A steganographic scheme based on the Wada index

A steganographic scheme based on the Wada index

Loreta Saunoriene[1†] and Minvydas Ragulskis[1*†]

[1*]Center for Nonlinear Systems, Kaunas University of Technology, Studentu 50-146, Kaunas, 51368, Lithuania.

*Corresponding author(s). E-mail(s): minvydas.ragulskis@ktu.lt;
†These authors contributed equally to this work.

Abstract

A steganographic technique based on the Wada index is proposed in this paper. The definition of a perfect covering of the carrier image is introduced. Perfect coverings are used to produce a unique representation of the carrier image what enables the consecutive modification of pixels in the carrier image without destructing Wada indexes in previous overlapping observation windows. The only required information for the decoding step is the stego image itself. The stego image is split into dichotomous shares according to the Wada index. The decoding scheme is based on the disjunction of shares with odd indexes. Computational experiments are used to demonstrate the efficacy of the proposed scheme. The proposed steganographic scheme based on the Wada index ensures that the secret image is not leaked from the modified bit planes with lowest indexes, the stego image is robust against RS steganalysis algorithms, and the payload capacity of the carrier image is comparable to grayscale LSB schemes.

Keywords: Wada index, Perfect covering, Steganography, Carrier image

1 Introduction

The lakes of Wada are three (or more) disjoint connected open sets of the plane with the counterintuitive property that they all have the same boundary. The lakes of Wada were introduced by Kunizo Yoneyama in 1917, who credited the discovery to Takeo Wada [1].

With the advent of the era of powerful digital computers, Wada basins of attraction became an important topic in computational analysis of non-linear systems [2]. A Wada basin has the property that every neighborhood of every point on the boundary of that basin intersects at least three basins.

The visualization of Wada basins for a nonlinear system possessing several coexisting attractors can be executed in a form of a colormap where every point in the phase space of initial conditions is assigned to a different color (representing the attractor to which the system will evolve from this initial condition). Computational and topological analysis of such Wada colormaps have attracted a lot of interest during the recent years [3, 4, 5]. The uncertainty of a response to a perturbation of a nonlinear system possessing the Wada property is higher if compared to a fractal basin boundary [6, 7, 8].

However, it is important not only to detect if the investigated basin of attraction does possess the Wada property. It is also important to quantify the complexity of the Wada basin in terms of the number and the proportion of different colors in phase space. The Wada index recently introduced in [9] helps to achieve these goals. The Wada index can be used to distinguish fractal and Wada

basins of attraction. Also, the Wada index does measure the randomness of the distribution of different colors in a basin of attraction represented as a color digital image. That allows to represent the uncertainty of the dynamical system with a greater accuracy. Finally, the algorithm for the computation of the Wada index is relatively simple, fast, and well-applicable for different basins of attraction represented as two-dimensional digital color images [9].

Any steganography scheme can be characterized by the following four features: imperceptibility, security, payload capacity, and robustness [10, 11].

Imperceptibility is the key feature and strength of any steganographic technique as hiding the secret data in the digital image should not be detected by a naked human eye or with the use of statistics [11, 12]. Any steganography technique is regarded as secure if the secret data is not detectable by statistical means, or removal after being detected by the attacker [11]. An efficient steganographic system always aims at sending maximum information using minimum cover media. The payload capacity (the embedding rate) is defined as the amount of information hidden (in bits) comparative to the size of the carrier image. Keeping higher payload capacity without sacrificing imperceptibility and security is a major challenge in steganography [11, 12, 13]. The robustness represents the ability of the embedding and decoding scheme even if the stego image is corrupted by a third hand using image processing techniques like rotation, scaling, resizing etc. [11].

Steganographic techniques can be classified according to the embedding domain into spatial and transform domain steganography techniques [14]. The simplest method to embed the data into digital image is based on updating the values of cover pixels within the spatial domain of this image [15]. The spatial-domain methods are based on different bit-wise algorithms which implement the noise manipulation and bit insertion by applying different techniques [15]. Well-known contemporary spatial domain steganography techniques are reviewed below.

Least Significant Bit (LSB) steganography is a technique in which the last bit of each pixel of the carrier image is replaced with the data bit of the secret message [16]. Although small modifications in last bits are not detectable by the naked eye, they can be easily detected by the bit-plane or RS analysis [17, 18]. In recent years, different modifications of this technique have been proposed in order to achieve higher security, better imperceptibility, and higher payload capacity [19, 20, 21].

The Pixel-Value Differencing (PVD) steganographic scheme relies on the occurring difference among pixel values [22, 23]. The carrier image is divided into non-overlapping blocks of two joined pixels where the difference within every block is changed in order to embed the secret information. The main disadvantage is that the embedding capacity has a direct relation to visual quality of stego image [24].

Difference Expansion (DE) steganography was proposed by Tian in 2003 [25]. Secret bits of data are embedded into a pair of pixels while leaving the average value of this pair of pixels unchanged. Both the payload capacity and the visual quality of the stego image are sufficiently high for DE steganography [25, 26].

Multiple Bit Planes Based (MBPB) steganography was first introduced in 2006 as an extension to the basic LSB substitution technique. In MBPB steganography, bit planes with higher complexity are preselected to hide secret data [11, 27]. Such encoding technique results in higher embedding capacity and is more robust against the steganalysis comparing with standard LSB technique. The main drawback is that the stego image is vulnerable against geometrical attacks [11, 27].

Gray Level Modification (GLM) steganography schemes were introduced as a modification of the pixel brightness adjustment-based embedding [28]. The secret data bits are embedded in the brightness adjustment between adjacent pixels which depends on the nature of the embedding scheme. GLM schemes help to provide better quality stego images due to the indirect embedding process [29].

The Exploiting Modification Direction (EMD) steganography was first proposed by Zhang and Whang in 2006 [30]. They group all pixels in the carrier image into n pixels per group. A pixel in each group is modified by 1 to hide a secret digit in a $(2n+1)$-ary notational system [31]. However, the payload of the basic EMD scheme is quite low.

The main objective of this paper is to present a new steganographic scheme based on the Wada index. The paper is structured as follows. The list of notations and symbols is given in Section 2. The

modified Wada index is presented in Section 3. Perfect coverings and their properties are introduced and analyzed in Section 4. The proposed steganographic scheme is described in Section 5. Computational experiments and comparisons with alternative steganographic techniques are presented in Section 6. The robustness of the proposed scheme is investigated in Section 7. Finally, concluding remarks are given in the last section.

2 The list of notations

The following notations will be used throughout the paper:

- s – the size of the border of a $s \times s$ square observation window measured in the number of pixels; $s \geq 2$.
- m – the number of different colors in the $s \times s$ observation window; $m \geq 1$.
- ν_k, $k = 1, 2, \ldots, m$ – the number of the k-th color pixels in the $s \times s$ observation window.
- $p_k = \frac{\nu_k}{s^2}$, $k = 1, 2, \ldots, m$ – the discrete probability of the k-th color in the $s \times s$ observation window.
- The indicator function $\mathbf{1}_2^{(s)}$ is equal to 1 if the number of colors in the $s \times s$ observation window is greater or equal than 2: $\mathbf{1}_2^{(s)} = \begin{cases} 1, & m \geq 2, \\ 0, & m = 1. \end{cases}$
- The indicator function $\mathbf{1}_3^{(s)}$ is equal to 1 if the number of colors in the $s \times s$ observation window is greater or equal than 3: $\mathbf{1}_3^{(s)} = \begin{cases} 1, & m \geq 3, \\ 0, & m \leq 2. \end{cases}$
- $e^{(s)}(p_1, p_2, \ldots, p_m) = -\sum_{k=1}^{m} p_k \log(p_k)$ – the Shannon entropy of different colors in the $s \times s$ observation window.
- The Wada index $\omega^{(s)}$ in the $s \times s$ observation window reads [9]:

$$\omega^{(s)}(p_1, p_2, \ldots, p_m) = \frac{m}{\log(m)} \mathbf{1}_3^{(s)} e^{(s)}$$
$$= \begin{cases} 0, & m < 3, \\ -\frac{m}{\log(m)} \sum_{k=1}^{m} p_k \log(p_k), & m \geq 3. \end{cases}$$

- The Wada index $W^{(s)}$ for a digital image reads [9]: $W^{(s)} = \frac{\sum_{k=1}^{N} \omega_k^{(s)}}{\sum_{k=1}^{N} \mathbf{1}_{2,k}^{(s)}}$ where $\omega_k^{(s)}$ and $\mathbf{1}_{2,k}^{(s)}$ is the Wada index $\omega^{(s)}$ and the indicator function $\mathbf{1}_2^{(s)}$ in the k-th observation window.
- C – the grayscale carrier image. The size of C (measured in pixels) is $n_x \times n_y$.
- T – the grayscale stego image. The size of T (measured in pixels) is $n_x \times n_y$.
- S – the dichotomous secret image. The size of S (measured in pixels) is $(n_x - s + 1) \times (n_y - s + 1)$.
- H_q – the dichotomous q-th share; $q = 1, \ldots, m$. The size of H_q (measured in pixels) is $(n_x - s + 1) \times (n_y - s + 1)$.

3 The modified Wada index

Let us define a modified indicator function

$$\mathbf{I}_q^{(s)} = \begin{cases} 1, & m = q, \\ 0, & m \neq q, \end{cases} \tag{1}$$

where m is a pre-determined number of colors in the $s \times s$ observation window; $1 \leq m \leq s^2$. Then, the modified Wada index in the $s \times s$ observation window is defined as:

$$\omega_q^{(s)}(p_1, p_2, \ldots, p_m) = \frac{m}{\log(q)} \mathbf{I}_q^{(s)} e^{(s)}$$
$$= \begin{cases} 0, & m \neq q, \\ -\frac{m}{\log(m)} \cdot \sum_{k=1}^{m} p_k \log(p_k), & m = q. \end{cases} \tag{2}$$

Finally, the modified Wada index $W_q^{(s)}$ for a digital image is defined as:

$$W_q^{(s)} = \frac{\sum_{k=1}^{N} \omega_{q,k}^{(s)}}{\sum_{k=1}^{N} \mathbf{I}_{q,k}^{(s)}}, \tag{3}$$

where $\omega_{q,k}^{(s)}$ and $\mathbf{I}_{q,k}^{(s)}$ is the modified Wada index $\omega_q^{(s)}$ and the modified indicator function $\mathbf{I}_q^{(s)}$ in the k-th observation window.

3.1 The sharing scheme based on the modified Wada index

Let us consider a digital grayscale carrier image $C = (c_{k,l})$, $k = 1, \ldots, n_x$; $l = 1, \ldots, n_y$. The modified indicator function $\mathbf{I}_q^{(s)}$ is used to split the carrier image C into s^2 dichotomous shares $H_1, H_2, \ldots, H_{s^2}$ according to the following rule:

- Construct a covering scheme for the carrier image C by using overlapping $s \times s$ observation windows. For each $s \times s$ observation window use the indicator function $\mathbf{I}_q^{(s)}$, $q = 1, \ldots, s^2$ to determine the number of different grayscale levels in the current observation window.

- Mark the number of grayscale levels in each overlapping observation window in the appropriate dichotomous share: $H_q(r,t) = 1$ if $\mathbf{I}_q^{(s)}(C(r : r+s-1;\ t : t+s-1)) = 1$, where r and t are the coordinates of the top-left corner of the current observation window, and $(r : r+s-1;\ t : t+s-1)$ denotes the location of the current observation window.

Note that the size of the shares H_q is smaller than of the original image. Also, the conjunction of different shares is an empty set: $H_i \wedge H_j = [0]$, $i \neq j$; and the disjunction of all shares yields a full set: $H_1 \vee H_2 \vee \cdots \vee H_{s^2} = [1]$; where $[0]$ and $[1]$ are matrices of zeros and ones accordingly.

3.2 Example 1. A primitive illustration of the sharing scheme

Let us consider a 3×3 grayscale image defined as a matrix of pixels $\begin{bmatrix} 96 & 96 & 96 \\ 96 & 96 & 71 \\ 123 & 222 & 169 \end{bmatrix}$ (the "stego" image in Fig. 1), and a 2×2 dichotomous matrix $\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ (the "secret" image in Fig. 1). The stego image is covered by four different overlapping 2×2 observation windows (Fig. 1).

The brightness of all pixels is equal only in the observation window at the top-left corner of the stego image (Fig. 1). The dichotomous share H_1 depicts the location of all observation windows where $m = 1$. Only the top-left cell of H_1 is equal to 1 because all other three observation windows yield the values of m greater than 1.

Analogously, only the top-right observation window yields $m = 2$. Therefore only the top-right cell of the second share H_2 is equal to 1 (Fig. 1).

Only a single bottom-left observation window yields $m = 3$ – therefore the bottom-left cell of H_3 is equal to 1. Finally, only the bottom-right observation window yields $m = 4$ – therefore the bottom-right cell of H_4 is equal to 1 (Fig. 1).

All four different shares are shown in the lower row of Fig. 1 ($s^2 = 4$). The secret dichotomous image is revealed by computing the disjunction $H_1 \vee H_3$ (Fig. 1). In other words, the decoding procedure in Fig. 1 can be represented by a straightforward mapping:

$$T^{3\times 3} \to H_1^{2\times 2} \vee H_3^{2\times 2} = S^{2\times 2}. \qquad (4)$$

3.3 Example 2. Manipulations with the Wada index

Let us consider a 2×2 observation window where the modifications are allowed with the brightness of the bottom-right pixel only. If the brightness of all pixels is equal (the first row in Fig. 2), then the brightness of the bottom-right pixel can be increased or decreased by one step. This modification changes the number of different colors in the current observation window from $m = 1$ to $m = 2$ (Fig. 2).

The second row in Fig. 2 illustrates the situation when the number of different colors must be decreased from $m = 4$ to $m = 3$. Unfortunately, that cannot be reached by changing the brightness of the pixel by one step. One possibility is to decrease the brightness by 73 steps, resulting into $169 - 73 = 96$. Another option is to increase the brightness by 53 steps, resulting into $169 + 53 = 222$. Clearly, the magnitude of the change is lower in the second option – therefore the number 222 is shown in green (Fig. 2).

4 The definition of a perfect covering and its properties

Clearly, the main objective of any steganographic encoding scheme is to minimize any changes in the carrier image. However, it appears that the magnitude of the change cannot be always equal to 1 (Fig. 2). Moreover, any change in the bottom-right corner of the current observation window will also change the number of different colors in the adjacent overlapping observation windows.

Without loss of generality, let us consider $n_x = n_y = 5$ and $s = 2$ (Fig. 3). Let us assume that changes in the bottom-right corner of the current observation window are required at all possible locations over the carrier image (the worst-case scenario).

Let us start from $r = 1$ and $t = 1$. The initial position of the observation window is shown in solid black lines in Fig. 3(a). The first modification of the bottom-right pixel is marked by 1 (Fig. 3(a)). Let us denote the first observation window as window 1.

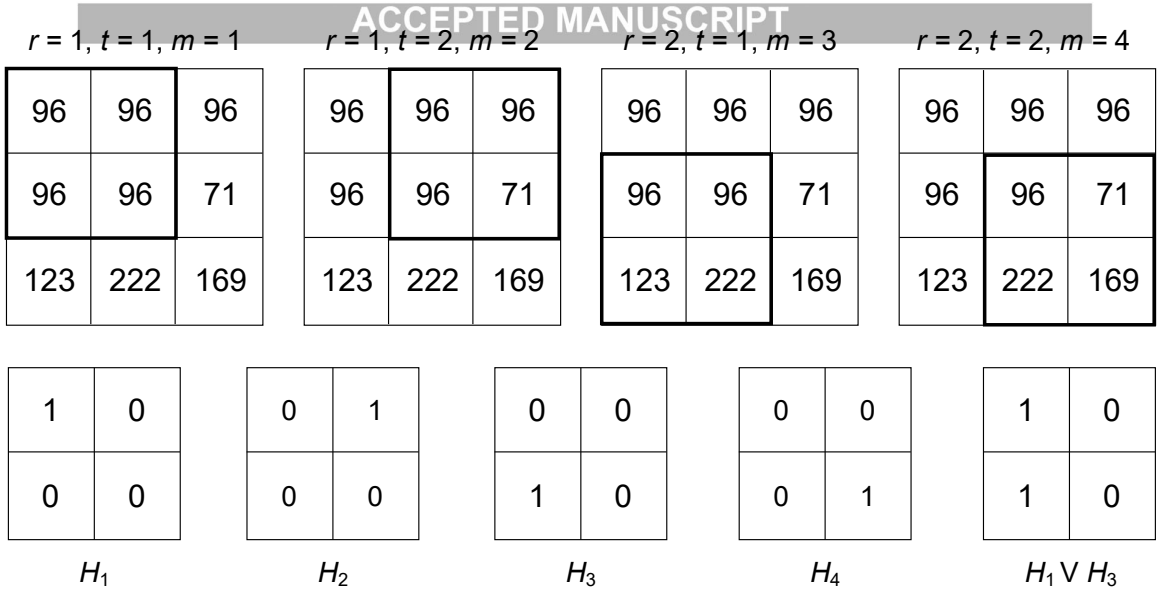

Fig. 1 The illustrative example depicting the sharing scheme (the decoding algorithm). The stego image is shown in the first row ($n_x = n_y = 3$); the size of the observation window is 2×2. The secret dichotomous image is $S = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$. The brightness of all pixels is the same in the observation window at $r = 1$ and $t = 1$ (that yields $m = 1$). Therefore, $H_1(1,1) = 1$. Two different grayscale levels (96 and 71) are observed at $r = 1$ and $t = 2$. Therefore, $H_2(1,2) = 1$. Three different grayscale levels (96, 123, and 222) are observed at $r = 2$ and $t = 1$. Therefore, $H_3(2,1) = 1$. Finally, four different grayscale levels are observed at $r = 2$ and $t = 2$. Therefore, $H_4(2,2) = 1$. The disjunction of all shares with odd indexes yields the secret

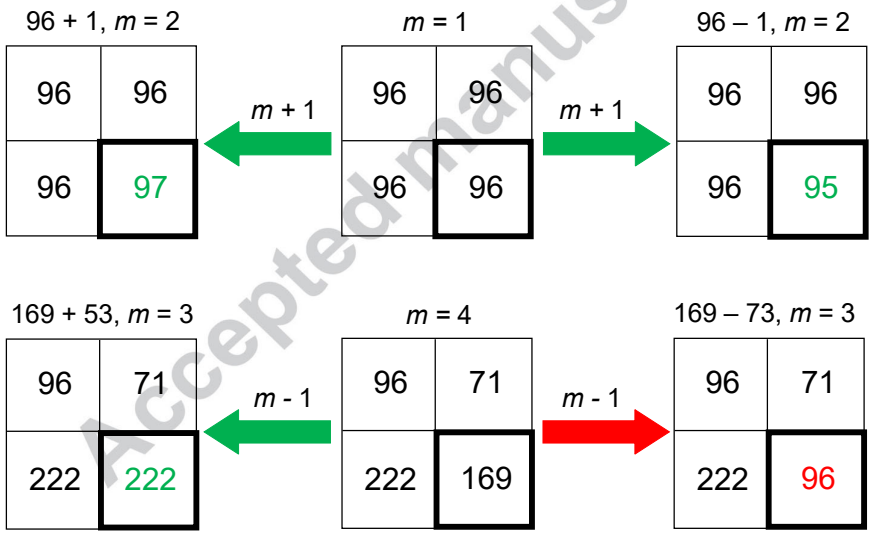

Fig. 2 The modification of the bottom-right pixel of the current observation window at $s = 2$. The first row illustrates the situation when the brightness of the pixel can be increased or decreased by one step. This modification changes the number of different colors in the current observation window from $m = 1$ to $m = 2$. The second row illustrates the situation when the number of different colors must be decreased from $m = 4$ to $m = 3$. Green color denotes the smallest possible change

Red arrows in Fig. 3 depict the trajectory of the observation window as it covers the whole carrier image. First, the observation window is shifted by one pixel to the right, and the modification is performed at a pixel marked by 2 (Fig. 3(a)). The observation window reaches the right border of the carrier image in three steps (Fig. 3(a)). Then, the observation window is returned to the left border of the carrier image and shifted by one pixel downwards (Fig. 3(a)). The process continues until the

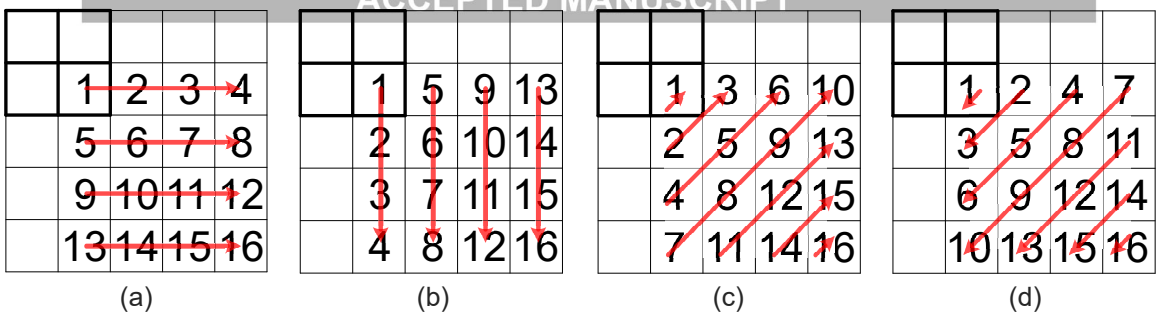

Fig. 3 Four perfect coverings at $n_x = n_y = 5$ and $s = 2$. The initial position of the observation window is shown in solid black lines. Red arrows depict the trajectory of the observation window as it covers the whole carrier image

bottom-right corner of the carrier image is reached (Fig. 3(a)).

The modification of the pixel marked by 1 will have a direct impact on modifications at windows 2, 5, and 6 (Fig. 3(a)). This is because pixel 1 does fit into the according observation windows (Fig. 3(a)). However, sequential modifications 2, 3, ..., 16 will never result into a conflict. In other words, the modification at the k-th window will not change the pre-set numbers of colors in all previous l-th windows; $l = 1, 2, \ldots, k-1$.

Definition 1 A covering is a perfect covering if a sequential modification at the current observation window does not cause conflicts in all previous observation windows.

Corollary 1 A covering is a covering with a recurrence if it is not a perfect covering.

Four perfect coverings are illustrated in Fig. 3. A covering with a recurrence is shown in Fig. 4. Steps 1, 2, 3, 4, and 5 do not cause any conflicts. However, step 6 (marked in red in Fig. 4) generates a conflict. The matter of fact is that the modification of pixel 6 can compromise the pre-set number of different colors in window 5. In other words, the previous modification at pixel 5 must be recalculated.

By the way, four perfect coverings depicted in Fig. 3 are not the only possible perfect coverings. Different combinations between perfect coverings shown in Fig. 3 can also produce a perfect covering (Fig. 5).

Corollary 2 A perfect covering does not exist for a carrier image with periodic boundary conditions.

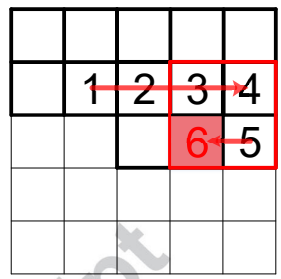

Fig. 4 A covering with a recurrence at $n_x = n_y = 5$ and $s = 2$. Steps 1, 2, 3, 4, and 5 do not cause any conflicts. However, step 6 (marked in red) generates a conflict because any changes in pixel 6 will change the Wada index of the observation window marked in red (the previous step)

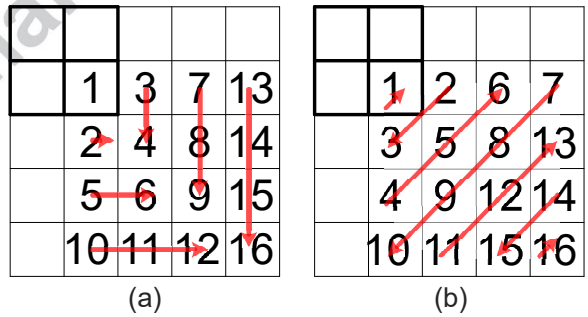

Fig. 5 Different combinations between perfect coverings shown in Fig. 3 also produce perfect coverings

Proof Without loss of generality let us set $n_x = n_y = 5$ and $s = 2$. Periodic boundary conditions of the carrier image imply that computations are performed on a surface of a torus (the Moore neighborhood of the pixel with coordinates $(1, 1)$ are pixels with coordinates $(1, 2)$, $(2, 2)$, $(2, 1)$, $(2, 5)$, $(1, 5)$, $(5, 5)$, $(5, 1)$, and $(5, 2)$ in the clockwise direction). Transitions 2, 3, and 4 do not generate any conflicts (Fig. 6). However, the next step from the observation window 4 to the observation window 5 generates a recurrence in window 1. □

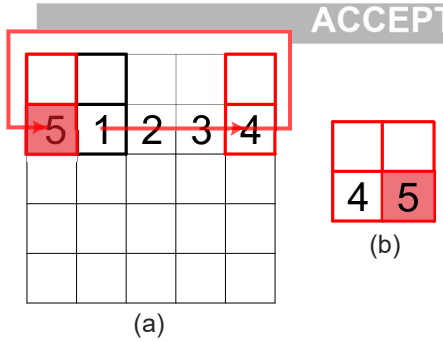

Fig. 6 A perfect covering does not exist for a carrier image with periodic boundary conditions. Transitions 2, 3, and 4 do not generate any conflicts. However, the next step from the observation window 4 to the observation window 5 generates a recurrence in window 1

Corollary 2 yields an important conclusion. If the size of the carrier image is $n_x \times n_y$ and the size of the observation window is $s \times s$, then the maximum size of the secret image produced by a perfect covering is $(n_x - s + 1) \times (n_y - s + 1)$.

Corollary 3 Let the carrier image and the secret image are given and fixed. Then the encoded stego image does not depend on the type of a perfect covering.

Proof Without loss of generality let us set $n_x = n_y = 3$ and $s = 2$ (Fig. 7). Panels (a), (b), (c), and (d) in Fig. 7 represent a horizontal perfect covering (Fig. 3(a)). Analogously, panels (e), (f), (g), and (h) represent a vertical perfect covering (Fig. 3(b)). The first step of the horizontal and the vertical coverings results into the same modification at the pixel with coordinates (2,2) (marked as $\tilde{C}_{2,2}$ in Fig. 7(a) and Fig. 7(e)). The second step of the horizontal covering results into the modification $\tilde{C}_{2,3}$ (Fig. 7(b)). The second step of the vertical covering results into the modification $\tilde{C}_{3,2}$ (Fig. 7(f)). The third step of the horizontal covering results into the modification $\tilde{C}_{3,2}$ (Fig. 7(c)). However, $\tilde{C}_{3,2}$ in Fig. 7(f) is exactly the same as $\tilde{C}_{3,2}$ in Fig. 7(c). This is because $\tilde{C}_{2,2}$ are the same in Fig. 7(a) and Fig. 7(e). In other words, the absence of recurrences yields the same pattern of modifications if only the covering is a perfect covering. □

5 The proposed steganographic scheme based on the Wada index

5.1 The encoding scheme

The main idea of the proposed encoding algorithm is to make minimal changes to the grayscale carrier image in such a way that the disjunction of all shares with odd indexes would yield the secret dichotomous image.

Let us select the size of the observation window $s = 3$ (resulting into nine different shares). The only changes are allowed in the bottom-right pixel of the current observation window. The carrier image must be covered by overlapping observation windows. The covering scheme must be a perfect covering scheme.

The bottom-right pixel of the current observation window does not need to be changed in two different cases:

- The number of different colors in the current observation window is odd, and the corresponding secret pixel is black.
- The number of different colors in the current observation window is even, and the corresponding secret pixel is white.

Let us consider a situation when both conditions are not satisfied, and the bottom-right pixel of the observation window must be changed. Two different situations are discussed below.

- The brightness of the bottom-right pixel does not coincide with the brightness of any other pixel in the current observation window. Then, the only option is to reduce m by one. The brightness of the bottom-right pixel must be changed (increased or decreased) to the nearest brightness of the remaining eight pixels in the current observation window.
- The brightness of the bottom-right pixel does coincide with the brightness of one (or more) pixels in the current observation window. In this case, the only option is to increase m by one. The brightness of the bottom-right pixel must be increased or decreased by the smallest possible integer number in such a way that the corrected brightness does not coincide with any other value in the observation window.

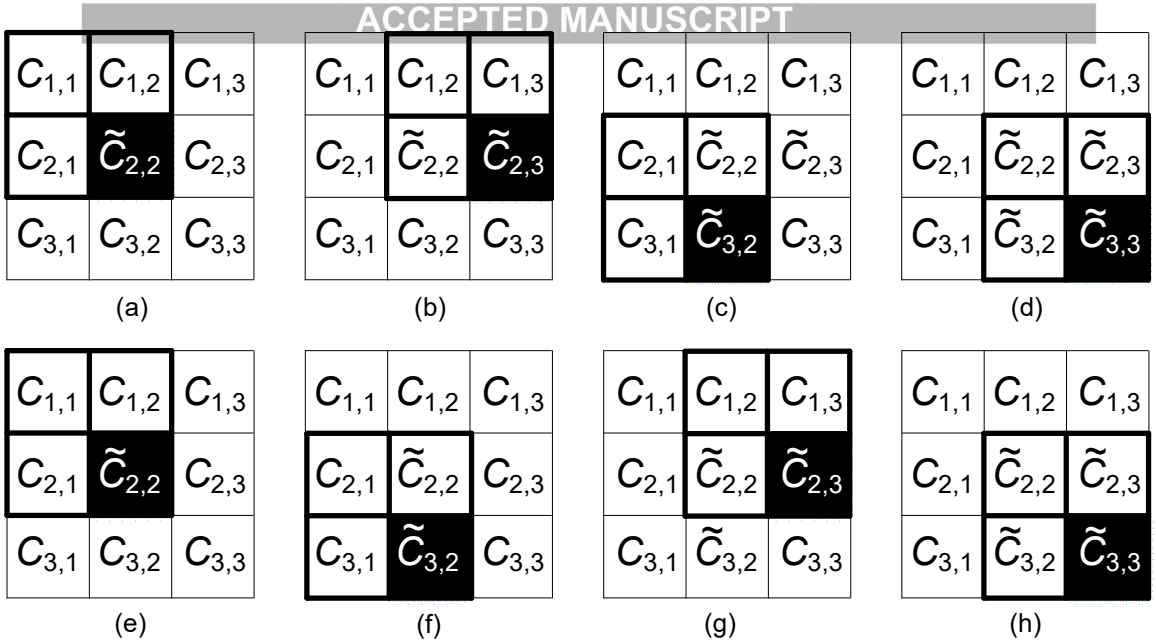

Fig. 7 The encoded stego image does not depend on the type of a perfect covering. Panels (a), (b), (c), and (d) represent a horizontal perfect covering (Fig. 3(a)). Panels (e), (f), (g), and (h) correspond to a vertical perfect covering (Fig. 3(b)). Letters marked with a wave depict pixels with a modified brightness. Black-marked cells depict modifications in the current observation window. The absence of recurrences yields the same pattern of modifications for horizontal and vertical perfect coverings (panels (d) and (h))

The process is continued with the next observation window until the whole covering of the carrier image is completed.

5.2 The decoding scheme

The only required information for the decoding step is the stego image itself. The decoding scheme is based on the disjunction of shares with odd indexes:

$$T^{n_x \times n_y} \rightarrow \bigvee_{k=1}^{\left[\frac{s^2}{2}\right]} H_{2k-1}^{(n_x-s+1)\times(n_y-s+1)} = S^{(n_x-s+1)\times(n_y-s+1)}, \quad (5)$$

where $[*]$ denotes the rounding operation.

6 Computational experiments

6.1 Computational experiments with the standard Lena image

Let us consider the standard Lena image (Fig. 8) as the carrier image. The dichotomous shares H_1, $H_2, \ldots, H_9$ are shown in Fig. 8. It is interesting to note that H_9 reveals the contours of the original image (Fig. 8). The fact that H_1 is empty is not surprising because the Lena image is a real digital photograph contaminated by the additive noise. Disjunctions of shares with odd and even indexes are shown in Fig. 8.

Next, the secret image S (the dichotomous city-map image shown in Fig. 9) is embedded into the standard Lena image. A naked eye cannot see any differences between the carrier image and the stego image (Figs. 8 and 9). However, the disjunction of shares with odd indexes reveals the secret (the disjunction of shares with even indexes reveals the inverse of the secret).

The portion of pixels modified in the carrier image, the magnitude of modifications, and the brightness histograms of the carrier and the stego images are presented in Fig. 10. The histogram of the differences between the carrier and the stego images is depicted in Fig. 11; the performance evaluation measures of the proposed encoding algorithm are shown in Table 1.

The number of modified pixels is rather high (49.38%), but it does correspond to the statistical estimate (around 50%). The number of pixels with the increased or the decreased brightness is

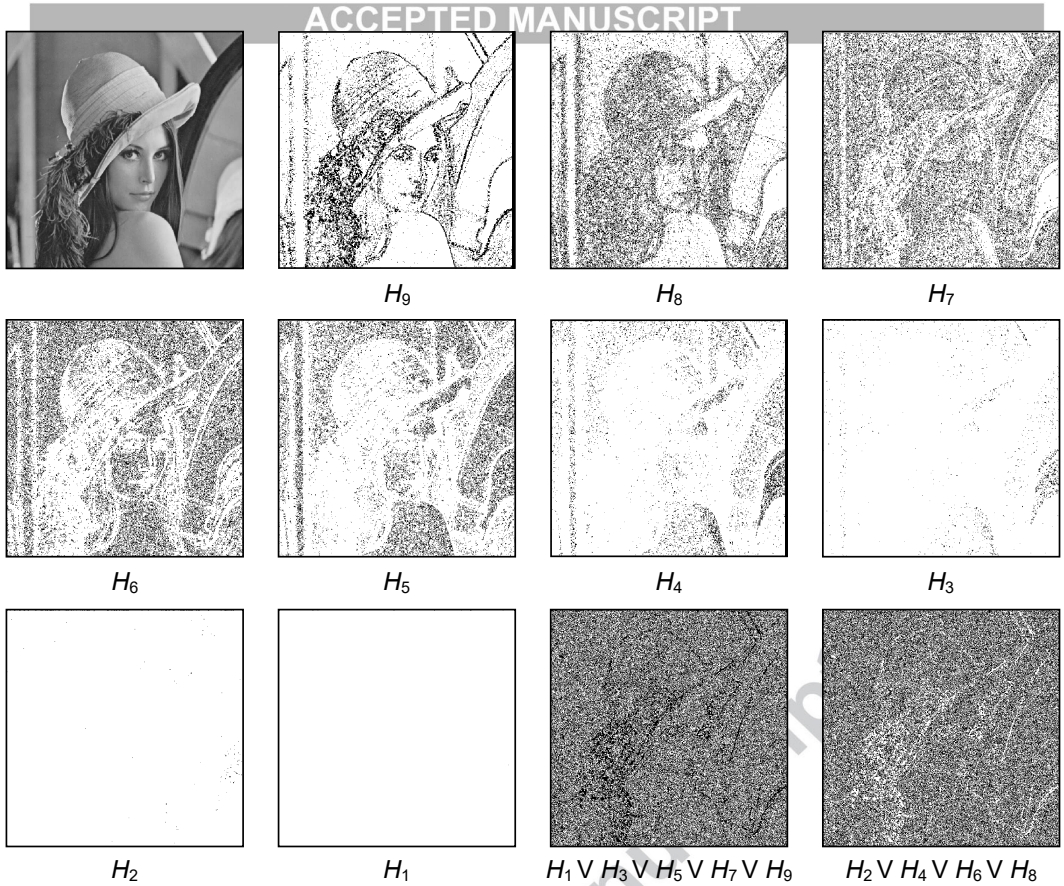

Fig. 8 Dichotomous shares H_1, H_2, ..., H_9 of the standard Lena image and the disjunctions of shares with even indexes $H_1 \vee H_3 \vee H_5 \vee H_7 \vee H_9$ and with odd indexes $H_2 \vee H_4 \vee H_6 \vee H_8$

almost the same (Table 1). The range of changes is high ($[-139;\ 143]$). However, large changes in the brightness of a pixel are very rare. The mean error (ME) representing the average change in the brightness is only -0.0428 (Table 1). Needless to say, the median of changes is 0 (Table 1). Mean absolute error (MAE), mean squared error (MSE), structural similarity index measure (SSIM), peak signal to noise ratio (PSNR) indexes show that the performance of the proposed scheme is comparable to the performance of the best contemporary steganographic schemes [11, 32].

6.2 Computational experiments with different carrier images

It is natural that the performance of the encoding algorithm depends on the characteristics of the carrier and the secret image. A sequence of synthetic digital images is designed in order to explore the functionality of the proposed encoding algorithm (Eq. 6).

The carrier image C is the standard Lena image L at $\gamma = 0$ (Eq. 6). The carrier image C is constructed as a weighted average of the standard Lena image L and the random noise R (the Lena image is gradually contaminated by the additive noise) for negative values of γ (Eq. 6). Analogously, the carrier image C is a weighted average of the standard Lena image L and a plain image P (the blurring effect) at positive values of γ (Eq. 6).

$$C = \begin{cases} (1+\gamma)\cdot L - \gamma \cdot R, & -1 \le \gamma < 0; \\ (1-\gamma)\cdot L + \gamma \cdot P, & 0 \le \gamma \le 1. \end{cases} \quad (6)$$

Some of the synthetic carrier images are depicted in the top row of Fig. 12 for illustrative purposes at $\gamma = -1,\ -0.75,\ -0.5,\ -0.25,\ 0,\ 0.25,\ 0.5,\ 0.75,\ 1$. In total 101 digital images (representing 101

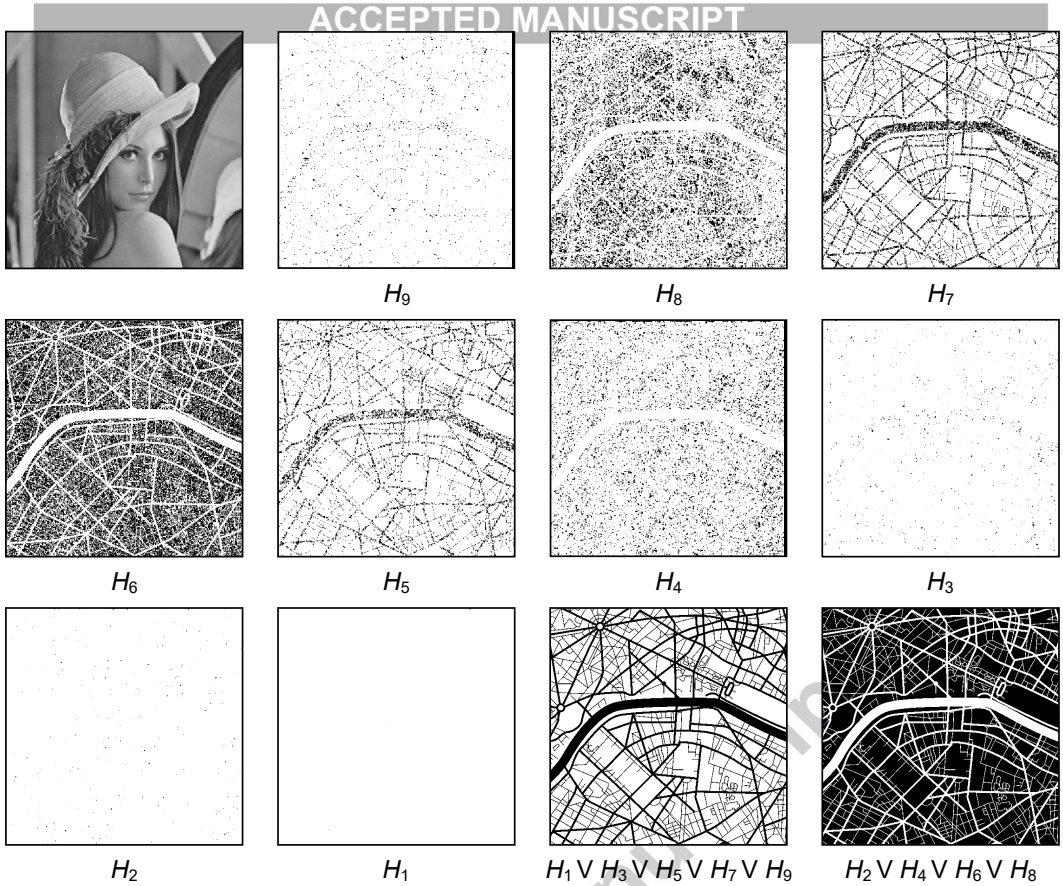

Fig. 9 The secret dichotomous city-map image is embedded into the standard Lena image. A naked eye cannot see any differences between the carrier image and the stego image (Figs. 8 and 9). The disjunction of shares with odd indexes $H_1 \vee H_3 \vee H_5 \vee H_7 \vee H_9$ reveals the secret (the disjunction of shares with even indexes $H_2 \vee H_4 \vee H_6 \vee H_8$ reveals the inverse of the secret)

discrete values of γ) are generated for running computational experiments visualized in Fig. 12.

Performance evaluation measures such as the range of corrections $[min, max]$, ME, MSE, PSNR, SSIM, and the correlation coefficient are calculated for the sequence of different carrier images (Fig. 12(a)–(e)). Note that most of these measures (except the correlation coefficient) demonstrate that the best performance of the proposed encoding technique is achieved when γ approaches to 1 (when the carrier image turns into an almost plain image).

Although some steganographic algorithms fail when encoding a secret into a plain carrier image [33, 34], the proposed technique deals well with such a task. The encoding of the secret image into the plain carrier image (the brightness of all pixels is equal to 128) is demonstrated in Fig. 13. The stego image produced by the proposed technique is shown in Fig. 13(b), the contrast-enhanced stego image is depicted in Fig. 13(c), the box marked in red is zoomed in Fig. 13(d). It is clear that the distribution of pixels in the stego image is random and does not reveal the secret image.

Computational experiments are continued with other carrier images (Cameraman, Peppers, Jetplane) and other secret images (Random and Checkerboard images). Performance measures for the proposed steganographic scheme based on the Wada index are depicted in Table 1.

6.3 Comparisons with alternative steganographic techniques

The standard LSB steganographic scheme is based on the modification of the 1st least significant bit of the pixel in the carrier image [10, 14]. Such a modification increases or decreases the brightness

Table 1 Performance evaluation measures for the computational experiments with different carrier and secret images

Performance measures	Lena			Cameraman		
	City-map	Random	Checkerboard	City-map	Random	Checkerboard
Pixels with increased brightness, %	24.32	24.48	24.41	24.56	24.68	24.31
Pixels with decreased brightness, %	25.06	25.04	24.98	24.73	24.82	24.60
The range of changes	[-139;143]	[-126;142]	[-110;154]	[-143;164]	[-131;136]	[-142;134]
Median of changes	0	0	0	0	0	0
Mean error	-0.0428	-0.0426	-0.0244	-0.0138	0.0032	-0.0344
MAE	1.5170	1.5154	1.5250	1.4589	1.4565	1.4630
MSE	20.9018	21.5322	21.5600	21.4351	20.8718	21.7500
SSIM	0.9692	0.9694	0.9691	0.9714	0.9713	0.9716
PSNR	34.9290	34.7999	34.8000	34.8195	34.9352	34.7600
Performance measures	Peppers			Jetplane		
	City-map	Random	Checkerboard	City-map	Random	Checkerboard
Pixels with increased brightness, %	24.73	24.66	24.64	24.75	24.93	24.80
Pixels with decreased brightness, %	24.83	24.90	24.87	24.54	24.59	24.42
The range of changes	[-162;114]	[-165;136]	[-149;119]	[-164;148]	[-116;143]	[-116;129]
Median of changes	0	0	0	0	0	0
Mean error	0.0117	0.0083	0.0034	0.0949	0.0905	0.0996
MAE	1.4223	1.4149	1.4480	1.5260	1.5313	1.5190
MSE	17.7861	17.4649	19.0100	21.2751	20.8216	20.9000
SSIM	0.9676	0.9682	0.9668	0.9720	0.9715	0.9721
PSNR	35.6300	35.7091	35.3400	34.8521	34.9457	34.9300

of a pixel by 1 what leads to the sufficiently high values of PSNR between the carrier and the stego images. Unfortunately, the secret message hidden using the standard LSB technique can be detected by RS analysis [17, 18]. Moreover, the secret image embedded using the standard LSB algorithm is leaked by the first bit plane of the stego image [14].

The two least significant bit (2LSB) algorithm is a generalisation of the standard LSB steganography. In 2LSB steganography, 2 bits of the secret information are embedded in the last two bit planes (bit plane 1 and bit plane 2) of the carrier image [35]. The main advantage of this technique is that the maximum encoding capacity of 2LSB is twice compared to the standard LSB algorithm. Unfortunately, the first two bit planes of the stego image also reveal the secret information. That is the main drawback of the 2LSB scheme [35].

The random 2LSB steganographic scheme is a modification of the 2LSB scheme. In random 2LSB, one secret bit is embedded either into the 1st or into the 2nd bit plane of the carrier image (the 1st or the 2nd LSB plane is chosen randomly) [14] . Note that the first 2 bit planes of the stego image obtained by the random 2LSB technique still reveal the secret information.

An improved version of the 2LSB scheme is proposed in [19]. The improved 2LSB scheme is based on the manipulation of the first two bit planes of the carrier image. The proposed scheme has the property of undetectability with respect to stego quality and keeps the same payload capacity as the 2LSB scheme [19]. The first two bit planes of the stego image do not reveal the secret information interpretable by a naked eye. However, one can clearly observe the fact that the first two bit planes are artificially modified.

Another way to hide secret information in higher bit planes (compared to the LSB scheme) is the Fibonacci-like steganography [36, 37]. Such type of steganographic scheme relies on the bit plane mapping instead of the bit plane replacement. This scheme guarantees the increased payload capacity by embedding two secret bits into three bits of the carrier pixel [36, 37]. Authors of [37] claim that the same embedding scheme can be also applied to different bit planes. That results

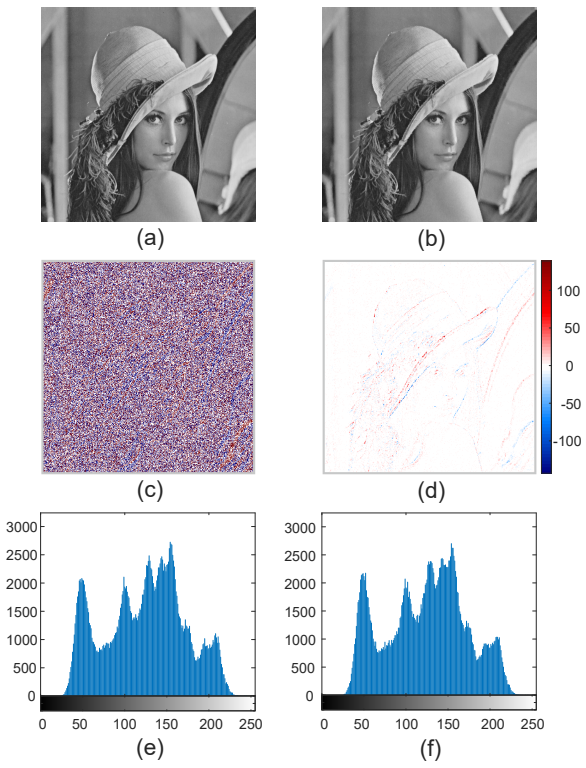

Fig. 10 The carrier image (panel (a)) and the stego image (panel (b)). Panel (c) shows pixels with and without modification. Non-modified pixels are shown in white, pixels with the increased brightness – in red, and pixels with the decreased brightness – in blue. Panel (d) shows the magnitude of modification of each individual pixel. The brightness histograms of the carrier and the stego images are depicted in panels (e)–(f)

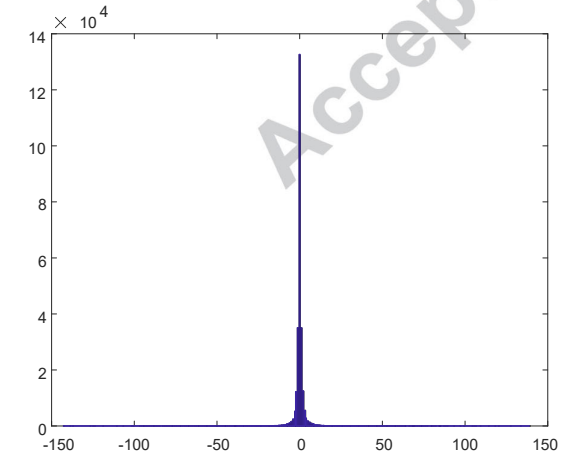

Fig. 11 The histogram of the differences between the carrier and the stego images

into a more robust data hiding algorithm. However, that also results into larger visual distortions. The drawback of such a scheme is that not all pixels of the stego image are used for the embedding of the secret image. Authors of [20] overcome this limitation by proposing a mapping algorithm which can be applied for all pixel brightness levels to embed secret bits by mapping one single secret bit onto the first 3 bit planes. For example, an adaptive payload and distribution based on image texture features is used in [38].

However, a straightforward encoding of the secret information into a bit plane with a higher index than 3 (or into several randomly selected bit planes with higher indexes) does automatically yield lower values of the PSNR between the carrier and the stego images. Moreover, a naked eye can recognize the secret information in the stego image if the index of the bit plane is higher that 4. Despite this fact, bit planes with higher indexes are still used in different steganographic schemes. However, other security means need to be employed to ensure the robustness of the stego image. For example, the Canny edge detection technique is used to identify true edge pixels, and the 4 least significant bits of edge pixels are manipulated by the 4LSB steganography [39]. Hiding data only in edges of a digital image improves the quality of the stego image significantly [39, 40], although the capacity of such schemes remains low [41].

The comparison of averaged performance evaluation measures for LSB, 2LSB, random 2LSB, improved 2LSB, random 3LSB, random 4LSB, and the proposed scheme is presented in Table 2. PSNR and SSIM are two measuring tools that are widely used in image quality assessment. SSIM is a newer performance evaluation measure that is designed based on three factors (luminance, contrast, and structure) to better suit the workings of the human visual system and is considered as a better measure of imperceptibility in all aspects [42]. It is worth noting that SSIM for the proposed scheme is comparable to SSIM for the LSB scheme. However, the proposed scheme is able to pass the RS steganalysis and the bit plane tests.

The steganographic scheme proposed in this paper is based on the modification of the brightness of the pixels in the carrier image according to the Wada index of its surrounding. Such an

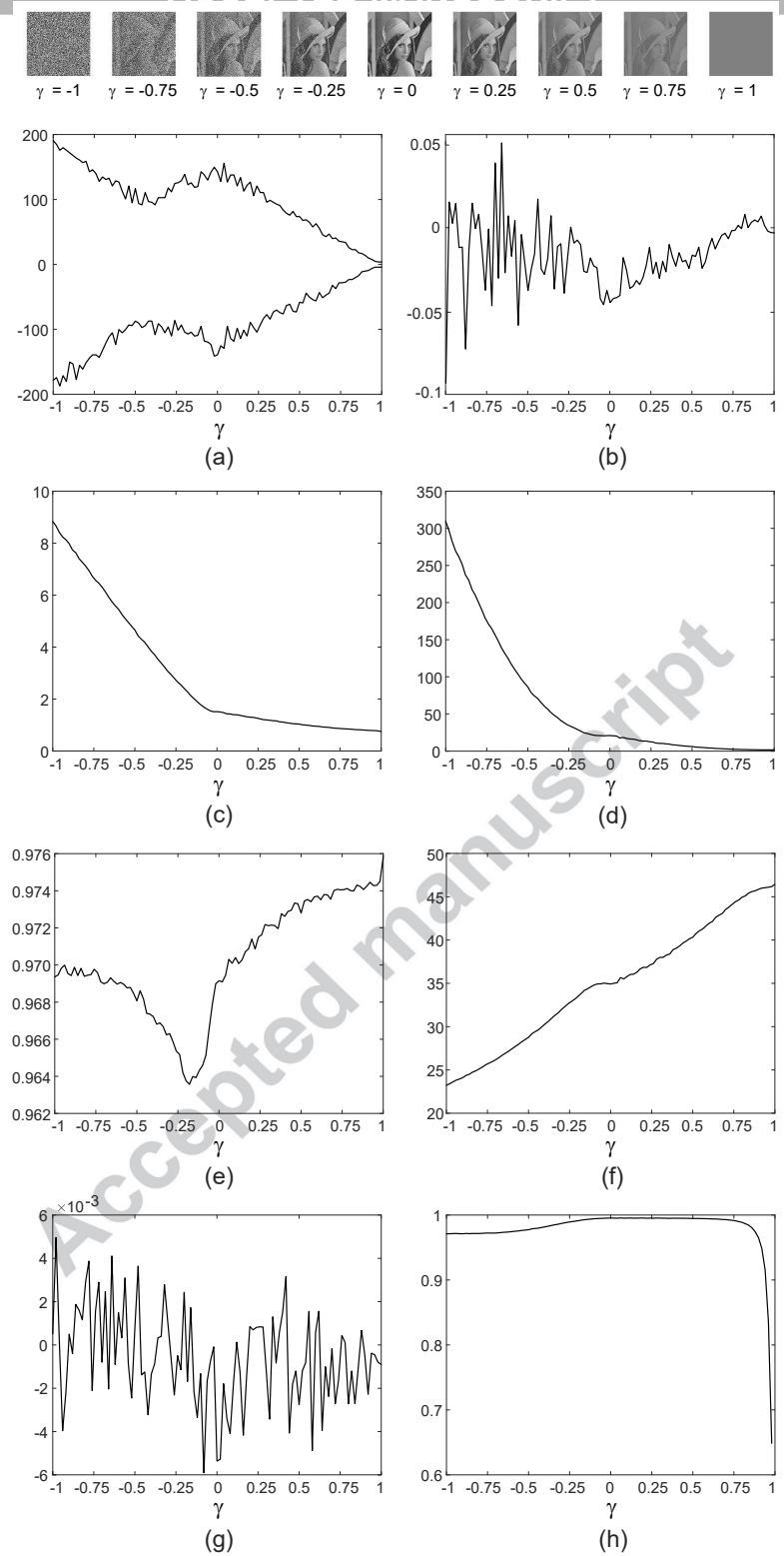

Fig. 12 Statistical characteristics of the proposed steganographic scheme. The secret dichotomous city-map image is embedded into the weighted average of the standard Lena image. (a) The range of corrections $[min, max]$; (b) ME between the carrier image and the stego image; (c) MAE between the carrier image and the stego image; (d) MSE between the carrier image and the stego image; (e) SSIM between the carrier image and the stego image; (f) PSNR between the carrier image and the stego image; (g) Correlation coefficient between secret image and the correction matrix; (h) Correlation coefficient between the carrier image and the stego image

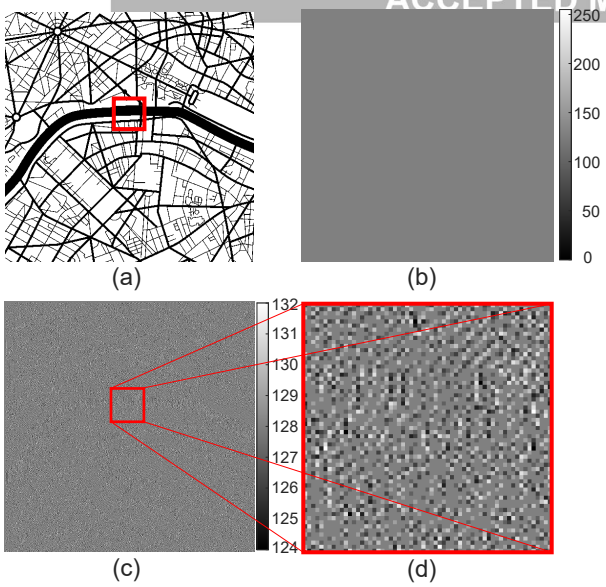

Fig. 13 Encoding the secret image (shown in panel (a)) into the plain carrier image (the brightness of all pixels is 128 in panel (b)). The contrast-enhanced stego image is depicted in panel (c) (note that the colorbar range is 124-132). The zoomed red-marked region in (c) is depicted in panel (d)

operation yields changes in several bit planes simultaneously for a single pixel. Let us consider that one needs to encode a single secret bit into the pixel which brightness is 135 (10000111 in the binary form), and the brightness of that pixel must be increased by 11. The resulting brightness is $135+11 = 146$ (10010010 in the binary form). The transition from 10000111 to 10**0**10**0**1**0** yields modifications in the 1st, the 3rd and the 5th bit plane. For example, hiding the secret city-map image into the carrier Lena image results into the following proportions of the modified bits in different bit planes: 34.76% in bit plane 1, 28.69% in bit plane 2, 20.00% in bit plane 3, 12.78% in bit plane 4, 7.93% in bit plane 5, 4.33% in bit plane 6, 2.51 % in bit plane 7, 1.24% in bit plane 8 (Fig. 19). This fact is represented by relatively large MSE in Table 2. Note that averaged performance evaluation measures in Table 2 are computed for different carrier images (Lena, Cameraman, Peppers, and Jetplane) and different secret images (City-map, Random, Checkerboard) (Table 1).

The number of modified bit planes during the process of encoding of one secret bit can vary from 1 to 8. However, both the number of the modified biplanes, and the indexes of the modified bit planes depend on two factors. The first factor is the Wada index of the observation window surrounding the current bit of the carrier image. The second factor is the dichotomous value of the current pixel in the secret image. As demonstrated previously, the number of modified bit planes and the indexes of the modified bilplanes can be considered as random numbers and are different for each individual pixel. Moreover, the proportion of modifications in bit planes with higher indexes is much smaller that the proportion of modifications in bit planes with lower indexes (Fig. 19). Finally, the payload capacity of the proposed steganographic scheme is almost 100%.

7 The robustness of the proposed scheme

7.1 The robustness of the proposed scheme to the partial destruction of the stego image

An important feature of a steganographic scheme is its robustness to the partial destruction of the stego image. The proposed scheme can withstand blockade of the stego image (Fig. 14). The part of the secret image in the blocked area is lost – but the secret is successfully decoded in the whole remaining area (Fig. 14).

The proposed scheme is not completely destroyed by the additive noise. Fig. 15(a) shows the stego image with 1% of pixels corrupted by the 'salt and pepper' type noise. Such a contamination of the stego image yields the secret image with 4.45% of incorrectly decoded pixels (Fig. 15(b)). 19.28% of pixels are decoded incorrectly if 5% of pixels of the original stego image are corrupted by the 'salt and pepper' type noise (Fig. 15(c)–(d)). That can be explained by the fact that a replacement of a single pixel in the stego image does change the number of different colors in nine adjacent 3×3 observation windows. Some of those changes (around a half) do not have any impact to the decoding algorithm (the Wada index of the current observation window remains unchanged). Nevertheless, the perturbation of the stego image is amplified around 4.5 times in the decoded secret image.

It is interesting to observe that the magnitude of the destruction of the recovered secret

Table 2 The comparison of average performance evaluation measures for LSB, 2LSB, random 2LSB, improved 2LSB, random 3LSB, random 4LSB, and the proposed scheme

Average performance measures	LSB	2LSB	Random 2LSB	Improved 2LSB	Random 3LSB	Random 4LSB	Proposed
MAE	0.4986	0.6937	0.7478	0.9969	1.1640	1.8986	1.4830
MSE	0.4986	1.5264	1.2469	1.4934	3.4928	11.0050	20.4425
SSIM	0.9729	0.9243	0.9392	0.9149	0.8689	0.7520	0.9700
PSNR	51.1525	46.3342	47.1733	46.3908	42.7000	37.7167	35.0383

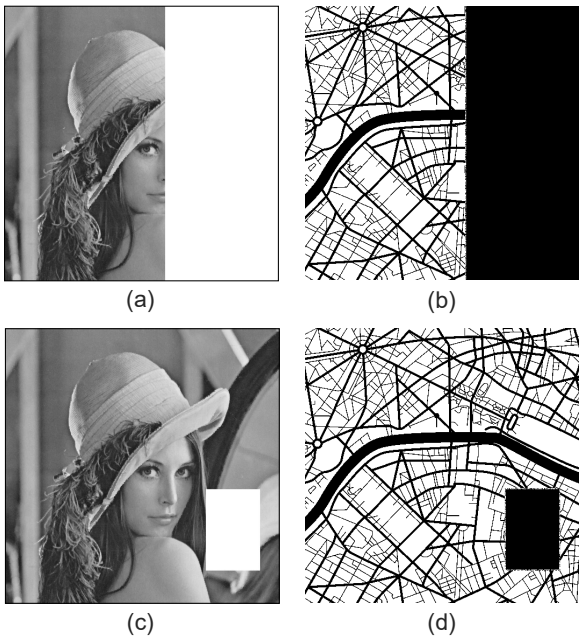

Fig. 14 The secret information is lost only within the blocked part of the stego image. Panels (a) and (c) represent stego images with blocked (white) rectangles; panels (b) and (d) show the decoded secret images

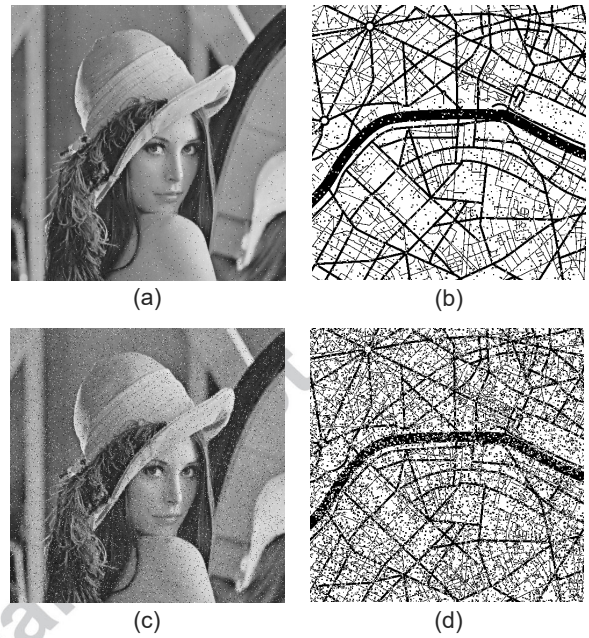

Fig. 15 The 'salt and pepper' type noise added to the stego image partially destroys the decoded secret. Stego images with 1% and 5% of pixels affected with the 'salt and pepper' type noise are depicted in panels (a) and (c) accordingly. The decoded secret images are shown in panels (b) and (d)

image does not strongly depend on the type of the noise added to the stego image. Fig. 16 shows the original stego image contaminated by the Gaussian noise with zero mean and variance equal to $1.5 \cdot 10^{-6}$ (panel (a)) and $5 \cdot 10^{-6}$ (panel (c)).

The Gaussian noise with variance equal to $1.5 \cdot 10^{-6}$ alters the brightness of 10.96% of pixels in the stego image. The Gaussian noise with variance $5 \cdot 10^{-6}$ changes 38.13% of pixels in the stego image. Clearly, such changes completely prevent the interpretation of the decoded secret (Fig. 16).

It is clear that the Gaussian noise with a higher variance fully destroys the secret. Such a feature of the proposed scheme can serve as an additional security factor for the proposed scheme. Adding a small amount of Gaussian noise does not make large changes to the stego image – but completely destroys the decoded secret. Note that PSNR between the original carrier image and the stego image is 34.9290. However, PSNR between the carrier image and the stego image with the additive Gaussian noise in Fig. 16(c) is almost the same (34.8420). In other words, the difference between both the non-perturbed stego image and the perturbed stego image are imperceptible to a naked eye. The receiver can eliminate the additive noise from the stego image (if only he knows the algorithm used to generate the noise) and can decode the non-destructed secret.

Note that adding (or subtracting) a constant to (from) the brightness of all pixels of the stego image does not destroy the secret (Fig. 17). That

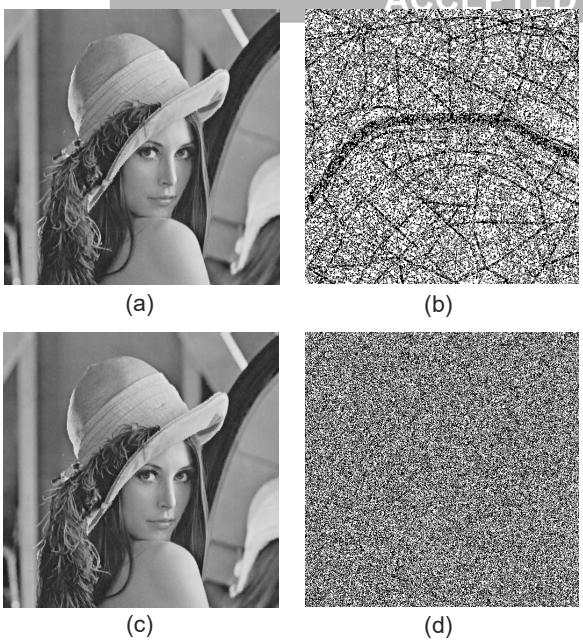

Fig. 16 The Gaussian type noise added to the stego image partially or fully destroys the decoded secret. Stego images with the added Gaussian noise (zero mean and the variance equal to $1.5 \cdot 10^{-6}$ and $5 \cdot 10^{-6}$) are depicted in panels (a) and (c). The decoded secret images are shown in panels (b) and (d) accordingly

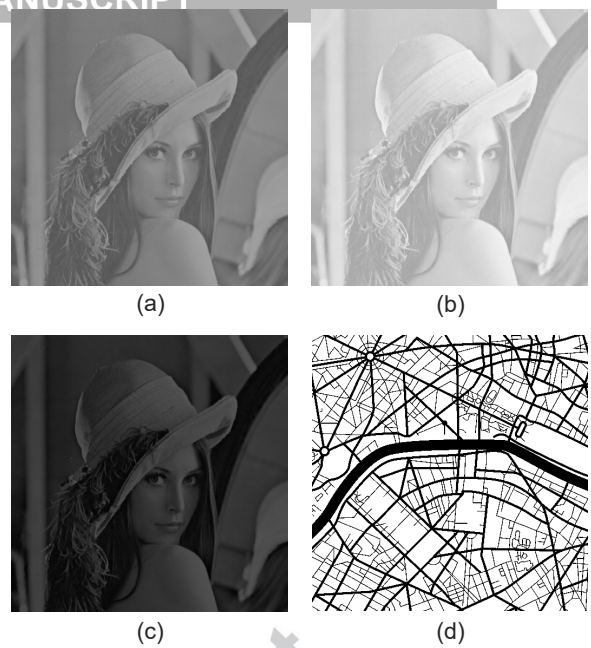

Fig. 17 The secret information is encoded in linearly transformed Lena image (panel (a)). If we add or subtract a constant value to/from each pixel of the stego image in (a), resulting modified stego images in panels (b) and (c) will be decoded correctly (panel (d))

can be explained by the fact that such a modification of the stego image does not change the number of different colors in the covering observation windows.

Attacks on stego images are broadly divided into image degradation, image enhancement, and geometric attacks [43]. Examples of geometric attacks are rotation, scaling, translation, shearing, warping and perspective transform. Unfortunately, the proposed scheme cannot withstand geometric and compression attacks because Wada indexes in overlapping observation windows are irrevocably destroyed.

7.2 The robustness of the scheme to steganalysis

The goal of steganalysis is to identify suspected images, determine whether or not they have a secret image encoded into them, and, if possible, recover that secret [44, 38, 45].

The brightness of each pixel of the carrier image is represented by eight bits. A straightforward statistical test for the determination of suspected images is based on the analysis of bit planes [46, 47, 48]. A real-life image (a digital photograph) is considered non-suspicious if its bit plane 1 or even the bit plane 2 are random images.

Figure 18 shows all eight bit planes of the original carrier image. Clearly, both bit plane 1 and bit plane 2 look completely random.

Figure 19 depicts all eight bit planes of the stego image carrying the secret image encoded by the proposed scheme. Bit plane 1 and bit plane 2 both look random (Fig. 19).

The proposed scheme can be considered as the geometric extension of the LSB steganography scheme. Really, the proposed scheme becomes the LSB scheme when $s = 1$. Eight bit planes of the stego image produced by the LSB steganography are depicted in Fig. 20.

The randomness of bit plane 1 and bit plane 2 in Fig. 19 is considered not by using some statistical algorithms. This is just a straightforward demonstration of the superiority of the proposed scheme against the LSB steganography. A more sophistical automatic tool is needed to test the robustness of the proposed scheme to steganalysis; the RS analysis [17] is used for that purpose.

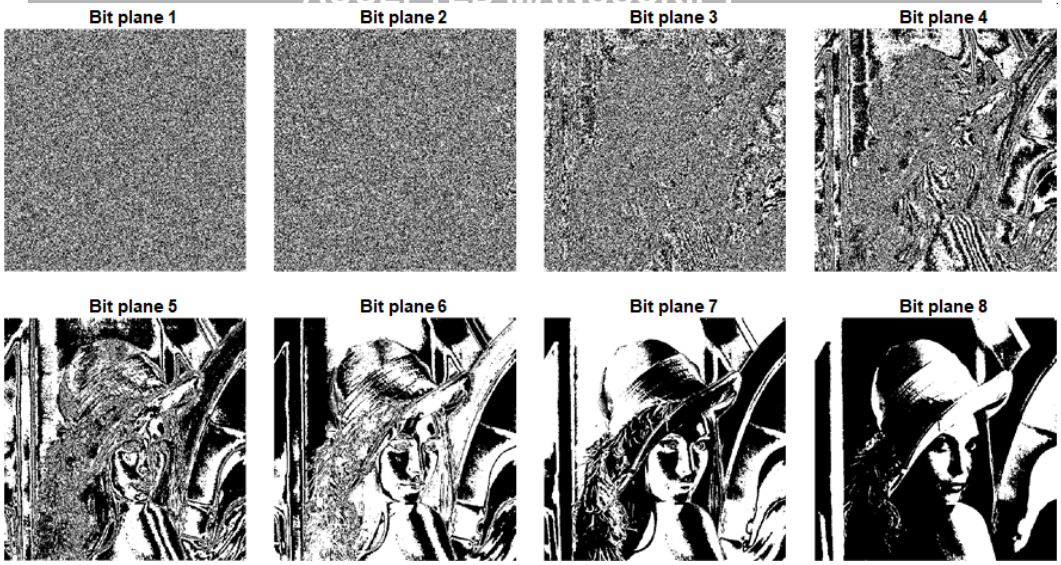

Fig. 18 Bit planes for the standard Lena image reveal no meaningful information in bit plane 1 and bit plane 2. This indicates that the picture is a real photograph

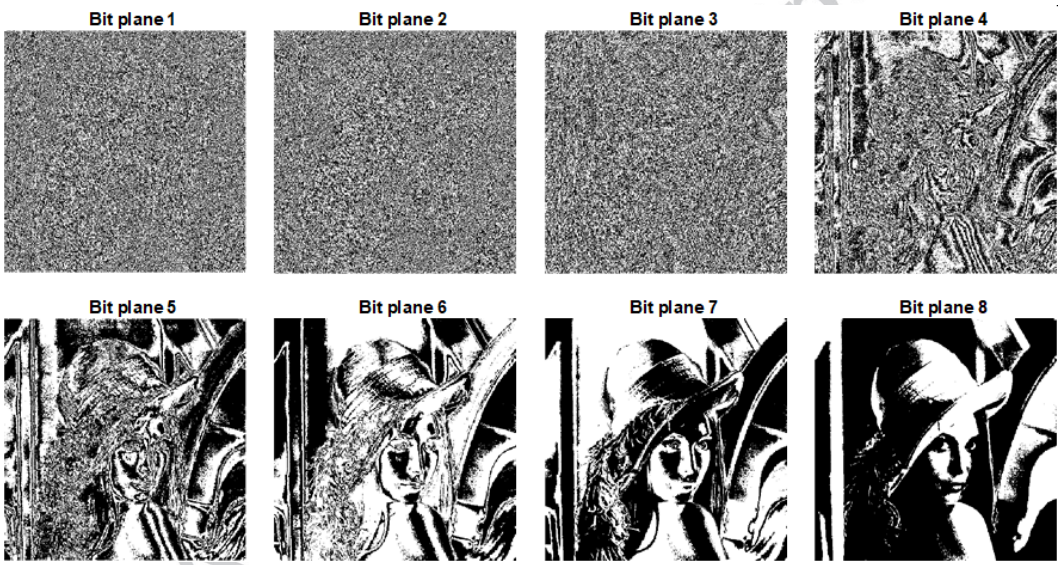

Fig. 19 Bit planes for the stego image carrying the secret dichotomous city-map image embedded into the standard Lena image. Bit plane 1 and bit plane 2 do not reveal any meaningful information. The proportions of modified bits in different bit planes are different: 34.76% in bit plane 1, 28.69% in bit plane 2, 20.00% in bit plane 3, 12.78% in bit plane 4, 7.93% in bit plane 5, 4.33% in bit plane 6, 2.51 % in bit plane 7, 1.24% in bit plane 8

Let us denote the number of regular groups for mask M as R_M (the percentage of all groups). Similarly, S_M denotes the relative number of singular groups. R_{-M} and S_{-M} are the numbers of regular and singular groups respectively for the negative mask $-M$. The statistical hypothesis of the RS analysis is that a typical image without embedded information (corresponding to the zero point on the x-axis) does produce approximately equal expected values of R_M and R_{-M} (the same holds for R_S and R_{-S}) [17].

The RS diagram for the original Lena image is depicted in Fig. 21(a) (the x-axis is the percentage of pixels with flipped least significant bits; the

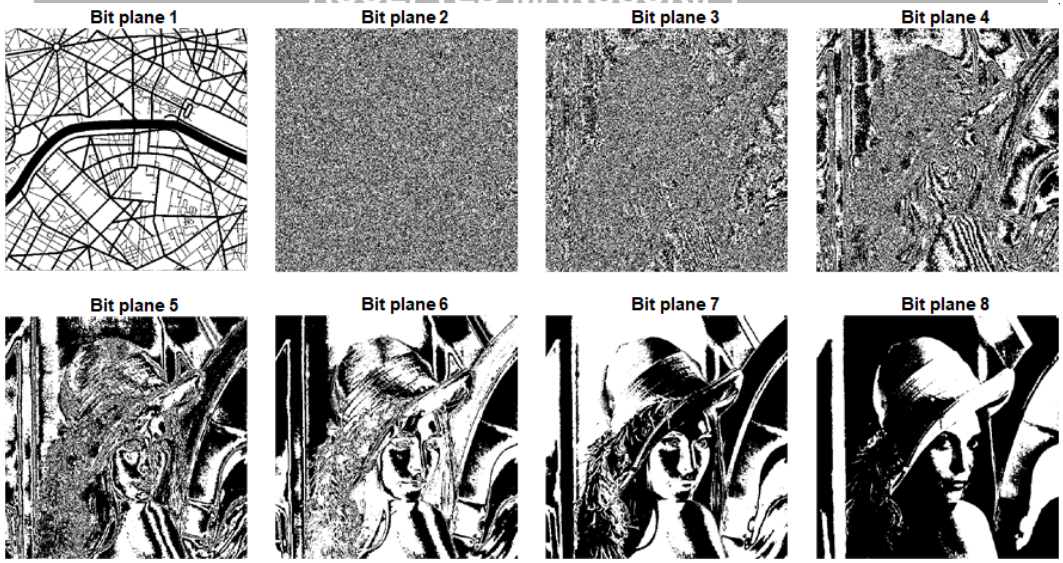

Fig. 20 Bit planes of the stego image produced by the LSB steganography (the secret dichotomous city-map image is embedded into the standard Lena image). The secret image is revealed in bit plane 1

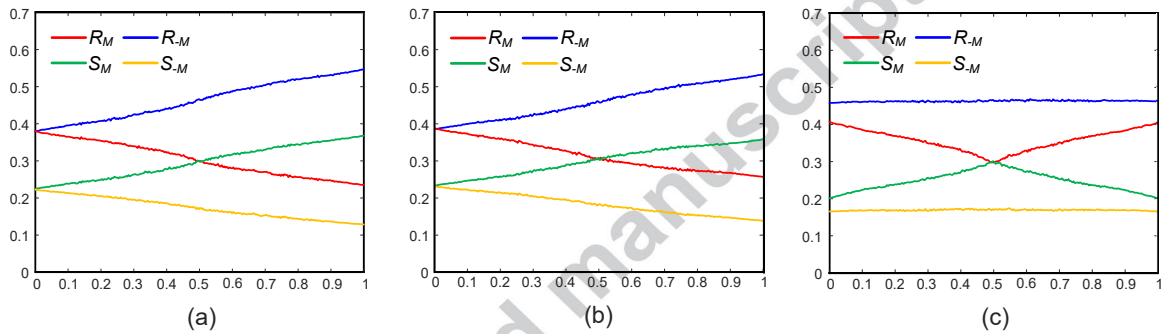

Fig. 21 RS diagrams show that the proposed steganographic scheme is robust to the RS steganalysis algorithms. The RS diagram for the standard Lena image is shown in panel (a). The RS diagram for the stego image carrying the secret dichotomous city-map image embedded into the standard Lena image is shown in panel (b). The RS diagram for the stego image produced by the LSB steganography (the secret dichotomous city-map image is embedded into the standard Lena image) is shown in panel (c)

y-axis is the relative number of regular and singular groups with masks M and $-M$). One can observe that $R_M \cong R_{-M}$ and $R_S \cong R_{-S}$ at $x = 0$ (Fig. 21).

The RS diagram for the Lena image with the secret image embedded using the proposed scheme (the stego image) is shown in Fig. 21(b). Again, $R_M \cong R_{-M}$ and $R_S \cong R_{-S}$ at $x = 0$ (Fig. 21(b)). Finally, the RS diagram for the Lena image with the secret image embedded using the LSB steganography is shown in Fig. 21(c). One can observe large differences between R_M and R_{-M} (also between R_S and R_{-S}) at $x = 0$ (Fig. 21(c)). One can conclude that the proposed scheme is robust to the discussed steganalysis algorithms (at $s = 3$).

8 Concluding remarks

A steganographic technique based on the Wada index is proposed in this paper. The modified indicator function is used to split the digital grayscale carrier image into dichotomous shares. The definition of a perfect covering of the carrier image with overlapping observation windows is introduced. Perfect coverings are exploited to produce a unique representation of the stego image. Computational experiments show that the statistical

performance indicators of the proposed scheme are comparable to the best available steganographic schemes. It is also demonstrated that the proposed scheme is robust to the partial destruction of the stego image and to the steganalysis algorithms.

The proposed steganographic scheme is based on two unique features. Firstly, it is based on perfect coverings of the carrier image. The fact that the stego image does not depend on the type of the perfect covering is far from being trivial. The proof of this feature is an important contribution of this paper.

Secondly, the proposed encoding scheme is based on the Wada index computed for each overlapping observation window in the perfect covering. That allows to exploit the concept of the Wada boundary in digital image steganography. The quantification of the uncertainty of the evolution of a dynamical system from the perturbed initial conditions helps to design a steganographic scheme robust to the steganalysis algorithms.

All computational experiments in this paper are performed at $s = 3$ (with nine shares). It is interesting to note that the proposed scheme degenerates into the LSB scheme at $s = 1$ (with no sharing of the carrier image). Therefore, the proposed scheme can be interpreted as the spatial extension of the LSB scheme with the distribution of the Wada uncertainty between the shares. Remarkably, such distribution of the uncertainty does not impact the first bit planes of the stego image. A higher number of shares (s^2 shares) can be used to completely dilute the uncertainty of modifications. However, it is shown that nine shares are completely sufficient to pass through the RS steganalysis.

The proposed steganographic scheme based on the Wada index ensures that the secret image is not leaked from the modified bit planes with lowest indexes, the stego image is robust against steganalysis algorithms, and the payload capacity of the carrier image is comparable to grayscale LSB schemes.

Declarations

- **Conflict of 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.
- **Data availability**
  The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

References

[1] Yoneyama, K.: Theory of continuous set of points (not finished). Tohoku Math. J., First Series **12**, 43–158 (1917)

[2] Kennedy, J., Yorke, J.A.: Basins of Wada. Physica D **51**, 213–225 (1991). https://doi.org/10.1016/0167-2789(91)90234-Z

[3] Osipov, A.V., Serow, D.W.: Fractional densities for the Wada basins. Nonl. Phen. Compl. Syst. **21**, 389–394 (2018)

[4] Zhang, Y.: Switching-induced Wada basin boundaries in the Henon map. Nonlinear Dyn. **73**, 2221–2229 (2013). https://doi.org/10.1007/s11071-013-0936-2

[5] Zhang, Y., Zhang, H., Gao, W.: Multiple Wada basins with common boundaries in nonlinear driven oscillators. Nonlinear Dyn. **79**, 2667–2674 (2015). https://doi.org/10.1007/s11071-014-1839-6

[6] Ziaukas, P., Ragulskis, M.: Fractal dimension and Wada measure revisited: no straightforward relationships in NDDS. Nonlinear Dyn. **88**, 871–882 (2017). https://doi.org/10.1007/s11071-016-3281-4

[7] Daza, A., Wagemakers, A., Georgeot, B., Guéry-Odelin, D., Sanjuán, M.A.F.: Basin entropy: a new tool to analyze uncertainty in dynamical systems. Sci. Rep. **6**, 3146 (2016). https://doi.org/10.1038/srep31416

[8] Wagemakers, A., Daza, A., Sanjuán, M.A.F.: How to detect Wada basins. Discrete Cont. Dyn.-B **26**(1), 717–739 (2021). https://doi.org/10.3934/dcdsb.2020330

[9] Saunoriene, L., Ragulskis, M., Cao, J., Sanjuán, M.A.F.: Wada index based on the weighted and truncated Shannon entropy. Nonlinear Dyn., 1–13 (2021). https://doi.org/10.1007/s11071-021-06261-1

[10] Lu, C.-S.: Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, p. 264. IGI Global, London (2004)

[11] Kadhim, I.J., Premaratne, P., Vial, P.J., Halloran, B.: Comprehensive survey of image steganography: Techniques, evaluations, and

trends in future research. Neurocomputing **335**, 299–326 (2019). https://doi.org/10.1016/j.neucom.2018.06.075

[12] Aini, D.N., Moses Setiadi, D.R.I., Putro, S.N., Rachmawanto, E.H., Sari, C.A.: Survey of methods in the spatial domain image steganography based imperceptibility and payload capacity. In: 2019 International Seminar on Application for Technology of Information and Communication (iSemantic), pp. 434–439 (2019). https://doi.org/10.1109/ISEMANTIC.2019.8884333

[13] Venkatraman, S., Abraham, A., Paprzycki, M.: Significance of steganography on data security. In: International Conference on Information Technology: Coding and Computing, 2004. Proceedings ITCC, vol. 2, pp. 347–351 (2004). https://doi.org/10.1109/ITCC.2004.1286660

[14] Shih, F.Y.: Digital Watermarking and Steganography: Fundamentals and Techniques, 2nd edn., p. 292. CRC Press, Boca Raton (2017)

[15] Alhomoud, A.M.: Image steganography in spatial domain: Current status, techniques, and trends. Intell. Autom. Soft Co. **27**(1), 69–88 (2021). https://doi.org/10.32604/iasc.2021.014773

[16] Neeta, D., Snehal, K., Jacobs, D.: Implementation of LSB steganography and its evaluation for various bits. In: 2006 1st International Conference on Digital Information Management, pp. 173–178 (2007). https://doi.org/10.1109/ICDIM.2007.369349

[17] Fridrich, J., Goljan, M., Du, R.: Detecting LSB steganography in color, and gray-scale images. IEEE Multimedia **8**, 22–28 (2001). https://doi.org/10.1109/93.959097

[18] Manoharan, S.: An empirical analysis of RS steganalysis. In: 2008 The Third International Conference on Internet Monitoring and Protection, pp. 172–177 (2008). https://doi.org/10.1109/ICIMP.2008.15

[19] Abdulla, A.A., Jassim, S.A., Sellahewa, H.: Secure steganography technique based on bitplane indexes. In: 2013 IEEE International Symposium on Multimedia, pp. 287–291 (2013). https://doi.org/10.1109/ISM.2013.55

[20] Abdulla, A.A., Sellahewa, H., Jassim, S.A.: Stego quality enhancement by message size reduction and Fibonacci bit-plane mapping. In: Chen, L., Mitchell, C. (eds.) Security Standardisation Research, pp. 151–166. Springer, Cham (2014)

[21] Swain, G.: Very high capacity image steganography technique using quotient value differencing and LSB substitution. Arab. J. Sci. Eng. **44**(4), 2995–3004 (2019). https://doi.org/10.1007/s13369-018-3372-2

[22] Wu, D.-C., Tsai, W.-H.: A steganographic method for images by pixel-value differencing. Pattern Recogn. Lett. **24**(9), 1613–1626 (2003). https://doi.org/10.1016/S0167-8655(02)00402-6

[23] Hussain, M., Wahab, A.W.A., Anuar, N.B., Salleh, R., Noor, R.M.: Pixel value differencing steganography techniques: Analysis and open challenge. In: 2015 IEEE International Conference on Consumer Electronics - Taiwan, pp. 21–22 (2015). https://doi.org/10.1109/ICCE-TW.2015.7216859

[24] Hussain, M., Wahab, A.W.A., Idris, Y.I.B., Ho, A.T.S., Jung, K.-H.: Image steganography in spatial domain: A survey. Process. Image Commun. **65**, 46–66 (2018). https://doi.org/10.1016/j.image.2018.03.012

[25] Tian, J.: Reversible data embedding using a difference expansion. IEEE Trans. Circ. Sys. Vid. **13**(8), 890–896 (2003). https://doi.org/10.1109/TCSVT.2003.815962

[26] Ahmad, T., Holil, M.: Increasing the performance of difference expansion-based steganography when securing medical data. The Smart Computing Review **4**, 307–322 (2014). https://doi.org/10.6029/smartcr.2014.04.007

[27] Nguyen, B.C., Yoon, S.M., Lee, H.-K.: Multi bit plane image steganography. In: Shi, Y.Q., Jeon, B. (eds.) Digital Watermarking, pp. 61–70. Springer, Berlin, Heidelberg (2006)

[28] Potdar, V.M., Chang, E.: Grey level modification steganography for secret communication. In: 2nd IEEE International Conference on Industrial Informatics, 2004. INDIN '04. 2004, pp. 223–228 (2004). https://doi.org/10.1109/INDIN.2004.1417333

[29] Safarpour, M., Charmi, M.: Capacity enlargement of the PVD steganography method using the GLM technique, vol. abs/1601.00299 (2016). http:

//arxiv.org/abs/1601.00299

[30] Zhang, X., Wang, S.: Efficient steganographic embedding by exploiting modification direction. IEEE Commun. Lett. **10**(11), 781–783 (2006). https://doi.org/10.1109/LCOMM.2006.060863

[31] Lin, K.Y., Hong, W., Chen, J., Chen, T.S., Chiang, W.C.: Data hiding by exploiting modification direction technique using optimal pixel grouping. In: 2010 2nd International Conference on Education Technology and Computer, vol. 3, pp. 3–1213123 (2010). https://doi.org/10.1109/ICETC.2010.5529581

[32] Pradhan, A., Sahu, A.K., Swain, G., Sekhar, K.R.: Performance evaluation parameters of image steganography techniques. In: 2016 International Conference on Research Advances in Integrated Navigation Systems (RAINS), pp. 1–8 (2016). https://doi.org/10.1109/RAINS.2016.7764399

[33] Gou, H., Swaminathan, A., Wu, M.: Noise features for image tampering detection and steganalysis. In: 2007 IEEE International Conference on Image Processing, vol. 6, pp. 97–100 (2007). https://doi.org/10.1109/ICIP.2007.4379530

[34] Luo, W., Huang, F., Huang, J.: Edge adaptive image steganography based on LSB matching revisited. IEEE T. Inf. Foren. Sec. **5**(2), 201–214 (2010). https://doi.org/10.1109/TIFS.2010.2041812

[35] Khalind, O., Aziz, B.: A better detection of 2LSB steganography via standard deviation of the extended pairs of values. In: Agaian, S.S., Jassim, S.A., Du, E.Y. (eds.) Mobile Multimedia/Image Processing, Security, and Applications 2015, vol. 9497, pp. 135–142 (2015). https://doi.org/10.1117/12.2184496

[36] Agaian, S.S., Cherukuri, R.C., Sifuentes, R.: A new secure adaptive steganographic algorithm using fibonacci numbers. In: 2006 IEEE Region 5 Conference, pp. 125–129 (2006). https://doi.org/10.1109/TPSD.2006.5507446

[37] De Luca Picione, D., Battisti, F., Carli, M., Astola, J., Egiazarian, K.: A Fibonacci LSB data hiding tecnique. In: 2006 14th European Signal Processing Conference, pp. 1–5 (2006)

[38] Liao, X., Yin, J., Chen, M., Qin, Z.: Adaptive payload distribution in multiple images steganography based on image texture features. IEEE T. Depend. Secure **19**(2), 897–911 (2022). https://doi.org/10.1109/TDSC.2020.3004708

[39] Khan, S., Ahmad, N., Ismail, M., Minallah, N., Khan, T.: A secure true edge based 4 least significant bits steganography. In: 2015 International Conference on Emerging Technologies (ICET), pp. 1–4 (2015). https://doi.org/10.1109/ICET.2015.7389227

[40] Khan, S., Naeem, M., Khan, T., Ahmad, N.: 4LSB based data hiding in complex region of digital images and its effects on edges and histogram. J. Eng. Appl. Sci. **36**, 67–75 (2017). https://doi.org/10.25211/jeas.v36i1.144

[41] Abdulla, A.A.: Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. PhD thesis, University of Buckingham (2015)

[42] Moses Setiadi, D.R.I.: PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimed Tools Appl. **80**, 1–22 (2021). https://doi.org/10.1007/s11042-020-10035-z

[43] Hosam, O.: Attacking image watermarking and steganography – a survey. Int. J. Inf. Comp. Sci. **11**, 23–37 (2019). https://doi.org/10.5815/ijitcs.2019.03.03

[44] Liao, X., Li, K., Zhu, X., Liu, K.J.R.: Robust detection of image operator chain with two-stream convolutional neural network. IEEE J. Sel. Top. Signa. **14**(5), 955–968 (2020). https://doi.org/10.1109/JSTSP.2020.3002391

[45] Liao, X., Yu, Y., Li, B., Li, Z., Qin, Z.: A new payload partition strategy in color image steganography. IEEE T. Circ. Syst. Vid. **30**(3), 685–696 (2020). https://doi.org/10.1109/TCSVT.2019.2896270

[46] Sahu, A.K., Sahu, M.: Digital image steganography and steganalysis: A journey of the past three decades. Open Computer Science **10**(1), 296–342 (2020). https://doi.org/10.1515/comp-2020-0136

[47] Ratan, R., Yadav, A.: Security analysis of bit plane level image encryption schemes. Defence Sci. J. **71**(2), 209–221 (2021). https://doi.org/10.14429/dsj.71.15643

[48] Wayner, P.: Chapter 17 - Steganalysis.

In: Wayner, P. (ed.) Disappearing Cryptography, 3rd edn. The Morgan Kaufmann Series in Software Engineering and Programming, pp. 337–353. Morgan Kaufmann, Boston (2009). https://doi.org/10.1016/B978-012374479-1.50022-8