Wireless Personal Communications (2022) 126:2579–2595
https://doi.org/10.1007/s11277-022-09830-8

H_{NMH}: A New Hybrid Approach Based on Near Maximum Histogram and LSB Technique for Image Steganography

Adnan Sondas[1] · **Harun Kurnaz**[1]

Accepted: 28 May 2022 / Published online: 3 August 2022

Abstract
In this paper, a new histogram-based approach for digital image steganography is introduced. It stems from the idea of utilizing the near maximum values in the image histogram distribution. Conceptually, depending on whether a brightness value with the highest number of occurrence (called as maximum histogram—MH) in the histogram is even or odd, pairs of brightness values next to it are reserved for data embedding. Consequently, data hiding is realized using a pixel pair by employing the LSB technique. Essentially differing from the traditional histogram-based methods in which usually all pixels except from the MH are shifted to create a gap next to the MH of the histogram, the proposed approach does not require such a shifting and largely preserves the visual quality of the cover image. When the number of occurrences is numerically examined in the histograms, it is clear that only three brightness values, (i.e., MH, MH+1 & MH+2 or MH, MH-1 & MH-2), are trivially changed in the stego image. In addition, the MH value information is not necessarily relayed to the recipient since the histogram value of the pixels modified after embedding data is prevented from exceeding the vertex value. Throughout a detailed experimental study, the PSNR results show that the proposed approach not only increases the visual quality of stego images but also makes a reasonably high imperceptibility compared to the similar works in the literature. Considering the proposed $\boldsymbol{H_{NMH}}$ method test results, the PSNR varies between 72.74 and 67.28 dB while the hidden data capacity can be achieved up to 12,759 Bits. The $\boldsymbol{H_{NMH}}$ outperforms its counterparts 3 to 8 times with regard to the data hiding capacity that is almost linearly increased by means of concurrent deployment into the multiple cover image partitions up to a certain saturation point.

Keywords Data hiding · Image steganography · Maximum histogram · LSB

✉ Adnan Sondas
asondas@kocaeli.edu.tr

Harun Kurnaz
harunkurnaz@gmail.com

[1] Department of Information Systems Engineering, Faculty of Technology, Kocaeli University, 41001 Kocaeli, Turkey

1 Introduction

This paper mainly focuses on a hybrid data embedding scheme based on near maximum histogram (MH) that is efficiently employed to hide data into a cover image making use of the Least Significant Bit (LSB) technique. It introduces a new approach shortly called as H_{NMH}, which stands for **H**ybrid image data hiding with **N**ear **M**aximum **H**istogram and LSB, along with a comparative performance evaluation study presented.

In conjunction with the emerging technologies, secure and secret data communication has become crucial where encryption and steganography play a major role. Steganography ensures that any important data is hidden in a cover medium and securely carried over the communication channels. The carrier object is mostly a file in which a secret message is embedded in. In the image steganography, a cover image is used to embed the secret data. The new carrier object obtained after embedding data is then called as stego or covered object [1, 2].

Today, besides image files, there are many other means such as IP packets, HTML files, XML files and videos used in digital data hiding methods. Obviously, digital media files (video, audio etc.) are the most favored ones due to their large sizes and high capacities for data hiding. Any steganography technique has to successfully meet three important requirements; security of the confidential communication, high data hiding capacity and resistance against intentional or unintentional attacks. In this presented work, it is aimed to improve a method that both assures high data hiding capacity with particularly low change in the cover image and is resistant against visual attacks.

There are several approaches to hide data into digital images presented in the literature while only a few are effectively implemented in the real world. Data can be hidden utilizing color (RGB) channels of an image based on weight [3] or by changing RGB channels randomly [4, 5]. In another method utilizing image histogram [6], data hiding can be better achieved based on histogram information arrangement in a circular cycle. It introduces a unique algorithm that the highest frequency value of the histogram is used to hide the secret data. This reversible data hiding method was indeed first inspired while the researchers were trying to restore the main cover image histogram after extracting hidden data from a stego image [6].

Meiamai et al. [7] proposed another image data hiding method in which the histogram values of the color components making up the image are utilized separately and then any known data hiding method is applied to each component individually. This approach was also introduced by using the classical LSB technique. In another effort [8], it was stated that keeping the colors unchanged by making changes in contrast to the frequency of each color value minimizes the differences between the histograms of the stego and cover images.

Proposing a lossless data hiding method based on histogram change, Xuan et al. [9] used the histogram brightness values in a certain range. There is another similar method to hide data according to the number of occurrences of the brightness values in the cover histogram [10]. Its algorithm basically determines the brightness value range and number of occurrences then data hiding is realized by using the repeating numbers and the bit value to be embedded accordingly. In addition, a similar method proposed by Chang et al. [11] makes us of image histogram based on an algorithm that utilizes the most repeating value. Similarly, some less known image data hiding methods based on histogram distribution are given in [12–14].

Islamy and Ahmad [15] proposes a histogram distribution-based method for image data hiding, where the secret data is embedded directly into the MH or next to it [16] by

using the contrast correction approaches. Then the two highest histogram values are used to indicate two brightness values next to them where the secret data is to be embedded. To increase the data hiding capacity, all processes are repeated in the new stego image formed. Thus, while the data hiding process, contrast reduction is also accomplished successfully. In this method, not only reference information about the data hiding points is needed to be sent to the receiver but also the image histogram is scrolled. In another effort, Chen et al. [17] introduced a method to correct the errors resulting from histogram shift. For this purpose, a guided forecast scheme was designed based on gradient-adjusted prediction and histogram shift. Thus, the data hiding capacity is increased while the errors caused by slipping is reduced. Pan et al. [18], rather than the histogram value with the highest number of occurrence (i.e., MH), proposed another approach to hide data using the ones next to MH. Thus, there is no need to send any key information along with the stego file. To overcome the low data hiding capacity problem thereby, it is suggested that the cover image is divided into some equal blocks and proposed data hiding method is applied for each block separately. However, although data hiding capacity is increased using this approach, scrolling takes place in the histogram unavoidably.

Most of the histogram-based data hiding methods available in the literature suggest creating a gap in the image histogram and require sending the MH reference information to the recipient. In the methods where it is necessary to send the MH value information to the recipient, it is indispensable to intervene creating gaps just next to the MH value (i.e., the one left or right) in the histogram. Considering all of these key points, when evaluating the most important advantages of the proposed H_{NMH} in this paper and contribution to the literature, four important features come to the fore. First of all, the proposed approach does not interfere with the MH value. In addition, it is assured that the histogram values of the pixels altered after data hiding do not exceed the vertex value. Thus, it is not necessary to send the MH value as a reference information to the receiver. Secondly, the proposed approach discards the need to create a gap in the image histogram distribution. Another key contribution of the presented work is about overcoming the low data hiding capacity problem compared to similar histogram-based methods in the literature. For this purpose, the data hiding algorithm is realized not using the MH value but the near ones next to it. Also, in the proposed approach, high data hiding capacities can be straightforwardly achieved by taking advantage of either the histogram distributions of all color channels (RGB) considering use of color cover images or the cover image segmentation technique. Finally, the proposed approach provides all of these contributions while assuring that the stego image significantly preserves the visual quality of the cover image. Given these features, the proposed H_{NMH} has distinct advantages over its counterparts as detailed in the following evaluation sections of the paper.

This paper is mainly organized in sections as follows. The proposed data hiding approach and its implementation details are presented in Sect. 2. A detailed experimental data hiding study compared to those of the traditional counterparts and steganalysis results are provided Sects. 3 and 4, respectively. Finally, conclusions are drawn in Sect. 5.

2 Proposed H_{NMH} for Image Steganography

This section describes the new data hiding approach and its components in detail. First, histogram & maximum histogram of a cover image and the LSB technique are described. Then, the proposed approach is given along with both data embedding and extraction

algorithms & procedures. Finally, use of well-known cover image segmentation concept in conjunction with the proposed approach is explained in order to maximize the data hiding capacity performance overall.

2.1 Image Histogram Usage in the Proposed Approach

The histogram refers to the distribution of pixel values in a digital image. This key information about the number of occurrences for each pixel value (or frequency of existence) and histogram distribution gives a clear idea about digital images [6, 10]. For example, the distribution of histogram values at various different points indicates that the image contains more colors or hues whereas a narrow histogram distribution suggests that the image consists of similar or very close pixel colors overall.

Contemporary steganography applications using digital images are based on usually making small changes in the numerical values of an image. Differences or distortions in numerical values are at very small levels such that they cannot be sensed via a human vision system. In classical histogram-based data hiding methods, first the histogram of a cover image file is created. In the histogram, the MH value (P) is obtained, and a gap is created next to it. For example, if P=120, histogram values for 121–254 are shifted to the range 122–255. Then the image is scanned thoroughly, and bits of the secret data are hidden using the pixels belonging to the P value. If the secret message bit is 0, the pixel value is not changed. Else, the pixel value is increased 1 (P+1) [6, 10].

When extracting the hidden data from the stego image, a histogram building process is performed similar to that of the initial data hiding. First, the P value is obtained. Then, the hidden data extraction is realized by subtracting 0 from the pixels with the P value or subtracting 1 from the pixels with (P+1) value. Finally, all of the pixels belonging to the (P+2) - 255 histogram values are retracted back to the left and the original cover image is successfully restored [6].

2.2 LSB Technique Usage in the Proposed Approach

One of the most fundamental ways in image steganography is the LSB technique where the main idea is to replace the secret data with the least significant bits of the cover image pixels. For example, assume that binary equivalent of a secret text to be hidden is obtained using the ASCII codes. Then, these binary values are used to hide the secret data in the LSB of the pixels as given in Equation (1) [19, 20].

$$\text{LSB of the pixel} = \begin{cases} 0, & \text{if the bit to hide is “0”} \\ 1, & \text{if the bit to hide is “1”} \end{cases} \tag{1}$$

As an example, let the letter “k”, i.e., $01101011_{(2)}$, is to be embedded using the LSB method then the three pixels of a color image file are shown in Table 1.

2.3 Near Maximum Histogram and LSB Hybrid Structure of the Proposed Approach

The proposed H_{NMH} is based on an algorithm essentially developed through a hybrid use of the image histogram distribution and classical LSB technique. The histogram information of a cover image is used to determine the pixel values where the secret message is to be embedded and the LSB technique is then used to hide data into the related pixel

Table 1 A sample data hiding application of the LSB technique using a color image (the bits indicated with red color are modified while the ones with blue are not as a result of the process)

	Cover image			Stego image		
Channel	Pixel-1	Pixel-2	Pixel-3	Pixel-1	Pixel-2	Pixel-3
R	00101011	00101010	11001100	00101010	00101010	11001101
G	10101101	10101100	10101111	10101101	10101101	10101111
B	11001000	10101101	10101000	11001001	10101100	10101000

values. Firstly, the brightness value (**P**) with the highest number of occurrence (i.e., vertex value) is obtained from the cover image histogram, which is called maximum histogram (MH). The MH is the key parameter as a reference value in the proposed approach. In Eq. (2), the selection of pixels (p_g) to be used for data hiding is given. In the data hiding process, if the brightness value of the reference **P** value is even then the two lower brightness values, otherwise the two bigger brightness values of the **P** in the image histogram are used for embedding the secret data [21].

$$\mathrm{p}_g = \begin{cases} (P-1) \text{ and } (P-2), & \text{if } P\mathrm{mode}(2) = 0 \\ (P+1) \text{ and } (P+2), & \text{if } P\mathrm{mode}(2) = 1 \end{cases} \tag{2}$$

where p_g is the selected pixel to be used for data hiding and **P** is the brightness value with the highest number of occurrences.

An image histogram whose MH and vertex points are indicated is given in Fig. 1. In the proposed H_{NMH}, the MH is indirectly utilized for data hiding depending on whether its value is even or odd as a reference point. According to the **P** value obtained as a reference point, the proposed algorithm determines the pixels in the image to hide data. One of the most important features of the proposed approach is that it eliminates the need to send the **P** value to the receiver as opposed to classical MH based methods, which is explained in the following paragraphs.

The flow charts for both data hiding and extraction processes of the proposed H_{NMH} are presented in Fig. 2 and Figure 3, respectively.

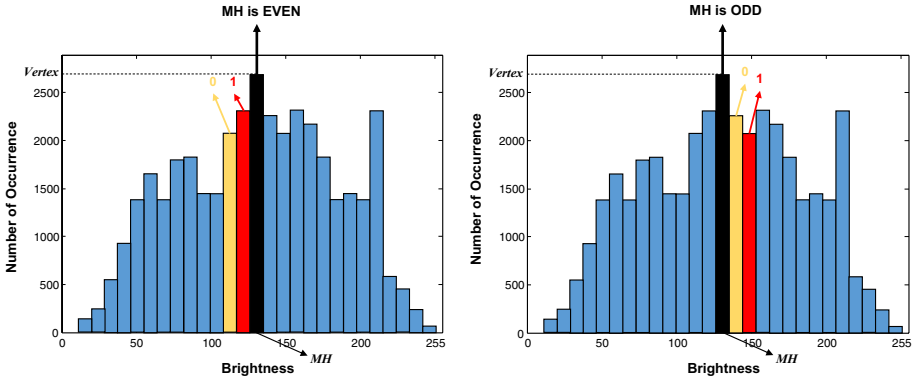

Fig. 1 Determination of the brightness value (**P**) of the pixels to be used for data hiding in the proposed approach

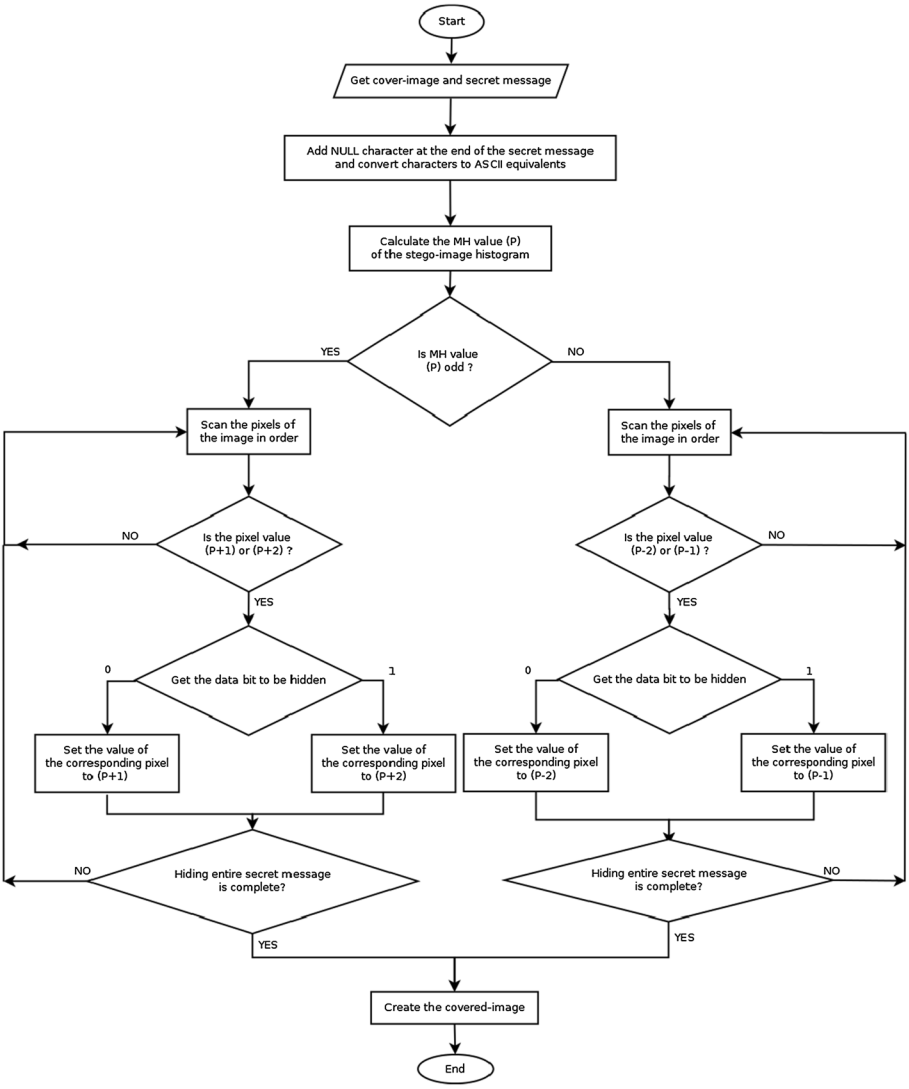

Fig. 2 Data hiding flowchart of the proposed H_{NMH}

In the H_{NMH} approach, the ASCII equivalent of each text character in the secret message is converted into a binary code. Each character is then expressed as a 9-bit binary block to be able to use other language characters in addition to English alphabet. The steps for data hiding procedure in the proposed H_{NMH} are as follows (Fig. 2):

Step 1. The characters of the secret message are converted into ASCII equivalents followed by a NULL, i.e., $(000000000)_2$, code at the end to obtain the secret data to embed.
Step 2. The image histogram of the cover image is created.
Step 3. Using the histogram distribution, the MH value (**P**) is obtained.

Step 4. **P** is identified as odd or even and accordingly the pixels with regard to this obtained **P** are decided by using the Eq. (1).

Step 5. Considering the secret data bit value and Step-4, the image pixels are searched sequentially starting from the first one.

Step 6. If the secret data bit value "1" is to be hidden, the pixel value of the first neighbor, i.e., (P-2), (P-1) or (P+1), (P+2), value is modified to be (P-1) or (P+2). On the other hand, the secret data bit value "0" is to be hidden, the pixel value of the first neighbor, i.e., (P-2), (P-1) or (P+1), (P+2), value is modified to be (P-2) or (P+1).

Step 7. Until embedding the whole secret data bits into the cover image is complete, it keeps return to Step-5.

For example, assume that the binary code equivalent for a character in a secret message is $(101110110)_2$ and that a cover image with the brightness values and number of occurrences are given as in Table 2.

With regard to the Table 2, the most repeated (MH) pixel value is P=160 for the given the cover image histogram. Since the **P** value is even, the pixels with the brightness values on its left side (i.e., 158 and 159) are utilized to hide the secret data. The pixels with (P-1) and (P-2) values are sequentially searched in the cover image. If the secret data bit to be hidden is "0", the pixel value pixel is set to "158" else if the secret data bit to be hidden is "1", the value of the pixel is set as "159". The first bit of the secret data (i.e., 101110110_2) starts with "1". After that, the cover image is scanned until any pixel with the value of either "158" or "159" is reached. If the latter is first encountered one, no change is made to its brightness value; else, if the former is first encountered one, then its brightness value is changed to "159". For the following secret data bit "0", the cover image is keep scanned once again from the last pixel processed. If the first pixel value in turn is "158", no change is made on the pixel with neither "158" nor "159" brightness values, else if the first pixel value in turn is "159" than it is changed to "158". This process cycle similarly repeats until the whole secret data bits are completely hide into the cover image pixels. Finally, the stego image is obtained and relayed to the receiver through a communication channel. It should be noted that the most repeated brightness value (P) is not changed as a result of the data hiding algorithm employed that is an important feature of the proposed approach. The algorithm utilizing a counter also makes sure that the number of occurrence (vertex) of the **P** value is not exceeded by any other resulting (P-2), (P-1), (P+1) & (P+2). It is ensured that the numbers of occurrence for the neighboring histogram values still remain lower than that of the **P** after completing data embedding.

In three-channel images such as RGB, the proposed algorithm can also be easily applied by obtaining histogram distributions separately for each channel, subject to the same process explained above.

On the receiver side, a hidden data bit array can be recovered only by using the proposed data extraction algorithm together with any stego image created by using the proposed data hiding algorithm. The i^{th} element of the hidden bit array (b_i) and the pixel value obtained during the stego image scanning (p_t) can be extracted according to Eq. 3.

Table 2 A sample application of LSB technique in the introduced approach

	(P-2)	(P-1)	P	(P+1)	(P+2)
Brightness Value	158	159	160	161	162
Number of Occurrence	2532	2556	2728	2547	2378

$$b_i = \begin{cases} 0, & \text{if P is even and } p_t = (P-2) \\ 1, & \text{if } P \text{ is even and } p_t = (P-1) \\ 0, & \text{if } P \text{ is odd and } p_t = (P+1) \\ 1, & \text{if } P \text{ is odd and } p_t = (P+2) \end{cases} \tag{3}$$

where b_i is one bit of the hidden data, p_t is the pixel value obtained during the stego image scanning and **P** is the brightness value with the highest number of occurrences.

The steps for hidden data extraction procedure in the proposed H_{NMH} are as follows (Fig. 3):

Step-1. Using the stego image histogram distribution, the MH value (P) is obtained.
Step-2. **P** is identified as odd or even, and then accordingly with regard to this obtained **P**, the pixels carrying the hidden data are decided by using the Eq. (2).

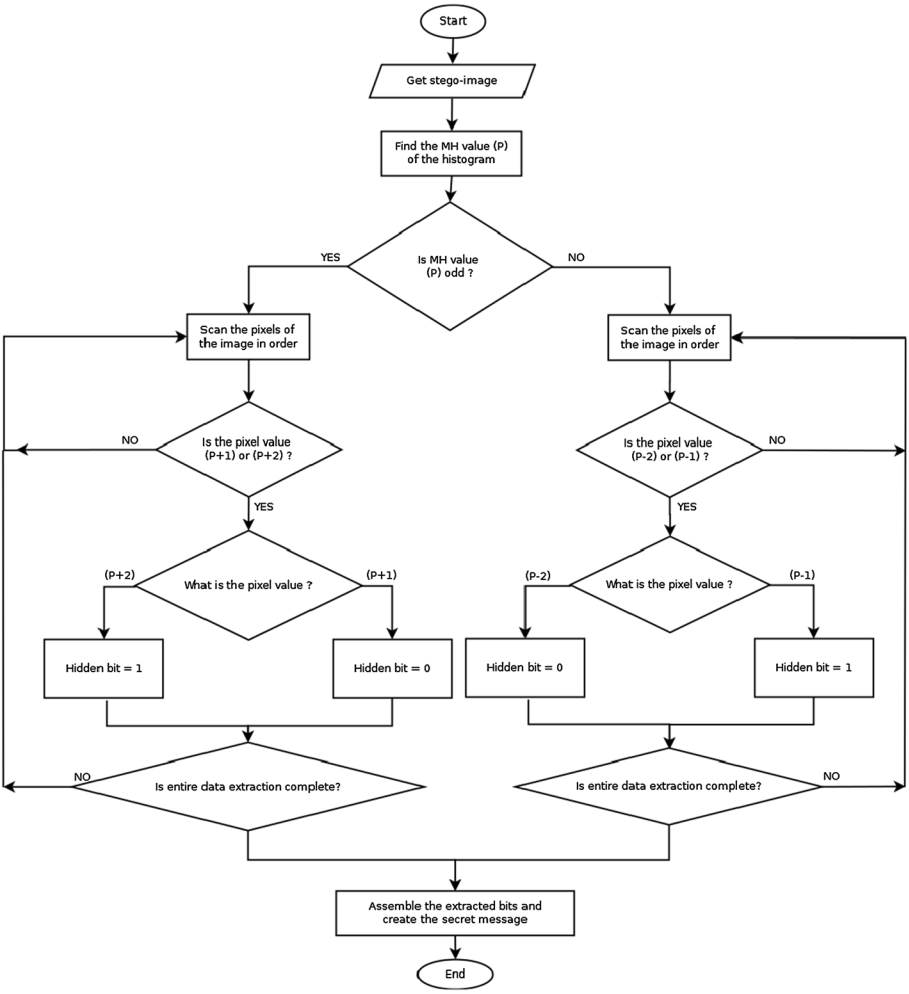

Fig. 3 Hidden data extracting flowchart of the proposed H_{NMH}

Step-3. Sequentially all of the image pixel values are scanned and according to Eq. (3), hidden data bits are extracted and then included into the secret data bit array.
Step-4. Go to the Step-3 and repeat until the value of NULL (i.e., 000000000_2) is reached, which indicates end of the hidden data.
Step-5. The obtained hidden data bits array is then divided into 9-bit blocks, and analogous to the way in the data hiding part of the proposed algorithm, the secret message is recovered.

2.4 Cover Image Segmentation for Increasing the Data Hiding Capacity

In the proposed approach, the cover pixels are not completely used to hide secret data, rather only the pixels of two brightness values next to the MH value are utilized. This fact restricts the data hiding capacity as the cover image is not fully utilized. Generally, these pixels are also placed in a particular region of a cover image. Therefore, in the proposed approach, data hiding does not take place in many portions of the cover image practically, meaning that these parts are not fully considered for an efficient application. In order to hide data all over the cover image and thus to increase the total data hiding capacity, the proposed H_{NMH} is not applied to whole image at once indeed. Initially, the cover image is divided into small equal parts then the new data hiding algorithm is applied separately for each one [22]. As a result, the data hiding process is realized in pixels with different brightness values in different cover image parts distinctly. This also contributes to ensuring the data privacy and security of the secret data.

The proposed cover image partitioning algorithm used to increase the total data hiding capacity offered by the proposed H_{NMH} is described in Fig. 4. As seen from this figure, after the cover image is divided into small equal parts, secret data is embedded into these individual parts in a Raster Scanning Order [23]. Since the MH value of each individual part is different, the secret data is hidden in different pixels of a certain brightness value in the related part. By this way, an increase and variation in data hiding capacity is highly achievable.

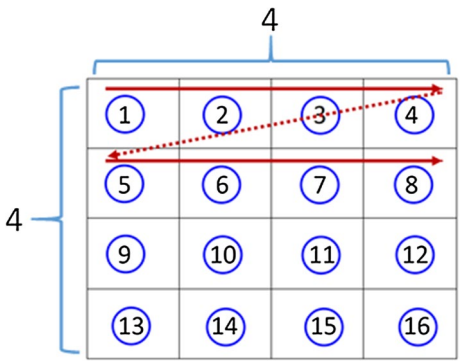

Fig. 4 The scanning order for data hiding in 4×4 cover image blocks

3 Experimental Results of the Proposed H_{NMH}

The proposed H_{NMH} has been implemented and tested on various well-known cover images by using MATLAB. Baboon, Peppers, Lena, Barbara, House, Fruits, Airplane and Zelda 8-bit grayscale images with 512×512 size are used as standard cover images for fairness of the comparisons (Fig. 5). In an extensive test and validation study, various lengths of random text messages have been used as secret data.

The results of the proposed data hiding approach are evaluated base on achievable data hiding capacity and visual quality assessment. Peak Signal to Noise Ratio (PSNR) results are presented to perceive the visual quality of the stego images.

The I_O and I_C in Eqs. (4) and (5) represent the cover and stego images respectively while M and N indicate the test cover image dimensions. Mean Squared Error (MSE) varying between 0 and 1 shows the square error resulting from the change of pixels in the stego image as a result of the data hiding operations. If the stego and cover images are exactly the same, the MSE value is 0 whereas it is 1 indicating the worst possible distortion [24].

PSNR metric is used to express the image visual quality, and there is an inverse proportional relationship between PSNR and MSE. That is to low MSE means relatively few errors and high visual quality. As the similarity between the stego and cover images increases so does the PSNR value. That is to when the stego and cover images are the same, the PSNR value is infinite.

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE(I_O, I_S)}\right) \tag{4}$$

$$MSE(I_O, I_S) = \frac{1}{M \times N} \times \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} \left[I_O(m,n) - I_S(m,n)\right]^2 \tag{5}$$

The data hiding approach developed within the scope of this presented research work has a significant advantage over its counterpart methods available in the literature. In Table 3

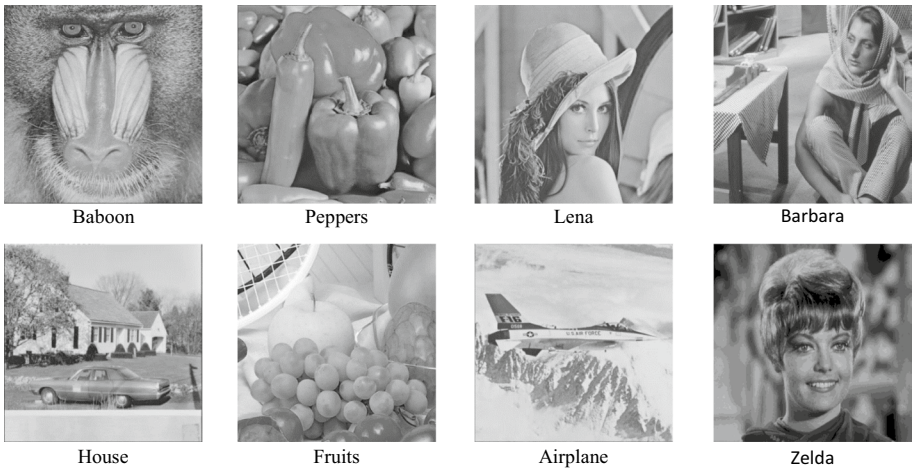

Fig. 5 The grayscaled cover images used for testing the proposed approach

Table 3 Test results for the proposed H_{NMH}

Test image	Capacity (Bits)	Hidden data (Bits)	Number of modified pixels	PSNR (dB)
Barbara	3906	**3898**	905	**72.74**
Lena	4982	4956	1089	71.78
Baboon	5914	5693	1284	71.23
Fruits	6541	6361	1425	70.77
Zelda	5017	4842	1271	70.47
Peppers	5744	5503	1459	69.76
House	11469	11470	2762	67.90
Airplane	12767	**12759**	3183	**67.28**

shows the test results of the H_{NMH} obtained using the test images given in Fig. 5 is shown. The data hiding capacity and hidden data size results are different from each other with respect to the cover image and random secret data used. Considering the PSNR and hidden data capacity test results, the former varies between 72.74 dB and 67.28 dB while the latter changes between 3,898 Bits and 12,759 Bits (these extreme values are given in bold in Table 3). As expected, while the hidden data size increases, the PSNR results decrease with respect to the number of modified pixels in the cover image. It can be deduced from the performance results that although the number of secret data bits that can be hidden is high enough well compared to some studies given in the literature [10, 25], the data hiding capacity may still need to be increased even more.

In the proposed H_{NMH} approach, not all of the cover image pixels are utilized to embed the data at all. Therefore, the data hiding capacity could remain relatively low. However, a well-known image partitioning technique described in Sect. 2.4 is used to improve data hiding capacity of the H_{NMH}. Figure 6 shows that the data hiding capacity is almost linearly increased as a result of dividing the cover images for 2×2, 4×4, 8×8, 16×16, 32×32 and 64×64 number of equal blocks.

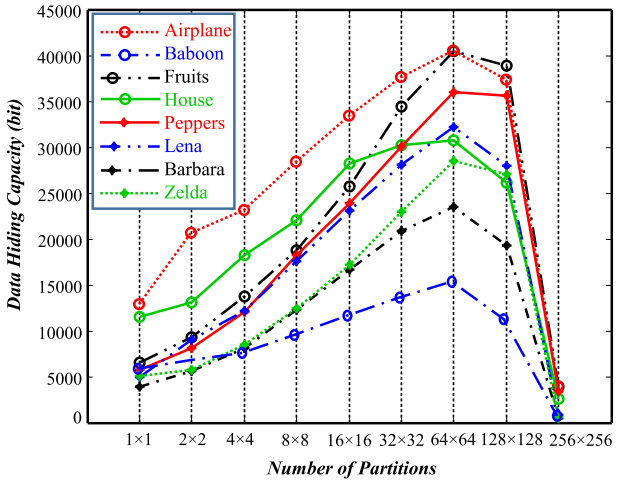

Fig. 6 The effect of the cover image segmentation on increased data hiding capacity for the proposed H_{NMH}

As seen from the data hiding capacity graphics of the different test images, the number of hidden data bits that can be embedded increases 3 to 8 times when the cover images are divided up to 64×64 pieces. On the other hand, when the test images are divided into 128×128 and above, the number of hidden data bits that can be embedded dives unacceptably as there are very few bits embedded in each block as both the vertex value of MH and accordingly the number of pixels that can be used for data hiding reach to the lowest limits. When the number of pixels is low as a result of image partitioning, the vertex value of the MH (P) drops too much and sometimes neighboring values, i.e., (P-2), (P-1), (P+1) and (P+2) may not be exist even in the relevant image blocks. Considering this crucial performance analysis point with regard to the proposed H_{NMH}, use of cover image partitioning is suggested for up to 64×64 blocks as the best trade-off between the data hiding capacity and PSNR results.

The image partitioning applied to the grayscale (8-bit) cover images can also be used for the RGB (24-bit) cover images. The only difference is in that 1 bit of the secret data can be hidden in 1 pixel in the greyscale cover image while 3 bits of the message can be hidden in RGB. Therefore, the proposed approach can achieve much better data hiding capacities.

Data hiding capacity results of the introduced H_{NMH} are comparatively given in the Table 4. The obtained results are normalized with those of the Solak [25] that includes a closer counterpart method with respect to the introduced H_{NMH} as well as other well-known similar methods presented in the literature. The data hiding capacity of the H_{NMH} is 4.61 to 12.32 times higher compared to the method presented in [25]. In overall assessment, the proposed approach achieves higher data hiding capacities compared to similar methods and offers at least 1.78 times (Ni et al. [6]) better data hiding capacity while remaining supreme in terms of PSNR results given and analysed below.

In Table 5, stego image quality results of the proposed approach are compared to those of its counterpart methods. In various image steganography methods, stego image quality assessment is considered much more crucial than achieving high data embedding capacity. As it can be understood from the Table 5, presenting the PSNR results of the test images with respect to the data hiding capacities, only the experimental results for the same data hiding capacities are provided to assure a fair comparison between the proposed and other methods. The results clearly state that the proposed H_{NMH} is superior to the other methods in terms of PSNR metric. Considering the data hiding capacity results of all classical methods are close to that of the proposed approach, the PSNR results for the H_{NMH} is reasonably better than the others. The most important reason for the obtained high data hiding capacity results in the proposed approach is due to the developed hybrid near maximum histogram and LSB based approach together with cover image partitioning. Besides, apart from

Table 4 Normalized data hiding capacity comparisons of the proposed H_{NMH}

	Normalized data hiding capacity (Solak [25] = 1 Bit)							
	Peppers	Fruits	Lena	Zelda	Barbara	Airplane	Baboon	House
[25]	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
Proposed	***12.32***	11.91	11.81	10.98	10.58	5.21	5.03	***4.61***
[12]	–	–	8.44	–	–	–	2.83	–
[26]	11.44	–	8.21	–	–	–	–	–
[15]	2.07	–	2.59	–	–	–	2.12	–
[6]	–	–	2.00	–	–	2.08	1.78	2.15

Table 5 Stego image (64×64) quality assessment results for the proposed H_{NMH}

	Proposed		Solak [25]		Ni [6]		Islamy [15]		Rahman [27]	
	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)	Capacity (bits)	PSNR (dB)
Baboon	15284	65.74	3037	50.35	5421	48.20	6440	65.41	8192	75.99
Barbara	23458	64.32	2217	54.12	–	–	–	–	–	–
Zelda	28427	63.42	2588	53.55	–	–	–	–	–	–
House	30679	63.37	6655	54.57	14310	48.30	–	–	8192	69.84
Lena	32181	62.98	2726	53.69	5460	48.20	7047	64.85	8192	63.90
Peppers	35985	62.52	2920	52.41	–	–	6037	66.33	8192	68.54
Airplane	40444	62.15	7770	54.48	16171	48.30	–	–	–	–
Fruits	40461	62.13	2298	51.17	–	–	–	–	–	–

the proposed H_{NMH}, previous histogram-based methods shift all of the pixels in the histogram in order to keep the MH value unchanged in the resulting stego image, consequently resulting in low and sometimes unacceptable PSNR results.

4 Steganalysis Performance of the Proposed H_{NMH}

Another key aspect for evaluating the new data hiding methods is related to the robustness against steganalysis tests and attacks in order to ensure a high-level undetectability by third parties. Table 6 presents the steganalysis study results for the proposed approach along with four other classical methods also fundamentally based on translations or changes in the cover image histogram distribution.

Figure 7 presents a test cover image histogram (Barbara) as well as 1×1 and 64×64 stego image histograms obtained as a result of hiding maximum length of secret data by using the proposed H_{NMH}. Comparing the original and resulting image histograms, any change cannot be visually determined by the human eye. Moreover, when the number of occurrences is numerically examined in the histograms, it is understood that only two brightness values, i.e. 160 and 161, have been trivially changed in the 1×1 stego image (Table 7).

In addition, both invisibility performance and resistance to known attacks (e.g., first order statistical attacks) of the resulting stego images as the final part of evaluating the proposed approach are assured by using the StegSpy [27]. The StegSpy is one of most used essential tools for invisibility and robustness assessments of any data hiding method. It is well noted that the StegSpy could not detect any suspicious process or hidden data within the 512×512 sized stego images obtained by using the proposed H_{NMH}.

5 Conclusion

In this presented work, a hybrid data hiding approach based on the near MH values of an image histogram and LSB has been developed. In the proposed H_{NMH}, depending on whether the maximum value of the histogram distribution is odd or even, the brightness values to hide the secret data bits are determined which are namely the neighbor ones next to the MH. Differing mainly from its counterparts, the proposed approach does not require any shift in the resulting histogram distribution. In addition, the H_{NMH} eliminates the need

Table 6 Histogram test results and comparisons for the Proposed H_{NMH}

Data Hiding Method	Histogram Change Result
Proposed H_{NMH}	Distribution varies very little (only 3 values may vary)
Islamy [15]	Distribution varies very little (only 2 values may vary)
Solak [25]	Distribution Varies
Ni [6]	Distribution varies
LSB	Distribution varies

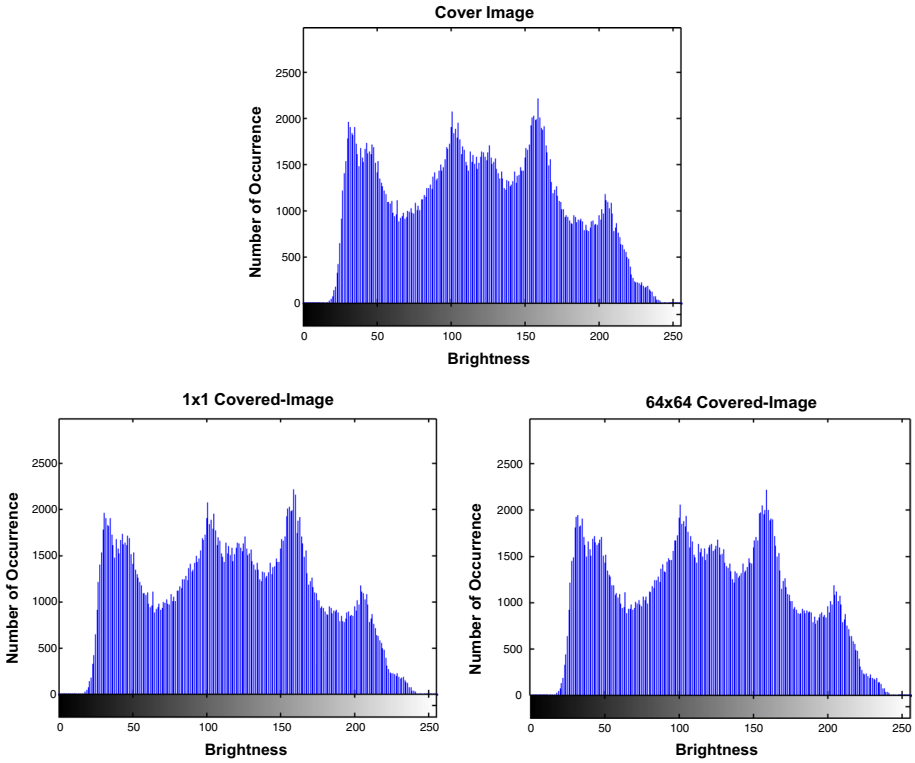

Fig. 7 Comparison of the image histograms before and after employing the introduced H_{NMH}

Table 7 Brightness values and changes in the number of occurrences

Brightness Value	159	160	161
Number of occurrence at cover image	2217	2007	1899
Number of occurrence at 1×1 Stego image	2217	2161	1745

to send the highest brightness value (MH) reference information to the receiver since it assures this value is kept as the maximum still after the data embedding process.

Having analyzed the experimental PSNR results for the proposed H_{NMH}, it is concluded that visual quality of the stego images is at least 9 dB better than the similar studies presented in the literature. The most important reason for this is that the proposed approach does not impose any gaps or shift in the resulting image histogram. Therefore, there is not much change in the image histogram distribution of the cover after the secret data is embedded. Considering the proposed H_{NMH} method test results, the PSNR varies between 72.74 and 67.28 dB while the hidden data capacity changes between 3898 Bits and 12759 Bits. Also, it has been shown that the data hiding capacity of the proposed H_{NMH} method test results, the PSNR varies between 72.74 dB and 67.28 dB while the hidden data capacity changes between 3898 Bits and 12759 Bits. Also, it has been shown that the data hiding capacity of the proposed H_{NMH} can be increased up to 8 times as a result of dividing the cover image into multiple equal parts before starting to hidden the secret data. As a final

remark, the secret data can be hide in the cover image after encryption if it is necessary to hide data more securely in order to contribute to durability. Future work on increasing the data hiding capacity is considered.

References

1. Patel Z. V. & Gadhiya S. A. A survey paper on steganography and cryptography. https://oaji.net/articles/2015/1250-1430899120.pdf
2. Yalman, Y., Cetin, O., Erturk, I., & Akar, F. (2014). *Veri Gizleme*. Turkey: Beta Yayinevi.
3. Chrysochos, E., Fotopoulos, V., Skodras, A. N. & Xenos M. (2007). Reversible Image Watermarking Based on Histogram Modification. In *11th Panhellenic Conference on Informatics with international participation, Patras, Greece*.
4. Gutub, A. (2010). Pixel indicator high-capacity technique for RGB image based steganography. *Journal of Emerging Technologies in Web Intelligence, 2,* 56–64. https://doi.org/10.4304/jetwi.2.1.56-64.
5. Solak, S., & Altinisik, U. (2019). Image steganography based on LSB substitution and encryption method: adaptive LSB+3. *J. Electron. Imag., 28*(4), 043025.
6. Ni, Z., Shi, Y. Q., Ansari, N., & Su, W. (2006). Reversible data hiding. *IEEE Transactions on Circuits and Systems for Video Technology, 16*(3), 354–362.
7. Meiamai, V., Minu, A., & Devi, R. A. (2013). Histogram technique with pixel indicator for high fidelity steganography. *International Journal of Engineering and Technology, 5*(3), 2134–2137.
8. Al-Husainy, M. A. F. (2015). Image steganography method preserves the histogram shape of image. *European Journal of Scientific Research, 1*(130), 101–106.
9. Xuan, G., Shi, Y. Q., Chai, P., Cui, X., Ni, Z., & Tong, X. (2007). *Optimum Histogram Pair Based Image Lossless Data Embedding. Lecture Notes in Comp. Sci.* (p. 5041). Berlin: Springer.
10. Yalman, Y., & Erturk, I. (2009). Imge Histogrami Kullanilarak Geometrik Ataklara Dayanikli Yeni Bir Veri Gizleme Teknigi Tasarimi ve Uygulamasi, XI. *Akademik Bilisim Konferanslari, 1*, 537–544.
11. Chang, C., Tai, W. L. & Chen, K. N. (2008). Lossless Data Hiding Based on Histogram Modification for Image Authentication. In *IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing* (pp. 506–511).
12. Lin, Y. C., & Li, T. S. (2011). Reversible image data hiding using quad-tree segmentation and histogram shifting. *Journal of Multimedia, 6*(4), 349–358.
13. Kuo, W. C., Wang, C. C., & Huang, Y. C. (2015). Binary power data hiding scheme. *AEU - International Journal of Electronics and Communications, 69,* 1574–1581.
14. Hwang, J. H., Kim, J. W., & Choi, J. U. (2006). *Optimum Histogram Pair Based Image Lossless Data Embedding, Lecture Notes in Comp. Sci.* (Vol. 4283, pp. 348–361). Berlin: Springer.
15. Islamy, C. C., & Ahmad, T. (2019). Histogram-based multilayer reversible data hiding method for securing secret data. *Bulletin of Electrical Engineering and Informatics, 8*(3), 1128–1134.
16. Wu, H. T., Dugelay, J. L., & Shi, Y. Q. (2015). Reversible image data hiding with contrast enhancement. *IEEE Signal Processing Letters, 22*(1), 81–85.
17. Chen, X., Sun, H., Xiang, L., & Yang, B. (2015). Histogram shifting based reversible data hiding method using directed-prediction scheme. *Multimedia and Tools Application, 74,* 5747–5765.
18. Pan, Z., Hu, S., Ma, X., & Wang, L. (2015). Reversible data hiding based on local histogram shifting with multilayer embedding. *Journal of Visual Communication and Image Representation, 31,* 64–74.
19. Fridrich, J. (2010). *Steganography in Digital Media Principles, Algorithms, and Applications*. Cambridge: Cambridge University Press.
20. Tutuncu, K., & Demirci, B. (2018). Adaptive LSB steganography based on chaos theory and random distortion. *Advances in Electrical and Computer Engineering, 18*(3), 15–22.
21. Kurnaz, H., Konyar, M. Z., & Sondas, A. (2020). A new hybrid data hiding method based on near histograms. *European Journal of Science and Technology, 18,* 683–694.
22. Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., & Buchanan, W. J. (2021). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wireless Personal Communications,* 1–28.
23. Aydogan, T., & Bayilmis, C. (2017). A new efficient block matching data hiding method based on scanning order selection in medical images. *Turkish Journal of Electrical Engineering and Computer Sciences, 25*, 461–473.

24. Nassar, S. S., Ayad, N. M., Kelash, H. M., El-Sayed, H. S., El-Bendary, M. A., El-Samie, A., & Faragallah, O. S. (2016). Secure wireless image communication using LSB steganography and chaotic baker ciphering. *Wireless Personal Communications, 91*(3), 1023–1049.
25. Solak, S. (2019). Histogram-based reversible data hiding method using maximum histogram value. *International Marmara Sciences Congress,* 323–327.
26. Tai, W. L., Yeh, C. M., & Chang, C. C. (2009). Reversible data hiding based on histogram modification of pixel differences. *IEEE Transactions on Circuits and Systems for Video Technology, 19*(6), 906–910.
27. Rahman, S., Masood, F., Khan, W. U., Ullah, N., Khan, F. Q., Tsaramirsis, G., Jan, S., & Ashraf, M. (2020). A novel approach of image steganography for secure communication based on LSB substitution technique. *Computers, Materials and Continua, 64*(1), 31–61.
28. StegSpy, Web Adress: http://www.spy-hunter.com/stegspy.

Adnan Sondas is an assistant professor at the University of Kocaeli. He received his MS and PhD degrees in Electronics and Computer Education Dept. from the University of Kocaeli in 2006 and 2011, respectively. His current research interests include electromagnetic structures, steganography and virtual reality

Harun Kurnaz is a PhD student at Information Systems Engineering Dept. from the University of Kocaeli. He received his MS degree in Information Systems Engineering Dept. from the University of Kocaeli in 2019. He has been working as an information technologies teacher since 2008.