

A Steganographic Scheme Based on Perfect Coverings of Dichotomous Shares with Sparse Observation Windows

Loreta SAUNORIENE¹, Jurate RAGULSKIENE¹, Marius SAUNORIS²,
Minvydas RAGULSKIS^{1,*}

¹ Kaunas University of Technology, Department of Mathematical Modelling,
Studentu st. 50-146, 51368 Kaunas, Lithuania

² Kaunas University of Technology, Department of Electronics Engineering,
Studentu st. 50-443, 51368 Kaunas, Lithuania

e-mail: loreta.saunoriene@ktu.lt, jurate.ragulskiene@ktu.lt, marius.saunoris@ktu.lt,
minvydas.ragulskis@ktu.lt

Received: April 2025; accepted: October 2025

Abstract. A steganographic scheme based on perfect coverings of dichotomous shares with sparse observation windows is presented in this paper. The manipulations with pixels are based on the number of different colours in the sparse cells of the current observation window. The conditions for the existence of perfect coverings for different architectures of sparse observation windows are derived. The number and distribution of active cells in the current observation window contribute to the additional security of the proposed scheme. This paper also provides performance measures, statistical features, and demonstrates the robustness of the proposed steganographic scheme.

Key words: steganography, perfect covering, sparse observation window.

1. Introduction

Image steganography is the science and art of hiding secret information within an image using various methods and techniques (Kaur *et al.*, 2022; Setiadi *et al.*, 2023). Image steganography ensures that hidden data remain invisible to the human eye, allowing safe communication and data storage (Rahman *et al.*, 2023a).

Least significant bit (LSB) substitution is one of the most well-known techniques in spatial domain steganography. In LSB, the least significant bit of each pixel in the carrier image is modified to embed one bit of the dichotomous secret message (Kurak and McHugh, 1992). These adjustments are almost imperceptible to the human eye. However, traditional bit plane analysis can easily uncover the hidden secret information (Wayner, 2009; Sahu and Sahu, 2020). In recent decades, various improvements of LSB steganography have been introduced making the detection of the concealed data more challenging.

*Corresponding author.

For example, two least significant bit (2LSB) technique enhances the conventional LSB method by embedding two bits of secret information into the last two bit planes of the carrier image (Khalind and Aziz, 2015). In the random 2LSB technique, a single secret bit is inserted randomly into either the first or the second bit plane. Different manipulations with the indices of the bit planes are used to enhance the existing LSB techniques (Abdulla et al., 2013; Al-Faydi et al., 2023; Njoum et al., 2024).

Multiple Bit Planes Based (MBPB) steganography extends LSB methods by employing the bit planes with greater complexity for embedding secret data (Nguyen et al., 2006). LSB Matching technique (LSB-M) is a variation of LSB substitution, which adds or subtracts 1 from the pixel value instead of directly replacing the least significant bit (Luo et al., 2010) what makes LSB-M technique more resistant to steganalysis than the standard LSB technique. Pixel Value Differencing (PVD) hides information by modifying the difference between two neighbouring pixel values (Hussain et al., 2015). Larger differences allow more bits to be hidden, while smaller differences allow fewer bits.

The main challenges in image steganography include achieving a high embedding capacity and ensuring a high level of security (Aini et al., 2019; Zhang et al., 2019; Li et al., 2024; Liu et al., 2024). The security of a steganographic scheme largely depends on the effectiveness of its embedding strategy and is based on two key factors: imperceptibility, meaning the hidden data remains undetectable within the medium, and confidentiality, ensuring that only the intended recipient can detect and extract the concealed information (Ghoul et al., 2023; Mukherjee and Paul, 2024). Together, these factors protect the hidden content from unauthorized detection and access (Luo et al., 2023; Sreenidhi et al., 2024).

The integration of adaptive embedding techniques, cryptography, and chaotic systems into the steganographic schemes can significantly enhance the security of the hidden information (Haverkamp and Sarmah, 2024; Mukherjee and Paul, 2024; Xing et al., 2022). For example, embedding the secret information in the sparse representation of the carrier image, in the edge or noisy areas conceals data where it is least noticeable, reducing the risk of detection (Nipanikar et al., 2018; Rashid and Majeed, 2019; Setiadi et al., 2024; George et al., 2024). Encrypting the hidden data before embedding ensures that the message remains unreadable, even if detected (Rahman et al., 2023b; Rajabi-Ghaleh et al., 2024; Haverkamp and Sarmah, 2024). Incorporating randomization and perturbations generated by different chaotic systems into steganographic schemes helps to hide the message in a way that makes it difficult to detect (Laimeche et al., 2020; EL-Hady et al., 2024; Aziz et al., 2015).

An alternative approach to the development of steganographic schemes is proposed in Saunoriene and Ragulskis (2023) where the concept of the Wada index is used to extend the classical LSB technique. In this scheme, the grayscale carrier image is covered by overlapping square windows of a specified size. The process of hiding secret information relies on manipulating the number of distinct grayscale levels within these overlapping windows (Saunoriene and Ragulskis, 2023). This scheme ensures that the bit planes of the resulting stego image do not reveal the hidden message. Furthermore, the stego image is resistant to steganalysis algorithms, and its payload capacity is comparable to that of grayscale LSB techniques (Saunoriene and Ragulskis, 2023).

However, according to the “no-free-lunch” theorems (Wolpert and Macready, 1997; Wolpert, 2013), every algorithm has its drawbacks. A possible drawback of the steganographic scheme based on the Wada index is a rather simple decoding process. One needs to use an observation window (the size of the window must be predefined) and count the number of different colours in that window (of course, one needs to know that the number of different colours must be counted).

The primary objective of this paper is to introduce the concept of a sparse observation window into the steganographic scheme based on the Wada index. Sparse observation windows with randomly distributed active cells could seriously increase the confidentiality of the scheme (the distribution of active cells would serve as an additional secret key for the proposed scheme).

However, the decoding algorithm of the steganographic scheme based on the Wada index is rather simple because it is based on the computation of the number of different colours in the current observation window. The main contribution of this paper is the introduction of sparse observation windows. A straightforward computation of the number of different colours in the current observation window becomes insufficient for decoding the secret. This paper also answers a number of other important questions about the existence of perfect coverings, the structure of dichotomous shares, and the robustness of the proposed scheme to different attacks.

The paper is structured as follows. Preliminaries on the steganographic scheme based on the Wada index are given in Section 2. Rectangular observation windows are discussed in Section 3. Sparse observation windows are introduced in Section 4. The security of the proposed steganographic scheme is investigated in Section 5. The robustness of the proposed scheme is presented in Section 6. Concluding remarks are given in the final section.

2. Preliminaries and Motivation

The steganographic scheme based on the Wada index is introduced in Saunoriene and Ragulskis (2023). The secret dichotomous image S is embedded into the grayscale carrier image C producing the grayscale stego image T . The size of the carrier and the stego images (measured in pixels) is $n_x \times n_y$; the size of the rectangular observation window is $r_x \times r_y$; the size of the secret image S is $(n_x - r_x + 1) \times (n_y - r_y + 1)$. The carrier image C is split into $r_x \cdot r_y$ dichotomous shares $H_k, k = 1, 2, \dots, r_x \cdot r_y$. The size of H_k is $(n_x - r_x + 1) \times (n_y - r_y + 1)$.

2.1. The Decoding Scheme

The schematic description of the standard steganographic scheme based on the Wada index is presented in Fig. 1. Let us consider $n_x = 3; n_y = 4; r_x = r_y = 2$ (Fig. 1). The decoding process of the standard scheme is based on the number of different colours (different grayscale levels) of pixels in the current observation window. The stego image T is covered by overlapping observation windows resulting into the size of the dichotomous

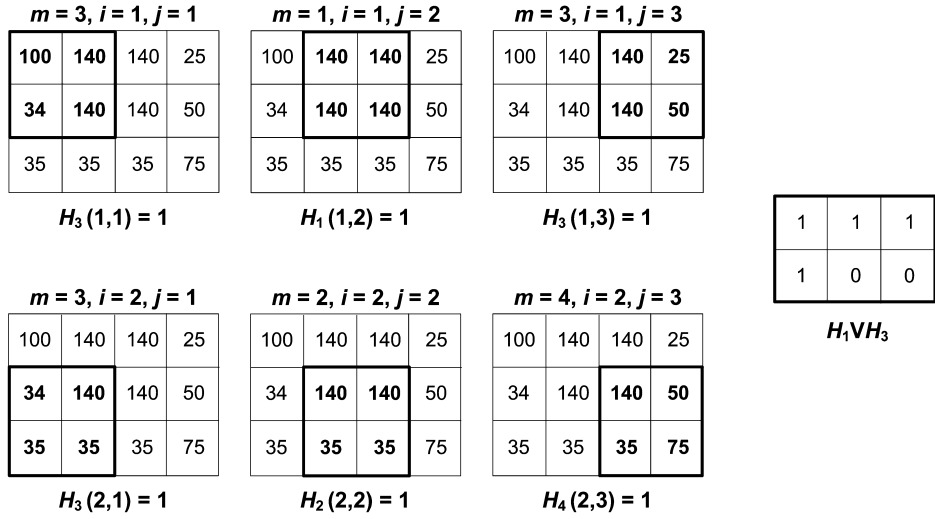


Fig. 1. The decoding process of the standard steganographic scheme based on the Wada index. The size of the stego image is 3×4 pixels, and the size of the observation window is 2×2 cells. The size of the secret image is 2×3 pixels which corresponds to all possible different locations of the observation window. The parameter m shows the number of different colours in the current observation window; i and j depict the coordinates of the current observation window; $H_k, k = 1, \dots, 4$ are dichotomous shares (the number of shares is predefined by the size of the observation window). The disjunction of shares with odd indexes leaks the secret.

secret S equal to 2×3 pixels (Fig. 1). The size of the observation window results into 4 dichotomous shares $H_k, k = 1, \dots, 4$ (the size of all shares is 2×3 pixels). All cells of all shares H_k are set to zero at the beginning of the decoding process.

The number of different colours in the observation window located at the top left corner of the stego image T is $m = 3$ (Fig. 1). The coordinates of this observation window are $i = 1$ and $j = 1$ (Fig. 1). Since the number of different colours in this observation window is $m = 3$, the third share H_3 is modified. The cell of H_3 located at the local coordinates $i = 1$ and $j = 1$ is flipped from zero to one (Fig. 1). The process is continued until the observation window reaches the bottom left corner of the stego image T ($i = 2; j = 3$). Finally, the disjunction of shares with odd indexes leaks the dichotomous secret S (Fig. 1).

The decoding scheme of the secret image S is represented as the disjunction of shares with odd indexes:

$$T^{n_x \times n_y} \rightarrow \bigvee_{k=1}^{\lfloor \frac{r_x \cdot r_y}{2} \rfloor} H_{2k-1}^{(n_x - r_x + 1) \times (n_y - r_y + 1)} = S^{(n_x - r_x + 1) \times (n_y - r_y + 1)}, \quad (1)$$

where $\lfloor \cdot \rfloor$ denotes the rounding operation.

2.2. The Encoding Scheme

Such a straightforward decoding scheme defines the structure of the encoding algorithm. Let us consider the current 2×2 observation window resulting into $m = 3$ different colours

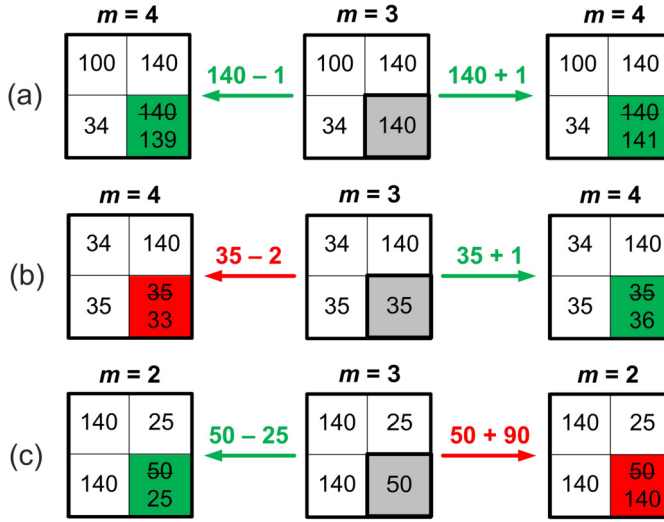


Fig. 2. A schematic diagram illustrating how the number of different colours in the current observation window can be changed. The size of the observation window is 2×2 cells; the modifications are allowed only in the bottom right cell. Panel (a) depicts a situation when the number of different colours $m = 3$ is increased to 4 (note that it is impossible to decrease m to 2). The number 140 can be decreased by 1 or increased by 1. Both options result into a minimal modification equal to 1. Panel (b) also illustrates the increase of $m = 3$ to 4. However, it is not possible to decrease 35 by 1 (that would result into $m = 3$). The minimal modification is possible only by adding 1 to 35. Panel (c) shows the situation when $m = 3$ is decreased to 2 (note that it is impossible to increase $m = 3$ to 4). The minimal modification is executed by $50 - 25 = 25$.

(Fig. 2). Let us assume that the coordinates of the current observation window are i, j . No modifications are required in the current observation window if $S(i, j) = 1$ because $H_3(i, j) = 1$ and the disjunction of shares with odd indexes will result into 1. However, modifications are required in the current observation window if $S(i, j) = 0$. Then, the number of different colours in the current observation window should be changed to $m = 2$ or $m = 4$ (Fig. 2).

Let us assume that the modifications in the current observation window are allowed only in the bottom right cell (marked in gray in Fig. 2). Figure 2(a) depicts a situation when m cannot be decreased to 2 (the modifications are allowed only in the bottom right cell). The number 140 can be decreased by 1 or increased by 1. Both options result into a minimal modification equal to 1.

Figure 2(b) also illustrates a situation when m can be only increased to 4. However, it is not possible to decrease 35 by 1 (that would result into $m = 3$). The minimal modification is possible only by adding 1 to 35.

Finally, Fig. 2(c) illustrates the situation when $m = 3$ is decreased to 2 (note that it is impossible to increase $m = 3$ to 4). The minimal modification is executed by $50 - 25 = 25$.

2.3. The Concept of the Perfect Covering

Without loss of generality, consider a carrier image C of size 5×5 (Fig. 3(a)). The 2×2 observation window is used to encode the 4×4 secret image S into the carrier image C

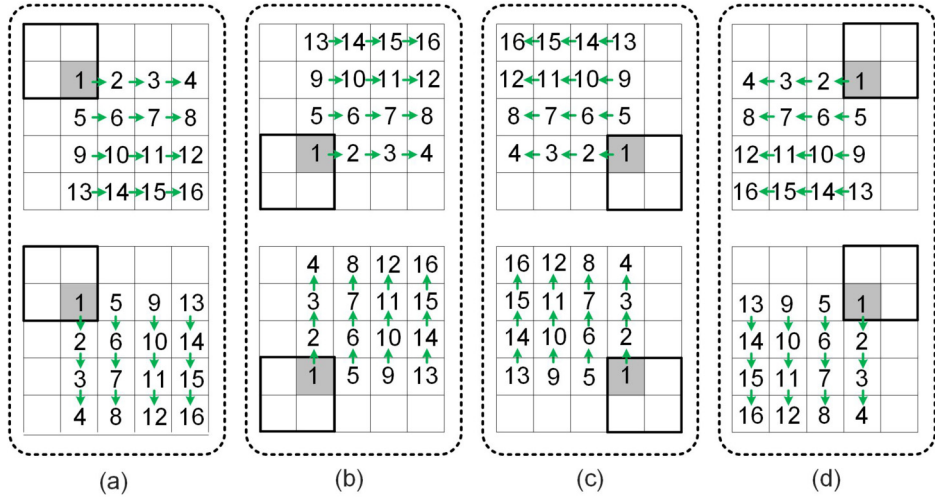


Fig. 3. The construction of the perfect covering scheme requires three different definitions. The first is the size and the initial position of the observation window (the 2×2 highlighted rectangle). The second is the location of the cell where the modifications are allowed inside the current observation window (marked as a gray-shaded cell in the initial observation window). Finally, the covering strategy must be defined (marked by green arrows). The perfect covering ensures that the change in the current observation window does not cause any changes in all previous observation windows (in terms of the number of different colours). Different perfect coverings are depicted in panels (a), (b), (c), and (d).

(Fig. 3). Let us assume that the observation window (depicted by the highlighted rectangle) is initially placed at the top left corner of the carrier image.

The number of different colours in the current observation window can be changed (if required) by modifying the value in the cell positioned at the bottom right corner of the observation window (the modifying cell is marked in gray in Fig. 3). The local coordinates of the modifying cell are (2, 2). When the first modification is made (indicated by “1”), the observation window travels by one pixel to the right. Green arrows indicate the travel direction of the current observation window and the numbers mark the sequential order of modifications. After each modification, the observation window travels by one pixel to the right until it reaches the right edge of the carrier image. Then the observation window travels by one pixel downwards, and the process is repeated from the left edge of the carrier image. The process continues until the observation window reaches the bottom right corner of the carrier image.

Such a covering scheme is a perfect covering scheme, as the changes in the current observation window do not change the number of different colours in any previous observation windows (Saunoriene and Ragulskis, 2023). This covering scheme is denoted as the perfect covering scheme $\mathcal{P}_{2 \times 2}^{(2,2)}$ (the numbers in the subscript denote the size of the observation window; the numbers in the superscript denote the local coordinates of the modifying cell).

Note that the perfect covering scheme $\mathcal{P}_{2 \times 2}^{(2,2)}$ can be executed by moving the observation windows horizontally or vertically over the carrier image C (Fig. 3(a)). However,

both vertical and horizontal encodings result in the same stego image T (Saunoriene and Ragulskis, 2023).

2.4. The Motivation of this Paper

The existing steganographic scheme based on the Wada index (Saunoriene and Ragulskis, 2023) possesses a number of advantageous features. The statistical performance measures of the steganographic scheme based on the Wada index are comparable with the performance measures of the best LSB-type schemes (Saunoriene and Ragulskis, 2023). The payload capacity of the carrier image is also comparable to grayscale LSB schemes (Saunoriene and Ragulskis, 2023). The secret information is encoded into the different bit planes which guarantees that the secret image is not revealed from the bit planes with lower indexes (Saunoriene and Ragulskis, 2023). Moreover, the proposed scheme is robust to the steganalysis algorithms (Saunoriene and Ragulskis, 2023).

The well-known “no-free-lunch” theorems (Wolpert and Macready, 1997; Wolpert, 2013) imply that every algorithm has some drawbacks in specific conditions and situations. One of the potential drawbacks of the steganographic scheme based on the Wada index (Saunoriene and Ragulskis, 2023) is a rather simple decoding scheme. It is sufficient to compute the number of different colours in the current observation window (applied to the carrier image C) to identify the current pixel in the secret image S (of course, the eavesdropper would need to know the size of the observation window, and that the number of different colours must be counted).

The motivation of this paper is to propose a very different approach to the structure of the observation window. It is not necessary to count the number of different colours in all cells of the current observation window. The number (and the distribution) of active cells inside the current observation window could be a parameter contributing to the additional security of the steganographic scheme. Of course, such modifications of the observation window raise many important questions about the existence of the perfect covering scheme, about the applicable patterns of the distribution of active cells in the observation window, about the statistical features of such a steganographic scheme. Seeking answers to those questions is the main objective of this paper.

3. Rectangular Observation Windows

As defined previously, $\mathcal{P}_{2 \times 2}^{(2,2)}$ is a 2×2 perfect covering scheme with the modifying cell located at the local coordinates $(2, 2)$.

What happens if the observation window is initially placed at any other corner of the carrier image, not necessarily at the top left corner (Fig. 3(b)–(d))?

Positioning the observation window at the left-bottom corner of the carrier image can also result in a perfect covering (Fig. 3(b)) if the coordinates of the modifying cell are set to $(1, 2)$ and the travel direction is set from left to right (horizontal perfect covering) or from bottom to top (vertical perfect covering) as illustrated in Fig. 3(b). Such a covering scheme is denoted as $\mathcal{P}_{2 \times 2}^{(1,2)}$.

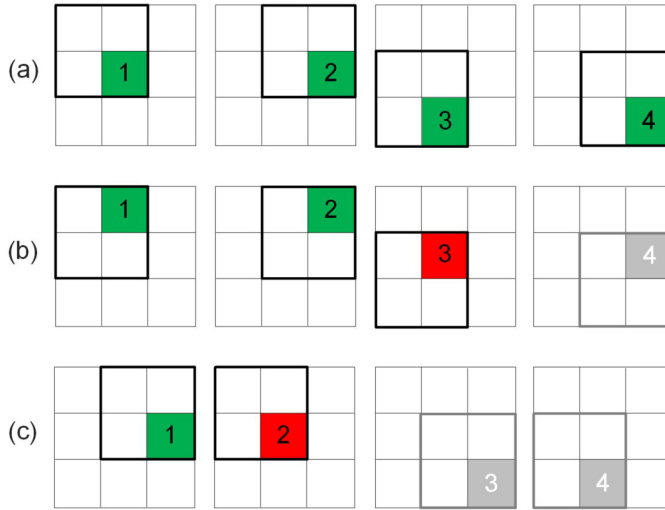


Fig. 4. The initial position of the observation window, the location of the modifying cell, and the covering strategy must be properly organized to yield a perfect covering. Panel (a) shows a perfect covering where the initial observation window is placed at the top left corner of the carrier image, the modifying cell is at the bottom right corner, and the covering strategy is horizontal (Fig. 3(a)). Panel (b) depicts a conflict in step 3 (the initial observation window is placed at the top left corner of the carrier image, the modifying cell is at the top right corner, and the covering strategy is horizontal (Fig. 3(a))). Panel (c) shows a conflict already in step 2 (the initial observation window is placed at the top right corner of the carrier image, the modifying cell is at the bottom right corner, and the covering strategy is horizontal (Fig. 3(d))).

Similarly, a perfect covering can be constructed by setting the initial position of the observation window at the bottom right corner of the carrier image and placing the modifying cell at local coordinates (1, 1) (Fig. 3(c)). Such a covering scheme is denoted as $\mathcal{P}_{2 \times 2}^{(1,1)}$.

Finally, placing the observation window at the top right corner of the carrier image and the modifying cell at local coordinates (2, 1) also results in a perfect covering (Fig. 3(d)). Such a covering scheme is denoted as $\mathcal{P}_{2 \times 2}^{(2,1)}$.

Note that the horizontal and vertical perfect covering schemes depicted in Fig. 3(b) result in identical stego images (Saunoriene and Ragulskis, 2023). The same holds true for the horizontal and vertical perfect coverings depicted in panels (c)–(d). However, we will show that schemes $\mathcal{P}_{2 \times 2}^{(2,2)}$, $\mathcal{P}_{2 \times 2}^{(2,1)}$, $\mathcal{P}_{2 \times 2}^{(1,2)}$, and $\mathcal{P}_{2 \times 2}^{(1,1)}$ do produce different stego images.

One should be careful with the selection of the horizontal and vertical travel directions for each particular perfect covering scheme. For example, a straightforward application of the horizontal left-to-right strategy may fail if the local coordinates of the modifying cell are not properly defined (Fig. 4). Figure 4(a) illustrates the perfect scheme $\mathcal{P}_{2 \times 2}^{(2,2)}$ (the size of the carrier image is 3×3).

However, $\mathcal{P}_{2 \times 2}^{(1,2)}$ is not a perfect covering scheme for the same left-to-right travel strategy (the first conflict occurs at the third step depicted in red in Fig. 4(b)). Analogously, $\mathcal{P}_{2 \times 2}^{(2,2)}$ is not a perfect scheme if the horizontal right-to-left strategy is used (the first conflict is generated at the second step marked in red in Fig. 4(c)).

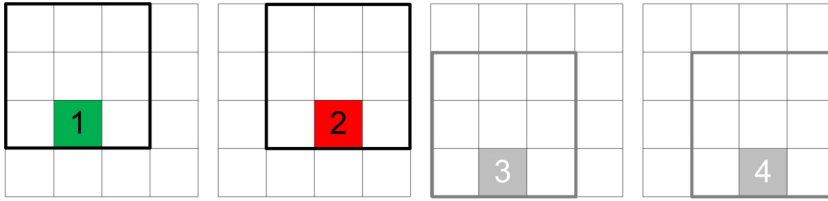


Fig. 5. The modifying cell must be located at one of the corners of the rectangular observation window. Otherwise, any combination of the initial position of the observation window and the covering strategy will result into conflicts. The conflict occurs in step 2 when the initial observation window is placed at the top left corner of the carrier image, the modifying cell is the bottom middle cell of the 3×3 observation window, and the covering strategy is horizontal (Fig. 3(a)).

So far, only 2×2 observation windows have been discussed. It appears that the modifying cells should be placed only in the corners of the rectangular observation window (this condition is automatically fulfilled for 2×2 observation windows). For example, both left-to-right and right-to-left travel strategies fail for the $\mathcal{P}_{3 \times 3}^{(3,2)}$ scheme (Fig. 5). The same holds true for the vertical bottom-to-top and top-to-bottom travel strategies. In other words, $\mathcal{P}_{3 \times 3}^{(3,2)}$ is not a perfect covering scheme.

Let us consider a secret dichotomous city-map image (510×510 pixels) shown in Fig. 6. The city-map image is encoded into the grayscale Lena carrier image (512×512 pixels). The size of the observation window used for the encoding is fixed to 3×3 pixels. Four different perfect covering schemes $\mathcal{P}_{3 \times 3}^{(3,3)}$, $\mathcal{P}_{3 \times 3}^{(1,3)}$, $\mathcal{P}_{3 \times 3}^{(1,1)}$, $\mathcal{P}_{3 \times 3}^{(3,1)}$ (Fig. 3(a)–(d)) are used to encode the secret city-map image into the carrier Lena image.

It is interesting to observe that four perfect covering schemes yield four different stego images (the middle row in Fig. 6). Although no differences can be noticed by a naked eye, the modifications in the carrier image made during the encoding of the secret image into the carrier image are different (the bottom row in Fig. 6).

The statistical measures such as the range of the performed changes, the mean error (ME), the mean absolute error (MAE), the mean square error (MSE), the peak-signal-to-noise ratio (PSNR), the structural similarity index (SSIM) describe the difference between the original carrier and stego images and help to evaluate the performance of the employed steganographic scheme. The values of these performance measures are presented in Table 1 for each perfect covering scheme $\mathcal{P}_{3 \times 3}^{(3,3)}$, $\mathcal{P}_{3 \times 3}^{(1,3)}$, $\mathcal{P}_{3 \times 3}^{(1,1)}$, and $\mathcal{P}_{3 \times 3}^{(3,1)}$. However, neither of the four coverings significantly outperforms the other.

Therefore, changing the position of the modifying cell does not significantly increase the effectiveness of the encoding strategy (Table 1). Also, it is important to observe that the decoding of the secret information from the stego image does not depend on a particular encoding scheme $\mathcal{P}_{3 \times 3}^{(3,3)}$, $\mathcal{P}_{3 \times 3}^{(1,3)}$, $\mathcal{P}_{3 \times 3}^{(1,1)}$, or $\mathcal{P}_{3 \times 3}^{(3,1)}$. The decoding process requires to cover the stego image by overlapping observation windows in any order (and evaluate the number of different colours in each observation window). Therefore, the individual selection of a scheme ($\mathcal{P}_{3 \times 3}^{(3,3)}$, $\mathcal{P}_{3 \times 3}^{(1,3)}$, $\mathcal{P}_{3 \times 3}^{(1,1)}$, or $\mathcal{P}_{3 \times 3}^{(3,1)}$) has no impact on the safety of the decoding scheme.

So far, the 2×2 and 3×3 observation windows have been used in the perfect covering schemes. A natural question is whether better performance measures could be achieved

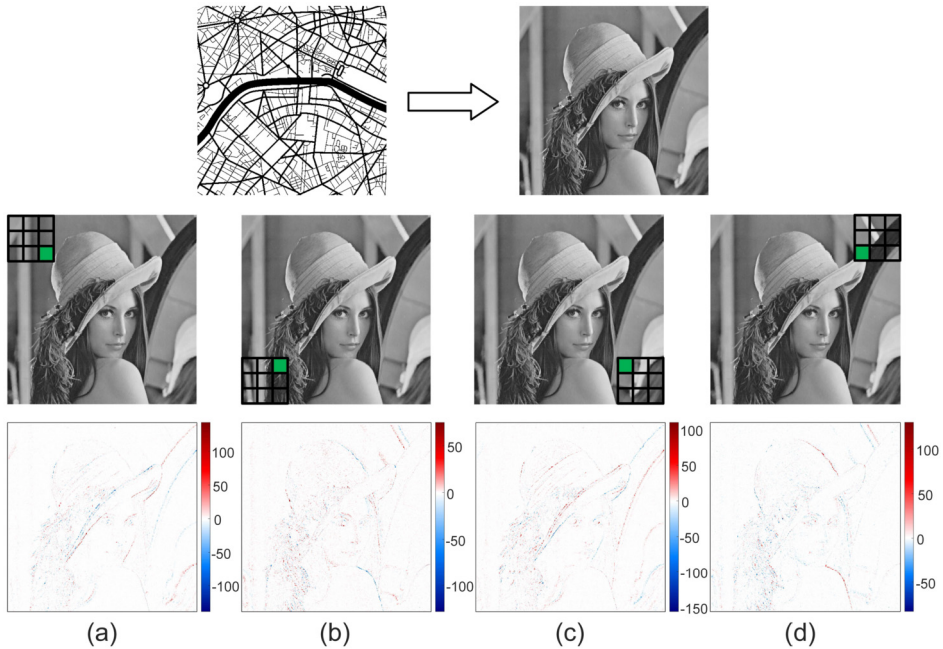


Fig. 6. The secret dichotomous city-map image (510×510) is encoded into the grayscale Lena carrier image (512×512) employing four different perfect coverings in Fig. 3. The initial position of the 3×3 observation window is shown (out of scale) on top of the Lena image (the modifying cell is marked in green). Stego images produced by four different perfect coverings are depicted in panels (a), (b), (c), and (d) accordingly. The images in the bottom row of panels (a)–(d) illustrate the magnitude of the performed modifications.

Table 1
Performance measures of the encoding algorithm for different perfect covering schemes.

Performance measure	$\mathcal{P}_{3 \times 3}^{(3,3)}$	$\mathcal{P}_{3 \times 3}^{(1,3)}$	$\mathcal{P}_{3 \times 3}^{(1,1)}$	$\mathcal{P}_{3 \times 3}^{(3,1)}$
Range	$[-139; 143]$	$[-128; 75]$	$[-156; 110]$	$[-83; 130]$
ME	-0.0428	-0.0706	-0.0478	-0.0085
MAE	1.5710	1.3077	1.5204	1.2987
MSE	20.9018	13.7056	21.4416	13.4223
PSNR	34.9290	36.7618	34.8182	36.8526
SSIM	0.9692	0.9758	0.9689	0.9760

when the size of the observation window is increased. Unfortunately, the results shown in Fig. 7 do not indicate such an improvement. Computational experiments are continued with the secret dichotomous city-map image encoded into the grayscale Lena image using the perfect covering scheme $\mathcal{P}_{r \times r}^{(r,r)}$. The range of changes is not significantly decreased at $r = 20$ (Fig. 7). The minimum ME is reached at $r = 2$, the minimum of MAE and MSE – at $r = 4$. The maximum values of SSIM and PSNR are achieved at $r = 4$.

Therefore, larger rectangular observation windows do not help to achieve better performance features and a higher security of the decoding scheme. Another approach is required to achieve these purposes.

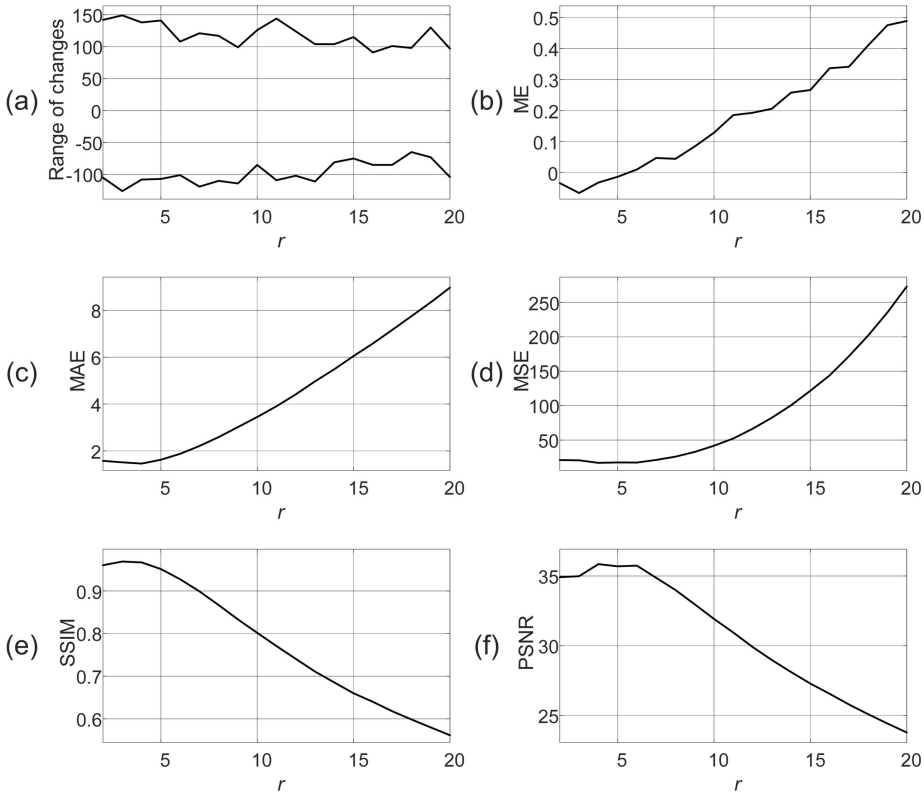


Fig. 7. Performance measures of the standard steganographic scheme based on the Wada index for different sizes of the observation window. The secret dichotomous city-map image is encoded into the grayscale Lena image using the perfect covering scheme depicted in Fig. 6(a). The size of the square observation window is set to $r = r_x = r_y$.

4. Sparse Observation Windows

Up to now, rectangular observation windows have been used to count the number of different colours and to perform necessary modifications in the carrier image at the modifying cell located at one of the corners of this rectangle.

Let us introduce the concept of an active and a passive cell inside the observation window. Active cells are used to compute the number of different colours in the current observation window (passive cells are not used for counting). Also, the modifying cell must be one of the active cells (otherwise the number of different colours measured at the locations of the active cells of the current observation window would not change).

An observation window with at least one passive cell is defined as a rectangular sparse observation window (SOW). The notion of SOW is represented by the size of the rectangular observation window and the location of the modifying cell (the active cells are plotted in white, and the passive cells are shown in gray). For example, the SOW shown in Fig. 8(a) is denoted as $\tilde{\mathcal{P}}_{3 \times 6}^{(3,6)}$ and two active cells are located at the top left and bottom right corners of the rectangular window.

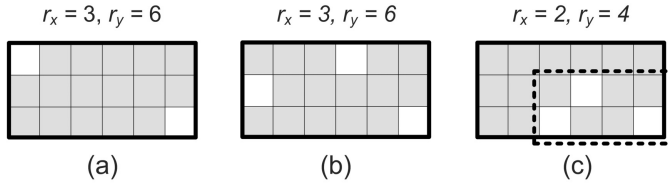


Fig. 8. The effective size of the rectangular sparse observation window is predetermined by the location of active cells. The size of the rectangular SOW is 3×6 in panels (a) and (b). However, the effective size of the observation window is only 2×4 in panel (c). Note that the effective size of the rectangular SOW does not depend on the type of the perfect covering scheme.

Note that such a definition of SOW requires a proper placement of active cells inside the observation window. It is assumed that the size of the rectangular window of SOW is minimal (effective) to accommodate all active cells. For example, the effective size of SOW in Fig. 8(c) is 2×4 , not 3×6 .

4.1. The Definition of a Perfect SOW

The concept of a perfect covering scheme is presented in Saunoriene and Ragulskis (2023) and is also used in this paper. However, it appears that special care must be taken for the selection of the modifying cell in SOW (otherwise the SOW may not produce a perfect covering).

Let us consider $\tilde{\mathcal{P}}_{3 \times 6}^{(3,6)}$ shown in Fig. 9(a) (the modifying cell is plotted in green). It is clear that this SOW results into a perfect covering if the scheme depicted in Fig. 3(a) is used.

It appears that the modifying cell can be located not only in the corners of the rectangular observation window. In fact, $\tilde{\mathcal{P}}_{3 \times 6}^{(3,4)}$ (Fig. 9(b)) and $\tilde{\mathcal{P}}_{3 \times 6}^{(3,1)}$ (Fig. 9(c)) also result into perfect covering schemes.

However, the placement of the modifying cell cannot be arbitrary. For example, $\tilde{\mathcal{P}}_{3 \times 6}^{(3,4)}$ (Fig. 9(d)), $\tilde{\mathcal{P}}_{3 \times 6}^{(2,6)}$ (Fig. 9(e)), and $\tilde{\mathcal{P}}_{3 \times 6}^{(2,3)}$ (Fig. 9(f)) are not perfect covering schemes if the horizontal scheme depicted in Fig. 3(a) is used (the modifying cell is marked in red).

Figure 10 is used to demonstrate that SOW $\tilde{\mathcal{P}}_{3 \times 6}^{(2,6)}$ does not result into a perfect covering when the scheme in Fig. 3(a) is used. The size of the carrier image is set to 5×8 pixels (Fig. 10). Initially, the SOW is placed at the top left corner of the carrier image (the global coordinates of the top left cell of the current SOW are (1, 1)). The SOW then travels horizontally from left to right until the top left corner of the SOW reaches pixel (1, 3) of the carrier image (Fig. 10). Note that no conflict with previous observation windows is generated at steps 1, 2, and 3 (the modifying cell is shown in green). However, a conflict occurs at step 4 (Fig. 10). The global coordinates of the modifying cell at this step are (3, 6). However, this cell is an active cell of the SOW at step 3. Changing the value of the modifying cell at step 4 can change the number of different colours measured by the SOW at previous step 3. Thus, the conflict with the previous SOW appears at step 4 and the modifying cell is now plotted in red.

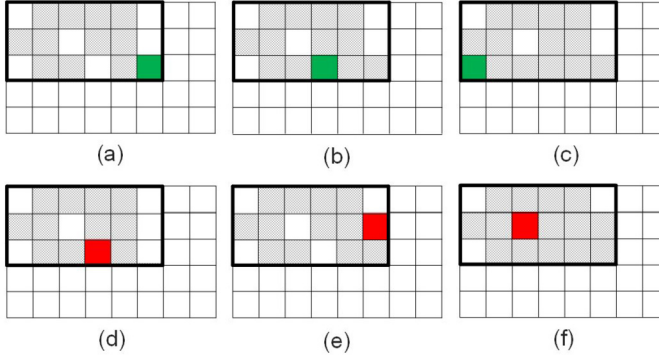


Fig. 9. Perfect SOW yields the perfect covering. The architecture of a perfect SOW depends on the type of the covering scheme (the covering scheme depicted in Fig. 6(a) is used for further illustrations). Active cells are not allowed in rows below the modifying cell and on the right hand side of the current row. Panels (a), (b) and (c) depict perfect SOW (the modifying cell is plotted in green). Panels (d), (e) and (f) show non-perfect SOWs (the modifying cell is plotted in red).

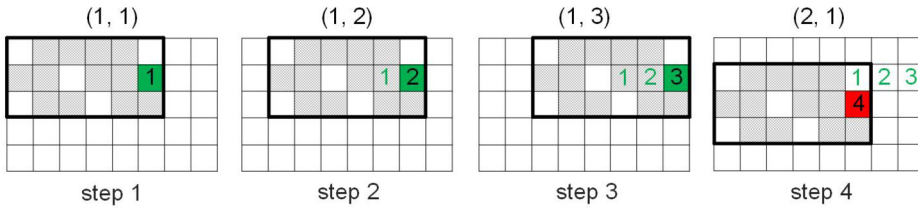


Fig. 10. The SOW shown in Fig. 9 (e) causes a conflict using the covering scheme depicted in Fig. 3(a). Initially, the SOW is placed at the top left corner of the carrier image (coordinates at the top left SOW cell are (1, 1), the coordinates of the modifying cell are (2, 6)). Horizontal shifts to the right hand corner of the carrier image do not generate any conflicts with previous observation windows. However, a conflict occurs at step number 4. The coordinates of the modifying cell at step number 4 are (3, 6). However, coordinates of one of the active cells at step number 3 are also (3, 6).

4.2. Partially Overlapping Boundary Conditions

In Saunoriene and Ragulskis (2023), it is demonstrated that the steganographic scheme based on the Wada index does not support overlapping periodic boundary conditions. In other words, the size of the secret image S is always smaller than the size of the carrier image C . For example, if we consider the scheme $P_{3 \times 6}^{(3,6)}$, we can encode the secret image S that contains $(n_x - r_x + 1) \times (n_y - r_y + 1)$ pixels into the carrier image C , containing $n_x \times n_y$ pixels.

It is interesting to observe that partially overlapping periodic boundary conditions are applicable for the perfect covering scheme based on the SOW. However, there is one condition: the last row of the SOW should contain only one active cell, which is a modifying cell (Fig. 11(a)–(b)). Modifying cells that allow partially overlapping periodic boundary conditions are depicted in green in Fig. 11(a)–(b). Otherwise, partially overlapping periodic boundary conditions are impossible (Fig. 11(c)–(d)). Modifying cells that do not

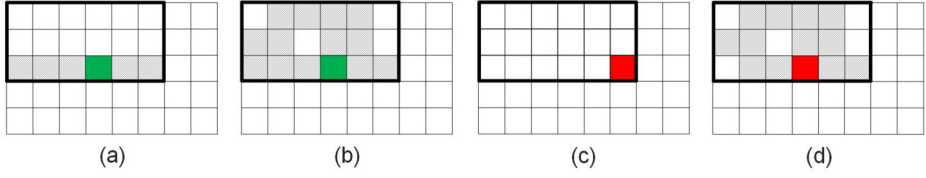


Fig. 11. Partially overlapping periodic boundary conditions are possible if the last row of the SOW contains only one active cell. Such situations are depicted in panels (a) and (b). Otherwise, partially overlapping periodic boundary conditions are impossible (panels (c) and (d)). The green and the red cells depict the modifying cells allowing (or not allowing) partially overlapping periodic boundary conditions.

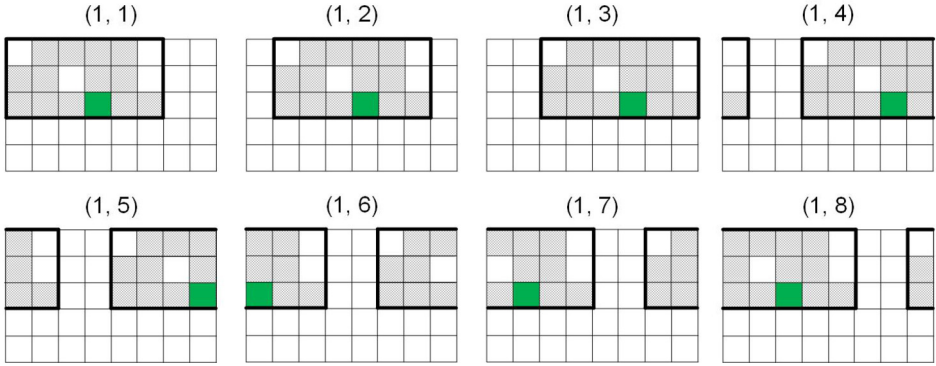


Fig. 12. The SOW depicted in Fig. 11(b) allows partially overlapping periodic boundary conditions. The width of the carrier image is 8 cells, the width of the SOW is 6 cells. The coordinates of the top left corner of the SOW can vary from (1, 1) to (1, 8) without causing any conflicts with all previous observation windows. The same reasoning holds for all lower rows.

allow the use of partially overlapping periodic boundary conditions are depicted in red in Fig. 11(c)–(d).

Figure 12 shows that no conflict with all previous observation windows is generated if partially overlapping periodic boundary conditions are used with the perfect SOW scheme $\tilde{P}_{3 \times 6}^{(3,4)}$.

If partially overlapping periodic boundary conditions (using a SOW containing a single active cell in the last row) are applied, the width of the encoded secret image can be expanded to match the width of the carrier image. For example, secret image S containing $(n_x - r_x + 1) \times n_y$ pixels can be encoded into the carrier image C , containing $n_x \times n_y$ pixels (using the perfect SOW scheme $\tilde{P}_{3 \times 6}^{(3,4)}$ (Fig. 11(a)–(b))).

4.3. The Distribution of Observable Pixels in the Carrier Image

It is interesting to observe how the pixels of the carrier image are processed during the encoding and the decoding of the secret image while using perfect covering schemes. Let us consider the $P_{3 \times 6}^{(3,6)}$ covering scheme, and the size of the carrier image 20×20 (Fig. 13(a)). The colour scheme in Fig. 13(a) depicts how many times a pixel is measured (when evalu-

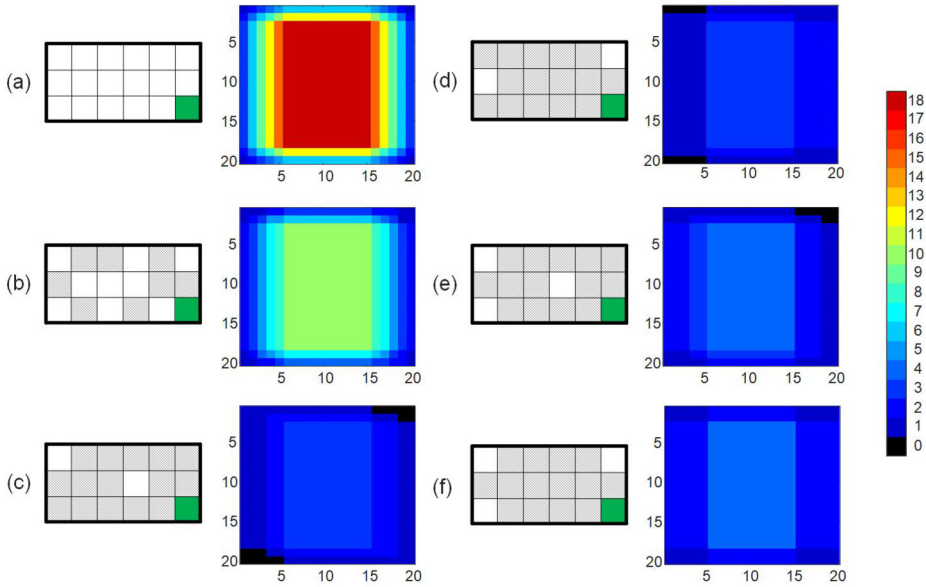


Fig. 13. Not all perfect SOWs exploit all pixels of the carrier image in the process of encoding and decoding of the secret image. The size of the carrier image is 20×20 pixels, the size of the SOW is 3 cells. The colour plot for each SOW shows how many times each pixel of the carrier image plays a role in the encoding algorithm when the used covering scheme is depicted in Fig. 3(a). Note that pixels coloured in black are not used in the encoding process at all.

ating the number of different colours in the current observation window) during the whole process of the encoding (and the decoding).

It appears that the number of times a pixel in the carrier image is evaluated does depend on its location (Fig. 13(a)). This effect can be explained by the fact that periodic boundary conditions are not possible for the scheme $P_{3 \times 6}^{(3,6)}$ (Saunoriene and Ragulskis, 2023). For example, the pixels on the corners of the carrier image are measured only once, while the pixels in the central part of the carrier image are measured 18 times during the whole process of the encoding (and the decoding) (Fig. 13(a)).

The situation changes when SOW are used instead of standard observation windows (without passive cells). The perfect covering schemes $\tilde{P}_{3 \times 6}^{(3,6)}$ with different ratios and distributions of the active and passive cells in the observation window are illustrated in panels (b)–(f) of Fig. 13. It can be observed that some pixels (in and around some of the corners of the carrier image) are not used even once in panels (c), (d), and (e) of Fig. 13. The mostly uniform distribution of the number of times a pixel is evaluated is achieved when the only four active cells are located at the corners of the observation window (Fig. 13(f)).

5. The Security of the Steganographic Scheme Based on SOW

The general concept of SOW-based scheme is somewhat similar to the steganographic scheme based on Wada index (Saunoriene and Ragulskis, 2023) (Fig. 14). The perfect

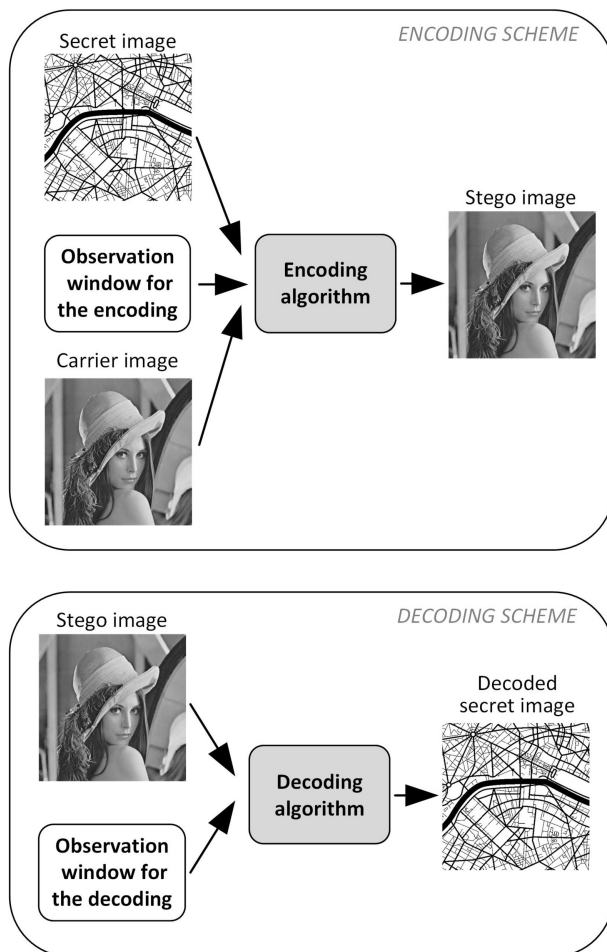


Fig. 14. A schematic diagram illustrating the basic steps of the encoding and decoding schemes. The encoding scheme requires the carrier image, the secret image, and the SOW (with the predetermined perfect covering scheme). The decoding scheme requires the stego image and the identical SOW used for the encoding.

covering scheme is employed to encode the secret image; the counting of different colours in the current observation window is used to decode the secret image. The major difference between the two schemes is in the structure of the observation window. Such a modification can be considered as a serious enhancement of the security of the proposed scheme.

Note that the statistical performance measures of the steganographic scheme based on the Wada index are comparable to the performance measures of the best LSB-type schemes (Saunoriene and Ragulskis, 2023). Moreover, this scheme is robust to the steganalysis algorithms (Saunoriene and Ragulskis, 2023), and the payload capacity of the carrier image is similar to the grayscale LSB schemes (Saunoriene and Ragulskis, 2023). The same holds true for the steganographic scheme based on SOW.

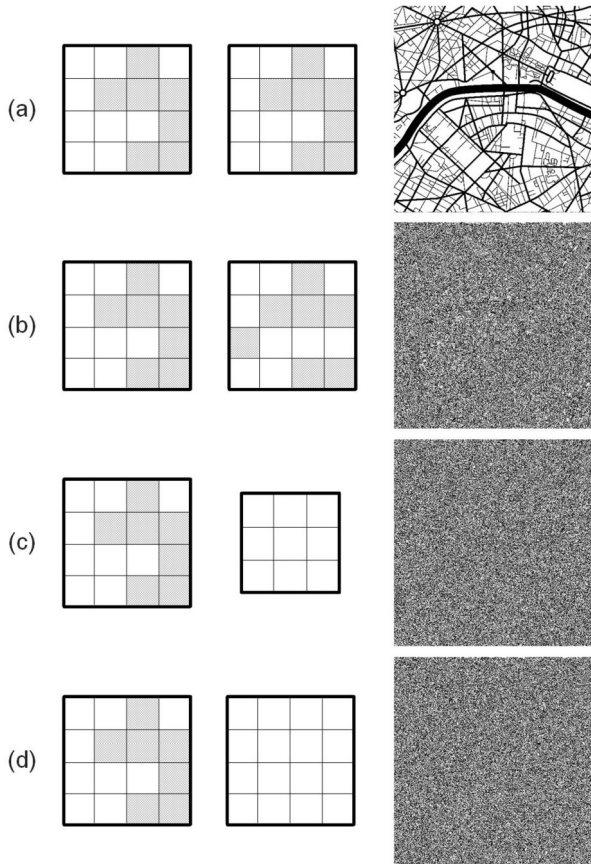


Fig. 15. The SOW used for the decoding must be identical to the SOW used for the encoding. The first column shows the SOW used to encode the city-map into the Lena image (the 4×4 SOW contains 9 active cells). The second column shows the SOW used to decode the secret image. The third column depicts the decoded image. Panel (a) illustrates a perfect decoding (the SOW used for decoding is identical to the SOW used for the encoding). A single permutation of the active cells in the SOW prevents the decoding of the secret image (panel (b)). Full 3×3 and 4×4 observation windows also fail to decode the secret (panels (c) and (d)).

However, the major advantage of the SOW-based scheme is the extra security feature which is enabled by SOWs. Let us assume that the secret city-map image (509×509 pixels) is encoded into the Lena carrier image (512×512 pixels) using a perfect SOW scheme $\tilde{P}_{4 \times 4}^{(4,2)}$ (Fig. 15). Note, that the SOW used for encoding the secret image in Fig. 15 comprises 9 active and 7 passive cells. It is important to observe that the secret image can be correctly decoded from the stego image if only the SOW used for the decoding is identical to the SOW used for the encoding. The first column in Fig. 15 shows the SOW used to encode the city-map into the Lena image; the middle column – SOWs used to decode the secret information from the stego image. The decoded secret images are depicted in the third column in Fig. 15.

Figure 15(a) demonstrates a successful decoding, when the SOW used for the decoding matches the SOW used for the encoding. A single permutation of the active cells in the

$$C_{16}^9 = 11440 \quad C_{12}^9 = 220 \quad C_{12}^9 = 220 \quad C_{12}^9 = 220 \quad C_{12}^9 = 220 \quad C_9^9 = 1 \quad C_9^9 = 1 \quad C_9^9 = 1 \quad C_9^9 = 1$$

Fig. 16. There exist 10564 different layouts of the 4×4 SOW with 9 active cells ($C_{16}^9 - 4 \cdot C_{12}^9 + 4 = 10564$). If the modifying cell is fixed at the bottom right corner of the SOW, the number of different layouts of the 4×4 SOW with 9 active cells decreases to: 6106 ($C_{15}^8 - 2 \cdot C_{11}^8 + 1 = 6106$).

SOW disrupts the decoding of the secret image (Fig. 15(b)). Similarly, full observation windows $P_{3 \times 3}^{(3,3)}$ and $P_{4 \times 4}^{(4,4)}$ are unable to decode the secret (Fig. 15(c)–(d)).

Also note that statistical performance indicators for the encoding scheme based on the perfect SOW $\tilde{P}_{4 \times 4}^{(4,2)}$ (containing 9 active cells) are at least as good as the same statistical indicators of the encoding scheme $P_{3 \times 3}^{(3,3)}$ or $P_{4 \times 4}^{(4,4)}$ based on the Wada index (Fig. 7). For example, for the encoding in Fig. 15(a), the range of modifications in the stego image is $[-78, 77]$, $ME = -0.0210$, $MAE = 1.1031$, $MSE = 7.3853$, $SSIM = 0.9823$, $PSNR = 39.4471$.

Further computational experiments are conducted with different standard carrier (Cameraman, Peppers, Jetplane) and secret images (Random, Checkerboard) (Table 2). Sparse observation window $\tilde{P}_{4 \times 4}^{(4,2)}$ presented in Fig. 15(a) is used for these computations.

Clearly, 9 active cells can be distributed in many different ways inside the 4×4 SOW. It is interesting to observe that there are 10564 distinct layouts of the 4×4 SOW consisting of 9 active cells and 7 passive cells ($C_{16}^9 - 4 \cdot C_{12}^9 + 4 = 10564$; Fig. 16). If the modifying cell is fixed at the bottom right corner of the 4×4 SOW with 9 active cells, the position of one active cell (out of 9) is already predefined. There are C_{15}^8 ways to distribute 8 active cells in the rest of 15 positions of the 4×4 observation window. However, some of these layouts consist of the first row and/or the first column containing only inactive cells, which produces the SOW of a smaller size than 4×4 (there are $2 \cdot C_{11}^8 - 1$ such inappropriate layouts). Thus, there are $C_{15}^8 - 2C_{11}^8 + 1 = 6106$ ways to distribute 9 active cells in 4×4 observation window if the modifying cell is fixed at the bottom right corner of the SOW.

6. The Robustness of the Proposed Scheme

Robustness to partial destruction of the stego image is one of the main features of the steganographic scheme. The proposed scheme is robust against partial blocking of a stego image (Fig. 17, blocked areas are depicted in white). Although it is impossible to decode the secret information from the blocked part of the stego image (black areas in the decoded secret images), the remaining part of the secret image can be decoded correctly (Fig. 17).

The “salt and pepper” noise applied to the stego image has a negative impact on the quality of the decoded secret image (Fig. 18). The higher is the density of the “salt and pepper” noise, the larger is the amount of incorrectly decoded secret pixels (Fig. 18).

The Gaussian noise applied to the stego image affects the quality of the decoded secret image as well (Fig. 19). The higher is the variance of the Gaussian noise, the larger is the

Table 2

Performance evaluation measures for the steganographic scheme with different carrier and secret images (sparse observation window $\tilde{P}_{4 \times 4}^{(4,2)}$ presented in Fig. 15(a) is used for the computational experiment).

Performance evaluation measures	Lena			Cameraman			Peppers			Jetplane		
	City-map	Random	Checker	City-map	Random	Checker	City-map	Random	Checker	City-map	Random	Checker
Pixels with increased brightness, %	24.41	24.5	24.6	24.68	24.81	24.73	24.55	24.5	24.29	24.76	24.79	24.89
Pixels with decreased brightness, %	24.59	24.79	24.64	24.52	24.52	24.51	24.86	24.72	24.68	24.46	24.45	24.32
The range of changes	[−78; 77]	[−82; 81]	[−71; 77]	[−112; 96]	[−107; 103]	[−107; 90]	[−96; 103]	[−92; 105]	[−81; 115]	[−96; 119]	[−80; 124]	[−115; 120]
Median of changes	0	0	0	0	0	0	0	0	0	0	0	0
ME	−0.0210	−0.0205	−0.0144	0.0075	0.0161	0.0203	−0.0157	−0.0224	−0.0192	0.0436	0.0365	0.0407
MAE	1.1031	1.1180	1.1107	1.1484	1.1563	1.1525	1.1888	1.1903	1.1697	1.2497	1.2346	1.2437
MSE	7.3853	7.6400	7.4456	9.2872	9.5251	9.4747	9.4435	9.4914	9.0201	11.4037	10.6796	11.0781
SSIM	0.9823	0.9818	0.9821	0.9767	0.9759	0.9765	0.9790	0.9790	0.9794	0.9798	0.9803	0.9800
PSNR	39.45	39.30	39.41	38.45	38.34	38.37	38.38	38.36	38.58	37.56	37.85	37.69

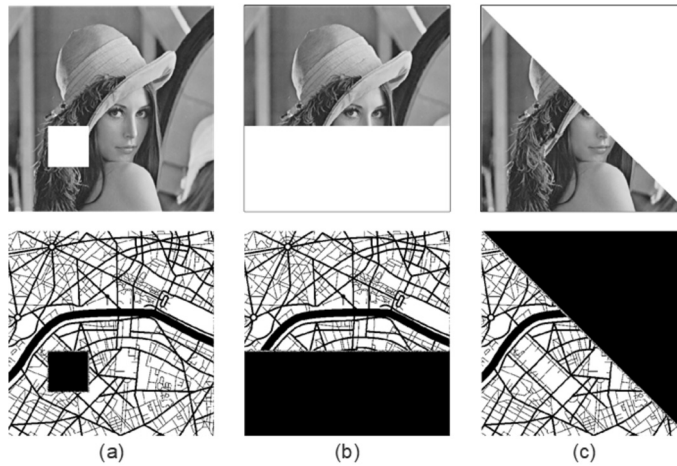


Fig. 17. The robustness of the proposed steganographic scheme against partial blocking of the stego image: the secret image cannot be decoded from the blocked part of the stego image. The blocked part of the stego image is indicated in white, the lost part of the decoded secret – in black.

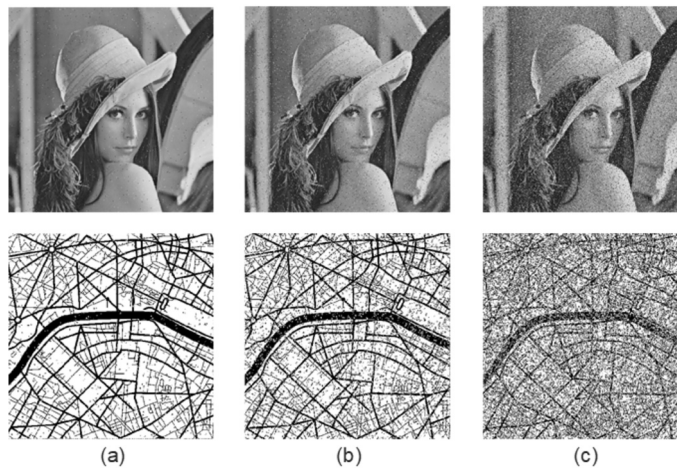


Fig. 18. The “salt and pepper” noise applied to the stego image reduces the quality of the decoded secret image. Higher noise density results into larger amount of incorrectly decoded secret pixels. The density of the “salt and pepper” noise applied to the stego image is equal to 0.005 in panel (a), 0.025 in panel (b), and 0.1 in panel (c).

amount of incorrectly decoded secret pixels. For example, the secret image can be decoded and fully recognized if the stego is degraded by the Gaussian noise with zero mean and variance equal to $7.5 \cdot 10^{-7}$ (Fig. 19(a)). Unfortunately, it is impossible to decode the secret image if the stego image is affected by the Gaussian noise with higher variances (Fig. 19(c)).

Let us suppose that the brightness of the stego image is adjusted by adding a constant $c = 50$ to the brightness of all pixels in the stego image (values greater than 255 are

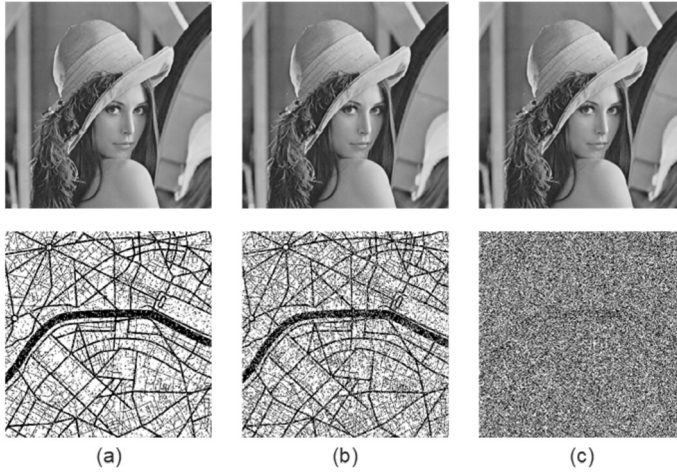


Fig. 19. The Gaussian noise applied to the stego image affects the quality of the decoded secret image. The higher is the variance of the noise, the larger is the amount of incorrectly decoded secret pixels. The stego image is degraded by the Gaussian noise with zero mean and different variances: $7.5 \cdot 10^{-7}$ in panel (a), 10^{-6} in panel (b), and $3 \cdot 10^{-6}$ in panel (c).

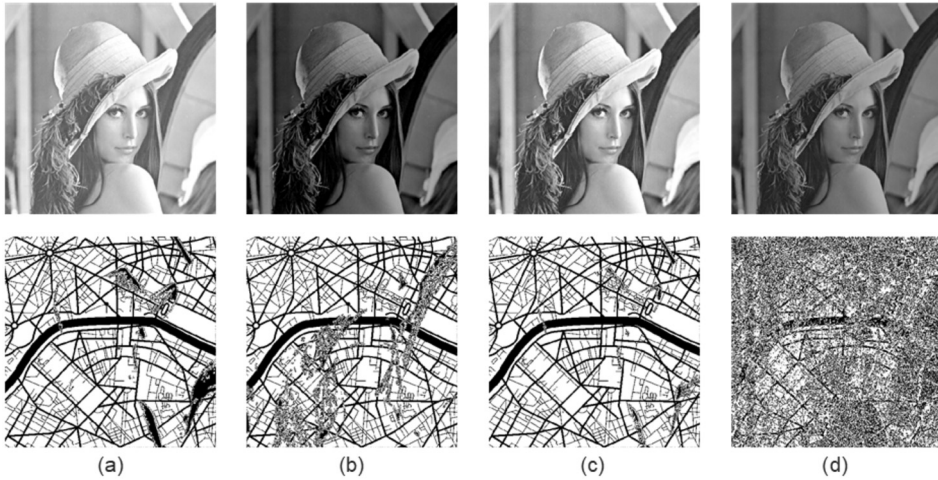


Fig. 20. The adjustment of the contrast of the stego image affects the quality of the decoded secret. The brightness of each pixel of the stego image is increased by 50 in panel (a) and decreased by 50 in panel (b). The brightness of each pixel of the stego image is increased by multiplying by 1.2 in panel (c) and decreased by multiplying by 0.8 in panel (d).

truncated to 255). The secret image is decoded correctly in those areas of the stego image where the original brightness of pixels is not greater than $255 - c$ (Fig. 20(a)).

If the brightness of the stego image is modified by subtracting a constant $c = 50$ (values lower than 0 are truncated to 0, the encoded secret image remains undamaged in the areas where the brightness of original pixels in stego image is not less than c (Fig. 20(b)).

Figure 20(c)–(d) demonstrates the influence of the multiplicative brightness adjustment of the stego image on the secret decoded image. The brightness of each pixel of the stego image is multiplied by $c = 1.2$ (values greater than 255 are truncated to 255; Fig. 20(c)). Similarly, the brightness of each pixel in the stego image is multiplied by $c = 0.8$ in Fig. 20(d). The damage to the secret decoded image is much greater in Fig. 20(d) than in Fig. 20(c) because the brightness range of the stego image is reduced to $[0, 204]$ when multiplied by $c = 0.8$ compared to the multiplication by $c = 1.2$ (the brightness range remains $[0, 255]$ then).

7. Discussion and Limitations

It is clear that the steganographic scheme based on the SOW outperforms the standard steganographic scheme based on the Wada index (Saunoriene and Ragulskis, 2023) in a sense of MAE, MSE, PSNR, and SSIM. The statistics of the scheme based on SOW is presented at the end of Section 5; the statistics of the standard scheme based on the Wada index proposed in Table 1. Comparison of the performance evaluation measures of the standard steganographic scheme and LSB, 2LSB, random 2LSB, improved 2LSB, random 3LSB, and random 4LSB steganographic schemes can be found in Saunoriene and Ragulskis (2023).

The proposed steganographic scheme has several other important advantages over the steganographic scheme based on the Wada index (Saunoriene and Ragulskis, 2023). The fact that the brightness of pixels is evaluated only in designated locations sparsely distributed in the current observation window yields a significant improvement in the security of the encoding scheme. For example, the 4×4 SOW comprising 9 active and 7 passive cells yields 10564 different layouts resulting into perfect coverings.

The apparent simplicity of the scheme is misleading. Several specific requirements are derived for the structure of the sparse observation windows capable of producing perfect coverings. A subtle interplay between the possible placement of the modifying cell and the active cells in the current observation window must be identified and properly introduced into the encoding process to guarantee the proper functioning of the proposed steganographic scheme.

The major advantages of the proposed scheme can be characterized by its ability to perform pixel modifications in different bit planes of the carrier image. The proposed scheme directly inherits this property from the steganographic scheme based on the Wada index (Saunoriene and Ragulskis, 2023). The robustness of this scheme to RS steganalysis is discussed in detail in Saunoriene and Ragulskis (2023). Analogous computational experiments demonstrate that the proposed scheme is also robust to RS steganalysis algorithms.

One of the limitations of the proposed steganographic scheme is the need to share information about the structure of the observation window between the communicating parties. In other words, the distribution of active cells and the location of the modifying cell must be exchanged between the parties before the secret image is decoded.

Another minor limitation of the proposed scheme is related to the payload capacity. In fact, the payload capacity of the scheme is comparable to LSB schemes. However, the

proposed architecture of the observation window implies that some pixels lying on the borders of the carrier image are not employed in the process of encoding and decoding the secret image (Fig. 13).

Finally, one must keep in mind that not every distribution of active cells and the modifying cell inside the observation window results into a perfect SOW. Therefore, communicating party responsible for the encoding of the secret must know the basic rules governing the structure of a perfect SOW.

In the decoding stage, the number of different colours is estimated in each of the overlapping observation windows. There are $(n_x - r_x + 1) \cdot (n_y - r_y + 1)$ observation windows in the $n_x \times n_y$ stego image, covered by $r_x \times r_y$ SOW (with r_a active cells). The time complexity to determine the number of different values within a single observation window and decode the brightness of the corresponding secret pixel is $O(r_a \log_2 r_a)$. In the encoding stage, one has to determine if the number of different colours in the current observation window is odd or even, and to make a decision if a modification is required ($O(r_a \log_2 r_a)$ operations). Statistically, changes are required for around a half of the pixels in the carrier image. The number of operations needed to modify the number of colours in each observation window is also $O(r_a \log_2 r_a)$.

The encoding and decoding algorithms are implemented in Matlab and executed on a MacBook Air M2 (8-core CPU, 8-core GPU, 16-core Neural Engine, 100 GB/s memory bandwidth). The decoding of the 510×510 secret image from the 512×512 stego image employing 4×4 SOW with 9 active cells takes 15.23 seconds on average (based on 100 identical decoding runs). However, since the sequence in which the brightness of secret pixels is decoded does not have any influence on the reconstructed secret image, the process could be executed simultaneously across multiple CPU cores, which would result in a considerably higher processing speed. For the same 510×510 secret image to be encoded in the 512×512 carrier image (using 4×4 SOW with 9 active cells), the process takes 22.14 seconds on average (based on 100 identical encoding runs).

The time required to run the encoding algorithms using high-resolution digital images prevents a possible application of the proposed scheme on edge devices using video streams. However, the enhanced security measures of the proposed scheme (compared to the steganographic proposed in Saunoriene and Ragulskis (2023)) make it an attractive alternative to many classical steganographic schemes.

The proposed steganographic scheme is capable of encoding dichotomous secret images only. In principle, the scheme could be extended to grayscale secret images. However, the Wada membership function defining the decision to modify a pixel should be modified. The decision making process cannot be based on the odd or even number of different pixels in the current observation window (Saunoriene and Ragulskis, 2023). The ability to encode a grayscale image would immediately open the possibility to encode RGB color images (by hiding R, G, and B components of the colour image separately). Such modifications remain a definite objective of future research.

References

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

- Aini, D., Setiadi, D.R.I.M., Putro, S., Rachmawanto, E., Sari, A. (2019). 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. <https://doi.org/10.1109/ISEMANTIC.2019.8884333>.
- Al-Faydi, S.N.M., Ahmed, S.K., Al-Talb, H.N.Y. (2023). Improved LSB image steganography with high imperceptibility based on cover-stego matching. *IET Image Processing*, 17(7), 2072–2082. <https://doi.org/10.1049/ipr2.12773>.
- Aziz, M., Tayarani-N, M.H., Afsar, M. (2015). A cycling chaos-based cryptic-free algorithm for image steganography. *Nonlinear Dynamics*, 80, 1271–1290. <https://doi.org/10.1007/s11071-015-1943-2>.
- EL-Hady, M., Abbas, M.H., Khanday, F.A., Said, L.A., Radwan, A.G. (2024). DISH: digital image steganography using stochastic-computing with high-capacity. *Multimedia Tools and Applications*, 83, 66033–66048. <https://doi.org/10.1007/s11042-023-17998-9>.
- George, R., Navanesan, L., Thangathurai, K. (2024). Revisiting the steganography techniques with a novel region-based separation approach. *Multimedia Tools and Applications*, 83, 71089–71114. <https://doi.org/10.1007/s11042-023-17961-8>.
- Ghoul, S., Sulaiman, R., Shukur, Z. (2023). A review on security techniques in image steganography. *International Journal of Advanced Computer Science and Applications*, 14(6). <https://doi.org/10.14569/IJACSA.2023.0140640>.
- Haverkamp, I., Sarmah, D.K. (2024). Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis. *International Journal of Information Security*, 23, 2607–2635. <https://doi.org/10.1007/s10207-024-00853-9>.
- Hussain, M., Wahab, A.W.A., Anuar, N.B., Salleh, R., Noor, R.M. (2015). Pixel value differencing steganography techniques: analysis and open challenge. In: *2015 IEEE International Conference on Consumer Electronics – Taiwan*, pp. 21–22. <https://doi.org/10.1109/ICCE-TW.2015.7216859>.
- Kaur, S., Singh, S., Kaur, M., Lee, H.-N. (2022). A systematic review of computational image steganography approaches. *Archives of Computational Methods in Engineering*, 29(7), 4775–4797. <https://doi.org/10.1007/s11831-022-09749-0>.
- Khalind, O., Aziz, B. (2015). 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. <https://doi.org/10.1117/12.2184496>.
- Kurak, C., McHugh, J. (1992). A cautionary note on image downgrading. In: *Proceedings Eighth Annual Computer Security Application Conference*, pp. 153–159. <https://doi.org/10.1109/CSAC.1992.228224>.
- Laimeche, L., Meraoumia, A., Bendjenna, H. (2020). Enhancing LSB embedding schemes using chaotic maps systems. *Neural Computing and Applications*, 32, 16605–16623. <https://doi.org/10.1007/s00521-019-04523-z>.
- Li, X., Li, X., Zhao, Y., Cho, H. (2024). Dual-domain joint optimization for universal JPEG steganography. *Journal of Visual Communication and Image Representation*, 101, 104151. <https://doi.org/10.1016/j.jvcir.2024.104151>.
- Liu, F.-Q., Liu, T., Yan, B., Pan, J.-S., Yang, H.-M. (2024). Non-iterative reversible information hiding in the secret sharing domain. *Journal of Visual Communication and Image Representation*, 100, 104096. <https://doi.org/10.1016/j.jvcir.2024.104096>.
- Luo, J., He, P., Liu, J., Wang, H., Wu, C., Zhou, S. (2023). Reversible adversarial steganography for security enhancement. *Journal of Visual Communication and Image Representation*, 97, 103935. <https://doi.org/10.1016/j.jvcir.2023.103935>.
- Luo, W., Huang, F., Huang, J. (2010). Edge adaptive image steganography based on LSB matching revisited. *IEEE Transactions on Information Forensics and Security*, 5(2), 201–214. <https://doi.org/10.1109/TIFS.2010.2041812>.
- Mukherjee, I., Paul, G. (2024). High capacity secure dynamic multi-bit data hiding using Fibonacci Energetic pixels. *Multimedia Tools and Applications*, 83, 5181–5206. <https://doi.org/10.1007/s11042-023-15504-9>.
- Nguyen, B.C., Yoon, S.M., Lee, H.-K. (2006). Multi bit plane image steganography. In: Shi, Y.Q., Jeon, B. (Eds.), *Digital Watermarking*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 61–70. https://doi.org/10.1007/11922841_6.
- Nipanikar, S.I., Hima Deepthi, V., Kulkarni, N. (2018). A sparse representation based image steganography using Particle Swarm Optimization and wavelet transform. *Alexandria Engineering Journal*, 57(4), 2343–2356. <https://doi.org/10.1016/j.aej.2017.09.005>.

- Njoum, M., Sulaiman, R., Shukur, Z., Qamar, F. (2024). High-secured image LSB steganography using AVL-tree with random RGB channel substitution. *Computational Materials Science*, 81, 183–211. <https://doi.org/10.32604/cmc.2024.050090>.
- Rahman, S., Uddin, J., Zakarya, M., Hussain, H., Khan, A.A., Ahmed, A., Haleem, M. (2023a). A comprehensive study of digital image steganographic techniques. *IEEE Access*, 11, 6770–6791. <https://doi.org/10.1109/ACCESS.2023.3237393>.
- Rahman, S., Uddin, J., Hussain, H., Ahmed, A., Khan, A.A., Zakarya, M., Rahman, A., Haleem, M. (2023b). A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image. *Scientific Reports*, 13(1). <https://doi.org/10.1038/s41598-023-41303-1>.
- Rajabi-Ghaleh, S., Olyaeefar, B., Kheradmand, R., Ahmadi-Kandjani, S. (2024). Image security using steganography and cryptography with sweeping computational ghost imaging. *Frontiers in Physics*, 12. <https://doi.org/10.3389/fphy.2024.1336485>.
- Rashid, R.D., Majeed, T.F. (2019). Edge based image steganography: problems and solution. In: *2019 International Conference on Communications, Signal Processing, and their Applications (ICCSA)*, pp. 1–5. <https://doi.org/10.1109/ICCSA.2019.8713712>.
- Sahu, A.K., Sahu, M. (2020). Digital image steganography and steganalysis: a journey of the past three decades. *Open Computer Science*, 10(1), 296–342. <https://doi.org/10.1515/comp-2020-0136>.
- Saunoriene, L., Ragulskis, M. (2023). A steganographic scheme based on the Wada index. *Multimedia Tools and Applications*, 82, 40503–40529. <https://doi.org/10.1007/s11042-023-14888-y>.
- Setiadi, D.R.I.M., Rustad, S., Andono, P.N., Shidik, G.F. (2023). Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). *Signal Process.*, 206, 108908. <https://doi.org/10.1016/j.sigpro.2022.108908>.
- Setiadi, D.R.I.M., Rustad, S., Andono, P.N., Shidik, G.F. (2024). Graded fuzzy edge detection for imperceptibility optimization of image steganography. *The Imaging Science Journal*, 72(6), 693–705. <https://doi.org/10.1080/13682199.2023.2219880>.
- Sreenidhi, A., Shruti, B., Divya, A., Subhashini, N., Muthulakshmi, S. (2024). Highly secure LSB-based image steganography with four-factor security. In: Bandyopadhyay, S., Balas, V.E., Biswas, S.K., Saha, A.K., Thounaojam, D.M. (Eds.), *Intelligent Computing Systems and Applications*. Springer Nature Singapore, Singapore, pp. 319–328.
- Wayner, P. (2009). Chapter 17 – Steganalysis. In: Wayner, P. (Ed.), *Disappearing Cryptography* (3rd ed.). The Morgan Kaufmann Series in Software Engineering and Programming. Morgan Kaufmann, Boston, pp. 337–353. 978-0-12-374479-1. <https://doi.org/10.1016/B978-012374479-1.50022-8>.
- Wolpert, D.H., Macready, W.G. (1997). No free lunch theorems for optimization. *IEEE Transactions on Evolutionary Computation*, 1(1), 67–82. <https://doi.org/10.1109/4235.585893>.
- Wolpert, D.H. (2013). Ubiquity symposium: evolutionary computation and the processes of life: what the no free lunch theorems really mean: how to improve search algorithms. *Ubiquity*, 2013(December). <https://doi.org/10.1145/2555235.2555237>.
- Xing, F., Yan, X., Yu, L., Sun, Y. (2022). Information hiding in the sharing domain. *Journal of Visual Communication and Image Representation*, 86, 103520. <https://doi.org/10.1016/j.jvcir.2022.103520>.
- Zhang, J., Lu, W., Yin, X., Liu, W., Yeung, Y. (2019). Binary image steganography based on joint distortion measurement. *Journal of Visual Communication and Image Representation*, 58, 600–605. <https://doi.org/10.1016/j.jvcir.2018.12.038>.

L. Saunoriene received the PhD degree from Kaunas University of Technology in 2007. Since 2011, she has been an associate professor at the Department of Mathematical Modelling at Kaunas University of Technology. Her research interests focus on the analysis and modelling of nonlinear systems.

J. Ragulskiene received the PhD degree from Lithuanian University of Agricultural Sciences and since 2010 she has been an associate professor at the Department of Mathematical Modelling at Kaunas University of Technology. Her research interests are focused on numerical algorithms and simulations.

M. Saunoris received the PhD degree from Kaunas University of Technology in 2007. Since 2009, he has been an associate professor at the Department of Electronics Engineering at Kaunas University of Technology. His research interests include computer simulation and signal processing techniques.

M. Ragulskis received the PhD degree from Kaunas University of Technology and since 2005 he has been a full professor at the Department of Mathematical Modelling at Kaunas University of Technology. His research interests are focused on nonlinear and complex systems.