding capacity can be dynamically achieved.

$$p_g = \begin{cases} (P-1)\ldots 0 & \textit{if P is even} \\ (P+1)\ldots 255 & \textit{if P is odd} \end{cases} \tag{3}$$

With regard to secret data, initially the American Standard Code for Information Interchange (ASCII) equivalents of the characters in the text message are converted into binary numbers (Fig. 3). Each character is represented in 9-bit binary numbers, considering different characters in other language alphabets. The fundamental rules that form the center of the proposed MPP approach and the procedures applied for data embedding are summarized step by step as follows:

Step 1. Each character of the secret text message is converted to its 9-bit ASCII equivalent. NULL $(000000000)_2$ is then appended to this obtained ASCII equivalent to indicate end of the message.
Step 2. The "P" value with the highest number of occurrence (Vertex) in the cover image histogram distribution is obtained.
Step 3. The number of pixel pairs (n) to be used for data hiding is pre-defined. If the maximum number of pixel pairs is to be used, this step is skipped.
Step 4. Depending on both the "n" value and whether the "P" value is odd or even, the brightness values of the pixels, where the secret data is to be embedded, are determined (Eqs. 2 and 3).
Step 5. The bit (binary) value of the secret data to be embedded into the cover image is read.
Step 6. The pixels of the cover image are scanned sequentially. When the pixel values determined according to Eqs. 2 and 3 are encountered, the secret data bit value obtained in Step 5 is placed in the relevant pixel by using LSB method.
Step 7. Return to Step 5 until all bits of the secret data are embedded into the cover image.

Figure 3 shows the flowchart of the proposed MPP approach for the data hiding phase. Yellow colored parts represent the different or newly added functions and processes of the new MPP approach with respect to the classical $\mathrm{H_{NMH}}$ method.

At the receiver side, the embedded data bit sequence is recovered from the stego image without any further information or prerequisite other than the embedded data extraction algorithm of the proposed MPP approach (Fig. 4). Hidden data extraction is performed according to Eq. 4 as follows:

$$b_i = \begin{cases} P\ is\ EVEN,\ p_t < P,\ 0\ if\ p_t \equiv 0 (mod\ 2) \\ P\ is\ EVEN,\ p_t < P,\ 1\ if\ p_t \equiv 1 (mod\ 2) \\ P\ is\ ODD,\ p_t > P,\ 0\ if\ p_t \equiv 0 (mod\ 2) \\ P\ is\ ODD,\ p_t > P,\ 1\ if\ p_t \equiv 1 (mod\ 2) \end{cases}, \tag{4}$$

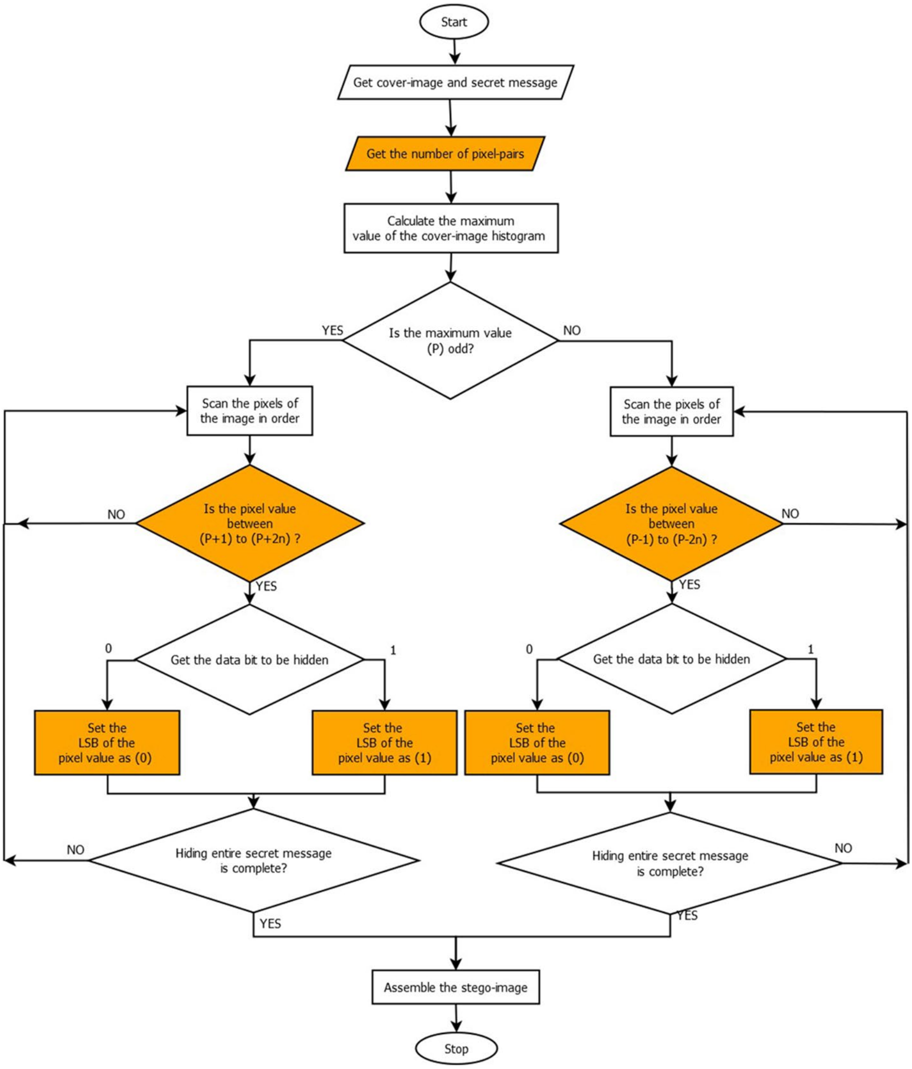

Start
Get cover-image and secret message
Get the number of pixel-pairs
Calculate the maximum value of the cover-image histogram
Is the maximum value (P) odd?
YES
NO
Scan the pixels of the image in order
Scan the pixels of the image in order
Is the pixel value between (P+1) to (P+2n) ?
NO
YES
Is the pixel value between (P-1) to (P-2n) ?
NO
YES
Get the data bit to be hidden
0
1
Get the data bit to be hidden
0
1
Set the LSB of the pixel value as (0)
Set the LSB of the pixel value as (1)
Set the LSB of the pixel value as (0)
Set the LSB of the pixel value as (1)
Hiding entire secret message is complete?
NO
YES
Hiding entire secret message is complete?
NO
YES
Assemble the stego-image
Stop

Fig. 3 Flow chart diagram of the proposed MPP approach for the data hiding phase

where p_t is the pixel value encountered during covered image scanning step, b_i is the i^{th} element of the hidden data bit sequence, and P is the maximum brightness value (Vertex). The fundamental rules that form the proposed MPP approach and its procedures for data extraction are summarized step by step as follows:

Step 1. The "*P*" value with the highest number of occurrence (Vertex) in the stego image histogram distribution is obtained.

Step 2. The number of pixel pairs (n) used for data hiding is determined. If the maximum number of pixel pairs is to be used, this step is skipped.

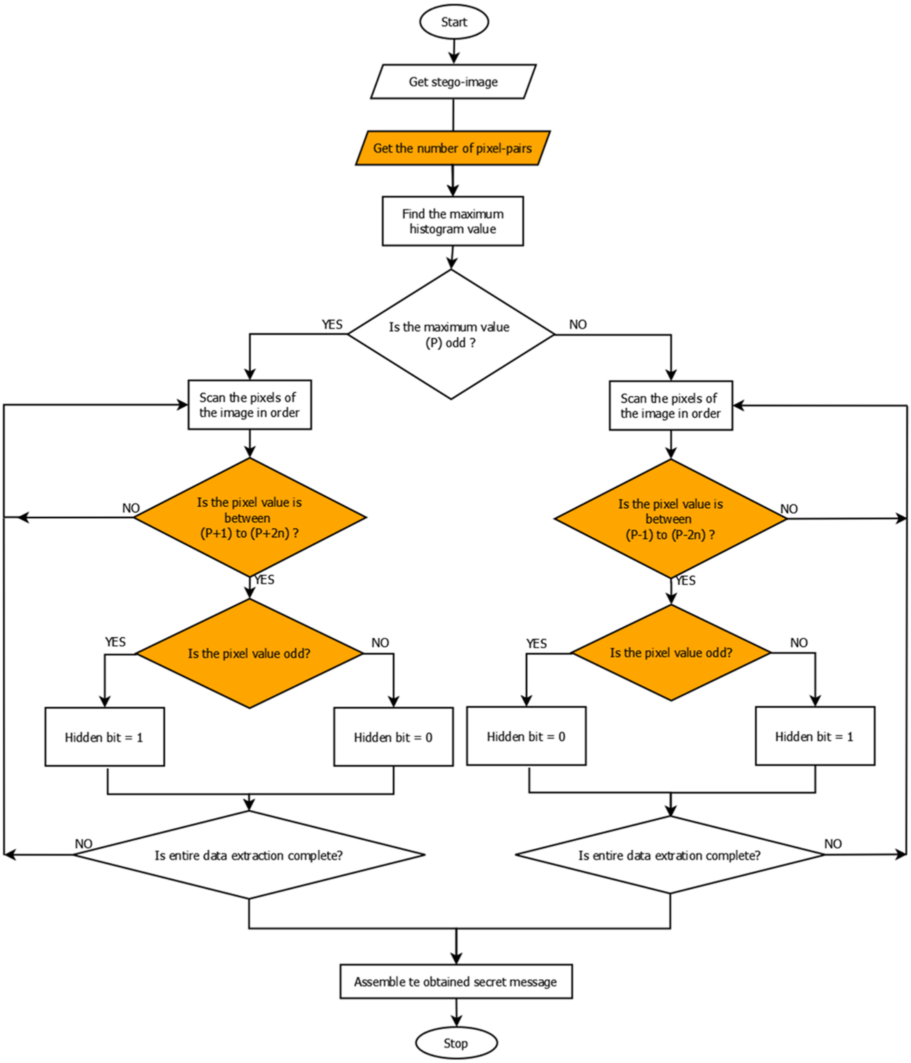

Start
Get stego-image
Get the number of pixel-pairs
Find the maximum histogram value
Is the maximum value (P) odd ?
YES
NO
Scan the pixels of the image in order
Scan the pixels of the image in order
Is the pixel value is between (P+1) to (P+2n) ?
NO
YES
Is the pixel value is between (P-1) to (P-2n) ?
NO
YES
Is the pixel value odd?
YES
NO
Is the pixel value odd?
YES
NO
Hidden bit = 1
Hidden bit = 0
Hidden bit = 0
Hidden bit = 1
Is entire data extraction complete?
NO
Is entire data extration complete?
NO
Assemble te obtained secret message
Stop

Fig. 4 Flow chart diagram of the proposed MPP approach for the data extraction phase

Step 3. Depending on both the “n” value and whether the “P” value is odd or even, the brightness values pointing out the pixels with hidden data are determined (Eq. 4).

Step 4. The pixels of the stego image are processed sequentially. Based on Eq. 4, the embedded data bits are determined and extracted into the secret data bit sequence array.

Step 5. Return to Step 4 until the NULL $(000000000)_2$ embedded bit pattern on the stego image is reached finally.

Step 6. The final array of secret data bits obtained in the extraction process is grouped into 9-bit blocks and ASCII coded characters are obtained. After all, the secret message is obtained by performing the necessary inverse conversion.

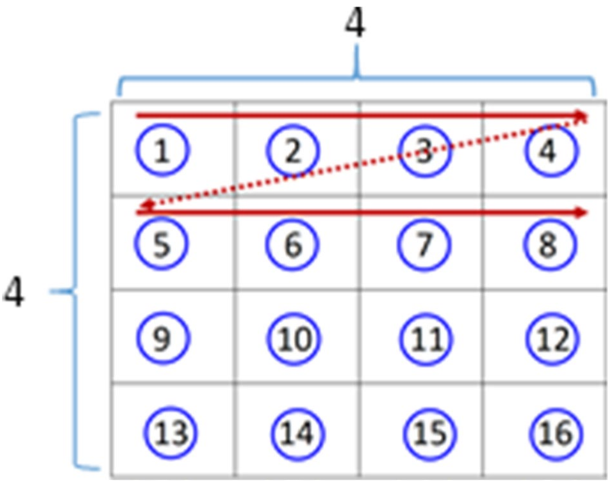
Figure 4 shows the flowchart of the proposed MPP approach for the hidden data extraction phase. The yellow colored parts represent the different or newly added functions and processes of the proposed MPP approach with respect to the classical H_{NMH} method.

2.3 Cover image segmentation usage together with the proposed MPP approach

When the H_{NMH} method is used together with the proposed MPP, only the pixels with brightness values to the left or right of the P value are utilized for data hiding, i.e., not all of the cover image pixels. In other words, the pixels where data is to be embedded are generally located in a specific region of the cover image. That is data hiding can be performed in some parts of the cover image while a remaining large part cannot be utilized efficiently by using the proposed MPP approach. In order to enable the data hiding in an almost all homogeneous manner over the entire cover image and thus to increase the total data hiding capacity, the cover image is divided into small equal parts (partitioning) then the proposed MPP approach is applied separately by considering the histogram of each distinct part independently [16]. Thus, data hiding can be performed on pixels with various brightness values in different parts of the cover image. This also contributes positively to the improvement of the data privacy and security results.

The cover image segmentation algorithm employed to increase data hiding capacity of the proposed MPP approach is presented in Fig. 5. After the cover image is divided into small equal parts, the secret data is embedded in these parts based on the Raster Scan Order direction [17] as shown by the red arrows. Since the "P" value of the histogram of each distinct cover image segment is different, the secret data is embedded into different pixels of a certain brightness value in the corresponding cover image part. As a result, in addition to a significant increase in total data hiding capacity, a high diversity of data embedding pixels can be well achieved with respect to the standard image data hiding method.

Fig. 5 Scan order direction for a sample 4×4 cover-image partitions



3 Experimental studies

MATLAB was used both to implement the proposed MPP approach together with the classical H_{NMH} image data hiding method and to determine its effectiveness with detailed performance tests carried out on different cover images. At the experimental study phase, well-known 8-bit grey-scale 512×512 Baboon, Airplane, Barbara, Fruits, House, Lena, Peppers and Zelda test cover images were used (Fig. 6). Variable-length secret text messages were embedded by using the proposed MPP approach on the cover images just after the segmentation process if any.

The performance evaluation study of the proposed MPP approach for the H_{NMH} method is carried out based on data hiding capacity, embedding efficiency and PSNR metrics. As it is well-known in analysis of image data hiding methods, the comparison of PSNR results for the cover image and stego image provides important information about the visual quality assessment and reflects the trade-off with the achieved data hiding capacity. As the visual difference between a cover image and its stego image version decreases, the PSNR value increases and converges to infinity [18]. The evaluation of the ratio of changing cover image pixels' value is called embedding efficiency, which is defined as the number of secret bits embedded per one embedding change. An increased embedding efficiency clearly implies less detectable traces in the stego image, resulting in better robustness against steganalysis techniques [3, 19].

Figure 7 shows the data hiding capacity and PSNR results for the test cover images, obtained by using the proposed MPP approach, which will be used as a reference in the following comparison and evaluation explanations. As it can be seen from the graphs, the proposed MPP approach increases the data hiding capacity 4.74 to 37.48 times. On the other hand, the PSNR results slightly decrease between 6.62 and 13.75 dB reflecting a reasonable trade-off but more degradation in the stego image quality. When the experimental results for all test cover images are considered together, it can be stated that the data hiding capacity increases 16.69 times on average compared to the classical H_{NMH} method.

Figure 8 shows the experimental results for the cover images that are first divided into 8×8 equal parts then each one employs the proposed MPP approach. Considering

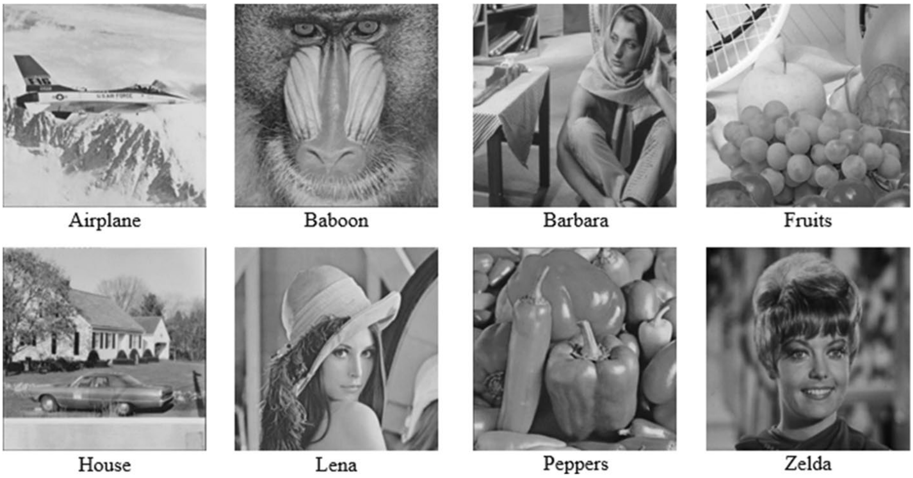


Fig. 6 Gray-scale cover images used in the experimental test phase

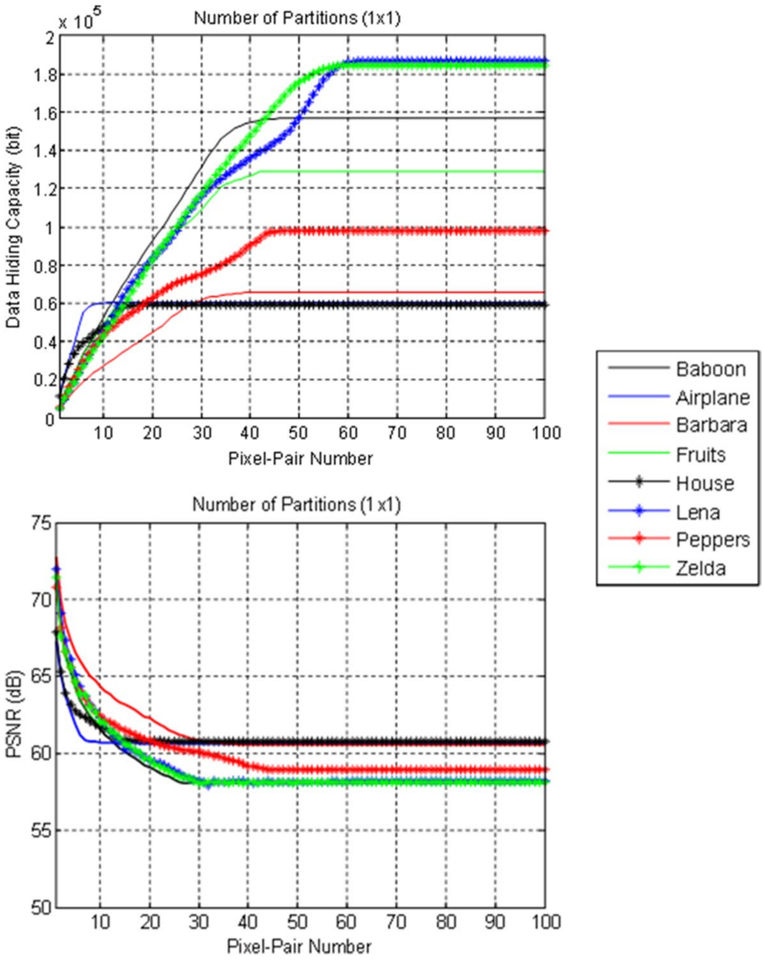


Fig. 7 Data hiding capacity and PSNR results for the proposed MPP approach

the data hiding capacity results for all of the test stego images together, 7.05% increased performance on average is achieved while the PSNR results reasonably decrease about 1.02 dB on average. When these results and the Fig. 7 are analyzed together, it is understood that the partitioning technique does not increase the data hiding capacity much, compared to the classical H_{NMH} method relatively [14]. This is due to the fact that almost all of the pixels are used for data hiding in the proposed MPP approach when the "*P*" value of the cover image is too high or too low. However, when the cover image is partitioned, the value of "*P*" for each equal part is different, which leads to a relative decrease in the amount of data that can be hidden, since the value of the pixels that the secret data to be hidden will change in each part. On the other hand, as an effortless consequence, the change in the value of "*P*" for each cover image partition contributes significantly to the security of the embedded data.

The obtained experimental results for improved data hiding capacities are given in Table 1 for the proposed MPP approach and classical H_{NMH} method with and without image partitioning. Table 2 also provides comparative results with respect to some of the

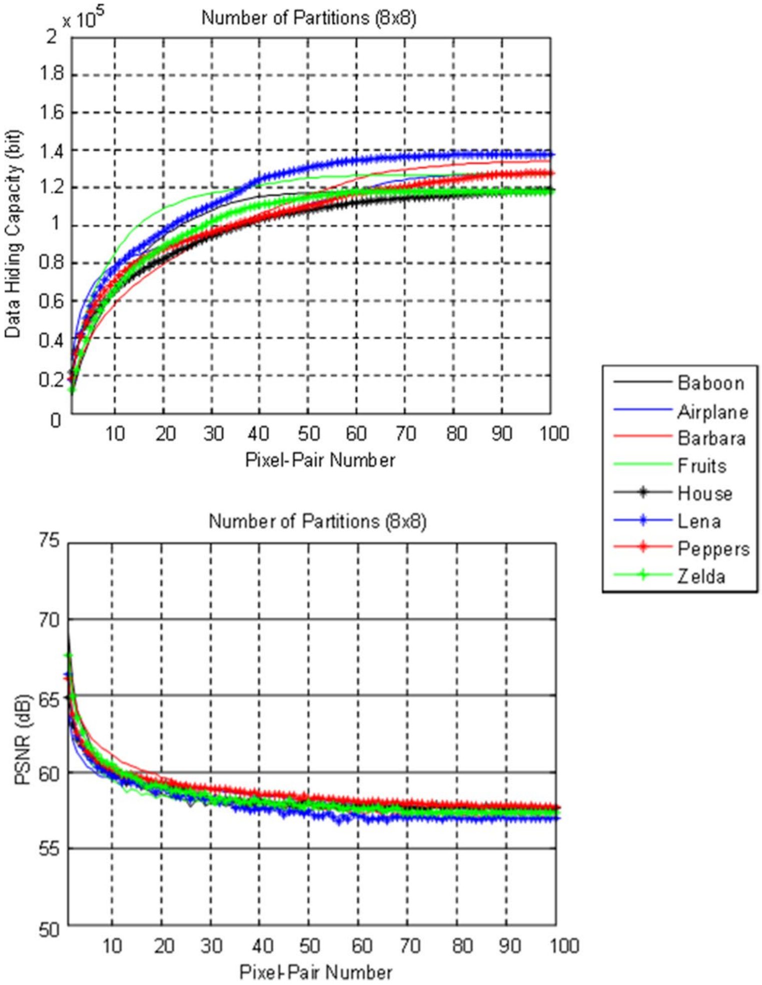


Fig. 8 Data hiding capacity and PSNR results for the proposed MPP approach with 8 × 8 cover image partitioning

current counterpart methods. It can be summarized that the data hiding capacity results of the proposed MPP approach are higher than those of the classical H_{NMH}. However, partitioning the cover image into very small parts (especially for 64 and above) does not necessarily increase the data hiding capacity of the MPP approach linearly. As a result, it is possible to use the partitioning process for the purpose of increasing data hiding capacity, but it only works up to a certain extend effectively with the proposed MPP approach, totally depending on the cover image distinctly. Besides, it is observed that the data hiding capacity performance of the proposed MPP approach deployed together with the cover image partitioning process may be worsen for some test cover images (e.g., Baboon). That is simply because the "*P*" values of these kind of cover images are not close to the extreme points. Moreover, while the total data hiding capacity is expected to increase by dividing the cover image into small equal parts, this process may lead to a degradation in the stego image quality especially after 8 × 8 segmentation.

Table 1 Experimental results for the proposed MPP approach and classical H_{NMH} method

	Data Hiding Capacity (Bit)				PSNR (dB)				Embedding Efficiency				Processing Time (Sec.)			
	Partitioning (1×1)		Partitioning (8×8)		Partitioning (1×1)		Partitioning (8×8)		Partitioning (1×1)		Partitioning (8×8)		Partitioning (1×1)		Partitioning (8×8)	
	H_{NMH}	H_{NMH} with the MPP	H_{NMH}	H_{NMH} with the MPP	H_{NMH}	H_{NMH} with the MPP	H_{NMH}	H_{NMH} with the MPP	H_{NMH}	H_{NMH} with the MPP	H_{NMH}	H_{NMH} with the MPP	H_{NMH}	H_{NMH} with the MPP	H_{NMH}	$H_{NMH}$with the MPP
Airplane	12,767	60,557	28,345	127,731	67.29	60.67	63.88	57.58	4.01	4.14	4.06	4.29	3.22	5.58	1.33	4.49
Baboon	5914	156,785	9517	118,628	71.23	56.80	68.94	57.60	4.60	4.40	4.37	4.01	2.98	6.79	1.40	4.12
Barbara	3906	65,836	12,246	134,016	72.75	60.57	67.65	57.09	4.32	4.40	4.19	4.02	3.14	5.58	1.17	4.29
Fruits	6541	128,889	18,704	127,381	70.78	57.65	65.92	57.59	4.59	4.41	4.28	4.29	3.17	6.54	1.20	4.31
House	11,469	59,284	22,041	119,714	67.90	60.80	64.74	57.61	4.15	4.19	3.85	4.05	3.23	5.49	1.20	4.44
Lena	4982	186,725	17,570	137,855	71.78	56.16	66.33	57.00	4.41	4.53	4.23	4.05	3.09	7.33	1.41	4.39
Peppers	5744	97,719	18,234	127,698	69.77	58.94	65.96	57.70	3.19	4.50	4.22	4.41	3.42	6.12	1.18	4.28
Zelda	5017	184,481	12,493	118,111	70.47	56.12	67.32	57.36	3.28	4.43	3.95	3.77	3.15	7.08	1.15	4.31

Table 2 Maximum data hiding capacity assessment results with respect to PSNR for the proposed MPP approach and its counterparts

	Proposed MPP		Rahman et al. [20]		Nazari et al. [21]		Solak et al. [3]		Shreelekshmi et al. [10]	
	Max. Capacity (bit)	PSNR (dB)	Max. Capacity (bit)	PSNR (dB)	Max. Capacity (bit)	PSNR (dB)	Max. Capacity (bit)	PSNR (dB)	Max. Capacity (bit)	PSNR (dB)
Airplane	60,557	60.67	--	--	179,124	41.58	7770	54.48	--	--
Baboon	156,785	56.80	8192	75.99	50,856	41.64	3037	50.35	157,286	55.00
Barbara	65,836	60.57	--	--	33,722	49.13	2217	54.12	157,286	54.33
Fruits	128,889	57.65	--	--	--	--	2298	51.17	--	--
House	59,284	60.80	8192	69.84	--	--	6655	54.57	--	--
Lena	186,725	56.16	8192	63.90	63,752	49.64	2726	53.69	157,286	54.14
Peppers	97,719	58.94	8192	68.54	74,672	45.51	2920	52.41	157,286	54.38
Zelda	184,481	56.12	--	--	--	--	2588	53.55	157,286	54.39

Considering the embedding efficiency metric given in Eq. 5, which should be maximum, to reflect the cover image degradation and to highlight the stego image quality [3, 19], the overall average of obtained results for the proposed MPP method is 4.38 and clearly better than that of the classical H_{NMH} (Table 1). On the other hand, increasing the number of partitions in the cover image up to 8×8, obviously extremely high data embedding capacities (Table 2) are achievable with a reasonable embedding efficiency trade-off.

$$\text{Embedding Efficiency} = \frac{1}{\text{Ratio of Modified Pixels}} \tag{5}$$

Considering the fact that steganography and cryptography methods jointly have well proven extremely effective in enabling secure connectivity, the proposed MPP approach can be accompanied with emerging solutions such as EGCrypto [22] in order to increase its deployment in real practical networking environments.

4 Conclusion

Increasing or maximizing the data hiding capacity has been one of the most challenging goals in contemporary image steganography research as well as preventing confidential information from falling into the hands of third parties. With regard to this difficult task, the MPP approach is proposed to improve the data hiding capacity of the classical H_{NMH} method known about its high performance in the literature.

In the classical H_{NMH} method and similar ones in the literature, only the pixels with two values to the right or left of the "*P*" value in the cover image histogram are used for data embedding. This obviously results in inefficient utilization of the cover image potential, and hence the data hiding capacity is insufficient or low for many applications. In the development stages of the proposed MPP approach, this crucial drawback has been taken into account such that pixels with all values to the right or left of the "*P*" value in the cover image histogram can be used for data embedding. Thus, the cover image can be utilized much more efficiently and the data hiding capacity increases considerably.

Experimental study results of the proposed MPP approach on different test cover images show that the data hiding capacity can be improved up to 37.48 times with well-trading of the PSNR results while maintaining the embedding efficiency. It is also concluded that an 8×8 cover image segmentation can provide about 7.05% additional increase in data hiding capacity for the proposed MPP approach.

Symbols AES: Advanced Encryption Standard; bpp: bit per pixel; DCT : Discrete Cosine Transform; DWT: Discrete Wavelet Transform; H_{NMH}: Hybrid Near Maximum Histogram data hiding method; LSB: Least Significant Bit data hiding method; MPP: Multiple-Pixel-Pair; MSE: Mean Squared Error; P: Brightness value with the maximum number of occurrence (Vertex); PSNR: Peak Signal to Noise Ratio (dB); PVD: Pixel Value Difference data hiding method

Funding Open access funding provided by the Scientific and Technological Research Council of Türkiye (TÜBİTAK). The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data availability The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

References

1. Yalman Y, Cetin O, Erturk I, Akar F (2014) Veri Gizleme (data hiding). Beta Yayınevi, Istanbul
2. Yalman Y, Erturk I (2014) Secret data embedding scheme modifying the frequency of occurrence of image brightness values. Sadhana Acad Proc Eng Sci 39(4):939–956
3. Solak S, Altinisik U (2019) Image steganography based on LSB substitution and encryption method: adaptive LSB + 3. J Electron Imaging 28(4):043025
4. Datta B, Roy S, Roy S et al (2019) Multi-bit robust image steganography based on modular arithmetic. Multimed Tools Appl 78:1511–1546. https://doi.org/10.1007/s11042-018-6195-y
5. Jung KH (2018) Data hiding scheme improving embedding capacity using mixed PVD and LSB on bit plane. J Real-Time Image Proc 14(1):127–136
6. Pradhan A et al (2018) Digital image steganography using LSB substitution, PVD, and EMD. Math Probl Eng 2018:1–11
7. Konyar MZ, Solak S (2021) Efficient data hiding method for videos based on adaptive inverted LSB332 and secure frame selection with enhanced Vigenere cipher. J Inform Secur Appl 63(C):1–12
8. Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37(3):469–474
9. Shukla AK et al (2018) A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing. IEEE Access 6:51130–51139
10. Shreelekshmi R, Wilscy M, Madhavan CV (2019) Undetectable least significant bit replacement steganography. Multimedia Tools Appl 78(8):10565–10582
11. Wang RZ et al (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn 34(3):671–683
12. Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circuits Syst Video Technol 16(3):354–362
13. Islamy CC, Ahmad T (2019) Histogram-based multilayer reversible data hiding method for securing secret data. Bull Electr Eng Inf 8(3):1128–1134
14. Sondas A, Kurnaz H (2022) H_{NMH}: a new hybrid approach based on Near Maximum Histogram and LSB technique for image steganography. Wireless Pers Commun. https://doi.org/10.1007/s11277-022-09830-8
15. Kurnaz H, Konyar MZ, Sondas A (2020) A new hybrid data hiding method based on near histograms. Eur J Sci Technol 18:683–694
16. Masood F, Driss M, Boulila W, Ahmad J, Rehman SU, Jan SU, Buchanan WJ (2021) A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wireless Pers Commun 1–28
17. Aydogan T, Bayilmis C (2017) A new efficient block matching data hiding method based on scanning order selection in medical images. Turkish J Electr Eng Comput Sci 25:461–473
18. Sencar HT, Ramkumar M, Akansu AN (2004) Data hiding fundamentals and applications. Elsevier, Academic, New York
19. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. Doctor of Philosophy Thesis, University of Buckingham
20. Rahman S, Masood F, Khan WU, Ullah N, Khan FQ, Tsaramirsis G, Jan S, Ashraf M (2020) A novel approach of image steganography for secure communication based on LSB substitution technique. Computers Mater Continua 64(1):31–61
21. Nazari M, Ahmadi ID (2020) A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity. Multimedia Tools Appl 79:13693–13724. https://doi.org/10.1007/s11042-019-08415-1

22. Kaur M et al (2023) EGCrypto: a low-complexity elliptic galois cryptography model for secure data transmission in IoT. IEEE Access 11:90739–90748. https://doi.org/10.1109/ACCESS.2023.3305271

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.