

# Hiding health report in X-ray images to protect people privacy

Enas Ali Jameel, Sameera Abbas Fadhel

Department Computer Science, College of Computer Science and Mathematics, University of Mosul, Mosul, Iraq

---

## Article Info

### Article history:

Received Apr 24, 2021

Revised Mar 10, 2022

Accepted Mar 18, 2022

---

### Keywords:

Steganography

Sudoku method

Turtule shell hiding algorithm

X-ray images

---

## ABSTRACT

X-rays images are a popular medical diagnoses method. These images are hard to read and to be understandable outside the medical community. However, the radiologist writes a report of the X-ray. This report can be understandable easily which, can impact the privacy of the patients' medical records. To tackle this issue, in this work, X-ray image steganography algorithm based on Sudoku mathematical game is proposed. The method converts the image into triangular shaped blocks. Subsequently, the data is encoded and segmented two bits at the time to be embedded in the image. To evaluate the algorithm, eight different X-ray images from all X-ray types have been utilized for data hiding process. The algorithm has been compared to the lest significant bit (LSB) and the turtle shell algorithms using the mean square error (MSE) and peak signal to noise ratio (PSNR) performance metric. The proposed algorithm obtained higher bit per pixel embedding capacity with 2 bpp which is higher than LSB and turtle shell. Moreover, the algorithm has higher PSNR compared to turtle shell algorithm.

*This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.*



---

## Corresponding Author:

Enas Ali Jameel

Department Computer Science, College of Computer Science and Mathematics

University of Mosul, Mosul, Iraq

Email: Enasaljameel@uomosul.edu.iq

---

## 1. INTRODUCTION

The main steganography is the field of encryption that hides different information in other digital content. Videos, images, texts and audio files can be utilized to hide the data [1]. This process is utilized to transmit or store the data without any suspicious of hackers or any man in the middle. This method is utilized to enhance the data cryptography. Image steganography has dominated [2]. In the method, an image, known as the cover image, is leveraged to hide different data, such as, text, videos or other images [3], to be transmitted over unsecure and public networks, such as, the Internet. The hidden data or information follow a number of preprocessing steps, such as, encoding, compression and sometimes encryption using different symmetric encryption algorithms, such as, data encryption standard (DES) and advanced encryption standard (AES) [4].

In image steganography, five main parameters are used to assess and evaluate the image hidden techniques. First, the visual quality of the image after the data hiding process should be acceptable. In other words, anyone look to the image should not find any visual quality issues. Second, the capacity of the data that can be hidden in the image should be as much as possible. However, when the data capacity of the hidden data is increased the quality of the image decreases. Third, if the cover image is captured by a third party and the figured the image has been modified, the original data should be hard to restructure or understandable. Fourth, the size of the cover image before and after the hiding process should be the same. This process is the same as the output of any encryption algorithms. In this way, no new transmission or storage overheads are required. Finally, the computational power required to hide the data in the cover image should not add massive overhead since these techniques may be utilized in low battery and low-computational power

devices, such as, smartphones and different Internet of things devices. These devices generate massive amount of data from their attached sensors and required to be transmit safely to other location for processing [5].

In image-data hiding techniques, any type of images can be utilized for the steganography process. However, most of these techniques utilize gray scale images [6]-[8]. When gray scale images are transmitted or exchanged passive attackers on these systems may suspicious especially if well-known colorful images are used in the process. However, if the cover images are gray scale or black-white images, no suspicious is found. One of the most popular gray scale images are the x-ray images that radiologists captured for different parts of the human body for different type of diagnosis. The information found in these images is private information. The radiologists are responsible of extracting useful information from these images. Subsequently, they write a report for the doctors to summarize what can be found in these images for further diagnosis. In other words, the useful information in these images is hard to be seen by normal humans if the report that summarizes the image is hidden. Steganography can hide this report in the X-ray image.

Hiding massive capacity data in images without impacting their visual quality attracted the researchers over the years. Many methods and techniques have been proposed. One of the oldest and most popular techniques is to hide the data in the least significant bit (LSB) of every pixel in the grayscale image [9]. This technique is simple, however the capacity of the data embedded is small since each pixel hide only one bit '1 bpp'. Moreover, the original cover image cannot be obtained and the data can be detected and extracted easily by attackers. Many researchers attempted to modify this technique. In [10], LSB hiding technique and proposed the pixel direction method that hides two data bits by reversing the direction of pixel pair. Zhang and Wang [11], proposed the exploiting modification direction algorithm (EMD). In this technique a number of pixels are used as a cover to hide different type number of bits. However, the capacity of this technique is 1 bpp. To increase the capacity of EMD, EMD-2 and 2EMD have been proposed in [12]. Pramanik *et al.* [13], attempted to send completely automated public turing test to tell computers and humans apart (CAPTCHA) data hidden in a cover image utilizing LSB. However, to enhance the security of the data, the CAPTCHA is encrypted before transmitting. Al-Momin *et al.* [14], attempted to enhance the capacity and security by converting the image into blocks and utilizes LSB to embed the data in the cover image in two methods to enhance the peak signal to noise ratio (PSNR) of the cover image. In [15], LSB and secret maps techniques have been utilized to enhance the security of data embedding in the cover image. A random insertion process is used to reduce the impact of data regenerating by hackers. In [16], LSB and knight tour algorithm has been utilized to randomize the data embedding process. In [17], the security enhancement of data embedding utilizing LSB used 5D hyper-chaos system. All of these enhancements attempted to randomize the embedding process or to encrypt the data before the embedding process. All of these techniques did not enhance the data embedding capacity.

To increase the capacity of the hidden data, sudoku math game has been utilized. In this game, a matrix called a reference matrix consists of 9 rows, 9 columns, and 9 blocks are constructed. The idea of this game is fill in the matrix with the numbers from 1 to 9 in a way that each block, row and column have the numbers without duplication. This game has been utilized since the digital images are two-dimensional matrices. Moreover, the hidden data can be viewed as the numbers that should be filled in Sudoku game. This method has been utilized in [18], [19]. However, the visual quality of the output image was low. Chang *et al.* [20], modified the blocks in the Sudoku game to generate a hexagonal shaped block. This method has been called turtle shell method. These hexagonal shaped blocks consisted of 8 numbers. This reduced the number in Sudoku blocks from 9 numbers to 8 numbers. This reduction allowed the authors to easily encodes the data and generate a sequence of bits that can be segmented into three bits. These three bits can be hidden in the turtle shell blocks. However, the capacity of this technique is only 1.5 bpp.

Yang *et al.* [21], the differences between two adjacent pixels have been utilized to hide data. The proposed algorithm named pixel-value differencing (PVD) that has been proposed reduced the visual quality of the output image. To enhance the visual quality of PVD, machine learning has been utilized in [22].

The capacity of the turtle shell technique motivated researchers to propose a new data embedding methods to increase the number of hidden bits per pixels. In [6], the authors modified the original turtle shell method to embed 4 bits rather than 3 bits in each pixel pair. This process enhanced the capacity from 1.5 bpp to 2 bpp. In [23], two layers shell has been constructed to improve the capacity of the process. In [24], a novel embedding process has been proposed to increase the capacity of the data by creating a new data embedding matrix with different 4 bits. In [25], a modified version of the turtle shell has been proposed to embed smartphones data into cover images to enhance the storage capacity. The proposed method utilizes a very simple blocks in the cover image which can be easily cracked.

In this work, a new image data hidden algorithm based on the turtle shell hiding process [20] is proposed, named triangle blocks X-ray steganography (TBXS). This algorithm is proposed to hide the X-ray reports written by the radiologists inside the X-ray image to enhance the privacy of the data in one hand and to keep the image and the report in the same file for further analysis and diagnosis by the doctors on the other hand. The proposed algorithm increases the capacity of the hidden data in the image by a modified shell that

leverage triangles with four pixels rather than eight pixels as in the original turtle shell algorithm. The algorithm has been written and evaluated with different types of X-ray images. Our results have shown that the modified triangle shapes can increase the capacity of the hidden data and has no impact on the quality of the utilized image.

The rest of this paper is utilized as follows: section 2 introduces triangle blocks X-ray steganography (TSXS) data embedding and extraction processes. Section 3 overviews the experiment and discuss the obtained results. We conclude this paper in section 5.

## 2. TRIANGLE BLOCKS X-RAY STEGANOGRAPHY THE PROPOSED METHOD

Explaining TBXS is a lightweight simple algorithm. It adopts the permutation process leveraged in any encryption algorithm. It is based on the Sudoku math and adopts a similar turtle shell extraction and embedding process. The algorithm has three main steps: reference matrix generating, the embedding, and the extraction process. The following subsections describe these steps. Figure 1 shows the flow chart of the proposed method.

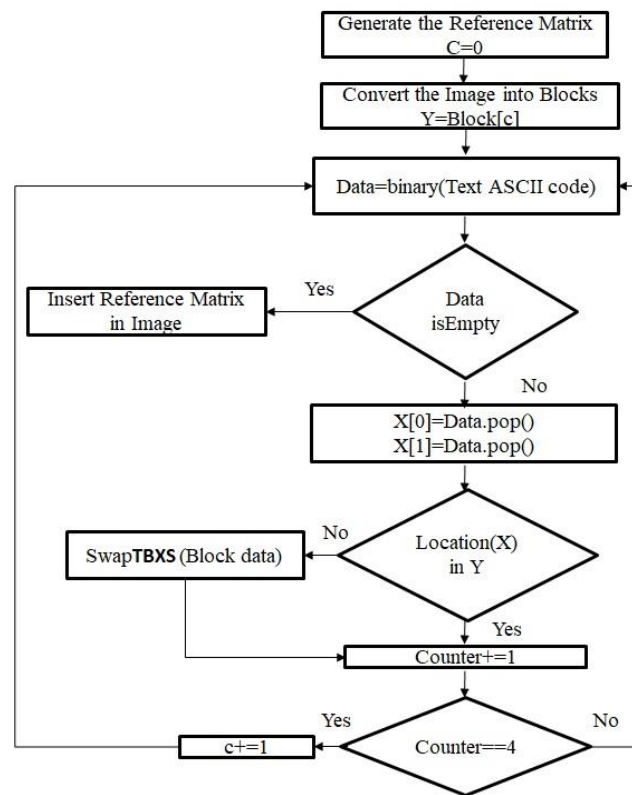


Figure 1. Flowchart of TBXS

### 2.1. The reference matrix

The algorithm generates a 2D matrix, called the reference matrix. This matrix is constructed with the same size of the image that will be utilized to hide the data. This image is called the cover image. The size of this matrix is small. Each cell of this matrix is two bits only, which means that an image of  $800 \times 600$  pixels requires approximately 117 bytes for this matrix if the entire image is used for the steganography process. However, the size of this matrix should be smaller than the size of the image since the cover image also will be utilized to carry the matrix after the permutation process. The reference matrix is filled in way similar to turtle shell algorithm to solve the Sudoku game. Four numbers are used to fill the matrix from zero to three. These numbers are presented in binary form using two bits. To fill in the matrix, the first row has to be filled with the number in increment way using (1). With the first cell equal zero. This means that the value in the rows differs with '1'.

$$\text{Cell}_i = (\text{cell}_{i-1} + 1) \bmod 4 \quad (1)$$

After the first row is filled, the columns of the matrix are filled with the numbers by adding '2' and '3'. When the matrix is filled, virtual triangle shapes is constructed using four cells, one cell in one row and the other three in another row. These triangles have all the numbers without duplications. Figure 2 shows the generated matrix of size 7×6 with the virtual triangle's blocks.

We can observe from Figure 2 that the cells of the matrix are two types: internal and external. The internal cells are the cells that belong to at least one triangle and the external cells are the cells that have no triangles, colored in blue. Moreover, the four cells in each triangle are edge cells, colored in red, and a core cell, colored in green. Each cell in the matrix is mapped to one pixel in the cover image. It worth mentioning that there is a relation between the size of the matrix and the data to be hidden as in (2) and its size cannot exceed the size of the image.

$$\text{Matrix} = \frac{\text{data (bits)}}{2} \quad (2)$$

The reference matrix is utilized in the embedding and the extraction process. However, for the extraction process, the matrix has to be transmitted from the source to the destination. To do that, the matrix can be embedded also in the cover image by stealing the last two bits from the black pixels in the X-ray image.

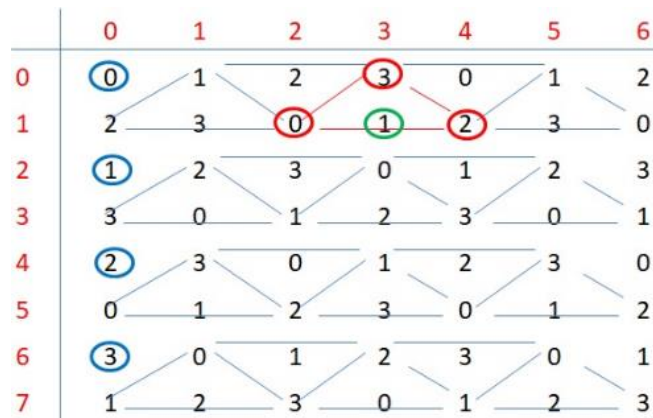


Figure 2. The reference matrix

## 2.2. The embedding process

To embed and hide data in the cover image, permutation of the pixels is used. First, the data that will be hiding in the image should be encoded 'converted to binary'. Second, the data will be segmented into blocks of two bits. The value of these two bits' blocks will be used for the hiding process using the reference matrix. The reference matrix will be shown as a row vector. Each value in the matrix will be mapped to one block of the data. The mapping process follows the following three roles.

- 1) If the data to be hiding equals the value in the matrix's cell, no changes will be taken. This is the simplest role.
- 2) If the data to be hiding no equal to the value in the matrixes cell, in this case, the cell type is important.
  - If the cell is a core cell, find the value that equal the data in the same triangle and swap these two values and swap the corresponding cover image pixels.
  - If the cell is an edge cell, swap the edge with the value from the same triangle that the cell is a head cell in that triangle. In Figure 2 we can observe that the edge cells belong to one or three triangles. If it belongs to three triangles, in one of them, the edge is located in the triangle head.
  - If the cell is an external cell, find the value in the surrounding box and swap. The box is defined as 2×2 matrix. The cell is any edge of the box. The box should be in the same lines of the triangles created as in Figure 2.

After swapping the pixels and the reference matrix is generated, the data of this matrix is converted to 1D line vector. Each cell of this vector consists of two bits. These two bits will be embedded in the cover image after stilling two low significant bits from the black pixels in the image. The size of the data will also be embedded in the cover image for the extraction process.

As an example of the insertion process as shown in the Figure 3, the data (2, 1, 0, 0) will be embedded and hide inside the image. The locations of these bits have been decided to be (1, 5), (0, 0), (3, 4), and (2, 1) where the first location is the row number and the second number is column in the matrix. These numbers have been obtained after the data has been encoded and segmented into 2 bits' blocks. To embed the first number '2' in location (1, 5), '3' has been located in this location. '3' is a core number in the triangle, this means that swap operation is performed between '3' and '2' in the same triangle. The second example is to embed number '1' in location (0, 0). This location is an external location. It does not belong to any triangle. To embed the data, the box that contain location (0,0) in its edge is used and a swap to the left occurs.

For the third example '0' will be embed in location (3,4). In this location '3' is located. '3' is an edge between 3 different triangles. However, it is the head point in the middle triangle. The swap occurs between this location and the edge in the same triangle where 3 is a head point.

For the final example '0' will be embed in location (2, 1). In this place '2' is found. '2' is an edge node between two triangles. It is a head point in the first one. A swap occurs between this location and the '0' in the same triangle. We can observe also from this example that the only '0' located is the one inside this triangle. In this case, the swap operation is easy.

After swap operation performed, the matrix is embedded in the cover image by utilizing the two last bits from each black pixel. The cover image will also be contained the size of the data that will be used in the extraction process. In this case, the cover image will be transferred to the destination with reference matrix for the extraction process. After receiving the message at the destination, the message will be ready for the extraction process. This process is explained in the next subsection.

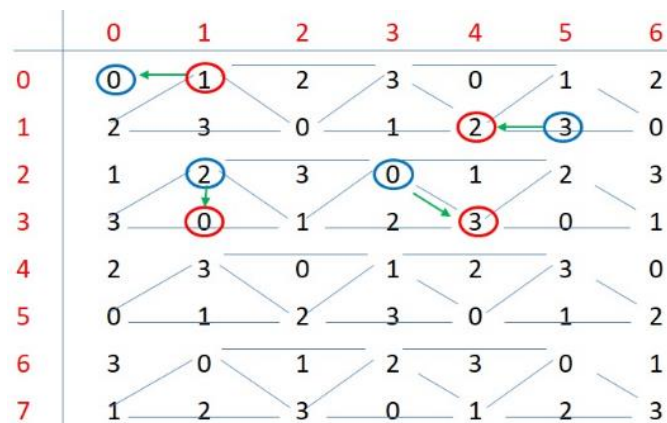


Figure 3. Embedding process example

### 2.3. The extraction processes

To extract the data, form the cover image, the reference matrix has to be extracted first from the image. Each pixel with the value higher than 252 is leveraged for this process. After reconstructing the reference matrix, the differences between the original reference matrix and the received matrix make it simple to extract the data form the pixels and to re-structure the original X-ray image.

## 3. SIMULATION OF THE PROPOSED METHOD AND RESULT DISCUSSION

To evaluate the algorithm, nine different X-ray images have been used. X-ray images have many types, such as, abdominal, barium, bone, chest, dental, extremity, hand, joint and mammogram. One image from each type has been downloaded and used in this work. The algorithm had been written using Matlab. Two other algorithms have been written to compare the performance of TBXS: turtle shell [20] and LSB [8]. These two algorithms are popular algorithms in image steganography field [26], [27]. A random number generator has been written to generate random number and the modular operation has been used to convert the generated numbers into series of zeros and ones. Three performance metrics have been used in this work as in [8]: PSNR, mean square error (MSE), and the embedding capacity measure. The computer used in this work is Intel i5-10300H 4 cores with 2.5 GHz and 16 GB RAM.

PSNR is used to evaluate the visual quality of the image. With higher value of PSNR, the image visualization quality increases. PSNR can be calculated using (2). This value is calculated in db. As shown in PSNR, the value depends on the MSE in its calculation. In (3) shows MSE calculation.

$$PSNR = 10 \left( \frac{255^2}{MSR} \right) \quad (3)$$

Where  $H$  is the height of the image and  $W$  is the width of the image in pixels.  $X_{ij}$  is the value of the pixel  $x$  in location  $(I, J)$  in the cover image before embedding the data and  $Y_{ij}$  is the value of pixel in location  $(I, J)$  after the embedding process.

$$MSR = \frac{1}{H \times W} \sum_{i=0}^H \sum_{j=0}^W (X_{ij} - Y_{ij})^2 \quad (4)$$

We can observe from (2) and (3) that with higher mean square error (MSR), lower PSNR is obtained. This means a higher PSNR and a lower MSR is required for higher visualization quality. Finally (3) calculates the bit embedding capacity.

$$C = \frac{B}{H \times W} \quad (5)$$

Where  $B$  is the number of bits embedded in the image.

Figure 4 shows the nine X-ray images utilized in this work before and after the hiding process. The images have been labeled I1 to I9 in the rest of the results. Table 1 shows the MSR of the TBXS and the other two algorithms. We can observe TBXS has lower MSR than the turtle shell algorithm. However, the LSB computed better MSR value. However, TBXS has higher capacity with 1.9 bpps which is higher than LSB, which has 1 bpps and turtle shell, which has 1.5 bpps. Moreover, TBXS has the possibility to convert the received image into the original cover image. This is not possible in LSB. The values computed in Table 1 are the average values of 30 runs of the code over the nine images. The random data generator has generated different random data in the iterations. Moreover, the size of the images is not the same. Table 2 shows the comparison in PSNR. We can observe that TBXS has higher PSNR value than the turtle shell. However, the value is lower than LSB.

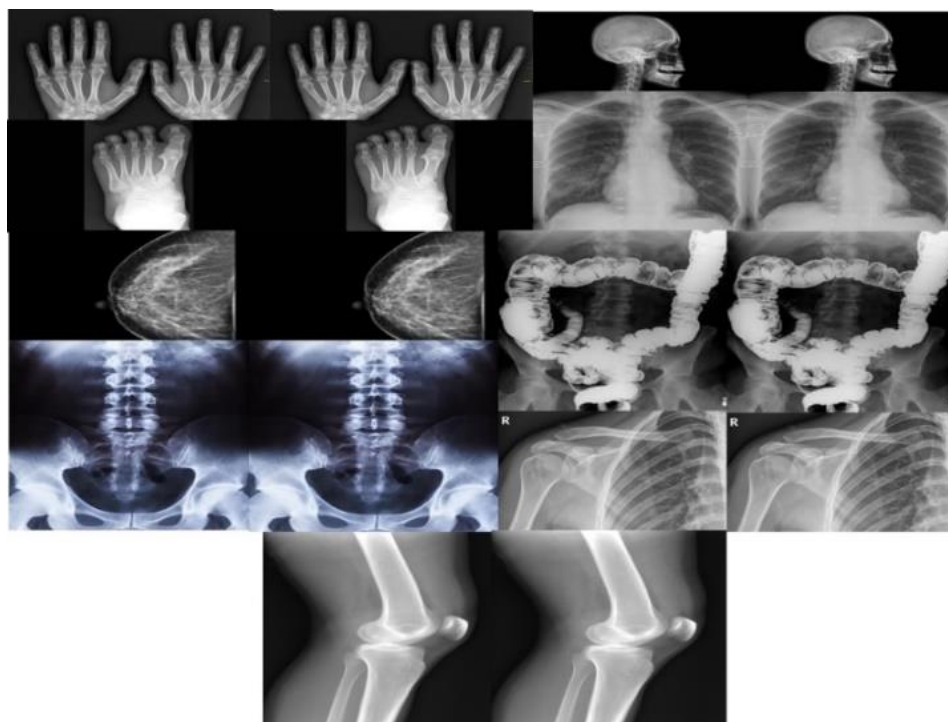


Figure 4. Nine X-ray Images from the nine X-ray categories. The first image is the cover image and the second is the image with the embedded data

Table 1. Comparison of the MSR values of the algorithms

	I1	I2	I3	I4	I5	I6	I7	I8	I9
TBXT	50.21	6.16	9.88	6.118	22.59	26.7	183.14	13.8	7.6327,
Turtle shell	123.93	18.599	28.96	10.9	57.677	82.18	422	39.44	21.8
LSB	0.2453	0.39866	0.403	0.249	0.109	0.2471	0.24	0.248	0.249

Table 2. Comparison of the PSNR values of the algorithms

	I1	I2	I3	I4	I5	I6	I7	I8	I9
TBXT	31.1224	40.22	38.18	40.2	34.59	33.86	25.5	36.7	39.3
Turtle shell	27.1989	35.43	33.51	37.7	30.52	28.98	21.8	32.177	34.7
LSB	54.2341	52.12	52	54.16	57.7	54.2	54.32	54.175	54.16

#### 4. CONCLUSION

X-ray images reports are documents that written in plain English and any person can read them. This can breach the privacy of people's medical reports. To secure these reports, steganography in X-ray images can be utilized. In this work, a new image steganography algorithm based on Sudoku method is proposed. The method generates a reference matrix with triangles' shaped blocks. Each cell in the matrix is represented with a two bits data. In this case, two bits can be embedded in the image in each hiding process. The algorithm has been evaluated and compared to LSB and turtle shell. The PSNR of the algorithm obtained higher value than the turtle shell method. The embedding capacity of the algorithm reached 1.92 bpps which is higher than LSB, 1 bpps and turtle shell, 1.5 bpps. In the future, different encoding techniques can be used to enhance the number of embedded bits in the images





#### REFERENCES

- [1] P. Wayner, *Disappearing cryptography: information hiding: steganography and watermarking*, USA: Morgan Kaufmann, 2009.
- [2] R. Poornima and R. J. Iswarya, "An overview of digital image steganography," *International Journal of Computer Science and Engineering Survey*, vol. 4, no. 1, pp. 23-31, Feb. 2013, doi: 10.5121/ijcses.2013.4102.
- [3] F. H. M. S. Al-Kadei, "Two-level hiding an encrypted image," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 18, no. 2, pp. 961-969, May 2020, doi: 10.11591/ijeecs.v18.i2.pp961-969.
- [4] W. Stallings, *Cryptography and network security*, India: Pearson Education, 2006.
- [5] M. Masoud, Y. Jaradat, A. Manasrah, and I. Jannoud, "Sensors of Smart Devices in the Internet of Everything (IoE) Era: Big Opportunities and Massive Doubts," *Journal of Sensors*, vol. 2019, 2019, doi: 10.1155/2019/6514520.
- [6] Y. Liu, C. -C. Chang, and S. T. Nguyen, "High capacity turtle shell-based data hiding," *IET Image Processing*, vol. 10, no. 2, pp. 130-137, 2016, doi: 10.1049/iet-ipr.2014.1015.
- [7] Y. Liu and C. -C. Chang, "A turtle shell-based visual secret sharing scheme with reversibility and authentication," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25295-25310, Feb. 2018, doi: 10.1007/s11042-018-5785-z.
- [8] C. Arcos, G. Brookfield, and M. Krebs, "Mini-sudokus and groups," *Mathematics Magazine*, vol. 83, no. 2, pp. 111-122, Apr. 2010, doi: 10.4169/002557010X482871.
- [9] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Reversible data hiding," *Proceedings. International Conference on Image Processing*, 2002, doi: 10.1109/ICIP.2002.1039911.
- [10] J. Mielikainen, "LSB matching revisited," in *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, May 2006, doi: 10.1109/LSP.2006.870357.
- [11] X. Zhang and S. Wang, "Efficient Steganographic Embedding by Exploiting Modification Direction," in *IEEE Communications Letters*, vol. 10, no. 11, pp. 781-783, November 2006, doi: 10.1109/LCOMM.2006.060863.
- [12] S. -Y. Shen and L. -H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions," *Computers & Security*, vol. 48, pp. 131-141, Feb. 2015, doi: 10.1016/j.cose.2014.07.008.
- [13] S. Pramanik, R. P. Singh, and R. Ghosh, "A new encrypted method in image steganography," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 14, no. 3, pp. 1412-1419, Jun. 2019, doi: 10.11591/ijeecs.v13.i3.pp1412-1419.
- [14] M. A. Al-Momin, I. A. Abed, and H. A. Leftah, "A new approach for enhancing LSB steganography using bidirectional coding scheme," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 5286-5294, Dec. 2019, doi: 10.11591/ijece.v9i6.pp5286-5294.
- [15] A. ALabaichil, M. A. A. K. Al-Dabbas, and A. Salih, "Image steganography using least significant bit and secret map techniques," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, Feb. 2020, pp. 935-946, doi: 10.11591/ijece.v10i1.pp935-946.
- [16] S. A. Nie, G. Sulong, R. Ali, and A. Abel, "The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 5218-5226, doi: 10.11591/ijece.v9i6.pp5218-5226.
- [17] J. N. Shehab, H. A. Abdulkadhim, and T. F. H. Al-Tameemi, "Robust large image steganography using LSB algorithm and 5D hyper-chaotic system," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 2, pp. 689-698, Apr. 2021, doi: 10.11591/eei.v10i2.2747.
- [18] X. Liao, S. Guo, J. Yin, H. Wang, X. Li, and A. K. Sangaiah, "New cubic reference table based image steganography," *Multimedia Tools and Applications*, vol. 77, no. 8, pp. 10033-10050, 2018, doi: 10.1007/s11042-017-4946-9.
- [19] W. Hong, T. Chen, and C. Shiu, "A Minimal Euclidean Distance Searching Technique for Sudoku Steganography," *2008 International Symposium on Information Science and Engineering*, 2008, pp. 515-518, doi: 10.1109/ISISE.2008.153.
- [20] C. C. Chang, Y. Liu, and T. S. Nguyen, "A Novel Turtle Shell Based Scheme for Data Hiding," *2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2014, pp. 89-93, doi: 10.1109/IIH-MSP.2014.29.





- [21] C. H. Yang, C. -Y. Weng, H. -K. Tso, and S. J. Wang, "A data hiding scheme using the varieties of pixel-value differencing in multimedia images," *Journal of Systems and Software*, vol. 84, no. 4, pp. 669-678, Apr. 2011, doi: 10.1016/j.jss.2010.11.889.
- [22] W. Hong and T. Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching," in *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 176-184, Feb. 2012, doi: 10.1109/TIFS.2011.2155062.
- [23] C. -F. Lee, J. -J. Shen, S. Agrawal, and Y. -H. Li, "High-capacity embedding method based on double-layer octagon-shaped shell matrix," *Symmetry*, vol. 13, no. 4, Apr. 2021, doi: 10.3390/sym13040583.
- [24] R. Honwade, S. Rangaswamy, B. R. Roshan Shetty, J. Rohith, and V. Mukund, "Steganography Using Sudoku Puzzle," *2009 International Conference on Advances in Recent Technologies in Communication and Computing*, 2009, pp. 623-626, doi: 10.1109/ARTCom.2009.116.
- [25] M. Z. Masoud, Y. Jaradat, A. Manasrah, I. Jannoud, and A. Zerek, "HidSave: An Image Steganography Technique based on SudoKu Method for Smartphones," *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI-STA*, 2021, pp. 887-890, doi: 10.1109/MI-STA52233.2021.9464512.
- [26] K. Bansal, A. Agrawal, and N. Bansal, "A Survey on Steganography using Least Significant bit (LSB) Embedding Approach," *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, 2020, pp. 64-69, doi: 10.1109/ICOEI48184.2020.9142896.
- [27] N. Kaur and S. Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques," *International journal of engineering trends and technology*, vol. 11, no. 8, pp. 388-392, May. 2014, doi: 10.14445/22315381/IJETT-V11P276.

## BIOGRAPHIES OF AUTHORS



**Enas Ali Jameel**     She have BSc degree in Computer Science from the Iraq, University of Mosul, collage of computer sciences and mathematics, department of computer science at 2006, she received her MSc degrees in computer Science form the same university and department at 2013 , she worked as a programmer at the same college till 2010, now she work as assistant lecturer at the college of computer science and mathematics (university of Mosul) specialized in data base. She can be contacted at email: enasaljameel@uomosul.edu.iq.



**Sammera Abbas Fadhel**     She graduated from Department of Computer Science College of Computer Science and Mathematics, University of Mosul, Iraq in 2006, she worked as a programmer at the same college till 2010, she finished MSC. Degree in 2013. Now she work as assistant lecturer at the college of computer science and mathematics (university of Mosul) specialized in information security. She can be contacted at email: sameeraabbasfadhel@uomosul.edu.iq.