Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-18476-6

A novel technique for image steganography based on maximum energy seam

Ron Shmueli[1] · Divya Mishra[2] · Tal Shmueli[3] · Ofer Hadar[2]

Received: 30 July 2022 / Revised: 4 October 2023 / Accepted: 29 January 2024

Abstract

Image steganography is the art of hiding information in a cover image in such a way that a third party does not notice the hidden information. This paper presents a novel technique for image steganography in the spatial domain. The new method hides and recovers hidden information of substantial length within digital imagery while maintaining the size and quality of the original image. The image gradient is used to generate a saliency image, which represents the energy of each pixel in the image. Pixels with higher energy are more salient and they are valuable for hiding data since their visual impairment is low. From the saliency image, a cumulative maximum energy matrix is created; this matrix is used to generate horizontal seams that pass over the maximum energy path. By embedding the secret bits of information along the seams, a stego-image is created which contains the hidden message. In the stego-image, we ensure that the hidden data is invisible, with very small perceived image quality degradation. The same algorithms are used to reconstruct the hidden message from the stego-image. Experiments have been conducted using two types of images and two types of hidden data to evaluate the proposed technique. The experimental results show that the proposed algorithm has a high capacity and good invisibility, with a Peak Signal-to-Noise Ratio (PSNR) of about 70, and a Structural SIMilarity index (SSIM) of about 1.

Keywords Image steganography · Covert channel · Seam carving · Information hiding · Cover image · Watermarking

✉ Divya Mishra
divya@post.bgu.ac.il

Ron Shmueli
rons@afeka.ac.il

Tal Shmueli
tal@shmueli.org

Ofer Hadar
hadar@bgu.ac.il

[1] Department of Electrical Engineering, AFEKA - College of Engineering, 218 Bnei Efrayim Rd, 69107 Tel-Aviv, Israel

[2] School of Electrical and Computer Engineering, Ben Gurion University of the Negev, David Ben Gurion Blvd 1, Beer-Sheva 84105, Israel

[3] Department of Computer Science, Bar-Ilan University, Ramat-Gan 52900, Israel

Published online: 06 February 2024

1 Introduction

The goal of steganography in our study is to hide information imperceptibly in a cover image so that the presence of hidden data cannot be detected by visual appearance. Images are a good carrier for transmitting secret messages over the internet, due to the redundant information in images and visual resilience to small changes in the original pixel values. In many applications, the most important requirement for steganography is the undetectability of the hidden data. This means that the image that contains the hidden data, the stego-image, should be visually and statistically similar to the cover image [1, 2]. Many digital steganography techniques have been proposed in recent years. All of them share the fundamental concept of injecting secret information into a cover image to generate a stego-image output as shown in Fig. 1.

Image steganography can be categorized into two different embedding domains, spatial domain [3] and frequency domain [1]. In spatial domain technology, secret information is embedded directly into pixel intensity values. In the frequency domain techniques, a discrete frequency transform (mainly DCT or DWT) is used and the secret information is embedded into the frequency coefficients of the cover image [1, 2]. The inverse transformation generates the image steganography. In both embedding domains, the process introduces distortion in the cover image, which could lead to steganographic detectability. The objective is to preserve the visual and statistical properties while embedding the message in the cover image, with a high embedding rate. The invisibility of any steganography technique in the spatial domain depends on the selection of pixels for embedding the secret message [4]. Due to the masking phenomenon of the human visual system [5], small distortions in pixels in smooth areas are much more noticeable than distorted pixels in high-frequency texture areas as described in Fig. 2. To maintain the visual properties of the image, the secret message should be embedded along the edges of the cover image, where the visual impairment is low [1, 6].

In this paper, we will introduce a novel image steganography technique, which embeds the secret message in the spatial domain. The proposed steganography technique is found to have excellent invisibility and high capacity. The paper is organized as follows: Section 2 discusses some well-known spatial domain image steganographic techniques. Section 3 introduces our novel steganography technique, which embeds the secret message in high-energy areas in the image. Section 4 contains experimental results and Section 5 concludes our work and elaborates on directions for future work.

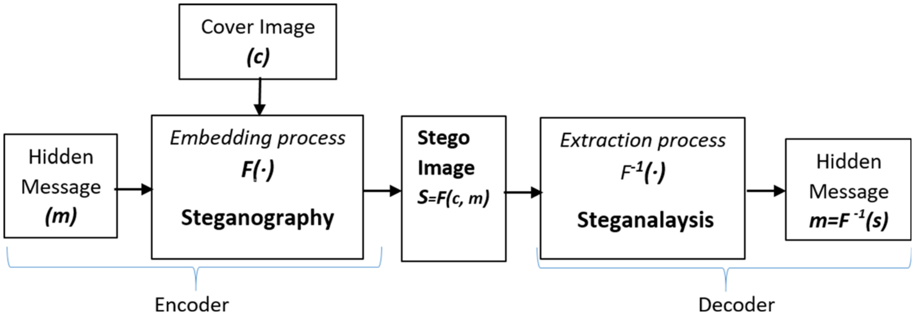


Fig. 1 General steganographic system

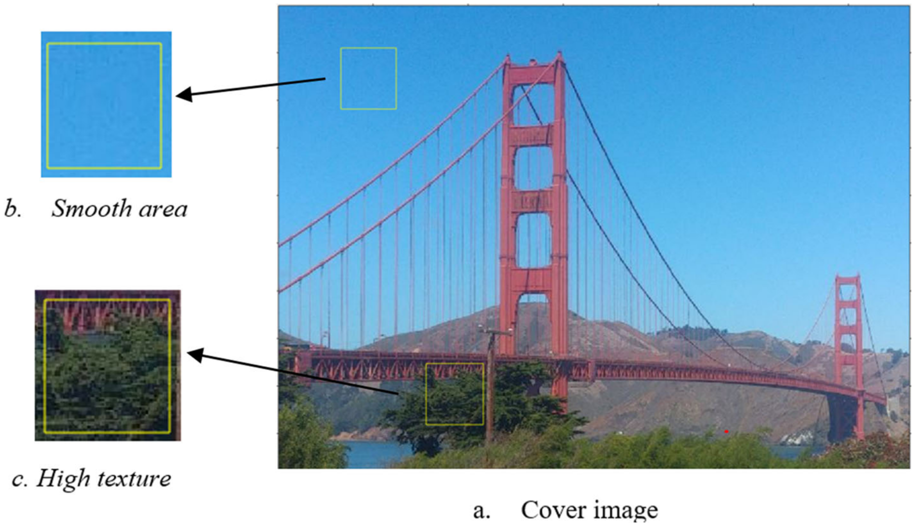


Fig. 2 Effect of embeding data in cover image (a) Cover image (b) Smooth area (c) High texture area

2 Related work

There are several steganographic techniques to embed data securely in an image and some tools to detect the presence of a secret message in a steganogram. Image steganography can be divided into two main types: spatial or frequency domain steganography.

Spatial domain steganography changes some bits in the image pixels during data hiding. When hiding data in a pixel, the physical location of a pixel is considered and then the binary format of that pixel value is used to hide the data. The most common methods are based on least-significant-bit (LSB) substitution [7]. There are several sophisticated LSB approaches to embed secret data by replacing k LSBs of a pixel with k secret bits [4]. In some of the LSB approaches, the choice of embedding positions within a cover image depends on a pseudo-random number generator without considering the relationship between the image content itself and the visual impairment of the secret message [8]. Several variances of wet paper codes, which did not consider visual impairment, were proposed as a tool for constructing steganographic schemes with an arbitrary selection channel that is not shared between the sender and the recipient [9, 10]. Other methods use the fact that human vision can tolerate severe changes in the edge region to increase the quality of the stego-images [3, 6, 11]. These methods can embed most secret data along sharper edges and can achieve more visually imperceptible stego-images.

Random location algorithms do not take into account the human visual system (HVS), so degradations might be more noticeable. In our scheme, however, we choose the locations of the embedded bits in the best location in terms of minimum reduction of the perceived image quality. One more advantage of our scheme in comparison with other schemes is that we don't need to send the locations of the affected pixels, whereas in some of the other schemes the location of those pixels must be signaled to the other side.

When using a cover image in the spatial domain, the main issue is to select the best location in the image to hide the secret information. Pixels within high-frequency texture areas are a better choice for embedding the secret information since the visual impairment is low.

Image texture is highly dependent on image content. To make the perceived degradation of the original image low, our proposed scheme embeds the secret bits into high-texture areas while keeping smooth regions as they are. Several visual texture measures are considered for defining the energy of an image. For simplification, a simple image operator called Max Energy Seam (MES) is introduced in this paper. The operator is based on the idea of seam carving that supports content-aware image resizing [12]. There have been several recent studies that locate and preserve the key visual elements in the image [13, 14]. Those studies locate the best-connected seam or area of low-energy pixels crossing the image from top to bottom or from left to right. In our study, we locate the connected seams or area of high-energy pixels crossing the image from left to right. By inserting the secret message in an image along the MES, we could hide a large amount of data that could fit a given image size. Embedding the information in a location of high energy texture will be less noticeable by the HVS compared to smooth areas where the sensitivity of the HVS is more dominant.

3 Methodolgy

3.1 The encoder- steganography

A color image I_{RGB}, which uses three color planes, R, G, and B, is represented by the intensity image I as in (1). To ensure synchronization between the decoder and the encoder during the energy calculation. The encoder and the decoder use the same method. The n least significant bits of the three image plans, R, G, and B, were reset to generate the saliency map without any influence on the original image. The RGB image (after the reset of the LSBs) is converted to grayscale values by forming a weighted sum of the R, G, and B components as in (1), where k represents the number of hidden bits that could be inserted to each channel.

$$I(i) = 0.2989 * 2^k \lfloor \frac{R(i)}{2^k} \rfloor + 0.5870 * 2^k \lfloor \frac{G(i)}{2^k} \rfloor + 0.1140 * 2^k \lfloor \frac{B(i)}{2^k} \rfloor \tag{1}$$

where k=1,2,3,4,5.

There are several possible image importance measures found in the literature as the energy function, which we could support to guide our best connected MES [12, 14]. A good and simple example of the energy function e(·) is to use the gradient magnitude of the image I, which usually indicates an edge. The edges are the part of the image that is potentially suitable for message embedding. This example of e(·) for an image could be represented as in (2):

$$e(I) = \mid \frac{\partial I}{\partial x} \mid + \mid \frac{\partial I}{\partial y} \mid \tag{2}$$

Each pixel p in an image I has a certain amount of energy represented by the gradient function e (·). Pixels with higher energy in e(·) are more salient, and they are good candidates for embedding the secret message. Those pixels are less noticeable by the HVS compared to smooth areas. Given a gradient function e(·) of an image, on the encoder side, the pixels with the highest energy in the gradient image were selected to carry the secret message. At the same time, they should maintain the possibility of decoding the message on the decoder side. This leads to our strategy of selecting a seam in the image that has the maximum energy in the gradient image. A seam is defined as an eight-connected path of pixels in the image from left to right. It's not essential to have an eight-connected seam from a left-to-right pixel, but only one pixel per column will be selected. From [12] the formal mathematical definition for the horizontal seam S^y (from left to right) in an n×m image I is:

$$S^y = \{S_j^y\}_{j=1}^m = \{(j, y(j))\}_{j=1}^m, \quad s.t. \quad \forall j, \mid y(j) - y(j-1) \mid \leq 1 \tag{3}$$

Where y is a mapping $y : [1...m] \rightarrow [1...n]$ The pixels of the path of horizontal seams S^y will therefore be:

$$I_y^s = \{I(S_j^y)\}_{j=1}^m = \{I(j, y(j))\}_{j=1}^m \tag{4}$$

Given an energy function e, we can define the cost of horizontal seams as:

$$E(S) = E(I_S^y) = \sum_{j=1}^{m} e(I(S_j^y)) \tag{5}$$

The optimal horizontal seam S* is the seam which maximizes the energy function:

$$S_y^* = \max_{\mathbf{s}} E(s) = \max_{\mathbf{s}} \sum_{j=1}^{m} e(I(S_j^y)) \tag{6}$$

In the same way, we could use a vertical seam or both types of seams. In this study, for simplicity, we introduced only horizontal seams. Using both types of seams could enable the assimilation of a greater amount of hidden information to fit into the image.

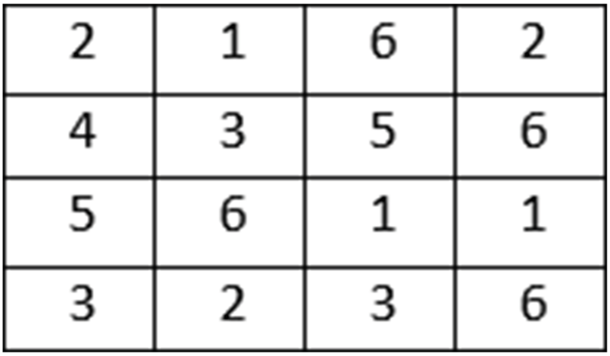
The optimal horizontal seam can be found using dynamic programming. The first step is to traverse the gradient image from the second column to the last column and compute the cumulative maximum energy M for all possible connected seams for each entry (i, j) as in (7):

$$M(i, j) = e(i, j) + max(M(i-1, j-1), M(i-1, j), M(i-1, j+1)) \tag{7}$$

For example, the energy function e(·) that represents the gradient magnitude of the image I as in Fig. 3:

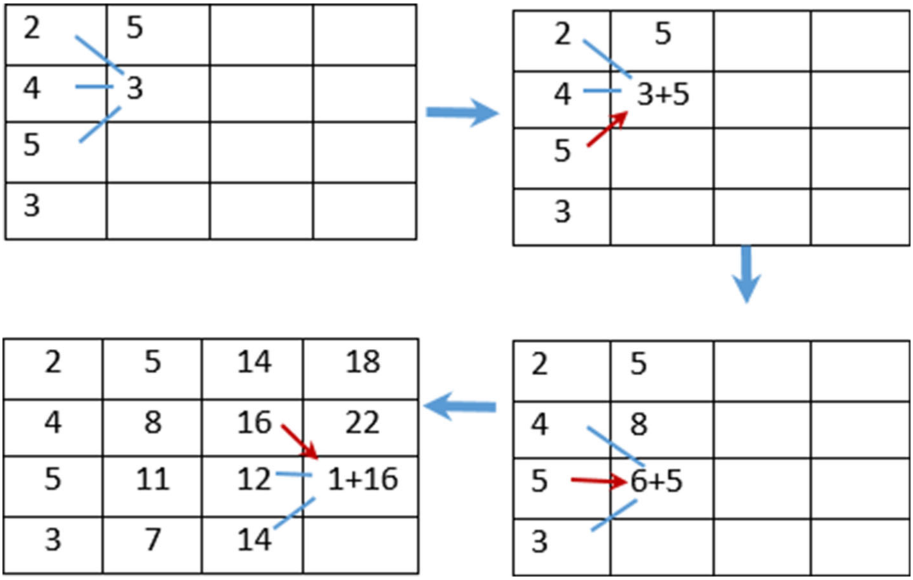
From the gradient function e(.) we compute the cumulative maximum energy M for all possible connected seams for each entry (i, j), as shown in Fig. 4, where the red arrow represents the selected value.

At the end of this process, the maximum value of the last column in M will indicate the end of the maximal connected horizontal seam. Hence, in the second step, we backtrack from this maximum entry on M to find the path of the horizontal Maximal Energy Seam (MES) as in Fig. 5. The definition of M for vertical seams is similar.



2	1	6	2
4	3	5	6
5	6	1	1
3	2	3	6

Fig. 3 An example of the gradient function e(·), which represents the energy



2	5		
4	3		
5			
3			

2	5		
4	3+5		
5			
3			

2	5		
4	8		
5	6+5		
3			

2	5	14	18
4	8	16	22
5	11	12	1+16
3	7	14	

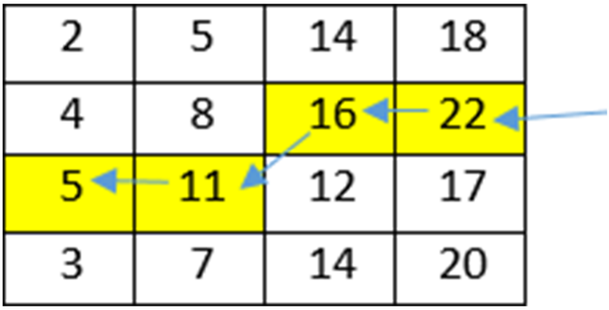
Fig. 4 The process of generating the cumulative maximum energy M

The process of generating the first MES is illustrated in Fig. 6. Figure 6(a) illustrates the first selected seam on top of the gradient image of the Golden Gate Bridge. The highlighted MES is the one that contains the most energy between all possible routes. In Fig. 6, the first MES is drawn on top of the bridge image to emphasize the location of the MES in the image.

This first MES is the most salient edge in the gradient image e(·) and it is a good candidate for secret message embedding. Within the MES, the secret data will embed only to pixels that satisfy a threshold value T which is calculated in the energy plan.

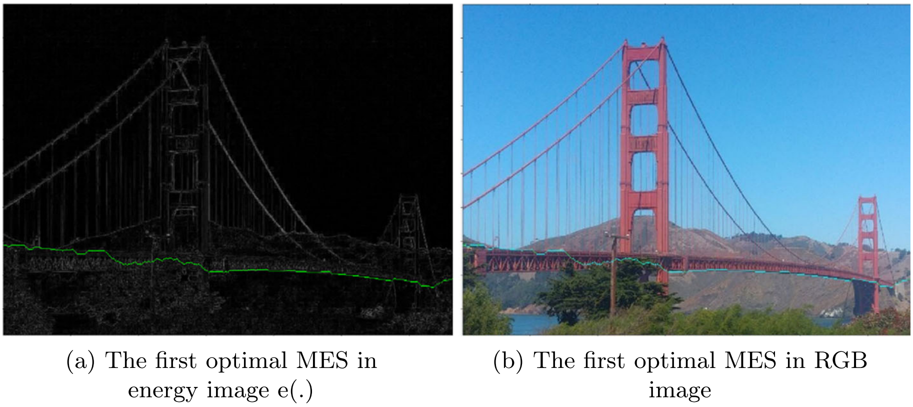
The threshold value T was calculated by finding the intensity level such that the desired k percentage of the image pixels is below this value. This is extracted from the normalized cumulative histogram of the gradient image e(·) where h(·) is the normalized histogram as in (8). The threshold is recalculated for each iteration of the algorithms which select one MES.

$$\sum_{j=1}^{T} \frac{h(j)}{mn} \geq k \tag{8}$$



2	5	14	18
4	8	16	22
5	11	12	17
3	7	14	20

Fig. 5 Backtrack from the maximum entry on M to find the path of the best MES


(a) The first optimal MES in energy image e(.)

(b) The first optimal MES in RGB image

Fig. 6 The green line indicates the location of the first optimal MES with the max energy

where T is the threshold.

The secret message bits are inserted into the LSBs of each of the RGB channels that belong to the MES. Figure 7 and (9) represents the case where each channel carries one secret bit. It is possible to increase the amount of secret data carried by the cover image by using two or more LSBs for each of the RGB channels, as described in (1) [4, 7, 15] using two or more bits will result in larger quantity integration and could therefore result in reduced image quality.

The embedding operation of 1-LSB steganography may be described by the following equation:

$$R(i) = 2\lfloor\frac{R(i)}{2}\rfloor + S(j);\ G(i) = 2\lfloor\frac{G(i)}{2}\rfloor + S(j+1);\ B(i) = 2\lfloor\frac{B(i)}{2}\rfloor + S(j+2) \quad (9)$$

where $R(i)$, $G(i)$ and $B(i)$ belong to the $i - th$ selected pixel along the MES and $S(j)$ is the $j - th$ bit of the secret message .

To carve the n-th MES from the energy image, the energy of the n-1 MES was reset and the cumulative maximum energy M of the image is recalculated. Using dynamic programing, it is verified that there is no collision between pixels in different MES's which carry data. In case of collision, the partial MES is reset and the process restarts. The secret message is inserted into the LSBs of the selected path of the MES in the cover image to create the stego-image.

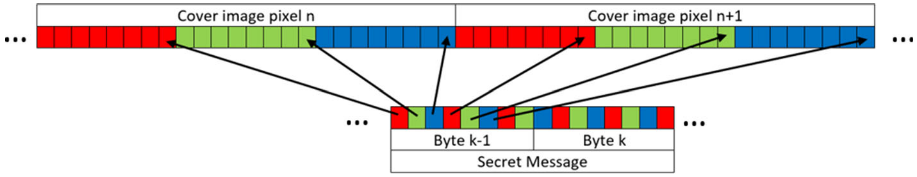


Fig. 7 Three bits of secret message, embedded into the LSBs of one RGB pixel of the cover image

3.2 The decoder-steganalysis

During the decoding the same process is applied. From the stego-image, the LSBs of the three image plans R, G, and B were reset. The RGB image (after the LSB reset) was converted to grayscale values by forming a weighted sum of the R, G, and B components as in (2). From the grayscale image the gradient image was generated as in (1). At each iteration, a new cumulative maximum energy M was generated with a new threshold and the MES's were created from them one by one. The LSBs of the RGB pixels along the MES's were carrying the secret data. Extracting and reordering the bits will yield the secret message.

4 Experimental results

To demonstrate the quality of the process, we emulated the algorithm using Matlab script. Several experiments were conducted:

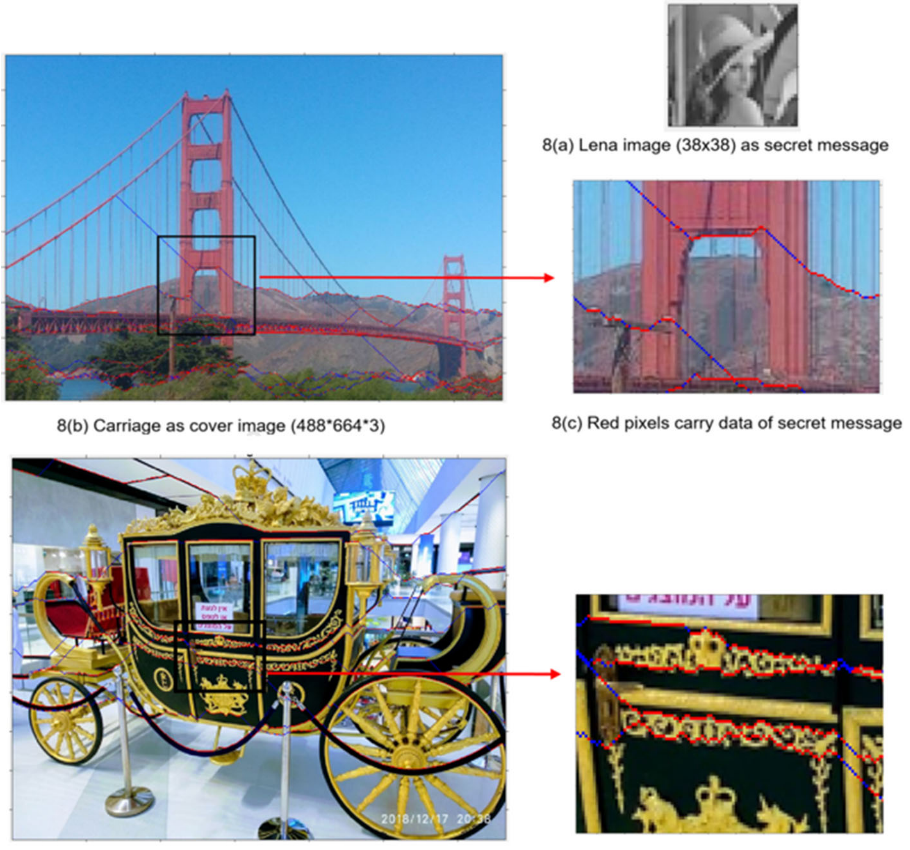
4.1 Lena image as a stego-data

In the first experiment, a small gray-level image of LENA was hidden in the RGB cover image of the Golden Gate Bridge (Fig. 8(a) and (b)). Lena's image size is 38 x 38 x 8 = 11,552 bits with a 24-bit header that is used to indicate the data type and the image size, yielding 11,576 bits of hidden data. As a cover image we use the Golden Gate Bridge RGB image, at a size of 488 x 664 = 297,472 pixels. The ratio between hidden message size in bits and the number of pixels in the cover image is about 3.8%. Figure 8(b) represents the iterative process that selects the best MES's to carry the hidden data in the cover image. The 11,576 secret bits are inserted into eight MES's. The red pixels along the MES represent pixels which carry the secret data. The blue pixels are not used to carry data, since they were under the calculated threshold (Fig. 8(c)). The length of each MES in the Golden Gate Bridge as a cover image is 664 pixels, the width of the image. Each pixel could carry three bits, so the maximum capacity of each MES is 1992 bits. Figure 8 shows that the MES lines are formed mainly on the edge lines. In the process of creating the MES's, the constraint of eight-connected path may cause intermediate transitions in smooth areas. Using the threshold T specified in (8) enables the assimilation of the hidden information only in the desired areas. In our tests, we use a high dynamic threshold with k = 0.9 in (8) which is updated at each iteration in order to ensure that the quality of the original image will not reduce. We repeat the same experiment using a Carriage image as cover image, Fig. 8(d) and (e).

The different amount of data that each MES carries for each image is illustrated in Table 1. The selected threshold influences the number of bits that each MES carries. Since each RGB pixel carries three bits from the stego-data and the secret message contains 11,576 bits, there is a 7/8 probability that the amount of 3,859 pixels could change. Assume the binomial distribution the probability of getting at least one change in a pixel is given by the cumulative mass function in (10), where n=3 and p=0.5.

$$Pr(1 \leq X \geq 3) = \sum_{i=1}^{3}((\overset{n}{i})p^{i}(1-p)^{(n-i)} \qquad (10)$$

The experimental results in Table 2 show that 2218 out of 3,859 pixels have been changed in the Golden Gate Bridge image, and 2305 out of 3,859 pixels have been changed in the



8(a) Lena image (38x38) as secret message

8(b) Carriage as cover image (488*664*3)

8(c) Red pixels carry data of secret message

8(d) Carriage as cover image (488*664*3)

8(e) Red pixels carry data of secret message

Fig. 8 Embedding Lena image [8(a)] into Golden Gate cover image [8(b)], and into Carriage cover image [8(d)]. The red part of the lines demonstrates the MES's that carry the data [8(c),8(e)]

Table 1 The amount of data that each MES is carrying

	Number of hidden bits per MES	
Stego seam #	Golden Gate image	Carriage image
1	1827	1749
2	1551	1566
3	1563	1623
4	1647	1566
5	1509	1584
6	1320	1374
7	1167	1404
8	993	711
SUM	11576	11576

Table 2 The number of bits that were modified in the pixels that belong to the MES

	Golden Gate image	Carriage image
One bit change	1,656	1710
Two bits change	519	552
Three bits change	43	43
Total	2218	2305

Carriage image, which is less than the calculated probability. Table 2 summarizes the number of bits that changed in each image. The visual impairment was so low that it was impossible for the HVS to distinguish between the original image and the stego-image.

To quantify the difference between the original image and the stego-image, we use three objective image quality assessments.

Mean Squared Error (MSE) between images x and y is given by:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - y_i)^2 \tag{11}$$

where N is the number of pixels in the image.

Peak Signal-to-Noise ratio (PSNR) [16, 17] is given by:

$$PSNR = 10\log_{10}\frac{\max(x^2)}{MSE} \tag{12}$$

where $max(x^2)$ is the maximum pixel value of the image x. Structural SIMilarity (SSIM) [16, 18, 19] index between images x and y [20]:

$$SSIM(x, y) = \frac{((2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2))}{((\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2))} \tag{13}$$

where $\mu_x, \mu_y, \sigma_x, \sigma_y$, and σ_{xy} are the local means, standard deviations, and cross-covariance for images x, y. The constants $C_1 = (K_1L)^2$ and $C_2 = (K_2L)^2$ are included to avoid unstable results when either $(\mu_x^2 + \mu_y^2)$ or $(\sigma_x^2 + \sigma_y^2)$ are very close to zero. L is the dynamic range of the pixel values and $K2 \ll 1$, $K1 \ll 1$ are small constants.

The MSE and the PSNR have clear physical meanings, but they are not matched to the perceived visual quality, the structural similarity (SSIM) predicts the perceived image quality [20]. For the Golden Gate image and the Carriage image, the SSIM calculation in this case yields the maximum possible value 1, which means a complete visual similarity between the original image and the stego-image. Table 3 shows the results of the PSNR, MSE and SSIM calculations.

The results indicate that the differences between the cover image and the stego-image are not large. The amount of information that can be embedded in the picture at a high level of

Table 3 The measures when using Lena image as stego-data

	Golden Gate image	Carriage image
SSIM	1	1
PSNR	70.3505	70.4522
SNR	66.1351	66.1134
MSE	0.0060	0.0059

concealment depends on the target image. The higher the texture, the more information can be embedded in the image. In our study, we used images with large smooth areas, allowing us to assimilate information at a density of about 5% of the image size, at high level of concealment.

4.2 Text data as a stego-data

The second experiment was conducted with text as the stego-data. The English pangram "The quick brown fox jumps over the lazy dog" is a sentence using every letter of the English alphabet . The sentence was repeated 43 times and used as stego-data. The data size was 43 chars x 33 lines x 8 bits = 11,352 bits, plus a 24-bit header, yielding 11,376 bits of hidden data that could influence 3,792 pixels in the cover image. (The size of the information is about the size of the previous experiment with the Lena image). As a cover image we use the same Golden Gate Bridge and Carriage images, as described in section 5a. The experimental results show that out of 3,792 pixels, 2,102 pixels have been changed. As in section 5a, the maximum capacity of each MES is 1992 bits. We ensured visual similarity between the original image and the stego image by using k=0.9 as a threshold in (8). Table 4 illustrates the measures between the stego-image and the original image: the MSE, PSNR and the SSIM. The SSIM is 1 since the original image and the stego-image were indistinguishable to the human eye.

The results indicate that the differences between the cover image and the stego-image are not large. The higher the texture of the cover image, the more information can be embedded in the image. In this experiment, the hidden information density is about 5% of the image size, with high level of concealment.

4.3 Iterative process to carve the MES's

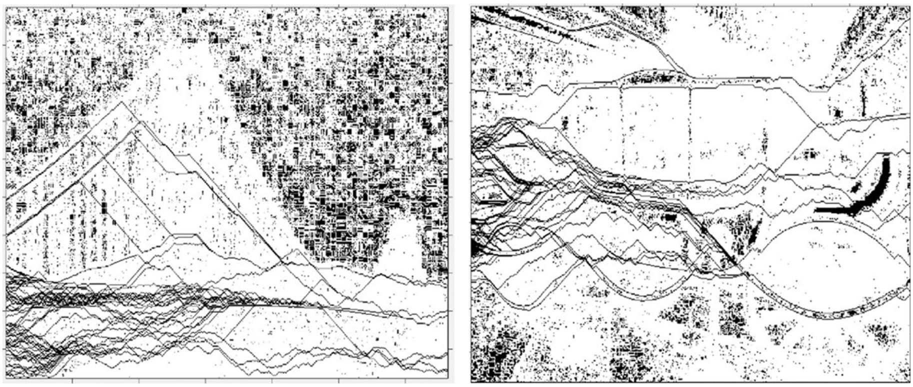
During the iterative algorithm, the MES's were generated without overlap between the pixels which carry data. During the process in the Golden Gate Bridge image, the algorithm generated 57 possible MES's. Eight of them fulfills the conditions of maximum energy and continuity along the horizontal axis, and also had values higher than the threshold as in (7). These eight MES's were selected to carry the secret data. Figure 9(a) demonstrates the 57 experimental MES's on top of the energy image. Figure 9(b) demonstrates the same action for the Carriage image. Here the algorithms found, from among 26 possible MES's, eight which fulfill the conditions and could carry the secret data.

4.4 Increasing the number of hidden bits per pixel

In order to test the strength of the algorithms and the sensitivity of human vision to the areas on which the hidden information was written, the following two experiments were conducted:

Table 4 The measures when using text as stego-data

	Golden Gate image	Carriage image
SSIM	1	1
PSNR	70.3826	70.4659
SNR	66.0438	66.2506
MSE	0.0060	0.0058



(a) The energy image of Golden Gate Bridge image, which contain 57 iteration to create MESs, eight of them were selected to carry the secret data

(b) The energy image of Carriage image, which contain 26 iteration to create MESs, eight of them were selected to carry the secret data

Fig. 9 The dynamic selection of MESs by generating valid options

In the first experiment, we use the fixed-size image of Lena that was hidden in the RGB cover image of the Golden Gate Bridge (as in Section 4.1). The hidden data size of 11,576 bits was embedded into the image at the size of 488x664 pixels of 24 bits. We control the number of hidden bits that have been written per pixel, in order to measure the stego-image quality with different quantity of MES's. In Table 5, the first row indicates the number of bits that were embedded per pixel. The other rows are the quality measures of the stego-image in each case. The last row is the number of MES's that contain the hidden data. From the quality measures (PSNR, MSE, SSIM), we can see that a large change in fewer MES's is more significant than small changes in more MES's. Since the MES's are located on the image edges, due to the Mach Bands effect, a large change in the values of the MES's is not perceived by the HVS. Together with a fine threshold of K=0.9, in all the illustrated cases it was impossible to distinguish from observation that the image has an unusual phenomenon in the zone of the MES's.

In the second experiment we used a different sized Lena image, which was hidden on a fixed-size (488 x 664 pixels) Golden Gate Bridge image that was used as cover image. In Table 6, the first and the second rows indicate the hidden data size that was embedded

Table 5 Quality measures of stego-image with the same stego-data, but with different number of hidden bits per pixel

Bits Per Pixel	3	6	9	12	15
PSNR	63.3670	66.6847	62.1507	55.6034	50.0105
SNR	59.0282	62.3459	57.8119	51.2646	45.6717
MSE	0.0299	0.0140	0.0396	0.1790	0.6487
SSIM	1.0000	1.0000	1.0000	0.9999	0.9995
MES's'	8	4	3	2	2

Table 6 Quality measures of stego-image with the different amounts of stego-data and with different numbers of hidden bits per pixel

	38 x 38	50 x 50	60 x 60	70 x 70	80 x 80
Hidden Data	12824	20024	28824	39224	51224
Bits Per Pixel	3	6	9	12	15
PSNR	63.3670	66.6847	62.1507	55.6034	50.0105
SNR	59.0282	62.3459	57.8119	51.2646	45.6717
MSE	0.0299	0.0140	0.0396	0.1790	0.6487
SSIM	1.0000	1.0000	1.0000	0.9999	0.9995
MES's'	8	4	3	2	2

into the cover image. Increasing the size of the hidden data influences the number of hidden bits that have been written per pixel by maintaining the same number of MES's (the last row). The other rows contain the quality measures of the stego-image in each of the cases. From the results, we can see that quality measures are affected by the amount of hidden information. But even with a large amount of hidden information, the objective measures (PSNR and MSE) are quite good, and the SSIM index also gives a good result. As in the previous experiment, due to the location of the MES's on the edges and as well as the Mach bands effect, a large change in the values of the MES's is not perceived by the HVS. Together with a fine threshold of K=0.9, in all the illustrated cases it was impossible to distinguish from observation that the image has an unusual phenomenon in the zone of the MES's.

5 Conclusion and future work

In this paper, we propose a new method for image steganography in the spatial domain. The method is based on LSB substitution, embedding the secret data into RGB images without creating a perceptible distortion. The method uses an energy function to define the saliency map of the image. From the saliency image a cumulative maximum energy matrix is created. The max energy horizontal seams are selected from the cumulative matrix and the secret message is embedded along the seams. The experimental results show that the algorithm has a fair capacity and good invisibility.. Some open issues that can be further incorporated in our future work include: diverse options for generating the saliency image; different approaches for selecting the MES's; and considering approaches to defense against attacks intended to destroy or detect the embedded information. Finally, the method presented here could be extended to video and audio signals.

Funding Open access funding provided by Afeka College of Engineering. Not Applicable

Data Availability All data generated or analysed during this study are included in this published article.

Declarations

Conflicts of interest The authors declare no conflict of interest.

Competing interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

1. Li Y, Xiong C, Han X, Xiang R, He F, Du H (2018) Image steganography using cosine transform with large scale multimedia application. Multimed Tools Appl 81:161
2. Baby D, Thomas J, Augustine G, George E, Michael NR (2015) A novel dwt based image securing method using steganography. Procedia Comput Sci 46:612–618
3. Luo W, Huang F, Huang J (2010) Edge adaptive image steganography based on lsb matching revisited. IEEE Trans Inf Forensics Secur 5(2):201–214
4. Wu D-C, Tsai W-H (2003) A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 24(9–10):1613–1626
5. Foley JM (1994) Human luminance pattern-vision mechanisms: masking experiments require a new model. JOSA A 11(6):1710–1719
6. Islam S, Modi MR, Gupta P (2014) Edge-based image steganography. EURASIP J Inf Secur 1:1–14
7. Thien C-C, Lin J-C (2003) A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern Recognit 36(12):2875–2881
8. Mielikainen J (2006) Lsb matching revisited. IEEE Signal Process Lett 13(5):285–287
9. Fridrich J, Goljan M, Soukal D (2004) Perturbed quantization steganography with wet paper codes. In: Proceedings of the 2004 workshop on multimedia and security, pp 4–15
10. Yin Z, Chang C, Zhang Y (2010) An information hiding scheme based on (7, 4) hamming code oriented wet paper codes. Int J Innov Comput Inf Control 6(7):3121–3130
11. Yang C-H, Weng C-Y, Wang S-J, Sun H-M (2008) Adaptive data hiding in edge areas of images with spatial lsb domain systems. IEEE Trans Inf Forensics Secur 3(3):488–497
12. Avidan S, Shamir A (2007) Seam carving for content-aware image resizing. In: ACM SIGGRAPH 2007 papers, p 10
13. Bylinskii Z, Kim NW, O'Donovan P, Alsheikh S, Madan S, Pfister H, Durand F, Russell B, Hertzmann A (2017) Learning visual importance for graphic designs and data visualizations. In: Proceedings of the 30th Annual ACM symposium on user interface software and technology, pp 57–69
14. Raz G, Shmueli R, Katz E (2016) Texture segmentation for seam carving. In: 2016 IEEE International conference on the science of electrical engineering (ICSEE), pp 1–5
15. Bandyopadhyay D, Dasgupta K, Mandal J, Dutta P (2014) A novel secure image steganography method based on chaos theory in spatial domain. Int J Secur Priv Trust Manage (IJSPTM) 3(1):11–22
16. Horé A, Ziou D (2010) Image quality metrics: Psnr vs. ssim. In: 20th International conference on pattern recognition, pp 2366–2369
17. Vranjes M, Rimac-Drlje S, Grgic K (2008) Locally averaged psnr as a simple objective video quality metric. In: 2008 50th International symposium ELMAR, vol 1, pp 17–20
18. Zhou W, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
19. Jiao S, Dong W (2013) Sar image quality assessment based on ssim using textural feature. In: 2013 Seventh international conference on image and graphics, pp 281–286
20. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612

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