ABSTRACT  Medical records are extremely sensitive information and may cause a violation of patients’ rights if the data is captured or altered. Such data requires uncompromising security during transmission or when the data is stored in medical datacenters. The most commonly used procedure is to hide sensitive information inside a cover medium without incurring any increase in data size or computational overhead. Even though many steganography techniques have been proposed in recent years, only a few have addressed issues related to protecting medical data. In this paper, we proposed a data hiding method based on magic cube generated using magic matrix. In the proposed method, 9 bits of secret data were embedded in each group of 4 pixels using secret keys that scattered values in the square template to make it more unpredictable. Experimental results showed that the proposed method achieved an embedding capacity of 2.25 bpp and an average PSNR of 44 dB outperforming previous methods.

INDEX TERMS  Steganography, magic cube, irreversible information hiding, magic matrix, embedding capacity.

I. INTRODUCTION  Medical information in the form of images comprises at least 90% of all the data in medical centers and hospital systems [1]. Medical records (i.e., medical images, medical records etc.) are extremely sensitive patient information and if the data is captured or altered due to cybercrime, it may cause a violation of patients’ rights and changes in medical treatment. Such data is often times transmitted to/from other hospitals or medical centers to improve the diagnostic outcomes and communicate to study a therapeutic patient [2]. Therefore, all patient records, especially medical images, require uncompromising security while data is being transmitted using the public network and also when the data is stored in the medical data center servers monitored by remote systems [3], [4]. Traditionally, private data was protected by using cryptographic methods. However, the downside of cryptography is that it makes the message suspicious enough to attract malicious attention. Alternatively, medical data can also be protected by using steganography techniques.

Steganography deals with concealing the fact that a message carries hidden content (images, files, audio, and video) using a cover medium. The advantage of steganography is that the secret messages carried by the stego image cannot easily attract malicious attention. In other words, it becomes difficult for humans to perceive the secret data in stego-image after it is hidden. Usually, medical records such as X-ray, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), ultrasound, etc. are handled, stored, and transmitted using the Digital Imaging and Communications in Medicine (DICOM) standard. The DICOM standard enables integration between devices, software, and platforms into a picture archiving and communication system (PACS). The DICOM format identifies a header that stores metadata of every image such as image size, data type, representation, etc... and patient information, exam, modality, acquisition parameters, physician, and health center [1], [5], [6]. The patient information in DICOM file must be securely stored within the network to avert tampering, illicit copying, and patient privacy disclosures to ensure copyright protection, and other information related security issues [7].

As the objectives of steganography are imperceptibility, robustness, embedding capacity of the hidden message, and resistance to tampering, the most commonly used procedure is to hide sensitive information inside a cover medium without incurring any increase in the data size and additional...
computational overhead. Considering these objectives, many information hiding techniques based on images have been discussed and studied in recent decades [8]–[11]. In 2004, Chan and Cheng proposed Least Significant Bit (LSB) substitution method [7] in which last 1 to 4 values of a binary cover pixel were replaced with secret data. The drawback of this method was that even though it had a high Embedding Rate (ER) and low distortion level, it was easy to detect the hidden information, making the security of hidden messages poor. In 2006, Zhang and Wang proposed Exploiting Modification Direction (EMD) method [12] which used an import extraction function. The secret message was first represented in (2n + 1)-ary representation system and was then carried by n cover pixels, where n was a system parameter. When n = 2, a Peak Signal To Noise Ratio (PSNR) and ER of 52.11 dB and 1.5 bpp, respectively. In 2018, Lee and Wang proposed a method based on magic signet [19] which achieved a PSNR and ER of 44.12 dB and 1.5 bpp, respectively. In 2014, Lee et al. proposed a method based on magic matrix and the characteristics of Sudoku [16]. This method achieved a PSNR and ER of 49.4 dB and 1.5 bpp, respectively. In 2003, Wu and Tsai proposed Pixel Value Differencing (PVD) method [14] which mainly involved calculating the difference between two pixel pairs. It used an interval scale to determine the length of the secret message that could be hidden. Thereafter, the secret message was embedded by modifying the two pixels. Because the variation was by two pixels, the relative distortion was less. Using this method, the average PSNR value achieved was 40.7 dB, and the ER was 1.5 to 1.6 bpp, depending on the length of interval scale respectively.

In 2014, Chang et al. suggested a data hiding method based on turtle shell [15]. This method used a magic matrix to embed secret messages which achieved a PSNR and ER of 49.4 dB and 1.5 bpp, respectively. In 2008, Chang et al. proposed a method that used magic matrix and the characteristics of Sudoku [16]. This method achieved a PSNR and ER of 44.85 dB and 1.5 bpp, respectively. In 2015, Kurup et al. proposed a method based on an octagon shell [17]. This method used a magic matrix to embed secret messages and achieved a PSNR and ER of 51.7 dB and 2 bpp respectively. In 2017, Lee et al. proposed a method based on magic square [18] which achieved a PSNR and ER of 44.12 dB and 2 bpp, respectively. In 2018, Lee and Wang proposed a method based on magic signet [19]. The magic signet hiding method was based on a 4 × 4 two-dimensional matrix, where values from 0 to 15 were randomly generated in the signet. Secret messages for every 4 bits were carried by two pixels to achieve an average PSNR and ER of 44.12 dB and 2 bpp respectively. The matrix in the above method was mostly constructed in a 2D manner; i.e. the x-axis and the y-axis of the matrix were constructed by a pair of pixels. Thereafter, replacement of coordinate positions was used to embed secret messages. In this paper, a new method based on 3D magic cube is proposed to achieve a higher ER and a good image quality. The proposed method is different from the previous methods based on the 2D matrix as it can be used to hide more secret messages (higher EC) while maintaining an acceptable image quality. The results show that the PSNR ranged from 41.55 to 43.71 dB at a fixed embedding rate of 2.25. The images still maintained a good visual quality at a fixed embedding rate. The proposed method also achieved an embedding capacity of 2.25 bpp and an average PSNR of 43 to 44 dB for nine standard test images. Moreover, the proposed method showcased better imperceptibility than methods [23] and [24] and the ER exceeded than methods [17], [19], [20], and [22] by more than 0.25 bpp. Therefore, the proposed method has more advantages compared to the previous methods. In the next section, we will introduce several related works.

II. RELATED WORKS
A. DATA HIDING SCHEME BASED ON TURTLE-SHAPED SHELLS

In 2014, Chang et al. developed a data hiding scheme based on turtle-shaped shells [15]. In their method, the secret data was represented in a binary format, 3 bits of which were embedded within every 2 pixels. Fig. 1 presents a magic matrix $M$ of size $256 \times 256$ based on turtle-shaped shells. In the matrix $M$, two adjacent elements in the same row have a difference of 1, and two neighboring elements present in the same column have an alternating difference of 2 and 3.

Let $M(p_i, p_{i+1})$ and $M(q_i, q_{i+1})$ be two numbers in the magic matrix $M$, where $(p_i, p_{i+1})$ and $(q_i, q_{i+1})$ represent the pairs of cover pixels and stego pixels, respectively. This is before/after a 3-bit secret data $s_i$ has been concealed.

If the number $M(p_i, p_{i+1})$ falls in a turtle-shaped shell, then the secret number $s_i$ also can be found in the same turtle-shaped shell, such that $s_i = M(q_i, q_{i+1})$. However, if $M(q_i, q_{i+1})$ is a number on the edge, then the number $s_i$ can be found in the surrounding three turtle shells. A calculation needs to be done to find the minimum distance between $(p_i, p_{i+1})$ and $(q_i, q_{i+1})$ under the condition that $s_i = M(q_i, q_{i+1})$. Another special case occurs when the number $M(q_i, q_{i+1})$ is not located in any turtle-shaped shell. The solution, as shown in Fig. 2 is to find the shortest distance between
(p_i, p_{i+1}) and (q_i, q_{i+1}) so that the number \( M(q_i, q_{i+1}) \) equals the secret data \( s_j \).

The limitation of the turtle shell scheme [15] was that the ER was limited. Thereafter, Lee et al. [20] proposed an algorithm based on the shape of a pencil to enhance ER while maintaining a good stego image visual quality. In Lee et al.’s method, each cover pixel pair carried a 4-bit secret data, thereby increasing the ER up to 2 bit per pixel (bpp), which was better than the previous techniques. However, compared to the turtle shell scheme, the pencil-shaped scheme involved more image distortion, which went up to 5 dB.

B. SUDOKU-BASED DATA HIDING SCHEME

In 2008 Chang et al. [16] proposed a Sudoku-based data hiding method which is a logic-based digital jigsaw puzzle designed to fill 9 × 9 squares grid with numbers from 1 to 9. In 1979, Garns invented Sudoku, which was released in 1986 by a Japanese publisher Nikoli and became internationally popular. A Sudoku box has nine 3 × 3 sub-boxes, each containing 1 to 9 digits. Each row and column of the Sudoku grid contains numbers from 1 to 9. Chang et al.’s method based on Sudoku not only improved the ability to hide secret data, but it also improved the security. According to Sudoku’s characteristics, each digit in the Sudoku square was decremented by one so that the square contained numbers from 0 to 8. Then it was required to convert the secret data in binary to a base-9 confidential message, and the pixel value was modified. After three candidate elements were obtained, they were compared with the original pixel \( M(p_i, p_{i+1}) \). Obtaining the candidate element \( M(q_i, q_{i+1}) \) with the shortest distance was the final step. This stego pixel pair \( (q_i, q_{i+1}) \) was then used to hide the secret data.

C. DATA HIDING TECHNIQUE BASED ON OCTAGON-SHAPED SHELL

In 2015, Kurup et al. [17] suggested a method based on octagon-shaped shell. An octagon contains numbers from 0 to 15, which represent four secret bits of secret data. In this method, the first step of the hiding process was to generate a 256 × 256 reference matrix. This matrix had two rules. The difference between adjacent pixels in the same row was set to 1 and the difference between two adjacent pixels in the same column was set to 4 or 5. The reference matrix was connected to multiple octagons. Each octagon had 16 numbers, which included 6 numbers in the middle of the octagon and 10 numbers at the edges. After the matrix was generated in the second step, all the elements were divided into two types: general elements and special elements. General elements referred to the middle or edge numbers in the octagonal line, and special elements referred to the numbers that were not located in any octagon. The pixels were modified according to the rules below:

Rule 1: If \( M(p_i, p_{i+1}) \) is a digit that is located in an octagon, then \( M(q_i, q_{i+1}) \) is one of the digits in this octagon.

Rule 2: If \( M(p_i, p_{i+1}) \) is an edge digit included in at least one octagon, then \( M(q_i, q_{i+1}) \) is one of the digits in all octagons that are adjacent.

Rule 3: If \( M(p_i, p_{i+1}) \) does not belong to any octagon, then \( M(q_i, q_{i+1}) \) is one of all digits in a 4 × 5 sub-block, where \( M(q_i, q_{i+1}) \) is located in the center of the sub-block.

D. DATA HIDING TECHNIQUE BASED ON SECURE MAGIC SIGNET

Furthermore, in 2018, Lee et al. [20] proposed an image hiding scheme based on secure magic signet which involved procedures such as matrix construction, message embedding, and data extraction. Here, a square template of \( N_1 \times N_2 \) digits was first created and then adapted to create a magic matrix of size 256 × 256.

1) CONSTRUCTION OF MAGIC MATRIX

First, a 2D magic matrix was constructed of size \( H \times W \) which was based on a square template of size \( h \times w \). We have used \( H = W = 256 \), and \( h = w = 4 \) as an example shown in Fig. 3. In hexadecimal representation system, 4 bits is denoted using a single digit. The square template contains \( N_1 \times N_2 \) digits ranging from 0 to \((N_1 \times N_2 - 1)\). The square template is like a seal affixed to the 2D matrix in a non-overlapping manner so that the magic matrix can be created.

2) GENERATION OF SECURE MAGIC SIGNET BY USING SECURE KEYS

A secure key \( SK_1 \) was used to generate a square template which generated \( 16! \approx 2.1e + 13 \) templates. Also,
The pixels are then categorized into pairs, so that each pair \((p'i, p'i+1)\) can be considered as a coordinate of the 2D magic matrix. Let \(M(p'i, p'i+1)\) and \(M(qi, qi+1)\) be the numbers in the magic matrix \(M\), where \((p'i, p'i+1)\) and \((qi, qi+1)\) represent the pairs of pixels before and after a 4-bit secret number \(s_j\) has been concealed, respectively. For a given secret digit \(s_j\) associated to a pixel pair \((p'i, p'i+1)\), the stego pixel pair \((qi, qi+1)\) can be resolved by finding the shortest distance between \((p'i, p'i+1)\) and \((qi, qi+1)\) under the condition that \(M(qi, qi+1)\) is equal to the secret data \(s_j\). The proposed scheme takes \((p'i, p'i+1)\) as the center location to find the nearest position, where \(M(qi, qi+1) = s_j\), without considering, whether the entry with the coordinate \((qi, qi+1)\) is located within the square matrix or not. This thereby increases the stego image quality.

### III. PROPOSED SCHEME

This section introduces the proposed method using an example. First the cover image is divided into \(2 \times 2\) non-overlapping blocks. Each block is represented by four cover pixels \((p1, p2, p3, p4)\), and the cover pixel value \(p1\) is located at the upper left-hand corner, \(p2, p3, p4\) are located at the upper right-hand, the lower left-hand, and the lower right-hand corners, respectively. A partial secret message is hidden into cover pixel value \(p1\) by using the LSB substitution hiding method and the stego-pixel value becomes \(q1\). Then the absolute difference \(d1, d2, d3\) of \(q1\) for \(p2, p3, p4\) is calculated and then contrasted with the coordinate position in the 3D magic cube such that \((x, y, z) = (d1, d2, d3)\). Each coordinate position \((x, y, z)\) in the magic cube carries a decimal value which is defined as \(M(d1, d2, d3)\).

The general data hiding method uses a matrix of two dimensions. However, to increase the embedding capacity and improve the image quality, a data hiding method based on a 3D magic cube is proposed in this paper. In the embedding procedure, a new coordinate \((x, y, z)\) is found around the coordinates of \((x, y, z) = (d1, d2, d3)\). The data \(s\) is then carried by finding the position \((d1, d2, d3)\) where \(M(d1, d2, d3) = s\). The inversion formula is applied to obtain the stego-pixel values. Thereafter, the original pixel values \((p1, p2, p3, p4)\) are modified to the stego-pixel values \((q1, q2, q3, q4)\).

#### A. 3D ARRAY CONSTRUCTION PROCEDURE

First, a 3D array is created. Before hiding secret data, 3D coordinate system is used to create a stereoscopic 3D array. The size is \(N_x \times N_y \times N_z\), where \(N_x = N_y = N_z = 256\). Then a 3D magic cube is designed according to some rules. The range of its x-axis is \(0 \leq x < n_x\), the range of its y-axis is \(0 \leq y < n_y\), and the range of its z-axis is \(0 \leq z < n_z\). An example of a magic cube with 3D array is displayed in Fig. 5.

To describe this magic cube, \(n_x = n_y = n_z = 4\) is taken as an example. The magic cube is composed of \(4^3 = 64\) small cubes. Each small cube has a corresponding coordinate \((x, y, z)\) and a magnitude \(M(x, y, z)\), where \(0 \leq (x, y, z) \leq 255\).
and $0 \leq M(x, y, z) \leq 63$. Therefore, in the $4 \times 4 \times 4$ magic cube, the coordinates will have numbers 0 to 63 and there will be 64 unrepeatable random values. Thereafter, the $256 \times 256 \times 256$ three-dimensional array is filled by stamping the signet. Fig. 6 shows a $4 \times 4 \times 4$ magic cube. One of the number $M(3, 3, 0) = 15$ is located at the coordinate $(3, 3, 0)$.

**B. EMBEDDING PROCEDURE**

The cover image $I$ is first divided into $2 \times 2$ non-overlapping blocks. Each block is represented by four cover pixels $(p_1, p_2, p_3, p_4)$. Then a $k_1$-bit data $s_1$ is extracted from the left side of secret message $S$. Secret data $s_1$ is hidden into the cover pixel $p_1$ using the LSB substitution data hiding method to become $q_1$. Then three absolute differences $d_1 = \text{abs}(q_1, p_2)$; $d_2 = \text{abs}(q_1, p_3)$; $d_3 = \text{abs}(q_1, p_4)$ are calculated, where the abs function computes an absolute value such that $d_1 \geq 0$, $d_2 \geq 0$, $d_3 \geq 0$.

Next, a $k_2$-bit data $s_2$ is extracted from the remaining secret message and the position $(d_1', d_2', d_3')$ is found which is nearest to the position $(d_1, d_2, d_3)$ and $M(d_1', d_2', d_3') = s_2$. Thereafter, the relationship is checked between $s_2$ and the value $M(d_1, d_2, d_3)$ by applying the following rules:

Case (1):

If $s_2 = M(d_1, d_2, d_3)$, then $(q_2, q_3, q_4) = (p_2, p_3, p_4)$.

Case (2):

If $s_2 \neq M(d_1, d_2, d_3)$, then $\exists (d_1', d_2', d_3')$, $d_1' \in ([d_1] - 7 : [d_1] + 7)$, $d_2' \in ([d_2] - 7 : [d_2] + 7)$, $d_3' \in ([d_3] - 7 : [d_3] + 7)$; s.t. $s_2 = M(d_1', d_2', d_3')$ and

The above steps are repeated until all the secret messages are hidden, and the stego image $I'$ is the output. Fig. 7 shows the flow chart of the embedding procedure.

**C. ILLUSTRATION OF THE EMBEDDING PROCEDURE**

Let us take an example that a secret message $S = (11001111)_2$ needs to be transmitted through a block with four pixels $(p_1, p_2, p_3, p_4) = (10, 12, 13, 14)$ from the original cover image. The embedding procedure can be illustrated as follows as shown in Fig. 8.

First, a 3-bit data $s_1 = (110)_2$ is extracted from the left side of secret message $S$. Secret data $s_1$ is hidden into the cover pixel $p_1$ using the LSB substitution data hiding method to become $q_1 = (00001110)$ as shown in Fig. 8(a). Then three absolute difference values,

\[d_1 = \text{abs}(q_1, p_2) = |14 - 12| = 2,\]
\[d_2 = \text{abs}(q_1, p_3) = |14 - 13| = 1,\] and
\[d_3 = \text{abs}(q_1, p_4) = |14 - 14| = 0,\]

are calculated as shown in Fig. 8(b).

Next, a 5-bit data $s_2 = (01111)_2 = 15$ is extracted from the remaining secret message. Since $M(d_1, d_2, d_3) = (2, 1, 0)$ which is not equal to the sub-message $s_2$, we cannot choose the first rule, but should choose the second rule to hide the second piece of information. According to the relationship between $s_2$ and the cubic value on the position $(d_1, d_2, d_3) = (2, 1, 0)$, $i$ locations are found near the position $(d_1', d_2', d_3')$, each of which has a value of 15. In Fig. 8(c) there are two locations with the position $(d_1', d_2', d_3') = (3, 0, 0)$ and $(d_1', d_2', d_3') = (3, 3, 0)$ which are near neighbors to the position $(d_1, d_2, d_3) = (2, 1, 0)$ such that the value $M(d_1', d_2', d_3') = M(3, 0, 0) = M(2, 1, 0) = 15$ and the value $M(d_1', d_2', d_3') = M(3, 3, 0) = M(2, 1, 0) = 15$. From Figure 8(d), we know that the
distance 2 from the position \((d'_{11}, d'_{21}, d'_{31})\) to the position \((d_{12}, d_{22}, d_{32})\). Thus \((d'_{11}, d'_{21}, d'_{31}) = (3, 0, 0)\) is used to hide the 5-bit data \(s_2 = (01111)\) in a decimal form. Then the pixel value on the top left \(q_1\) is used to extract the \(k_1\)-bit secret data \(s_1\) on the rightmost side of \(q_1\). The secret data \(s_2\) is converted from decimal to binary and \(s_1||s_2\) are concatenated. Finally in the last step \((k_1 + k_2)\)-bit secret data hidden in the block is extracted.

**D. MESSAGE EXTRACTION PROCEDURE**

The stego image is cut into 2 \(\times\) 2 non-overlapping blocks, and each block is represented by four cover pixels \((q_1, q_2, q_3, q_4)\). First, \((q_1, q_2, q_3, q_4)\) of the absolute difference is calculated such that \(d'_{11} = q_1 - q_2, d'_{21} = q_1 - q_3, d'_{31} = q_1 - q_4\).

Thereafter, by knowing the coordinate point \((d'_{11}, d'_{21}, d'_{31})\), the position values \(M(d'_{11}, d'_{21}, d'_{31})\) are obtained, which is the secret data \(s_2\) in a decimal form. Then the pixel value on the top left \(q_1\) is used to extract the \(k_1\)-bit secret data \(s_1\) on the rightmost side of \(q_1\). The secret data \(s_2\) is converted from decimal to binary and \(s_1||s_2\) are concatenated. Finally in the last step \((k_1 + k_2)\)-bit secret data hidden in the block is extracted.

**IV. EXPERIMENTAL RESULTS**

We used MATLAB R2017a platform to carry out the experiment. To evaluate performance of the proposed method, six medical images were used from the DICOM library [28] as the first set of test images shown in Fig. 9. The medical images had different textures and were applied through DICOM outcome. The second set of test images were
standard grayscale images used from the University of Southern California-Signal and Image Processing Institute (USC-SIPI) image database [21] as shown in Fig. 10. These images included the images of Lena, Baboon, Peppers, Boat, Airplane, Tiffany, Elaine, House, and Pirate.

To avoid subjective evaluation of human vision, a well-known measurement, peak signal to noise ratio (PSNR) is used to assess the degree of similarity between a hidden image and its original image. The equation for PSNR is defined in the following (1). For (2), the mean square error (MSE for short) stands for the difference between the stego-image and its original image sized $H \times W$ pixels. The higher the value of the peak signal to noise ratio, the better is the image quality, and the embedded secret messages cannot be easily perceived by the human eyes.

Embedded capacity (EC) also called payload is also an important metric to measure embedding performance. EC is measured by the maximum number of embedding bits. We use (3) to define the embedding rate (ER) to represent the maximum number of secret bits embedded in all pixels of the cover image. A high-capacity image can carry more secret messages at one time.

$$\text{PSNR} = 10 \times \log_{10} \left( \frac{255^2}{\text{MSE}} \right) \quad (1)$$

$$\text{MSE} = \frac{1}{H \times W} \sum_{i=1}^{H} \sum_{j=1}^{W} (I(i,j) - I'(i,j))^2 \quad (2)$$

$$\text{ER} = \frac{\text{EC}}{H \times W} \quad (3)$$

($H$ is the height of image, $W$ is the width of image, $I$ is the original image, and $I'$ is the cover image, EC is the embedding capacity.)

The proposed 3D cube-based data hiding method is a new method, which is different from the methods based on the 2D matrix. The proposed method increases the EC without much reduction in the image quality.

Table 1 showcases the PSNR of six medical test images as seen in Fig. 8. At a fixed embedding rate of 2.25, the PSNR ranged from 41.55 to 43.71 dB. The results show that medical images still maintained a good image quality at a fixed embedding rate.

Table 2 presents the PSNR, EC and ER for nine standard test images using the 3D magic cube method. The proposed method achieved an embedding rate of 2.25 bpp and an average PSNR of 43.99 db.
TABLE 3. Comparison of the proposed method with methods of Chang et al., Lee et al and Kurup et al.

| Image          | Lena    | Baboon  | Peppers | Boat   | Airplane | Average |
|----------------|---------|---------|---------|--------|----------|---------|
| Turtle-shape   | PSNR    | 49.42   | 49.39   | 49.40  | 49.40    | 49.39   | 49.40   |
|                | ER [bpp]| 1.5     | 1.5     | 1.5    | 1.5      | 1.5     | 1.5     |
| Sudoku         | PSNR    | 44.97   | 44.68   | 44.67  | 44.94    | 45.02   | 44.86   |
|                | ER [bpp]| 1.5     | 1.5     | 1.5    | 1.5      | 1.5     | 1.5     |
| Octagon-shape  | PSNR    | 51.84   | NA      | 51.11  | 51.80    | NA      | 51.58   |
|                | ER [bpp]| 2       | 2       | 2      | 2        | 2       | 2       |
| Pencil-shape   | PSNR    | 42.87   | 42.88   | 42.88  | 42.88    | 42.84   | 42.87   |
|                | ER [bpp]| 2       | 2       | 2      | 2        | 2       | 2       |
| Magic signet   | PSNR    | 44.14   | 44.14   | 44.14  | 44.02    | 44.17   | 44.12   |
|                | ER [bpp]| 2       | 2       | 2      | 2        | 2       | 2       |
| 3D-sudoku      | PSNR    | 43.31   | 41.25   | 41.30  | 41.23    | 41.28   | 41.27   |
|                | ER [bpp]| 2       | 2       | 2      | 2        | 2       | 2       |
| Proposed scheme| PSNR    | 43.97   | 44.09   | 44.00  | 44.03    | 43.95   | 44.00   |
|                | ER [bpp]| 2.25    | 2.25    | 2.25   | 2.25     | 2.25    | 2.25    |

TABLE 4. Comparison of main methods and PVD related methods.

| Image                  | Lena    | Baboon  | Peppers | Boat   | Airplane | Average |
|------------------------|---------|---------|---------|--------|----------|---------|
| Khodaei and Faez (Type 3 k=21)[21] | PSNR    | 37.63   | 36.29   | 37.97  | 37.29    | NA      | 37.30   |
|                        | ER [bpp]| 3.09    | 3.38    | 3.06   | 3.13     | NA      | 3.12    |
| Jung (2012)[24]        | PSNR    | 36.28   | 35.94   | 36.10  | NA       | 36.20   | 36.13   |
|                        | ER [bpp]| 3.00    | 3.00    | 3.00   | NA       | 3.00    | 3.00    |
| Mandal and Das (2012)[25] | PSNR    | 42.26   | 38.44   | 42.28  | NA       | 42.60   | 41.39   |
|                        | ER [bpp]| 0.6     | 0.6     | 0.6    | NA       | 0.6     | 0.6     |
| Chen (2014)[26]        | PSNR    | 43.70   | 41.70   | 43.40  | 42.70    | 44.10   | 43.12   |
|                        | ER [bpp]| 1.6     | 1.75    | 1.7    | 1.6      | 1.6     | 1.65    |
| Shen and Huang (2015)[27] | PSNR    | 42.46   | 38.88   | 42.58  | 41.60    | NA      | 41.41   |
|                        | ER [bpp]| 1.5     | 1.7     | 1.5    | 1.6      | NA      | 1.6     |
| Proposed scheme        | PSNR    | 43.97   | 44.09   | 44.00  | 44.03    | 43.95   | 44.00   |
|                        | ER [bpp]| 2.25    | 2.25    | 2.25   | 2.25     | 2.25    | 2.25    |

Table 3 compares the proposed method with the 2D matrix methods of Chang et al. [15], Kurup et al. [17], Lee and Wang [19] and Lee et al. [20], and Xia et al. [22]. The embedding rate of the proposed method is 2.25 bpp. It exceeds the octagon-shape [17], pencil-shape [20], magic signet [19], and 3D-sudoku [22] methods by more than 0.25 bpp. Notwithstanding the increased embedding rate, the PSNR does not reduce considerably. The average PSNR of the proposed method is 44 dB, which is higher than pencil-shape [20] and 3D-sudoku [22] methods.

Table 4 shows a comparison of our proposed method with the PVD methods, which include the methods of Khodaei and Faez [23], Jung [24], Mandal and Das [25], Chen [26], and Shen and Huang [27]. The results show that the EC of the proposed method is lower than methods [23] and [24] by about 1 bpp. However, the PSNR is about 6 dB higher. Moreover, it has better imperceptibility than methods [23] and [24]. In addition, the PSNR of the proposed method is higher than methods [25], [26], and [27] by a small difference; however, its embedding rate (bpp) is about 7 dB higher. The method can be used to hide more secret messages while maintaining an acceptable PSNR.

Figure 11 shows the PSNR of the methods of Khodaei and Faez [23], Jung [24], Mandal and Das [25], Chen [26], Shen and Huang [27], and the proposed method. The PSNR varies considerably for the test images of Lena, Baboon, Peppers, Boat, and Airplane. The PSNR variation for the Jung’s method [24] and the proposed method are relatively stable, compared to Khodaei and Faez [23], Mandal and Das [25], Chen [26], and Shen and Huang [27] methods.

V. CONCLUSION

With the objective to solve issues related to protecting medical data, we proposed a data hiding method in this paper, which is based on magic cube generated using magic matrix. In the proposed method, 9 bits of secret data were embedded in each group of 4 pixels using secret keys, maintaining the image quality at an average of 44.00 db. Compared to other 2D matrix methods, the proposed magic cube method achieved a higher EC and a stable image quality. Currently, there are not many 3D-based data hiding methods and future studies can carry out further research to design a better magic cube to further upgrade the image quality and ER.

REFERENCES

[1] L.-Q. Kuang, Y. Zhang, and X. Han, “Watermarking image authentication in hospital information system,” in Proc. Int. Conf. Inf. Eng. Comput. Sci., Dec. 2009, pp. 1–4.
[2] S. Chakraborty, S. Samanta, D. Biswas, N. Dey, and S. Chaudhuri, “Particle swarm optimization based parameter optimization technique in medical information hiding,” in Proc. IEEE-ICCIC, Madurai, India, Dec. 2013, pp. 1–6.
[3] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, “Relevance of watermarking in medical imaging,” in Proc. IEEE EMBS Int. Conf. Inf. Technol. Appl. Biomed., Arlington, VA, USA, Nov. 2000, pp. 250–255.
[4] Internet. Accessed: Apr. 23, 2015. [Online]. Available: https://www.benton.org/headlines/medical-data-has-become-next-cybersecurity-target
[5] Internet: About DICOM. The National Electrical Manufacturers Association (NEMA). Accessed: Apr. 23, 2015. [Online]. Available: http://medical.nema.org/Dicom/about-DICOM.html
[6] M. Haidekker, Image Storage, Transport, and Compression. Hoboken, NJ, USA: Wiley, 2011, pp. 386–412.
[7] C.-K. Chan and L. M. Cheng, “Hiding data in images by simple LSB substitution,” Pattern Recognit., vol. 37, no. 3, pp. 469–474, Mar. 2004.
X.-Z. Xie, Y. Liu, and C.-C. Chang, “Extended squared magic matrix for embedding secret information with large payload,” Multimedia Tools Appl., vol. 78, no. 14, pp. 19045–19059, Feb. 2019.

Y. Liu and C.-C. Chang, “A turtle shell-based visual secret sharing scheme with reversibility and authentication,” Multimedia Tools Appl., vol. 77, no. 19, pp. 25295–25310, Feb. 2018.

L. Liu, C.-C. Chang, and A. Wang, “Data hiding based on extended turtle shell matrix construction method,” Multimedia Tools Appl., vol. 76, no. 10, pp. 12233–12250, May 2016.

C.-F. Lee and Y.-X. Wang, “An image hiding scheme based on pixel value differencing and improving exploiting modification directions,” IEEE Commun. Lett., vol. 10, no. 11, pp. 781–783, Nov. 2006.

W.-C. Kuo, L.-C. Wuu, C.-N. Shyi, and S.-H. Kuo, “A data hiding scheme with high embedding capacity based on general improving exploiting modification direction method,” in Proc. 9th Int. Conf. Hybrid Intel1. Syst., Shenyang, China, 2009, pp. 69–73.

D.-C. Wu and W.-H. Tsai, “A steganographic method for images by pixel-value differencing,” Pattern Recognit. Lett., vol. 24, nos. 9–10, pp. 1613–1626, Jun. 2003.

C. C. Chang, Y. Liu, and T. S. Nguyen, “A novel turtle shell based scheme for data hiding,” in Proc. 10th Int. Conf. Inf. Hiding Multimedia Signal Process., Kitakyushu, Japan, Aug. 2014, pp. 89–93.

C.-C. Chang, Y.-C. Chou, and T. D. Kieu, “An information hiding scheme using sudoku,” in Proc. 3rd Int. Conf. Innov. Comput. Inf. Control, Liaoning, China, 2008, p. 17.

S. Kurup, A. Rodrigues, and A. Bhise, “Data hiding scheme based on octagon shaped shell,” in Proc. Int. Conf. Adv. Comput. Commun. Signal Process., IEEE, 2007, pp. 1613–1626.

C.-F. Lee, Y.-X. Wang, and A.-T. Shi, “Image steganographic method based on pencil-shaped pattern,” in Proc. ICMWT, Taichung, Taiwan, 2017, pp. 301–305.

C. F. Lee and Y. X. Wang, “An image hiding scheme based on magic signet,” J. Electron. Sci. Technol., vol. 18, no. 1, 2020, doi: 10.11989/JEST.1674-862X.8020620.

C.-F. Lee, Y.-X. Wang, and A. T. Shi, “Image steganographic scheme based on pencil-shaped pattern,” in Proc. ICMWT, Singapore: Springer, 2017, pp. 639–644.

B. B. Xia, A. H. Wang, C. C. Chang, and L. Liu, “An image steganography scheme using 3D-Sudoku,” J. Inf. Hiding Multimedia Signal Process., vol. 7, no. 4, pp. 836–845, 2016.

M. Khodaei and K. Faez, “New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing,” IET Image Process., vol. 6, no. 6, pp. 677–686, Aug. 2012.

W.-C. Kuo, Y.-H. Chen, and Y.-C. Huang, “High-capacity steganographic method based on division arithmetic and LSB replacement,” Imag. Sci. J. vol. 180, pp. 213–221, 2012.

J. K. Mandal, “Colour image steganography based on pixel value differencing in spatial domain,” Int. J. Inf. Sci. Techn., vol. 2, no. 4, pp. 83–93, Jul. 2012.

J. Chen, “A PVD-based data hiding method with histogram preserving using pixel pair matching,” Signal Process., Image Commun., vol. 29, no. 3, pp. 375–384, Mar. 2014.

S.-Y. Shen and L.-H. Huang, “A data hiding scheme using pixel value differencing and improving exploiting modification directions,” Comput. Secur., vol. 48, pp. 131–141, Feb. 2015.

DICOM Library. Accessed: Nov. 1, 2019. [Online]. Available: https://www.dicomlibrary.com

Y.-Z. Xie, Y. Liu, and C.-C. Chang, “Extended squared magic matrix for embedding secret information with large payload,” IEEE Access, vol. 7, pp. 141414–141425, 2019.

C. F. Lee, Y. X. Wang, and A. T. Shi, “A mini-sudoku matrix-based data embedding scheme with high payload,” IEEE Access, vol. 7, pp. 141414–141425, 2019.

S.-Y. Shen and L.-H. Huang, “A data hiding scheme using pixel value differencing and improving exploiting modification directions,” in Proc. 9th Int. Conf. Hybrid Intel1. Syst., Shenyang, China, 2009, pp. 69–73.

Y.-X. Wang received the Ph.D. degree in computer science and information engineering from National Taiwan University, Taiwan, in 1998. He is currently a Professor of information management with the Chaoyang University of Technology, Taiwan. Her research interests include steganography, image processing, information retrieval, and data mining.

J. K. Mandal, “Colour image steganography based on pixel value differencing in spatial domain,” Int. J. Inf. Sci. Techn., vol. 2, no. 4, pp. 83–93, Jul. 2012.

J. Chen, “A PVD-based data hiding method with histogram preserving using pixel pair matching,” Signal Process., Image Commun., vol. 29, no. 3, pp. 375–384, Mar. 2014.

S.-Y. Shen and L.-H. Huang, “A data hiding scheme using pixel value differencing and improving exploiting modification directions,” Comput. Secur., vol. 48, pp. 131–141, Feb. 2015.

DICOM Library. Accessed: Nov. 1, 2019. [Online]. Available: https://www.dicomlibrary.com

Y.-Z. Xie, Y. Liu, and C.-C. Chang, “Extended squared magic matrix for embedding secret information with large payload,” IEEE Access, vol. 7, pp. 141414–141425, 2019.