Multimedia Tools and Applications
https://doi.org/10.1007/s11042-021-10675-9

Retracing extended sudoku matrix for high-capacity image steganography

Xuejing Li [1,2] · Yonglong Luo [1,2] · Weixin Bian [1,2]

Received: 27 May 2020 / Revised: 17 November 2020 / Accepted: 4 February 2021
Published online: 18 February 2021

Abstract
Numerous data hiding algorithms have been devised for imperceptibly embedding secret messages into the cover media so as to securely transmit user privacy information over the public communication channels. Among them, the reference matrix-based schemes in spatial domain draw extensive concern on account of the simple but efficient embedding and extraction procedure. The core idea of the planar matrix-based method is let two contiguous cover pixels conceal a base-*N* secret digit with the guidance of reference matrix, such as Sudoku, Turtle Shell, and so on. A novel image data hiding scheme with great embedding efficiency is presented in this paper, which is based on retracing extended Sudoku (*RE-Sudoku*) reference matrix. Owing to the number of Sudoku solutions and various extension directions, viz., the multiformity of *RE-Sudoku* matrix, this scheme is exceedingly more secure than the previous methods. More momentously, the proposed two-dimensional reference matrix can guide two 9-ary notational system secret digits to be embedded into each cover pixel pair simultaneously; thereby resulting in a larger embedding rate which converges to 3.169 bits per pixel. The experimental results reveal that this image steganography outperforms the other related works in terms of hiding capacity while maintaining a desirable image quality around 40 dB. Furthermore, the security of our proposed scheme is verified by demonstrating its resistance to the pixel-value difference histogram (PDH) and regular/singular (RS) steganalysis.

Keywords Data hiding · Embedding capacity · Sudoku matrix · Image steganography

✉ Yonglong Luo
ylluo@ustc.edu.cn

[1] School of Computer and Information, Anhui Normal University, Wuhu, Anhui, China

[2] Anhui Provincial Key Laboratory of Network and Information Security, Wuhu, Anhui, China

1 Introduction

Modern information security technology with respect to the private data transmission can be divided into two branches: encrypting the original secret messages directly and embedding the secret messages into a cover medium imperceptibly, i.e., cryptography and steganography. Nevertheless, the encrypted private data generated by DES [4] or RSA [15] are prone to arousing suspicions and then being intercepted by malicious attackers during message passing. Therefore, data hiding is a more appropriate technique for covert communication due to the imperceptibility of the to-be-transmitted secret messages. The data hiding mechanism comprises two subdisciplines which are both utilized to embed secret information but rely on diverse objectives [9]; viz., steganography aims to conceal the existence of private information over the public communication channels while watermarking focuses on authenticating the integrity of multimedia content without tampering.

Generally, the kind of digital steganography carriers includes plain text, still image, audio stream, dynamic video, etc. There into, image steganography has become a research hotspot over the last decade because of the visual redundancy and the flexibility of image transmission via the Internet. There are three research orientations in data hiding algorithms for digital images, i.e., the compression domain [8], the transform domain [7], and the spatial domain [1–3, 5, 10, 11, 13, 14, 16, 17, 19–21, 23]. On account of the relatively higher embedding capacity and easier implementation, the image steganography in spatial domain has aroused considerable attentions. Meanwhile, the image data hiding in spatial domain can be roughly categorized into the least-significant-bit (LSB) substitution based methods [1, 14, 17], pixel value difference (PVD) based methods [5, 10, 19, 21], exploiting modification direction (EMD) based methods [11, 13, 16, 23], and reference matrix based methods [2, 3, 20]. The principal criteria to estimate the performance of image steganography are embedding payload, stego-image visual quality, and security. Accordingly, the embedding rate (ER) is calculated by the binary bit payload of each cover pixel while the peak signal-to-noise ratio (PSNR) represents the visual quality of stego image. Whereas these two indicators are contradictory and mutually restrictive; in other words, a large payload data hiding algorithm is likely to suffer from the poor image visual quality and is vulnerable to steganalysis. Hence, the tradeoff between ER and PSNR is a dominant focus for which scholars seek novel approaches.

The classic LSB substitution information hiding scheme [1] was first proposed by Bender et al. in 1996, which directly replaces the least significant bits of every pixel with binary secret stream. Although the LSB scheme is extremely simple and efficient to implement, the concealed messages can easily be detected through the uncomplicated statistical analysis attack such as chi-square detection [18] and RS steganalysis [6]. Subsequently, Mielikainen put forward the LSB matching revisited (LSB-MR) scheme [14] that embeds two secret bits into pairwise pixels. Although the embedding capacity of [1, 14] are both 1 bit per pixel (bpp), LSB-MR has higher security and image quality. Recently, the LSB Word-Hunt (LSB-WH) scheme presented in [17] is motivated to further reduce image distortion and effectively resist the statistical chi-square attack. To tackle the defect of LSB-based schemes that the hiding payload directly impacts the overall stego-image quality, Wu and Tsai [19] developed a PVD-based approach where the difference value between two contiguous cover pixels dictates the number of secret bits to be embedded. Additionally, some LSB and PVD hybrid steganographic approaches [5, 10, 21] have been proposed in order to improve the capacity and immunity to RS attack. In literature [23], Zhang and Wang brought up a novel image data hiding algorithm denoted as EMD whose principal idea is modifying no more than one pixel

value in n cover pixels unit to embed a base-$(2n+1)$ secret digit. Inspired by [23], Kim et al. fully exploited the modification directions of cover pixels called EMD-2 [11]. It allows at most two modification directions of the original n pixels group to be altered so as to conceal one $(2w+1)$-ary secret number, where w is equal to $8+5(n-3)$ except for the case that one 9-ary digit is embedded into two cover pixels. As a result, the ER of [11] method is higher than EMD with a similar image visual quality. In the motivation of [11, 23], some other algorithms [13, 16] continue to ameliorate the performance of EMD with respect to hiding efficiency. Shen and Huang [16] initially utilized a Hilbert filling curve to map the cover image into 1D sequence and then segmented it into several non-overlapping original pairs with two adjacent pixels. According to the pixel value differencing and modulus functions, the cover pixel pairs with larger differences are embedded with more secret data than the smooth regions. In 2017, Liu et al. [13] expanded the planar EMD formed matrix to a cross pattern composed of five 3×3 sub-blocks that embraces 45 elements. Each coordinate in this key matrix is associated with a single base-45 secret figure to be hidden, thus contributing to larger embedding payload of 2.5 bpp. Chang et al. presented a Sudoku magic matrix-based steganography [2], which guided a secret digit in 9-ary format to be embedded into each cover pixel pair. Therefore, the embedding rate reaches $log_2 9/2$ bpp and the value of PSNR is around 44 dB on average. For the sake of a better visual quality of stego-image, Liu and Chang devised the Turtle Shell-based key matrix in 2014 [3]. In accordance with the guidance of hexagon Turtle Shell, octal secret integers can be hidden in cover pixel pairs with minimal distortion, so image quality is improved at the expense of hiding capacity. Later on, the 3D-Sudoku algorithm of Xia et al. [20] regarded three-dimensional Sudoku solutions as magic matrix that impulses the embedding rate equivalent to 2 bpp, where the original three pixels in 8×8 plane or $4 \times 4 \times 4$ sub-cube can be modified to conceal a secret digit in $\log_2 64$-bit format. However, the aforementioned information hiding algorithms cannot satisfy the current pursuit of privacy protection in terms of high data transfer.

Aiming to further increase the embedding payload, a novel image steganography based on retracing extended Sudoku reference matrix, which is referred to as *RE-Sudoku* matrix, is illustrated in this paper. We arbitrarily extend each novenary number in the selected 9×9 Sudoku puzzle to a 3×3 sub-cell and then tile the extended Sudoku-based grid repeatedly to construct the two-dimensional 256×256 reference matrix. Generally speaking, the security of communication in image steganography depends on the confidentiality of embedding technique [9]. However, the security of our proposed scheme also depends on the confidentiality of key, viz., the specific selected reference matrix. Since the *RE-Sudoku* matrix is multifarious, namely, the solutions of Sudoku puzzle and extension directions are various, the proposed algorithm is extremely more secure than previous methods. More momentously, we utilize a single cover pixel pair to conceal base-9 secret digits twice so as to obtain larger hiding payload, i.e., the embedding rate of $log_2 9$ which converges to 3.169 bpp. As a result, the *RE-Sudoku* matrix-based scheme can reliably protect the to-be-transmitted private information and meet the requirement of high secret data transfer simultaneously. The corresponding results in the experimental section indicate that this proposed algorithm has the merit of hiding efficiency compared to other related schemes; meanwhile it maintains a satisfactory visual quality of stego image and resists steganalysis.

The rest of this paper is organized as follows. Section 2 gives a brief introduction of the Sudoku matrix-based method and the Turtle Shell matrix-based method while Section 3 elaborates the proposed high-capacity image data hiding algorithm based on retracing

extended Sudoku reference matrix. The specific experimental results and conclusion will be discussed in Section 4 and Section 5, respectively.

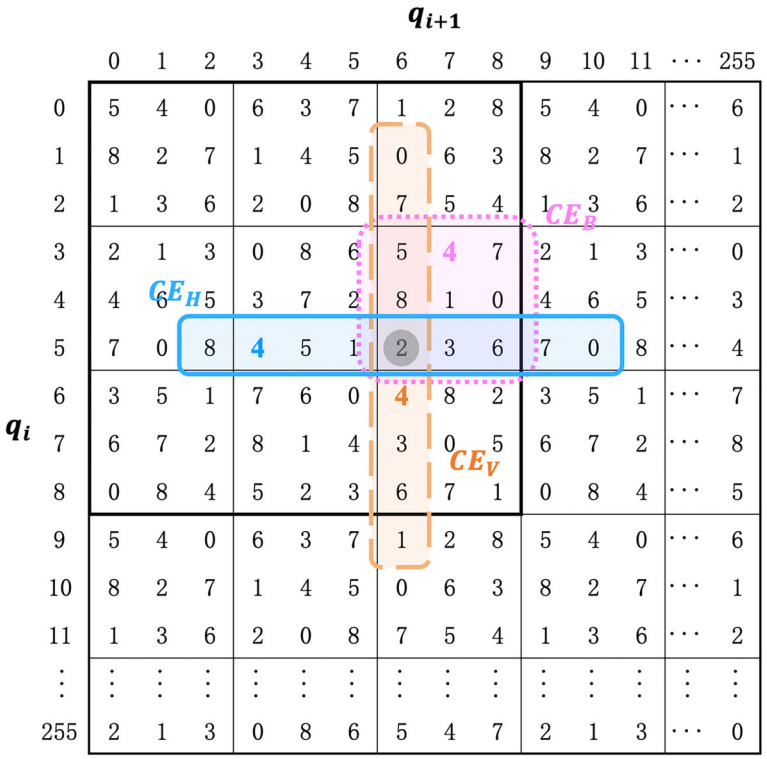
2 Related work

Owing to the flexibility of matrix construction and its simple but efficient hiding implementation, the reference matrix-based image data hiding algorithms have aroused substantial attentions. To facilitate the comprehension of our proposed image steganography, an abbreviated review of the Sudoku matrix-based scheme [2] and the Turtle Shell matrix-based scheme [3] will be separately introduced in the following Subsections.

2.1 Sudoku based scheme

Inspired by Sudoku games, Chang et al. presented state-of-the-art image steganography via choosing a Sudoku solution [2]. In this method, all digits in the selected 9 × 9 Sudoku puzzle are decreased by one to restructure a novel logic-based number placement grid whose elements range from 0 to 8. The formative 9 × 9 Sudoku-based grid is combined repeatedly to construct a 256 × 256 magic matrix M^* as depicted in Fig. 1. According to two adjacent cover pixels q_i and q_{i+1} of the original image, the pixel pair (q_i, q_{i+1}) is located onto the matrix M^* at q_i-th row and q_{i+1}-th column. Note that for each definite coordinate $M^*(q_i, q_{i+1})$, the corresponding set of abscissa and ordinate elements called CE_H and CE_V are filled with the disparate integers in 9-ary format. Moreover, the integers from 0 to 8 occur just once in each component 3 × 3 sub-block called CE_B. In this light, three sets of candidate elements CE_H, CE_V and CE_B are severally exhibited as solid line, dashed line and dotted line in Fig. 1 (assume the located coordinate is $M^*(5, 6) = 2$).

The core idea of this scheme is to embed a sequence of the converted novenary secret digits into cover pixel pairs with the guidance of Sudoku-based magic matrix. According to the inputted 9-ary digit d, $M^*(x_H, y_H)$, $M^*(x_V, y_V)$ and $M^*(x_B, y_B)$ can be chosen from three candidate element sets CE_H, CE_V and CE_B which are subject to the condition that $d = M^*(x_H, y_H) = M^*(x_V, y_V) = M^*(x_B, y_B)$. Afterwards, the Manhattan distance between the cover pixel pair (q_i, q_{i+1}) and each of these candidate elements is computed. For the sake of a smaller image distortion, the ultimate modified localization $M^*(q_i', q_{i+1}')$ is confirmed as per the minimum Manhattan distance. To better understand the hiding phase, a specific instance is displayed as here. Suppose that the original pixel pair (5, 6) is located in $M^*(5, 6) = 2$ and the to-be-concealed 9-ary secret digit is 4; then three candidate elements $M^*(5, 3)$, $M^*(6, 6)$ and $M^*(3, 7)$ are separately chosen from the sets CE_H, CE_V and CE_B whose values are all equal to 4. Since the Manhattan distance between cover pixel pair (5, 6) and the candidate element (6, 6) in set CE_V is the smallest compared to those of the other qualified elements, the final modified localization $M^*(6, 6)$ is concluded to imply the 9-ary secret digit 4. Similarly, the receiver can directly extract 9-ary secret stream according to the Sudoku magic matrix M^* used in the embedding procedure. For each non-overlapping pixel pair (q_i', q_{i+1}') in stego-image block i, the corresponding secret digit d is calculated by its definite position in the matrix, viz., $d = M^*(q_i', q_{i+1}')$. Ultimately, the extracted 9-ary digits are converted into the original binary secret stream. To summarize, the quality of stego image implemented by a selected Sudoku magic matrix is higher than 44 dB averagely with the embedding payload of $log_2 9/2$ bpp.



q_i \ q_{i+1}	0	1	2	3	4	5	6	7	8	9	10	11	⋯	255
0	5	4	0	6	3	7	1	2	8	5	4	0	⋯	6
1	8	2	7	1	4	5	0	6	3	8	2	7	⋯	1
2	1	3	6	2	0	8	7	5	4	1	3	6	⋯	2
3	2	1	3	0	8	6	5	4	7	2	1	3	⋯	0
4	4	6	5	3	7	2	8	1	0	4	6	5	⋯	3
5	7	0	8	4	5	1	2	3	6	7	0	8	⋯	4
6	3	5	1	7	6	0	4	8	2	3	5	1	⋯	7
7	6	7	2	8	1	4	3	0	5	6	7	2	⋯	8
8	0	8	4	5	2	3	6	7	1	0	8	4	⋯	5
9	5	4	0	6	3	7	1	2	8	5	4	0	⋯	6
10	8	2	7	1	4	5	0	6	3	8	2	7	⋯	1
11	1	3	6	2	0	8	7	5	4	1	3	6	⋯	2
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
255	2	1	3	0	8	6	5	4	7	2	1	3	⋯	0

Fig. 1 Demonstration of CE_H, CE_V and CE_B in a selected Sudoku magic matrix M^*

2.2 Turtle Shell based scheme

A novel turtle shell matrix [3] was devised for image data hiding in 2014, which is a hexagon consisting of eight diverse numbers from 000 to 111 in binary stream format. Herein, two digits inside hexagon are denoted as the back elements and the other six digits on the border of hexagon are denoted as the edge elements. Two crucial rules are designed for constructing the Turtle Shell-based matrix: the difference value between two consecutive coordinates in the same abscissa is set to "1" while the difference value between two consecutive coordinates in the same ordinate is set cyclically to "2" and "3". As a result, an example of the 256×256 Turtle Shell-based matrix T formed by several turtle shells is exhibited in Fig. 2. For each pairwise pixel (q_j, q_{j+1}), if the located coordinate $T(q_j, q_{j+1})$ is a back element, the 8-ary secret digit can be directly embedded into the subordinate turtle shell set; otherwise, we compute all the associate turtle shell sets which the edge element $T(q_j, q_{j+1})$ involved in so as to select an element equal to the octal secret digit with the shortest distance. The experiment shows that the image visual quality of [3] is improved to 49.5 dB and the hiding capacity drops to 1.5 bpp.

3 Proposed scheme

Since the modification direction in aforementioned matrix-based image data hiding algorithms is limited, the embedding capacity of secret information is not satisfied. In this light, a retracing extended

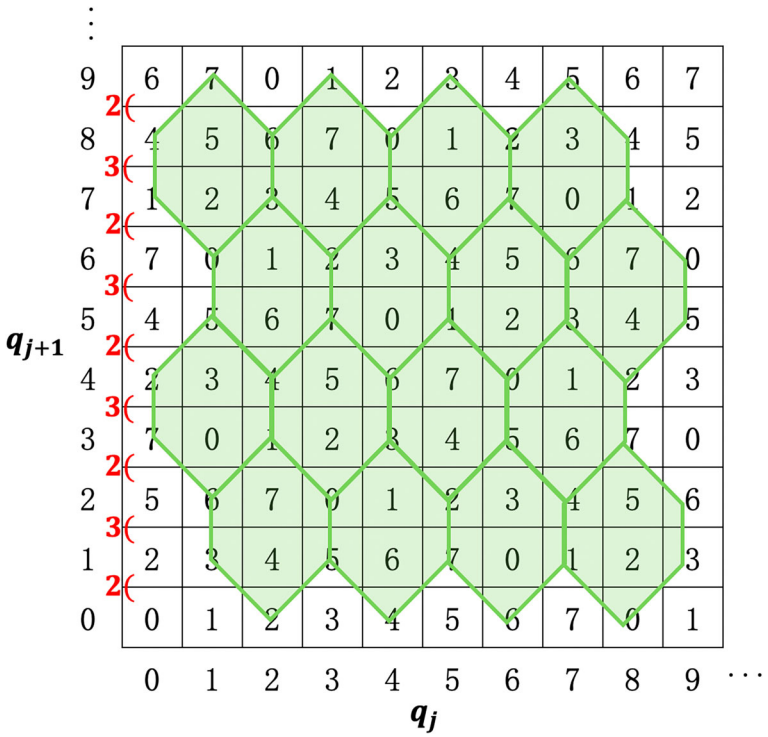


Fig. 2 The architecture of Turtle Shell-based matrix T

Sudoku reference matrix denoted as *RE-Sudoku* reference matrix is applied to the novel image steganography elaborated in this paper. The proposed *RE-Sudoku* matrix is exploited adequately via guiding two 9-ary notational system secret digits to be embedded into a cover pixel pair synchronously in order to achieve larger embedding payload with a desirable stego-image quality.

Presume that a binary bit stream S with n bits is the secret data which contains user privacy information to be imperceptibly transmitted and the original image I with size of $h \times w$ is the cover image to conceal secret data where parameters h and w severally represent the height and the width of I. These are referred to as $S = (b_1, b_2, \cdots, b_n)_2$ and $I = \{p_i | \, i = 1, 2, \cdots, h \times w\}$, respectively. In consideration of the further security, the to-be-transmitted secret information should be encrypted by symmetric encryption such as DES and AES or asymmetric encryption such as RSA before the hiding operation. Generally, after data pre-processing, the proposed image information hiding algorithm can be divided into the secret data embedding procedure and extraction procedure. To better comprehend the specific hiding principle, the implementation of constructing the two-dimensional *RE-Sudoku* reference matrix and the corresponding properties for this devised matrix are separately expounded on Sections 3.1 and 3.2. Accordingly, the concrete embedding and extraction cases will be depicted below in order to exemplify the feasibility of our proposed algorithm.

3.1 Construction of the retracing extended Sudoku matrix

Aiming for a better hiding efficiency, the proposed image steganography utilizes a retracing extended Sudoku reference matrix, viz., the *RE-Sudoku* matrix M to conceal the novenary

secret stream in cover image. The basic construction principle of *RE-Sudoku* reference matrix is to tautologically extend each number in the selected Sudoku puzzle to a square sub-cell consisting of more non-repetitive numbers. To be specific, each element in the arbitrarily selected Sudoku solution is scanned by proceeding continuously through all the rows in zig-zag order as shown in Fig. 3a, and then can be extended to a novel 3 × 3 sub-cell in accordance with a certain extension direction. An example of the extension direction is depicted in Fig. 3b; thereinto, the initial point (shown as the italic digit in circle) is the bottom-left corner element in this novel 3 × 3 sub-cell and then expands counter-clockwise from this position. Later on, a sequence of sub-cells are reorganized into the 27 × 27 extended Sudoku puzzle complying with the previous scanning rules, where the bold elements as depicted in Fig. 3c are the corresponding numbers in the original selected Sudoku solution. Ultimately, every digit in the extended Sudoku puzzle is subtracted by 1 to generate the Sudoku-based extended grid ranging from 0 to 8. Furthermore, the blue italic digits shown in Fig. 3d can restructure the Sudoku-based puzzle which satisfies the feature presented in Chang et al. method [2]. The detailed implementation of constructing the extended 27 × 27 Sudoku-based grid in 9-ary format is illustrated in Fig. 3.

To constitute the proposed *RE-Sudoku* reference matrix *M* as demonstrated in Fig. 4, the extended 27 × 27 Sudoku-based grid is tiled repeatedly and then the formative tiled matrix is truncated to a two-dimensional key matrix with size of 256 × 256. Note that in cryptography, even if the specific encryption algorithm is public, the encrypted information to be transmitted would still be secure as long as the key is not disclosed. The selected reference matrix in this image steganography is similar to the key of encryption algorithm which can guarantee the security of concealed information even if this scheme is public. Due to the multiformity of *RE-Sudoku* matrix, namely, Sudoku puzzle has numerous possible solutions and the extension direction is various as well, the specific reference matrix applied in the embedding procedure is difficult to find; thus our proposed *RE-Sudoku* based scheme outperforms the aforementioned image steganography with respect to security. In contrast to the previous methods [2, 3, 11, 23] where the cover pixel pair conceals only one secret digit, each coordinate in this devised

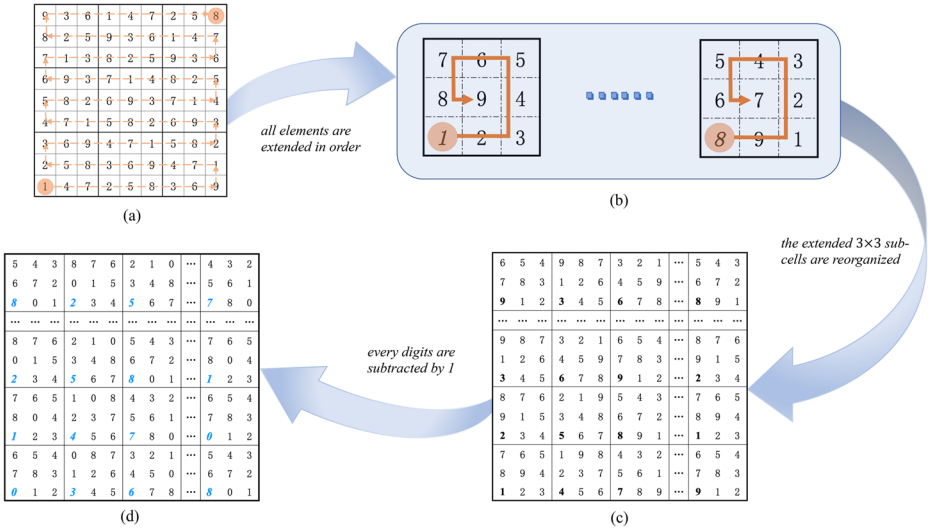


Fig. 3 Illustration of constructing the extended 27 × 27 Sudoku-based grid

reference matrix M can be embedded into two 9-ary notational system secret numbers simultaneously, which contributes to the higher capacity of $log_2 9$ bpp with a satisfactory image visual quality. To this end, the significant properties of our proposed reference matrix M are comprehensively discussed in the following Subsection so as to facilitate understanding of the hiding phase.

3.2 Properties for the RE-Sudoku matrix

In the *RE-Sudoku* reference matrix M, the abscissa and ordinate represent pixel values of two contiguous cover pixels p_i and p_{i+1}, respectively. As expected, the values of p_i and p_{i+1} range from 0 to 255 according to the dynamic spectrum of grayscale image pixels. It is apparent that every cover pixel pair (p_i, p_{i+1}) signifies the concrete localization in this two-dimensional matrix M, i.e., $M(p_i, p_{i+1})$. For each non-overlapping pixel pair (p_i, p_{i+1}), the corresponding coordinate $M(p_i, p_{i+1})$ pertains to a specific sub-cell $SC(x, y)$ which is defined by Eq. (1).

$$SC(x,y) = \begin{cases} \begin{bmatrix} M(3x,3y+2) & M(3x+1,3y+2) & M(3x+2,3y+2) \\ M(3x,3y+1) & M(3x+1,3y+1) & M(3x+1,3y+1) \\ M(3x,3y) & M(3x+1,3y) & M(3x+2,3y) \end{bmatrix} & if\ 0 \le x,y \le 84 \\ \langle empty \rangle & otherwise \end{cases} \quad (1)$$

Herein, $x = \lfloor p_i/3 \rfloor$ and $y = \lfloor p_{i+1}/3 \rfloor$ where the symbol $\lfloor \cdot \rfloor$ implies the floor function. Intuitively, the sub-cell $SC(x, y)$ contains nine elements when p_i and p_{i+1} are subject to $p_i < 255$ and $p_{i+1} < 255$; otherwise, $SC(x, y)$ is empty. As the italic numbers of the reference matrix M depicted in Fig. 4, these numbers in bottom-left corner of each $SC(x, y)$ represent the value of this sub-cell, which are referred to as $R(x, y)$. Mathematically, $R(x, y) = M(3x, 3y)$ and thus all elements $R(x,$

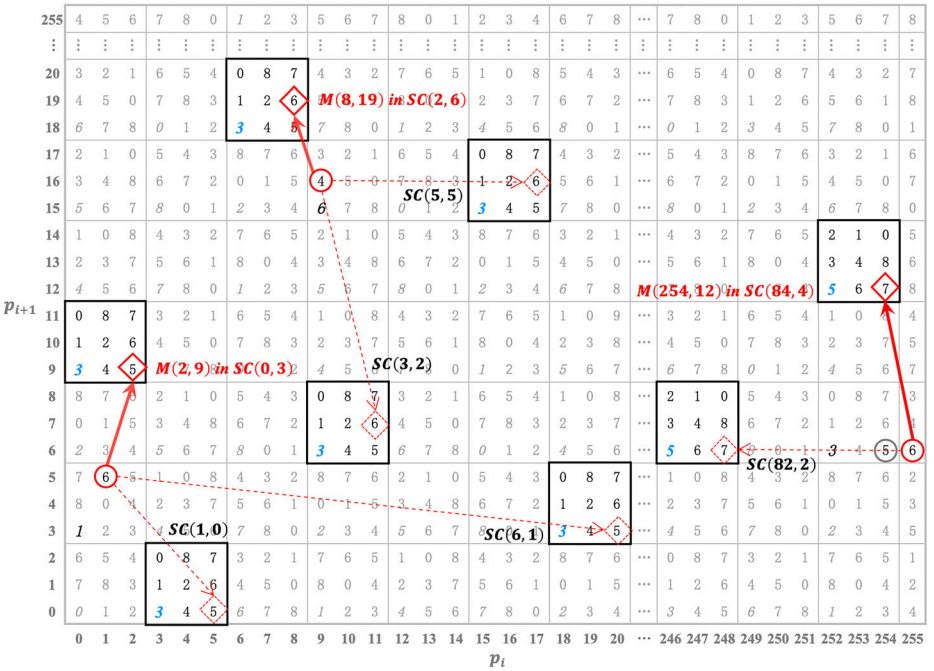


Fig. 4 The selected 256 × 256 *RE-Sudoku* reference matrix M

y) can reconstitute the 85 × 85 Sudoku sub-matrix R indicated in Fig. 5. In a nutshell, each $M(p_i, p_{i+1})$ in reference matrix M is represented by a certain coordinate of sub-matrix R through calculating Eq. (2).

$$R\left(\left\lfloor\frac{p_i}{3}\right\rfloor, \left\lfloor\frac{p_{i+1}}{3}\right\rfloor\right) = M\left(3 \times \left\lfloor\frac{p_i}{3}\right\rfloor, 3 \times \left\lfloor\frac{p_{i+1}}{3}\right\rfloor\right) \quad s.t. \quad 0 \le p_i, p_{i+1} \le 254 \tag{2}$$

As an example, the cover pixel pair is (8, 19); thus the definite coordinate $M(8, 19)$ located in the *RE-Sudoku* reference matrix M belongs to the sub-cell $SC(2, 6)$ which consists of nine elements, viz., $\{M(6, 18), M(6, 19), M(6, 20), M(7, 18), M(7, 19), M(7, 20), M(8, 18), M(8, 19), M(8, 20)\}$; in addition, $R(2, 6) = M(6, 18) = 3$ signifies the value of $SC(2, 6)$.

In method [2], the predominant feature of Sudoku matrix is applied to the process of data hiding; viz., three sets of candidate elements incorporate unrepeated novenary integers, respectively, in order to conceal a base-9 secret digit with higher image visual quality by discovering the minimum Manhattan distance. Similarly, the restructured 85 × 85 Sudoku based sub-matrix R satisfies the aforementioned property likewise. More specifically, the candidate group CG_h in the horizontal axis of Sudoku sub-matrix R is defined as

$$CG_h(x, y) = \begin{cases} \{R(x-4, y), R(x-3, y), \cdots, R(x+4, y)\}, & 3 < x < 82 \\ \{R(0, y), R(1, y), \cdots, R(8, y)\}, & x \le 3 \\ \{R(77, y), R(78, y), \cdots, R(85, y)\}, & x \ge 82 \end{cases}, \tag{3}$$

the candidate group CG_v in the corresponding vertical axis is described as

$$CG_v(x, y) = \begin{cases} \{R(x, y-4), R(x, y-3), \cdots, R(x, y+4)\}, & 3 < y < 82 \\ \{R(x, 0), R(x, 1), \cdots, R(x, 8)\}, & y \le 3 \\ \{R(x, 77), R(x, 78), \cdots, R(x, 85)\}, & y \ge 82 \end{cases}, \tag{4}$$

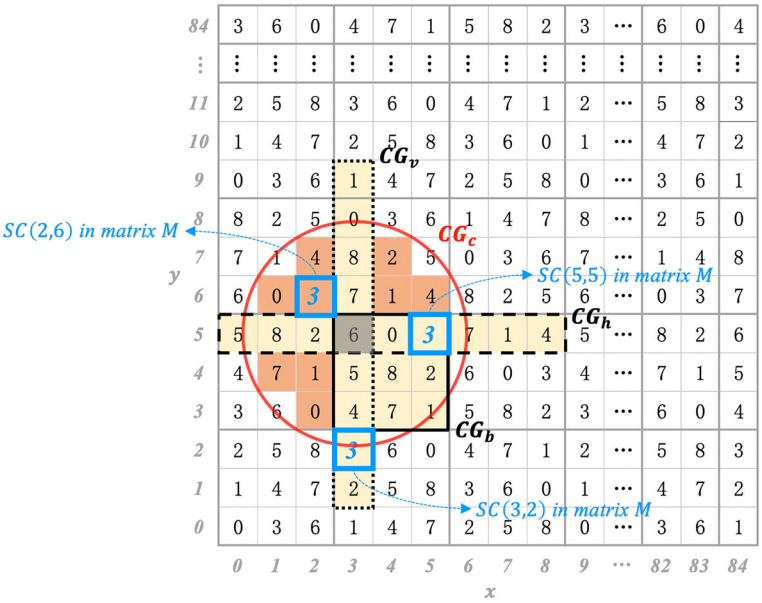


Fig. 5 The 85 × 85 Sudoku sub-matrix R

and the candidate group CG_b in the subordinative 3×3 sub-box is defined as

$$CG_b(x,y) = \begin{cases} \left\{R\left(\widetilde{x}+t_1, \widetilde{y}+t_2\right)\right\}, & \text{if } x < 84 \text{ and } y < 84 \\ \varnothing, & \text{if } x = 84 \text{ or } y = 84 \end{cases}, \quad (5)$$

where $\widetilde{x} = 3 \times \lfloor x/3 \rfloor$ and $\widetilde{y} = 3 \times \lfloor y/3 \rfloor$ while the integer parameters t_1 and t_2 are individually selected from 0 to 2 in sequence. According to the embedding implementation of the Chang et al. method [2], the Manhattan distance is the main metric for measuring suitable element to conceal a 9-ary secret digit with a smaller image distortion. Nevertheless, the image visual quality is primarily estimated by PSNR as defined in Eq. (10), which utilizes the square error of cover pixels value and corresponding stego pixels value, viz., the Euclidean distance of two pixel coordinates. Herein, the Euclidean distance is computed by following Eq. (6) where (x, y) and (x_k, y_k) represent the original coordinate and the coordinates in candidate groups, respectively. It is obvious that the Euclidean distance penalizes large deviation exceedingly more than slight deviation; namely, one pixel with an error of n has the identical consequence for PSNR as n^2 pixels with an error of 1. Therefore, the Euclidean distance is a more accurate distance measurement indicator of small image distortion than the Manhattan distance.

$$disE_{(x,y)}((x_k, y_k)) = \sqrt{(x - x_k)^2 + (y - y_k)^2} \quad (6)$$

Additionally, observe that some more appropriate coordinates in Sudoku sub-matrix R contribute to a smaller Euclidean distance, which are not considered in three candidate groups CG_h, CG_v and CG_b. For instance, suppose the original pixel pair is $(3, 5)$ and the to-be-embedded secret digit is 3. It can be intuitively deduced that $R(2, 6) = 3$ is qualified for concealing secret digit and the Euclidean distance between the original pixel pair $(3, 5)$ and this coordinate is minimum; viz., $disE_{(3,5)}((2, 6)) = \sqrt{2}$ is smaller than $disE_{(3,5)}((5, 5)) = 2$ (in CG_h and CG_b) and $disE_{(3,5)}((3, 2)) = 3$ (in CG_v). Hence, the coordinate $(2, 6)$ is more appropriate for ultimate modified localization than other qualified elements in candidate groups $CG_h(3, 5)$, $CG_v(3, 5)$ and $CG_b(3, 5)$. In this light, a novel group of candidate elements CG_c, which is depicted as the saffron yellow coordinates of sloid circle scope in Fig. 5, should be taken into consideration. The candidate group CG_c is defined as Eq. (7).

$$CG_c(x,y) = \left\{R(x_c, y_c) \mid f\left((x_c, y_c), \left(p_i, p_{i+1}\right)\right) < 5, R(x_c, y_c) \notin (CG_h \cup CG_v \cup CG_b)\right\}, \quad (7)$$

where (x_c, y_c) represents the elements embraced in group CG_c while formula f is calculated by Eq. (8). Thereinto, (x_1, y_1) and (x_2, y_2) signify the two compared coordinates. Due to the additional option of group CG_c, some more qualified candidate elements can be selected for a higher image quality.

$$f((x_1, y_1), (x_2, y_2)) = (x_1 - x_2)^2 + (y_1 - y_2)^2 \quad (8)$$

As is evident from the preceding analysis, the restructured 85×85 Sudoku sub-matrix R can be retraced to seek other qualified elements with smaller Euclidean distance that is equal to the base-9 secret digit s_j in candidate group CG_c. Hence, all qualified elements (x_h, y_h), (x_v, y_v), (x_b, y_b) and (x_c, y_c) in groups CG_h, CG_v, CG_b and CG_c are listed as candidates for the sake of implying the first 9-ary secret digit s_j. Accordingly, the sub-cells $SC(x_k, y_k)_{k = h,\ v,\ b,\ c}$ in *RE-Sudoku* reference matrix M contain the diverse novenary numbers calculated by Eq. (1). For

this characteristic, another 9-ary secret digit s_{j+1} can be embedded into the located sub-cells of reference matrix M as well; thereby resulting in larger embedding payload with an ideal stego-image quality. To facilitate the further comprehension, the embedding and extraction process is fully demonstrated as follows.

3.3 The embedding procedure

The core regulation of this proposed algorithm is to embed two 9-ary notational system secret digits into each corresponding cover pixel pair (p_i, p_{i+1}) simultaneously by referring to the selected 256×256 matrix which is constructed as described in Section 3.1. The elaborate embedding procedure of secret data is presented in the following steps.

Input: Grayscale cover image I sized $h \times w$, binary secret stream S and a selected Sudoku solution.

Output: Grayscale steganographic image I' sized $h \times w$.

Steps of the data embedding.

Stepo 1: (Image partition)

Map the original image I into a single-dimensional pixel sequence with the Hilbert filling curve as shown in Fig. 6 which can be previously conferred with communication parties, and then divide the pixel sequence into non-overlapping cover pixel pairs (p_i, p_{i+1}) where p_i and p_{i+1} are two contiguous pixels; among them, the parameter i is chosen sequentially from $\{1, 3, 5, \cdots, h \times w - 1\}$.

Step 1: (*Pre-preparation*)

Convert the binary secret bit stream $S = (b_1, b_2, b_3, \cdots, b_n)_2$ into a sequence of 9-ary numeral system secret stream S'; i.e., $S = (b_1, b_2, b_3, \cdots, b_n)_2 = (s_1, s_2, s_3, \cdots, s_{h \times w})_9 = S'$, where $n = \lfloor h \times w \times log_2 9 \rfloor$ denotes the sum total of binary secret digits. According to the selected Sudoku solution, the 256×256 *RE-Sudoku* reference matrix M and the homologous 85×85 Sudoku sub-matrix R are constructed as per the previous discussion.

Step 2: (*First secret digit embedding*)

Retrieve the cover pixel pair (p_i, p_{i+1}) from original grayscale image I and the corresponding two base-9 digits $(s_j, s_{j+1})_9$ from to-be-concealed secret stream S'. Therefore, the definite position of (p_i, p_{i+1}) is located onto the *RE-Sudoku* construction matrix when $p_i < 255$ and $p_{i+1} < 255$, viz., the coordinate $M(p_i, p_{i+1})$ where p_i and p_{i+1} denote the p_i-th horizontal axis and p_{i+1}-th vertical axis of reference matrix M, respectively. In particular, the abscissa p_i or ordinate p_{i+1} of the original pixel pair (p_i, p_{i+1}) is initially decreased by 1 if these variables conform to $p_i = 255$ or $p_{i+1} = 255$; thus the modified cover pixel pair is relocated to the coordinate $M(254, p_{i+1})$ or $M(p_i, 254)$. Subsequently, determine the sub-cell $SC(x, y)$ in matrix M that $M(p_i, p_{i+1})$ belongs to and the corresponding coordinate $R(x, y)$ in sub-matrix R that represents the value of sub-cell $SC(x, y)$; mathematically, $R(x, y) = M(3x, 3y)$ where $x = \lfloor p_i/3 \rfloor$ and $y = \lfloor p_{i+1}/3 \rfloor$.

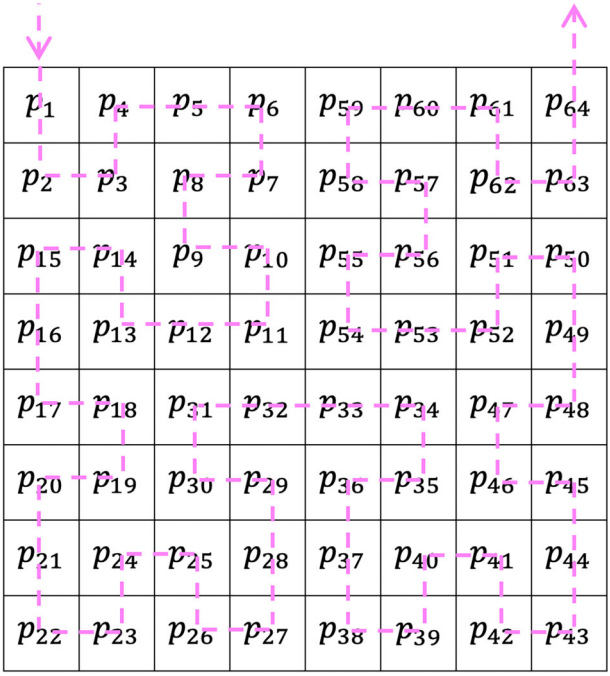


Fig. 6 Scan the cover image with Hilbert curve

Read the first converted 9-ary notational system secret digit s_j. If $s_j = R(x, y)$, no modification of localization is required; otherwise, the Sudoku sub-matrix R is retraced to search for suitable elements in the candidate groups $CG_h(x, y)$, $CG_v(x, y)$, $CG_b(x, y)$ and $CG_c(x, y)$ which are defined as Eqs. (3), (4), (5) and (7), respectively. Hence, the qualified coordinates (x_h, y_h), (x_v, y_v), (x_b, y_b) and (x_c, y_c) can be severally chosen from the preceding candidate groups that are subject to $R(x_h, y_h) = R(x_v, y_v) = R(x_b, y_b) = R(x_c, y_c) = s_j$. Accordingly, the sub-cells $SC(x_h, y_h)$, $SC(x_v, y_v)$, $SC(x_v, y_v)$ and $SC(x_c, y_c)$ in matrix M are listed as candidate sets to further conceal the second 9-ary secret digit.

Step 3: (*Second secret digit embedding*)

Calculate the elements in sub-cells $SC(x_h, y_h)$, $SC(x_v, y_v)$, $SC(x_v, y_v)$ and $SC(x_c, y_c)$ in line with Eq. (1) and then read the next converted 9-ary secret digit s_{j+1}. Scan all elements in aforementioned sub-cells of matrix M to find the appropriate coordinates which satisfy $M(x_h', y_h') = M(x_v', y_v') = M(x_b', y_b') = M(x_c', y_c') = s_{j+1}$. Afterwards, compare the corresponding Euclidean distance between the original cover pixel pair (p_i, p_{i+1}) and these candidate coordinates (x_h', y_h'), (x_v', y_v'), (x_b', y_b'), and (x_c', y_c') according to Eq. (6). Thus the final modified localization $M(p_i', p_{i+1}')$ is ascertained by referring to the minimum Euclidean distance, i.e., $(p_i', p_{i+1}') = min_{h,v,b,c}\{disE_{(p_i, p_{i+1})}((x_k', y_k'))\}$ where (x_k', y_k') is the qualified elements opted from the preceding four candidate groups.

Observe that not directly embed the second secret digit s_{j+1} into a certain candidate set $SC(x_k, y_k)$, whose representative value $R(x_k, y_k)$ has the minimum Euclidean distance in sub-matrix R, but list all qualified elements in the candidate sets $SC(x_h, y_h)$, $SC(x_v, y_v)$, $SC(x_v, y_v)$

and $SC(x_c, y_c)$ to find the most appropriate position with the truly minimum Euclidean distance between original cover pixel pair and ultimate modified localization in *RE-Sudoku* matrix M, which is exactly the reason that the qualified element of candidate set with the shortest distance in the first comparison may not necessarily be the suitable localization with the smallest image distortion. It is also the purpose of enumerating diverse candidate sets. The following embedding implementation will exemplify this point.

Step 4: (*Loop judgement*)

Set $i = i + 2$ and $j = j + 2$, then proceed to Steps 3 to 4 repeatedly until the end of secret digits stream. Ultimately, the stego image I' concealing all secret data is obtained so as to transfer user privacy information imperceptibly via the public communication channels.

The following example demonstrates the concrete steps of embedding the binary secret stream into the cover image.

Example 1 Assume the pixel pairs in cover image I are (1, 5), (9, 16), and (255,6) as the red circles depicted in Fig. 4 while the binary secret stream to be concealed is $S = (110011\ 111011\ 000101)_2$, that will be converted into 9-ary notational system secret messages and further split into three segments $(35)_9$, $(36)_9$, and $(57)_9$. Figure 7 illustrates this implementation and some specific description is supplemented as follows. By means of the data hiding phase, the ultimate modified stego pixel pairs are depicted as rhombuses which the solid arrows point to in Fig. 4.

(1). Embed the secret digits $s_1 = (3)_9$ and $s_2 = (5)_9$ into the first cover pixel pair (1, 5).

Locate the original pixel pair (1, 5) at coordinate $M(1, 5)$ on the basis of *RE-Sudoku* matrix M, then the representative value of sub-cell $SC(0, 1)$ which $M(1, 5)$ pertains to is calculated as $R(0, 1) = 1$. Obviously, $R(0, 1)$ is not equivalent to the first secret digit s_1, thereby retracing all the elements in candidate groups CG_h, CG_v, CG_b and CG_c of sub-matrix R to find the qualified elements that satisfy $R(6, 1) = R(0, 3) = R(1, 0) = s_1 = 3$. Afterwards, three candidate coordinates $M(20, 3)$, $M(2, 9)$ and $M(5, 0)$ whose values are all equal to the base-9 secret digit s_2 are separately chosen from the sub-cells $SC(6, 1)$, $SC(0, 3)$ and $SC(1, 0)$. Although the Euclidean distance between $R(0, 1)$ and $R(1, 0)$ is smaller than others in the sub-matrix R, the final

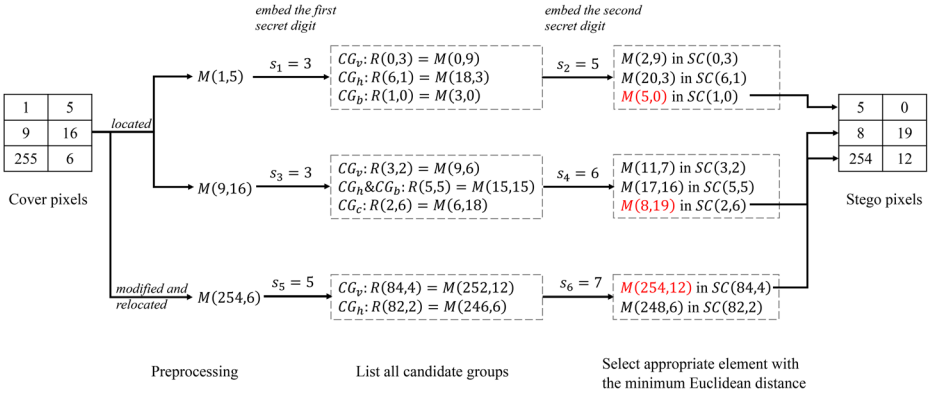


Fig. 7 Illustration of the embedding procedure referring to *RE-Sudoku*

modified position is $M(2, 9)$, which is embraced in sub-cell $SC(0, 3)$, not the coordinate $M(5, 0)$ of $SC(1, 0)$ with the smallest Euclidean distance in first comparison. Therefore, comparing the Euclidean distance between cover pixel pair $(1, 5)$ and the last qualified elements in all candidate sub-cells is decisive. As a result, replace the original pixel pair $(1, 5)$ with $(2, 9)$ owing to $disE_{(1,5)}(2, 9) = \sqrt{17}$ is less than $disE_{(1,5)}(5, 0)$ and $disE_{(1,5)}(20, 3)$.

(2). Embed the secret digits $s_3 = (3)_9$ and $s_4 = (6)_9$ into the second cover pixel pair (9, 16).

The definite localization of $M(9, 16)$ is ascertained as per matrix M and the matching coordinate $R(3, 5) = 6$ denoting the sub-cell $SC(3, 5)$ is computed as well. Carry out step 3, so that three satisfied points $(5, 5)$, $(3, 2)$ and $(2, 6)$ are opted from the candidate groups because these coordinate values in sub-matrix R are identical to s_3. In this light, the suitable coordinates in sub-cells $SC(5, 5)$, $SC(3, 2)$ and $SC(2, 6)$ of key matrix M are separately confirmed, i.e., $M(17, 16) = M(11, 7) = M(8, 19) = s_4$. Eventually, the modified stego pixel pair (8, 19) is determined by the minimum Euclidean distance between the original pixel pair and the aforementioned coordinate elements.

(3). Embed the secret digits $s_5 = (5)_9$ and $s_6 = (7)_9$ into the third cover pixel pair (255,6).

According to the foregoing discussion, the original pair (255,6) is previously modified to (254,6) as the gray circle exhibited in Fig. 4 and then can be relocated onto the matrix M at the position $M(254,6)$. Subsequently, figure out $R(84, 2) = 3$ representing the value of sub-cell $SC(84, 2)$ which the element $M(254,6)$ belongs to. It is apparent that $R(84, 2) \neq s_5$, thus the procedure of retracing Sudoku sub-matrix is applied. Since no qualified elements in $CG_c(84, 2)$ and $CG_b(84, 2)$ is empty, only two suitable coordinates $(82, 2)$ and $(84, 4)$ in sub-matrix R are selected from the corresponding candidate groups CG_h and CG_v. Continue to proceed with Step 4; hereto, the points (248,6) and (254,12) in matrix M are ascertained owing to the same value with s_6. The Euclidean distances between original pixel pair and the first located coordinates in $SC(82, 2)$ and $SC(84, 4)$ are identical, but the ultimate modification point is determined by the Euclidean distance of comparing the second candidate elements. Consequently, the pixel pair (255,6) of cover image is modified to the stego pixel pair (254,12) which fulfils the minimum Euclidean distance attribute in matrix M.

3.4 The extraction procedure

Upon receiving the grayscale steganographic image I' sized $h \times w$ and the selected Sudoku solution utilized in previous embedding phase, the concealed secret message S which contains user privacy information to be transmitted is accurately retrieved by means of the next extraction steps.

Input: Grayscale steganographic image I' sized $h \times w$ and a selected Sudoku solution.

Output: binary secret stream S.

Steps of the data extraction.

Step 1: (*Stego image partition*)

Scan the received stego image I' with Hilbert filling curve and partition it into non-overlapping pixel pairs (p_i', p_{i+1}') as the similar operation used in embedding phase, where $i \in \{1, 3, 5, \cdots, h \times w - 1\}$ and the pixel grayscale values are identical to p_i and p_{i+1}, respectively.

Step 2: (*Secret digits extracting*)

Retrieve the stego pixel pair (p_i', p_{i+1}') of image I' in sequence and then locate it onto in the *RE-Sudoku* reference matrix M which can be constructed as Section 3.1, thus the second embedded 9-ary secret digit is calculated by $s_{j+1} = M(p_i', p_{i+1}')$. Subsequently, seek out the definite sub-cell $SC(x', y')$ including the located coordinate $M(p_i', p_{i+1}')$, and the representative value of $SC(x', y')$ denoted as $R(x', y')$ is equal to the first concealed 9-ary digit, viz., $s_j = R(x', y') = M(3x', 3y')$ where $x' = \lfloor p_i'/3 \rfloor$ and $y' = \lfloor p_{i+1}'/3 \rfloor$.

If all the stego pixels in received image I' have been traversed, the extraction phase is finished and move to Step 3; otherwise, we set $i = i + 2$ and $j = j + 2$, then continue to repeat the aforementioned novenary secret digits extracting implementation.

Step 3: (*Binary conversion*)

Convert the extracted 9-ary notational system secret stream S' into a binary bit stream. Hereto, the secret data S implying all imperceptible privacy information is obtained exactly.

Similarly, provide an example to demonstrate the aforementioned extraction technique.

Example 2 Assume the obtained pixel pair (p_i', p_{i+1}') in the grayscale stego image I' is (8, 19). The corresponding base-9 concealed digit $s_{j+1} = M(8, 19) = 6$ can be computed directly. Furthermore, $M(8, 19)$ is involved in the sub-cell $SC(2, 6)$ of matrix M and the element in bottom-left concern of $SC(2, 6)$ denotes the first embedded secret digit, viz., $s_j = R(2, 6) = M(6, 18) = 3$. Hence, the all 9-ary secret data is extracted as $S' = (36)_9$. Finally, S' is converted to the original secret binary bit stream $S = (100001)_2$.

4 Experimental results

To demonstrate the superiority of our proposed scheme, eight grayscale images with size of 512×512 were used as cover images. Figure 8 exhibits these standard test images, viz., Lena, Boat, Barbara, Airplane, Goldhill, Elaine, Peppers and Baboon, which are selected from the USC-SIPI image database. All experiments were implemented on MATLAB R2018a software.

4.1 Simulation and comparisons

Two metrics are applied to basically estimate the performance of these data hiding algorithms, viz., hiding payload and stego-image visual quality. The embedding rate (ER) defined as Eq. (9) is aimed to typically measure the amount of secret data embedded into a single cover pixel.

$$ER = \frac{\|S\|}{H \times W} \ (bpp) \ , \tag{9}$$

where $\|S\|$ is a statistical value representing the sum total of concealed binary secret bits in the original image and is also referred to as embedding capacity (EC) while H and W severally denote the height and width of grayscale cover image.

To evaluate the visual quality of stego image, peak signal-to-noise ratio (PSNR) computed by Eq. (10) is chosen as the primary criterion.

$$PSNR = 10 \times log_{10} \frac{255^2}{MSE} \ (dB) \tag{10}$$

Herein, MSE is the mean square error between the original cover image and the steganographic image. MSE can be calculated by the following Eq. (11), where $I(i,j)$ and $I'(i,j)$ signify the pixel value of the original cover image and the corresponding stego image, respectively. Howbeit, these two indicators are inversely related and mutually restrictive, i.e., an image steganography with large embedding payload tends to result in a stego-image with relatively poor visual quality. The specific experimental analysis in this section will certify the *RE-Sudoku* reference matrix based scheme has an excellent tradeoff between ER and PSNR.

$$MSE = \frac{1}{H \times W} \times \sum_{i=1}^{W} \sum_{j=1}^{H} \left(I(i,j) - I'(i,j) \right)^2 \tag{11}$$

After embedding the to-be-transmitted privacy information into some test images by the proposed data hiding scheme, Fig. 9 illustrates the corresponding PSNR value histogram of stego-image when the embedding rate are 0.5 bpp, 1 bpp, 1.5 bpp, 2 bpp, 2.5 bpp and 3 bpp, respectively. Observe that they have an approximately similar stego image visual quality ~~in~~ under the identical embedding rate. Furthermore, the PSNR of stego image drops more sharply in small ER than its in large ER with the same increment of embedding payload. It is the reason that the image distortion principally depends on the specific selected data hiding algorithm or the number of embedded secret digits rather than a certain original cover image.

Fig. 8 Original standard test images. (**a**) Lena (**b**) Boat (**c**) Barbara (**d**) Airplane (**e**) Goldhill (**f**) Elaine (**g**) Peppers (**h**) Baboon

To summarize, our algorithm is effective for various test images since the visual quality of separate stego images performs stably under the same condition of hiding capacity.

The corresponding stego images with embedding rate of 1 bpp, 2 bpp and 3 bpp are shown in Fig. 10, respectively. It is intuitively clear that the few difference between the original image and these stego images cannot easily to be distinguished since a large PSNR value intrinsically implies the high similarity of images and even though at the maximum embedding rate of 3 bpp it can still maintain a desirable visual quality of approximately 40 dB as well.

Except for the PSNR, the quality index (QI) and the structural similarity (SSIM) are used as another two criteria to estimate the image visual quality which are severally computed by Eqs. (12) and (13).

$$QI = \frac{4\sigma_{12}\mu_1\mu_2}{(\sigma_1{}^2 + \sigma_2{}^2)(\mu_1{}^2 + \mu_2{}^2)} \quad , \tag{12}$$

where parameters μ_1 and σ_1 separately denote the mean value of pixels and standard deviation for the original cover image I. Similarly, parameters μ_2 and σ_2 are the mean value of pixels and standard deviation for the corresponding stego image I' while σ_{12} represents the covariance between images I and I'. Therefore, the maximum value of QI can be achieved (i.e., $QI = 1$) when the cover image and stego image are entirely equivalent.

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x{}^2 + \mu_y{}^2 + c_1\right)\left(\sigma_x{}^2 + \sigma_y{}^2 + c_2\right)} \tag{13}$$

Herein, μ_x, $\sigma_x{}^2$ and μ_y, $\sigma_y{}^2$ are the mean value and variance of blocks x and y for the cover image and stego image, respectively, while σ_{xy} is the covariance between image blocks x and y. In addition, the constants c_1 and c_2 are calculated by $c_1 = (k_1L)^2$ and $c_2 = (k_2L)^2$ where L is the dynamic range of image pixel values and $k_1 = 0.01$, $k_2 = 0.03$. Obviously, the stego image quality is much better when the value of SSIM is close to 1.

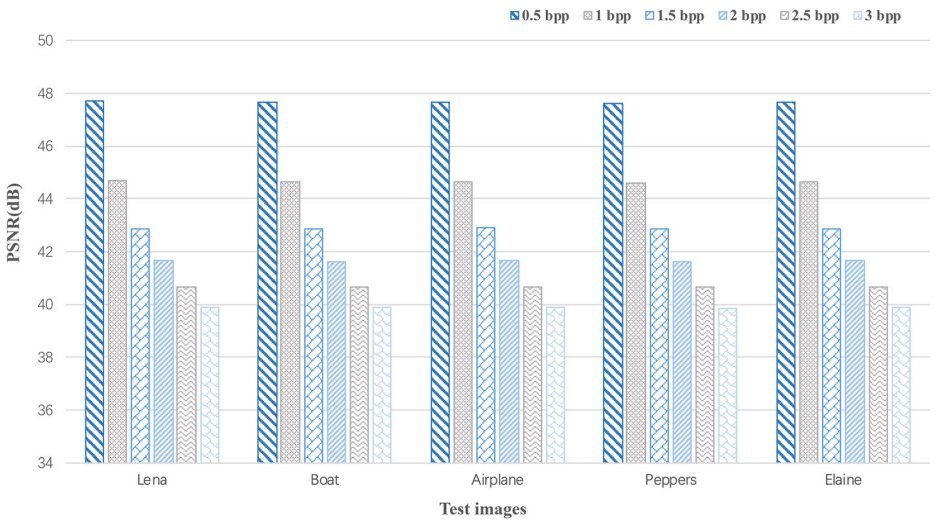


Fig. 9 Histogram of stego image PSNR versus ER for the proposed algorithm

(a) (b) (c)

Fig. 10 Stego images of 'Lena' under diverse embedding rate. (**a**) 1 bpp with 44.68 dB (**b**) 2 bpp with 41.65 dB (**c**) 3 bpp with 39.89 dB

The following Table 1 exhibits the simulation results of our proposed image data hiding algorithm with respect to performance.

In order to concretely demonstrate the merits of this novel proposed algorithm, the comparisons between our algorithm and several aforementioned methods [2, 3, 11, 13, 16, 20, 23] are illustrated in Tables 2 and 3, respectively. More specifically speaking, the schemes in [11, 13, 16, 23] are EMD-based information hiding techniques while the [2, 3, 20] schemes are all reference matrix-based image steganography in spatial domain. Table 2 compares the embedding payload and stego-image visual quality results of our proposed algorithm with those of the previous [11, 13, 16, 23] schemes. Herein, the method in [23] is the original one which can embed a $(2n+1)$-ary notational system secret number into the cover group of n pixels with, at most, one modification direction could be altered, and the [11] scheme referred to as EMD-2 is an improved method in hiding capacity that modifies no more than two pixels value of n cover pixels unit by increasing or decreasing 1. Afterwards, the scheme in [16] further enhances the embedding payload of cover image which is approximate to 1.56 bpp on average but it has a huge image distortion compared to the preceding two approaches. The method [13] put forward by Liu et al. obtains the largest hiding efficiency among the recent EMD-based information hiding schemes; however, the ER of [13] is merely limited to 2.5 bpp. It is apparent that the algorithm proposed in this paper can carry significantly more secret bits (viz., 3.169 bpp) than the other image data hiding methods in [11, 13, 16, 23] depicted in Table 2; meanwhile, it still retains a satisfactory PSNR that is slightly lower than the [13, 16] methods.

Table 1 Experimental results of the proposed algorithm

Images	EC (bits)	MSE	PSNR (dB)	QI	SSIM	ER (bpp)
Lena	830,976	7.0426	39.65	0.9985	0.9890	3.1699
Boat	830,976	7.0656	39.64	0.9984	0.9915	3.1699
Barbara	830,976	7.1029	39.61	0.9988	0.9925	3.1699
Airplane	830,976	7.0582	39.64	0.9984	0.9870	3.1699
Goldhill	830,976	7.0926	39.62	0.9985	0.9926	3.1699
Elaine	830,976	7.0801	39.63	0.9983	0.9900	3.1699
Peppers	830,976	7.0755	39.63	0.9988	0.9887	3.1699
Baboon	830,976	7.0533	39.64	0.9973	0.9948	3.1699
Average	830,976	7.0713	39.63	0.9984	0.9908	3.1699

Similarly, the comparison in Table 3 presents the experimental results of ER and PSNR between the reference matrix-based schemes [2, 3, 20] and our proposed algorithm. Among them, the [2] method based on Sudoku reference matrix is particularly discussed in Section 2.1 whose embedding capacity is identical to $log_2 9/2$ bpp while the Turtle Shell matrix-based scheme [3] elaborated in Section 2.2 can guide one octal secret integer to be embedded into a cover pixel pair that contributes to the ER of 1.5 bpp. The method [20] devised by Xia et al. refers to 3D-Sudoku construction matrix which conceals a 6-bit secret number in three cover pixels so its hiding capacity reaches 2 bpp. Note that this novel image steganography based on the *RE-Sudoku* reference matrix, which can concurrently embed two 9-ary secret digits into each original pixel pair, achieves an exceedingly higher embedding rate of $\log_2 9$ bpp than the other magic matrix-based data hiding schemes so far. Intuitively, the proposed algorithm has a respective large hiding capacity increment of 1.66 bpp, 1.66 bpp and 1.16 bpp compared to the schemes in Table 3. In addition, the construction expense of *RE-Sudoku* two-dimensional reference matrix is less than 3D-Sudoku matrix [20] because the key matrix used in Xia at el. method is three-dimensional which is much more complex than two-dimension. Therefore, it is reasonable that the tremendous improvement in ER with small reference matrix construction expense is at the slight sacrifice of stego-image visual quality. To summarize, the novel *RE-Sudoku* matrix based data hiding algorithm outperforms both EMD-based schemes [11, 13, 16, 23] and reference matrix-based schemes [2, 3, 20] in terms of embedding capacity while still maintaining a relatively desirable visual quality of stego image around 40 dB.

Figure 11 illustrates the average PSNR comparison results of the novel image data hiding algorithm and three LSB and PVD based hybrid steganographic approaches [5, 10, 21] for the eight standard test images shown in Fig. 7 under disparate hiding capacity conditions. It is intuitive that the *RE-Sudoku* reference matrix-based scheme proposed in this paper can maintain the excellent stego-image visual quality with different ER values from 0.3 bpp to 3.16 bpp. More momentously, the embedding payload of [5, 10, 21] schemes listed in the following illustration are merely restricted with 2.92 bpp, 3.07 bpp and 3.05 bpp; furthermore, the curve of our algorithm is higher than that of the other methods which implies a smaller image distortion. Hence, the proposed scheme can still achieve a higher visual quality of stego images than Yang et al. method [21], Khodaei et al. method [5] and Hussain et al. method [10] at different embedding rates.

Table 2 Comparisons of EMD-based information hiding schemes and the proposed algorithm

Images	Zhang and Wang's scheme [23]		Kim et al.'s scheme [11]		Shen and Huang's scheme [16]		Liu et al.'s scheme [13]		The proposed scheme	
	ER (bpp)	PSNR (dB)	ER (bpp)	PSNR (dB)	ER (bpp)	PSNR (dB)	ER (bpp)	PSNR (dB)	ER (bpp)	PSNR (dB)
Lena	1	52.12	1.37	50.86	1.53	42.46	2.5	41.84	3.16	39.65
Boat	1	52.11	1.37	50.64	1.55	41.60	2.5	41.83	3.16	39.64
Barbara	1	52.11	1.37	50.68	1.56	41.29	2.5	41.82	3.16	39.61
Airplane	1	52.10	1.37	50.79	1.57	42.33	2.5	41.83	3.16	39.64
Goldhill	1	52.11	1.37	50.71	1.54	41.80	2.5	41.81	3.16	39.62
Elaine	1	52.11	1.37	50.67	1.51	42.98	2.5	41.83	3.16	39.63
Peppers	1	52.12	1.37	50.78	1.54	41.25	2.5	41.77	3.16	39.63
Baboon	1	52.11	1.37	50.69	1.69	38.88	2.5	41.82	3.16	39.64
Average	1	52.11	1.37	50.75	1.56	41.57	2.5	41.82	3.16	39.63

Table 3 Comparisons among reference matrix-based image steganography

Images	Sudoku [2]		Turtle Shell [3]		3D-Sudoku [20]		Proposed	
	ER (bpp)	PSNR (dB)	ER (bpp)	PSNR (dB)	ER (bpp)	PSNR (dB)	ER (bpp)	PSNR (dB)
Lena	1.5	44.96	1.5	49.42	2	41.31	3.16	39.65
Boat	1.5	44.90	1.5	49.40	2	41.23	3.16	39.64
Barbara	1.5	44.67	1.5	49.41	2	41.32	3.16	39.61
Airplane	1.5	44.99	1.5	49.39	2	41.28	3.16	39.64
Goldhill	1.5	44.85	1.5	49.40	2	41.29	3.16	39.62
Elaine	1.5	44.92	1.5	49.41	2	41.31	3.16	39.63
Peppers	1.5	44.67	1.5	49.40	2	41.30	3.16	39.63
Baboon	1.5	44.68	1.5	49.39	2	41.25	3.16	39.64
Average	1.5	44.83	1.5	49.40	2	41.29	3.16	39.63

4.2 Security analysis

Generally, the security of any steganographic approaches is estimated by steganalysis which can be categorized into visual steganalysis and statistical steganalysis [9]. To theoretically evaluate the security of stego images after concealing privacy information by this proposed scheme, the pixel-value difference histogram (PDH) analysis technology [22] and RS steganalysis [6] are applied. Figure 12 depicts the pixel-value difference histograms of six cover images, viz., Lena, Boat, Barbara, Peppers, Goldhill, and Airplane that are selected from the above grayscale test images shown in Fig. 8, and their corresponding stego images yielded by our proposed scheme with the maximum embedding rate. Herein, PDH [22] indicates the frequency distribution of the difference values between two consecutive pixels in each non-overlapping image pixel pair, whose *x*-axis and *y*-axis separately represent pixel difference and

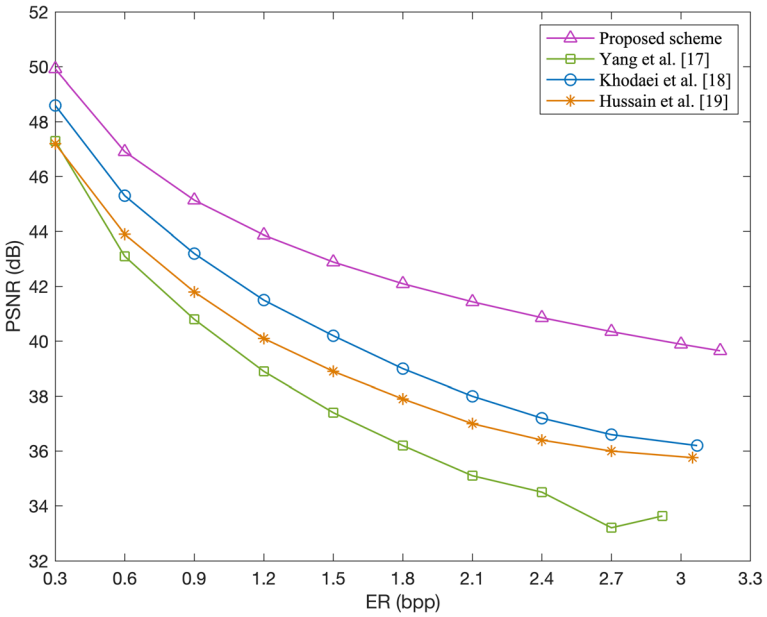


Fig. 11 PSNR value comparisons with disparate hiding efficiency

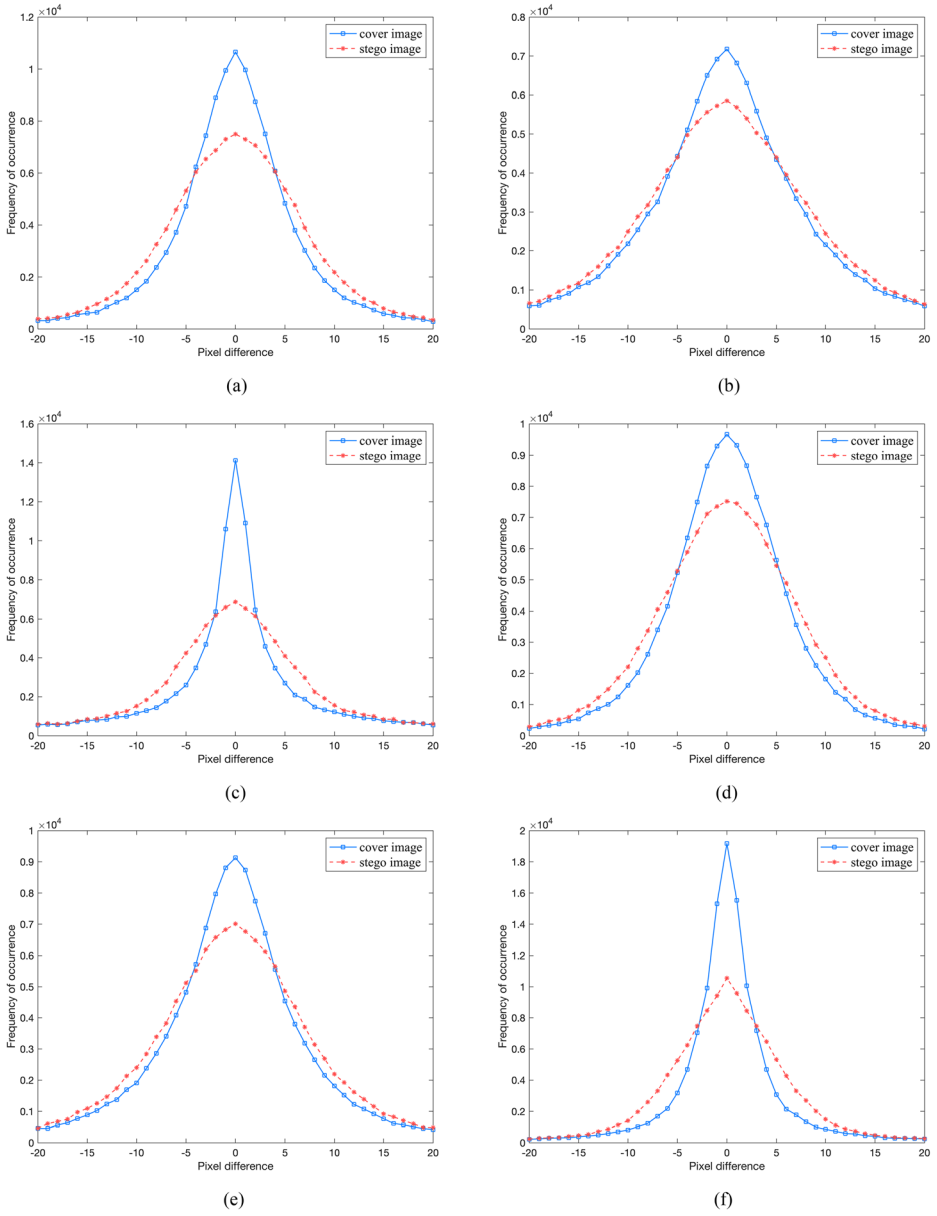


Fig. 12 PDH histograms between test images and the corresponding stego images. (**a**) Lena (**b**) Boat (**c**) Barbara (**d**) Peppers (**e**) Goldhill (**f**) Airplane

frequency of it. Visually, the histogram curves of six stego images as dashed lines depicted in Fig. 12 are macroscopically smooth and no step-effects or zig-zag appearance abiding by the feature of the natural image PDH. As a result, the *RE-Sudoku* matrix based algorithm is immune to the pixel-value difference histogram steganalysis.

The dual statistical analysis [6] is widely applied in image steganalysis since it can efficiently and accurately detect LSB embedding operations. In the process of RS steganalysis,

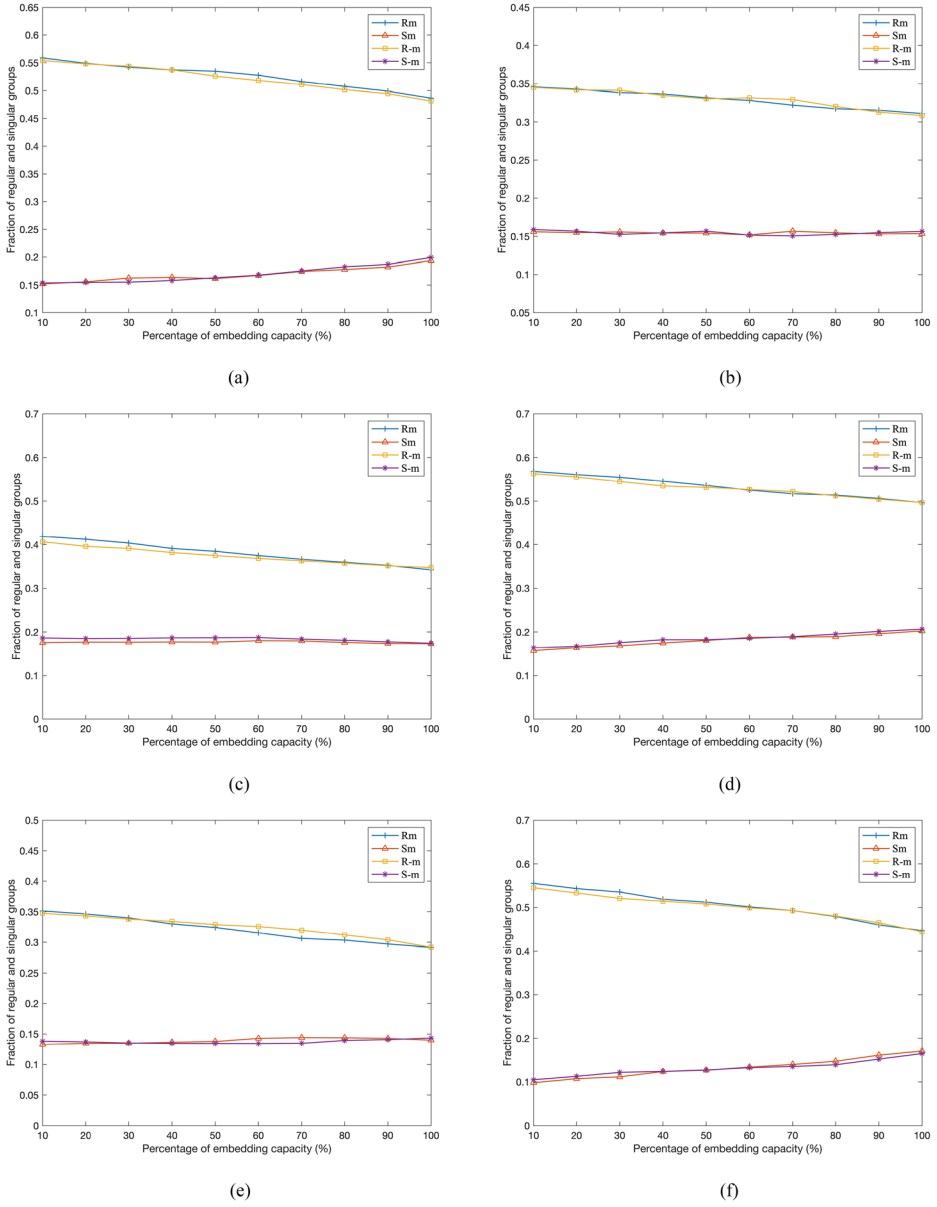


Fig. 13 RS diagrams of stego images yielded by the proposed scheme. (**a**) Lena (**b**) Boat (**c**) Barbara (**d**) Peppers (**e**) Goldhill (**f**) Airplane

the test image is initially divided into several non-overlapping blocks. Subsequently, these image blocks are separately classified into the regular group, the singular group and the unusable group as per the discrimination function f, flipping function F and mask M. Accordingly, the percentages of the regular groups and singular groups are denoted as R_m and S_m for mask M and as R_{-m} and S_{-m} for mask $-M$, respectively. For the typical original image, it must conform to the properties that $R_m \cong R_{-m}$ and $S_m \cong S_{-m}$. Ultimately, the

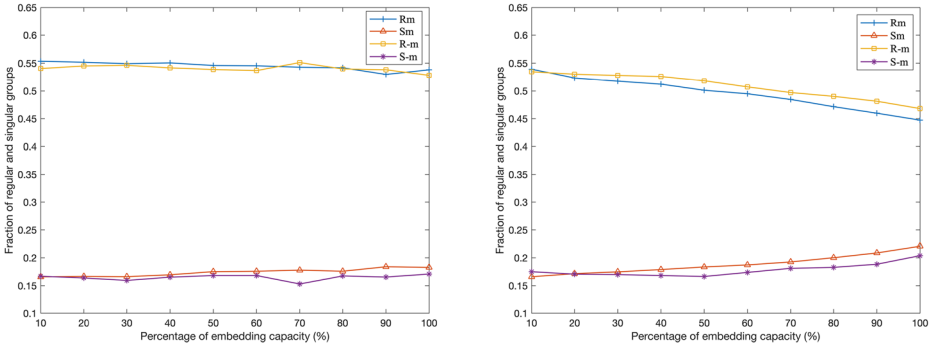


Fig. 14 RS-diagrams yielded by the dual statistics method for cover image 'Lena' produced by Sudoku-based schemes. (**a**) Sudoku method [2] (**b**) 3D-Sudoku method [20]

corresponding RS diagrams can be obtained, where the x-axis signifies the percentage of embedding capacity and the y-axis signifies the percentage of regular and singular groups with mask M and $-M$. The RS steganalysis diagrams of some stego images which are subject to the proposed algorithm as shown in Fig. 13 reflect it can withstand the dual statistical analysis for these well preserved curves. It is apparent upon observation that the experimental results verify that the novel image data hiding algorithm proposed in this paper resists the attack of PDH and RS image steganalysis, and thus has the security attribute.

Furthermore, the comparison experiments with other existing Sudoku-based image steganography [2, 20] have been conducted aiming to demonstrate the outperformance of our proposed data hiding technology with respect to security. It can be intuitively deduced that the RS diagram of 'Lena' image yielded by our scheme (as shown in Fig. 13 (a)) is relatively closer compared to the Chang et al. [2] and Xia et al. [20] schemes (as depicted in Fig. 14) since the expected values of R_m and S_m are seen equal to that of R_{-m} and S_{-m} with the increase percentage of embedding capacity. Accordingly, we can make a solid statement that the *RE-Sudoku* matrix based image steganography proposed in this paper is comparatively more secure against the RS detection attack than other Sudoku-based schemes [2, 20].

To further estimate the security of our proposed algorithm with respect to visual steganalysis, the enhancing LSBs attack [12] is applied. It extracts k LSBs of each pixel in the selected image and then copies them as the most-significant-bits (MSBs) followed by a sequence of 0 bits sized $8-k$ in order to restructure a new pixel. The ultimate formed pattern image can be used to detect the hiding substitution. If the stego-image is produced by LSB embedding method as shown in Fig. 15a, the corresponding attack on it will generate a certain regular pattern which is presented as Fig. 15b. In contrast, when the stego-image shown in Fig. 15c is yielded by the proposed scheme, the pattern image generated via the enhancing LSBs attack will appear in chaos as depicted in Fig. 15d that can successfully avoid the suspicions from malicious attackers.

5 Conclusions

A novel image data hiding algorithm via retracing the extended Sudoku reference matrix (*RE-Sudoku*) is minutely reviewed in this research paper. The principal idea of our proposed

(a) (b) (c) (d)

Fig. 15 Instance 'Elaine' for visual attack via the enhancing LSBs attack ($k = 3$). (**a**) Stego-image generated by LSB substitution (**b**) Enhancing LSBs attack on image (**c**) Stego-image generated by the proposed scheme (**d**) Enhancing LSBs attack on image

scheme is guiding two 9-ary notational system secret digits to be embedded into one pixel pair of the cover image simultaneously, thereby resulting in a larger embedding payload of $log_2 9$ bpp than the other aforementioned image steganography. Owing to the extension operation of original selected Sudoku matrix, each sub-cell can conceal two novenary integers. Furthermore, with consideration of four candidate groups in the 85×85 Sudoku sub-matrix formed later, more points are listed as candidate elements. In this light, retracing the final qualified elements in all candidate sub-cells to opt the more approximate coordinate according to the minimum Euclidean distance, and thus obtain a desirable stego-image visual quality with the PSNR around 40 dB. Herein, the selected reference matrix is similar to the key of encryption algorithm which can guarantee the security of concealed information although this hiding scheme may be disclosed. Since the *RE-Sudoku* construction matrix is multifarious (viz., the number of Sudoku solution and extension direction are various), it is difficult to seek out the concreate reference matrix utilized in the embedding procedure. Therefore, our proposed image steganography is extremely more secure than other related methods because its security not only depends on the confidentiality of embedding technique but also relies on the confidentiality of key matrix. Correspondingly, the experimental analysis demonstrates that this novel scheme has a satisfactory tradeoff between the embedding capacity and visual quality of stego image; meanwhile, it possesses the attack resistance of image steganalysis.

Acknowledgements This research work has been supported by the National Natural Science Foundation of China (No.61972439, No.61702010, No.61672039).

References

1. Bender W, Gruhl D, Morimoto N, Lu A (1996) Techniques for data hiding. IBM Syst J 35(3&4):313–336
2. Chang CC, Chou YC, Kieu TD (2008) An information hiding scheme using Sudoku. In proceedings of the third international conference on innovative computing information and control (IEEE, Dalian, Liaoning, China, 2008):17–17
3. Chang CC, Liu Y, Nguyen TS (2014) A novel turtle Shell based scheme for data hiding. In proceedings of the tenth international conference on intelligent information hiding and multimedia signal processing (IEEE, Kitakyushu, Japan):89–93
4. Davis R (1978) The data encryption standard in perspective. IEEE Commun Soc Mag 16(6):5–9
5. Faez K, Khodaei M (2012) New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing. IET Image Process 6(6):677–686
6. Fridrich J, Goljan M (2002) Practical steganalysis of digital images: state of the art. In Security and Watermarking of Multimedia Contents IV International Society for Optics and Photonics 4675:1–13

7. Hou D, Wang H, Zhang W, Yu N (2018) Reversible data hiding in JPEG image based on DCT frequency and block selection. Signal Process 148:41–47
8. Huang CT, Lin LC, Sun DE, Wang SJ (2019) A security-based steganographic scheme in vector quantization coding between correlated neighboring blocks. Multimed Tools Appl 78(3):3131–3151
9. Hussain M, Wahab AWA, Idris YIB, Ho AT, Jung KH (2018) Image steganography in spatial domain: a survey. Signal Process Image Commun 65:46–66
10. Hussain M, Wahab AWA, Javed N, Jung KH (2018) Recursive information hiding scheme through LSB, PVD shift, and MPE. IETE Tech Rev 35(1):53–63
11. Kim HJ, Kim C, Choi Y, Wang S, Zhang X (2010) Improved modification direction methods. Comput Math Appl 60(2):319–325
12. Liu Y, Chang CC, Nguyen TS (2016) High capacity turtle shell-based data hiding. IET Image Process 10(2):130–137
13. Liu Y, Chang CC, Huang PC (2017) Extended exploiting-modification-direction data hiding with high capacity. In Proceedings of the International Conference on Video and Image Processing (ACM press, Singapore):151–155
14. Mielikainen J (2006) LSB matching revisited. IEEE Signal Process Lett 13(5):285–287
15. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
16. Shen SY, Huang LH (2015) A data hiding scheme using pixel value differencing and improving exploiting modification directions. Comput Secur 48:131–141
17. Tavares R, Madeiro F (2016) Word-hunt: a LSB steganography method with low expected number of modifications per pixel. IEEE Lat Am Trans 14(2):1058–1064
18. Westfeld A, Pfitzmann A (2000) Attacks on Steganographic systems. In Proceedings of International workshop on information hiding (springer, Berlin, Heidelberg):61–76
19. Wu DC, Tsai WH (2003) A steganographic method for images by pixel-value differencing. Pattern Recogn Lett 24(9–10):1613–1626
20. Xia BB, Wang AH, Chang CC, Liu L (2016) An image steganography scheme using 3D-Sudoku. J Info Hiding Multimed Sign Proc 7(4):836–845
21. Yang CH, Weng CY, Wang S-J, Sun H-M (2010) Varied PVD+LSB evading detection programs to spatial domain in data embedding systems. J Syst Softw 83:1635–1643
22. Zhang X, Wang S (2004) Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security. Pattern Recogn Lett 25(3):331–339
23. Zhang X, Wang S (2006) Efficient Steganographic embedding by exploiting modification direction. IEEE Commun Lett 10(11):781–783