Watermarking in Medical Image

https://doi.org/10.3991/ijoe.v19i06.37591

Nashwan Alsalam Ali(✉), Iman I. Hamid
University of Baghdad, Baghdad, Iraq
nashwan_alsalam60@coeduw.uobaghdad.edu.iq

Abstract—Medical image security is possible using digital watermarking techniques. Important information is included in a host medical image in order to provide integrity, consistency, and authentication in the healthcare information system. This paper introduces a proposed method for embedding invisible watermarking in the 3D medical image. The cover medical image used is DICOM which consists of a number of slices, each one representing a sense, firstly must separate the ROI (Region of Interest) and NROI (Not Region of Interest) for each slice, the separation process performed by the particular person who selected by hand the ROI. The embedding process is based on a key generated from Arnold's chaotic map used as the position of a pixel in the slices with the highest saturation for embedding a secret message in the NROI because the ROI contains the information of the ill, so it cannot be modified. The evaluation of the proposed method using PSNR and MSE shows good results according to both requirements of the watermark system, the invisibility and quality of the watermarked medical image where the PSNR value is up to 43.3936 and MSE is up to 0.000041.

Keywords—watermarking, medical image, DICOM, Arnold cat map

1 Introduction

Digital information distribution has become more pertinent due to recent advancements in information and communication technologies. It is essential for several industries, including those in the public sector, the private sector, finance, and the healthcare industry, where the Internet must become the primary means of data distribution and interchange. [1–3]. Due to the rapid spread of illnesses brought on by patient-to-patient contact recently. As a result, all medical data is automated in Electronic Health Records (EHR), which keeps patients' past medical data electronically [4]. These records include personal information like name, age, and address; information about bodily functions like breathing rate, blood pressure, and heart rate; and images of medical scans like chest, kidney, and brain scans taken using CT and MRI machines.

Additionally, therapies and diagnoses for patients are also kept in the form of reports that include laboratory results, remarks for the doctor's analysis, and dosages of suggested medicines [5]. The typical medical imaging data format for storing CT and MRI images is called Digital Imaging and Communications in Medicine (DICOM) [6]. The National Electrical Manufacturers Association (NEMA) developed and owned the DICOM standard for transferring, viewing, organizing, and manipulating medical images [7]. It has received widespread endorsement and has been implemented in hospitals by several programs that support physicians' and specialists' decision-making processes. Such a DICOM format makes parsing and integration operations easier among various medical platforms and devices, which mostly rely on Picture Archiving and Communication Systems (PACS) [8]. There are two parts to DICOM image files: a header that contains metadata like the location of the examination, the equipment used, and other information that causes the header size to vary from image to image and further vary depending on the imaging modality; and a greyscale matrix that represents the image intensities. [9, 10]. The following components comprise a DICOM image file, as shown in Figure 1.

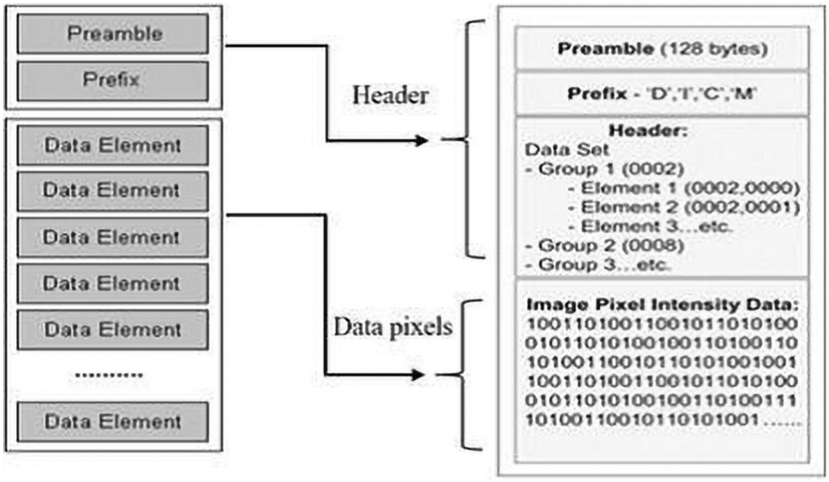

Fig. 1. The structure of DICOM [11, 12]

The structure of the DICOM image consists of the following four components:

- A preface (128-byte).
- The prefix (4-byte) for storing 'D,' 'I,' 'C,' and 'M' letters for the file format defining.
- Fields in metadata that are configured to store data.
- Data pixels used to create the picture in the DICOM file.

Numerous benefits come with the DICOM standard, such as quickly capturing and sharing medical images. Moreover, a clinician's decision-making and patient report-writing processes are also made simpler. Nevertheless, since it is simple to delete, modify, or otherwise disconnect the metadata, there are no security measures that safeguard the secrecy of the metadata or the authenticity of the images [13–15].

2 Related works

In [4], the authors proposed a modified least significant bit (LSB) approach capable of safeguarding and concealing medical data to address the critical authentication problem; the execution method was a logical bit shift. The results of the experiment showed that the suggested method could embed medical data without leaving an obvious falsehood in the stego image. When compared to prior research efforts, the outcome of this implementation demonstrates that the modified LSB image steganography outperforms the standard LSB technique with a higher PSNR value and a lower MSE value. For the proposed system, a new performance statistic called “shift count” was added. According to the study’s findings, the suggested protected medical information system was demonstrated to be effective in concealing medical data and producing undetected stego pictures with minimal entrenching falsifications.

In [8], the author proposed a steganography technique based on DICOM medical images, wherein one medical image serves as a cover image and the other as a hidden message image. The Preprocessing, data embedding using the discrete cosine transform (DCT), and an extraction step are the three primary components of this method. The effectiveness of the algorithm was assessed using the metrics of the Peak Signal to Noise Ratio (PSNR), the Magnetic resonance imaging (MRI) dataset, and the Mean Square Error (MSE). The experiment outcomes showed that embedding a DICOM image within another DICOM image of the same size resulted in high PSNR and high capacity of the concealed data.

In [16], the authors proposed a reversible watermarking method for DICOM (Digital Imaging and Communications in Medicine) images is suggested. It provides high embedding capacity (payload), security, and integrity of the watermarked image. Watermarks based on companding are embedded in lifting-based Discrete Wavelet Transform (DWT) domains to accomplish the desired result. The companding method is used during the embedding process to maximize the data-hiding capabilities. On the other hand, the system is made simple to implement by using a linear function, and it is made resilient against collusion by using a watermark that is reliant on the content. Simulated results show the suggested scheme’s advantage, which is also compared to a few other relevant methods.

In [17], the authors describe an algorithm created for Digital Imaging and Communications in Medicine (DICOM) medical images that uses secret-sharing steganography techniques to guarantee the integrity of sensitive patient data as well as the critical components of the image. The proposed method divides the images into two parts: region of non-interest (RONI) and region of interest (ROI). The information (map) required to recover the ROI before insertion is located in the RONI, whereas patient data and integrity hashes are placed inside the ROI. The usage of encryption ensures the security of the extraction procedure. The experimental results demonstrated great visual equivalence between the original (cover) and stego images in terms of PSNR for both types of images. Moreover, they demonstrate how effectively the suggested system can be employed as a steganography scheme in DICOM images with little smooth area. In [18], a technique based on the discrete wavelet transform is suggested for concealing sensitive information in DICOM images (DWT First, all slices of a 3D image) were segmented into a particular block size, and the host image was collected using a generated key. Next, the block number and slice number were chosen. Third, the low-high band was used for embedding after the generated number was added. Fourth, the Hessenberg transform was applied to the blocks to portion the band (low-high) into a particular size. The binary value of the secret information (image or text) was encoded by changing the positive value in the diagonal to odd values if the secret bit was one and to even values if it was zero. Several tests were used, including the mean square error, peak signal-to-noise ratio, and structural similarity index measure.

3 Arnold cat map

The Arnold cat map began its development as a Vladimir Arnold idea that was applied to a cat image. It is a formula that may be used to transform the pixels in an image. The pixels of the image appear to be randomly rearranged when applied the Arnold cat map transformation [19]. However, the original image can be recovered if this transformation is performed numerous times. Furthermore, for this straightforward discrete system, phase space is represented by a square, and the discrete Arnold cat map extends and folds the trajectories to reflect the scrambling effect of the Arnold cat map. The Arnold cat map changes the locations of the pixel values in the source image using ideas from linear algebra. The outcome will be a shuffled image with the exact same pixel values as the original image after applying the Arnold cat map [20]. The Arnold cat map's transformation is based on a matrix with a determinant of Equation (1), making it reversible, and is best explained as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ Q & PQ+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod(n) \tag{1}$$

Here, P and Q are integers, and (x, y) is the original position mapped to the new position (x_0, y_0). P and Q are normally considered prime numbers because they reflect the parameter employed in the transformation. The input to the cat map equation is the image pixel position; The cat map shuffles the position of the pixels in linear sequences of the image, resulting in the encrypted image. The procedure is repeated till the final pixel location [21, 22], and the encryption process is reversed during the decryption procedure based on Equation (2).

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} PQ+1 & -p \\ -Q & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} mod(n) \tag{2}$$

4 Performance assessment

The performance of the proposed method is assessed using the Peak Signal-to-Noise Ratio (PSNR), which is based on Mean Square Error (MSE). The PSNR is used to calculate the degree of noise between the original image and the output processed image (after the embedding process). It measures the quality of the output image that reflects the algorithm's Imperceptibility performance. As the high PSNR value as good, which means high similarity and better Imperceptibility [23–32]. The PSNR and MSE are calculated using Equations (3) and (4), respectively.

$$PSNR = 10\, log_{10}\left(\frac{MAx}{\sqrt{MSE}}\right) \tag{3}$$

$$MSE = \frac{1}{MN}\sum\sum[I(x,y) - I'(x,y)]^2 \tag{4}$$

where (*M* and *N*) are the image dimension, $I'(x, y)$ is the output image, $I(x, y)$ is the original image. When the (MSE) has a lower value, it means there is less of error. The MSE and PSNR have an inverse relation between them, which is reflected into a high value of PSNR when MES is less [18, 32].

5 The proposed method

In this paper, a newly proposed method is to hide a secret message representing the medical center's information, the date, and the patient's name in the 3D medical image (DICOM) to protect privacy and copyright. The 3D medical image contains a number of slices; the slices chosen for hiding the secret message (watermark) after converting to binary sequence, based on the saturation of each slice which represents the average of pixels' values, the slices with max saturation are selected for hiding the binary bits. The keys generated from the Arnold chaotic map are used to select the position of pixels in each slice for hiding and must be out of the region of interest (NROI), where the data in the region of interest is based on the diagnosis process of disease. The following are the main steps of the embedding proposed method.

5.1 Embedding proposed algorithm

```
Step1: Input 3D DICOM medical image.
Step2: Input secret message for embedding.
Step3: Convert the secret message to binary bit sequence.
Step4: Determine the saturation for each slice by computing the average for the pixel
       values in each slide.
        sum=0
        sum=sum+$a_{i,j}$
        Sat(n) =sum/ i*j
        Where $a_{i,j}$ is the original 3D medical image slice, and n is the number of the
        slice.
Step5: Apply Arnold chaotic map to generate the keys used as the pixel position
       where the embedding process is done.
Step6: Select the slices with max saturation based on the threshold value using trial
       and error.
```

Step7: Divide the binary sequence to the number of selected slices to see the number of bits embedded in each slice.
Step8: Separate the ROI and NROI in slices by hand.
Step9: Check the key generation from the chaotic map, if it is in ROI or NROI.
Step10: Use the keys outside the border of ROI as a position for embedding in slice selection.
Step11: Perform the embedding process by selecting the pixel for each slice with the highest saturation.
Step12: Repeat step11 until complete embedding all the bits sequence.
Step13: Display the watermarked 3D medical image.

5.2 Extraction proposed algorithm

The extraction process is the same as the embedding steps but in reverse order, in the following the main steps for the extraction process.

Step1: Input watermarked 3D DICOM medical image.
Step2: Compute the saturation for each slice by adding the pixel value for each position and compute the average for them.
Step3: Apply Arnold chaotic map to generate the keys used as the pixel position where the extraction process is done.
Step4: Select the slices with the highest saturation.
Step5: Separate the ROI by hand and NROI for each slice.
Step6: Check the key generation from the chaotic map, if it is in ROI or NROI.
Step7: Use the keys outside the border of ROI as a position for extraction in slices selecting.
Step8: Perform the extraction process in the selecting pixel for each slice with the highest saturation.
Step9: Repeat step8 until complete extraction of all the bits sequence based on the number of bits embedded in each slice.

6 Experimental results

This paper uses different secret messages to test the proposed algorithm with different lengths. MSE and PSNR are used as metrics to see the image quality because, after the embedding process, some of the image properties may be changed. Tables 2 and 3 show the MSE for all the DICOM slices with three different texts. A DICOM object has characteristics similar to other image file formats, such as file name, file ID, and a specific field representing pixel data size. Each slice in the object file generally refers to a single image with all its attributes. It may consist of many frames of data or multi-dimensional multi-frame images (a 3D or 4D array of data formed in a DICOM file). The frame or slice in DICOM may be of compressed file format, lossy or lossless for each slice in DICOM. Figure 2 depicts slices of a header image that were used as DICOM images to conceal hidden information.

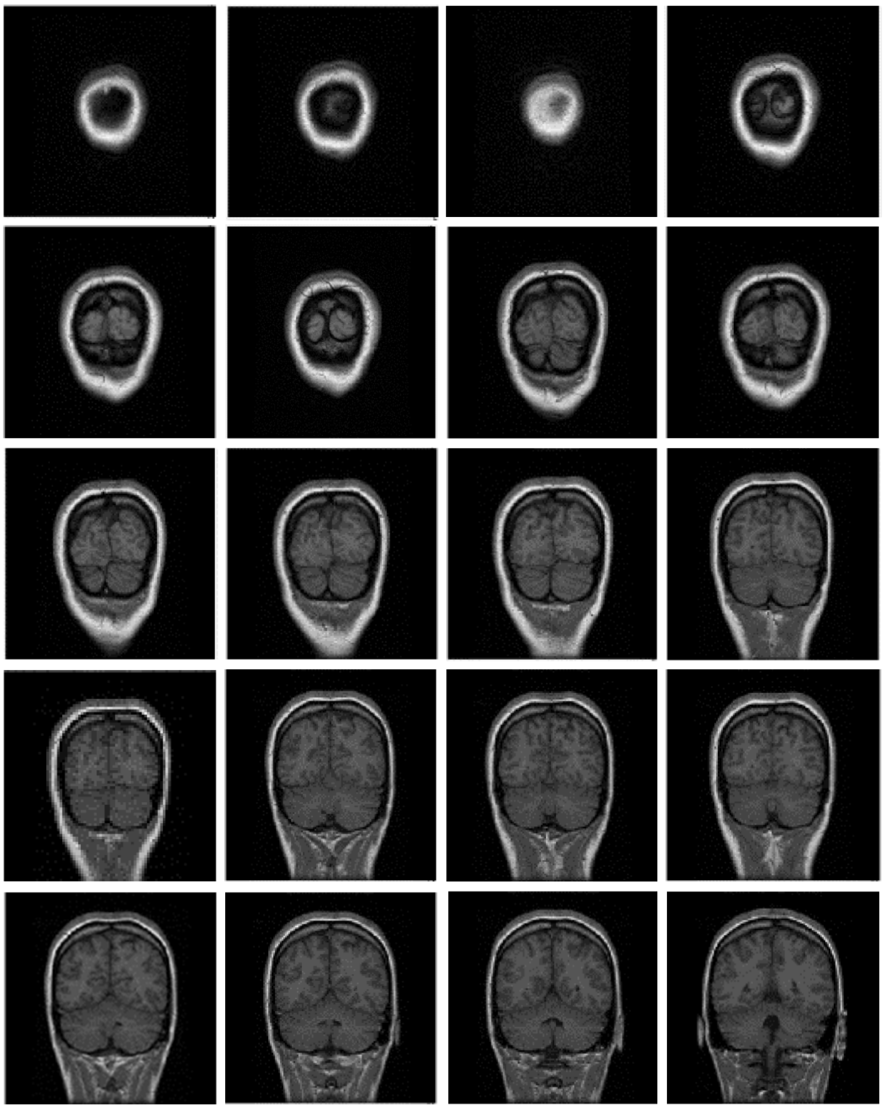

Fig. 2. The original slices of DICOM

Figure 3 shows one slice of DICOM slices used for embedding selection based on saturation values; firstly, the region of interest is selected by choosing the points of four corners for the region by hand, then using these pixels outside this region for embedding.

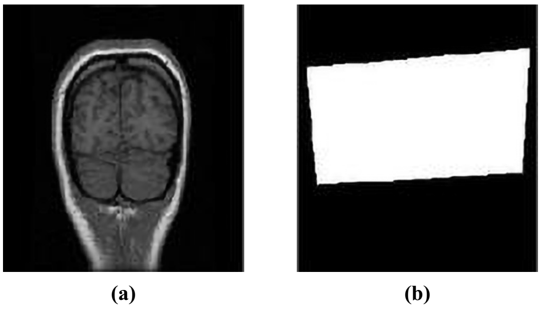

Fig. 3. (a) The original slice DICOM, (b) The selected ROI

Figure 4 shows the separated ROI and NROI used for embedding, the keys generated by the chaotic map used as a position for pixels used for embedding.

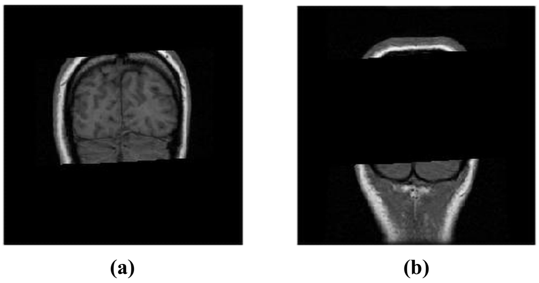

Fig. 4. (a) The ROI slice DICOM, (b) The NROI

The secret message is embedded in the region shown in Figure 4b, so there is no effect on the important information for the patient that needs the doctor to make the decision for a sick; after completing the embedding process in this slide, moving to another slide with less saturation and repeat the embedding process. Figure 5 shows the slide after the embedding process; for the eyes, there is no noticeable change.

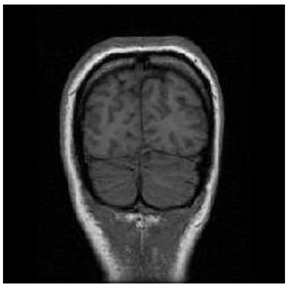

Fig. 5. The watermarked slice of the DICOM image

To test the result of the proposed algorithm, different secret messages are used with different lengths containing the medical center, date, and the patient's name shown in Table 1.

Table 1. Secret message samples

No.	Secret Message
1	Al-Krama hospital/23-5-202/Ahmed Mohammed
2	Al-Krama hospital /15-7-2022/Nabaa Ali
3	Al-Krama hospital /30-7-2022/Alaa jasem

PSNR test and MSE reflect the similarity between the watermarked 3D medical image and the original version; as the MSE decreases, the PSNR will increase. The following Tables 2 and 3 show the result of MSE and PSNR for each slice with different secret messages.

Table 2. MSE for DICOM slices

Slice Number	Message1	Message2	Message3
1	0.0001502	0.000100	0.000150
2	0.000300	0.000125	0.000250
3	0.000202	0.000122	0.000122
4	0.000238	0.000112	0.000210
5	0.000250	0.000148	0.000244
6	0.000275	0.000188	0.000290
7	0.000275	0.000188	0.000200
8	0.000222	0.000250	0.000290
9	0.000214	0.000178	0.000158
10	0.000214	0.000127	0.000163
11	0.000320	0.000198	0.000275
12	0.000377	0.000270	0.000275
13	0.000107	0.000046	0.000092
14	0.000153	0.000092	0.000153
15	0.000041	0.000031	0.000076
16	0.000125	0.000100	0.000130
17	0.000122	0.000092	0.000076
18	0.000100	0.000082	0.000082
19	0.000082	0.000122	0.000168
20	0.000056	0.000066	0.000066

Table 3. PSNR for DICOM slices

Slice Number	Message1	Message2	Message3
1	38.5	39.8	38.5
2	34.72	38.51	35.4
3	36.52	38.42	38.44
4	35.89	39.00	36.6
5	35.5	37.61	35.62
6	35.22	37.1	35.2
7	34.5	37.1	36.7
8	36.22	35.60	35.2
9	36.8	37.01	37.8
10	36.8	38.5	37.1
11	35	37	36
12	34	36	36
13	40	43.3936	40.3833
14	38.2	40.5	38.2
15	42.2	45.5	41.2
16	39	40	38.6
17	39.1	40.23	41.21
18	39.7138	40.3833	40.3833
19	40.3833	39.1339	37.7509
20	41.1751	41.1751	41.1751

From the results shown in Tables 2 and 3, the proposed method has good results according to the invisibility and the quality of the 3D watermarked image.

7 Conclusion

The proposed method uses the spatial domain, which is simple and not complex but gives good results according to the invisibility and the quality of the 3D watermarked medical image. The proposed method increases security by using the key generation based on Arnold's chaotic map and the concept of max saturation. From the results of the PSNR and MSE in the experimental section, it is clear that the proposed method gives good results according to the invisibility and the quality of the 3D watermarked medical image.

8 References

[1] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. O. Ogundokun, "A safe and secured iris template using steganography and cryptography," *Multimedia Tools and Applications*, vol. 79, no. 31–32, pp. 23483–23506, 2020. https://doi.org/10.1007/s11042-020-08971-x

[2] O. N. Akande, O. C. Abikoye, A. A. Kayode, O. T. Aro, and O. R. Ogundokun, "A dynamic round triple data encryption standard cryptographic technique for data security," in Computational Science and Its Applications – ICCSA 2020. ICCSA 2020, pp. 487–499, Springer, 2020. https://doi.org/10.1007/978-3-030-58817-5_36

[3] A. O. Christiana, A. N. Oluwatobi, G. A. Victory, and O. R. Oluwaseun, "A secured one-time password authentication technique using (3, 3) visual cryptography scheme," *Journal of Physics: Conference Series*, vol. 1299, no. 1, pp. 1–10, 2019. https://doi.org/10.1088/1742-6596/1299/1/012059

[4] R. O. Ogundokun and O. C. Abikoye, "A safe and secured medical textual information using an improved LSB image steganography," *International Journal of Digital Multimedia Broadcasting*, vol. 2021, 2021. https://doi.org/10.1155/2021/8827055

[5] N. A. Ali, "Watermarking in 3D models using depth path," *Iraqi Journal of Science*, vol. 60, no. 11, pp. 2490–2496, 2019. https://doi.org/10.24996/ijs.2019.60.11.21

[6] E. Seeram, "Medical imaging informatics: An overview, in Digital Radiography," *Springer*, pp. 165–183, 2019. https://doi.org/10.1007/978-981-13-3244-9_10

[7] "Overview of the content of the DICOM standard," Available: https://dicom.nema.org/medical/dicom/current/output/chtml/part01/sect_6.3.html

[8] A. Elhadad, A. Ghareeb, and S. Abbas, "Blind and high-capacity data hiding of DICOM medical images based on fuzzification concepts," *Alexandria Engineering Journal*, vol. 60, pp. 2471–2482, 2021. https://doi.org/10.1016/j.aej.2020.12.050

[9] H. B. Shin, H. Sheen, H. Y. Lee, J. Kang, D. K. Yoon, and T. S. Suh, "Digital imaging and communications in medicine (DICOM) information conversion procedure for SUV calculation of PET scanners with different DICOM header information," *Physica Medica*, vol. 44, pp. 243–248, 2017. https://doi.org/10.1016/j.ejmp.2017.05.063

[10] A. Al-Haj, "Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images," *Journal of Digital Imaging*, vol. 28, no. 2, pp. 179–187, 2015. https://doi.org/10.1007/s10278-014-9734-8

[11] A. F. Qasim, "Reversible and imperceptible watermarking approach for ensuring the integrity and authenticity of brain MR images," [Doctoral dissertation]: University of Salford, 2019.

[12] S. G. Shini, T. Thomas, and K. Chithraranjan, "Cloud based medical image exchange security challenges," *Procedia Engineering*, vol. 38, pp. 3454–3461, 2012. https://doi.org/10.1016/j.proeng.2012.06.399

[13] A. F. Qasim, R. Aspin, F. Meziane, and P. Hogg, "ROI-based reversible watermarking scheme for ensuring the integrity and authenticity of DICOM MR images," *Multimedia Tools and Applications*, vol. 78, no. 12, pp. 16433–16463, 2019. https://doi.org/10.1007/s11042-018-7029-7

[14] S. Das and M. K. Kundu, "Effective management of medical information through ROI-lossless fragile image watermarking technique," *Computer Methods and Programs in Biomedicine*, vol. 111, no. 3, pp. 662–675, 2013. https://doi.org/10.1016/j.cmpb.2013.05.027

[15] B. A. Shtayt, N. H. Zakaria, and N. H. Harun, "A comprehensive review on medical image steganography based on lsb technique and potential challenges," *Baghdad Science Journal*, vol. 18, no. 2, 2021. https://doi.org/10.21123/bsj.2021.18.2(Suppl.).0957

[16] A. Phadikar, P. Jana, and H. Mandal, "Reversible data hiding for DICOM image using lifting and companding," *Cryptography*, vol. 3, no. 21, pp. 1–19, 2019. https://doi.org/10.3390/cryptography3030021

[17] P. L. K. Mantos and I. Maglogiannis, "Sensitive patient data hiding using a ROI reversible steganography scheme for DICOM images," *J. Med. Syst.*, vol. 40, no.156, 2016. https://doi.org/10.1007/s10916-016-0514-5

[18] B. A. Hameedi, M. M. Laftah, and A. A. Hattab, "Data hiding in 3D-medical image," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 03, 2022. https://doi.org/10.3991/ijoe.v18i03.28007

[19] N. A. Abbas, "Image encryption based on independent component analysis and arnold's cat map," *Egypt. Inform. J.*, vol. 17, pp. 139–146, 2016. https://doi.org/10.1016/j.eij.2015.10.001

[20] A. A. P. Ratna et al., "Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion," *Adv. Sci. Technol. Eng. Syst.*, vol. 6, no. 1, pp. 316–326, 2021. https://doi.org/10.25046/aj060136

[21] B. A. Hameedi, A. A. Hattab, and M. M. Laftah, "A pseudo-random number generator based on new hybrid LFSR and LCG algorithm," *Iraqi Journal of Science*, vol. 63, no. 5, pp. 2230–2242, 2022. https://doi.org/10.24996/ijs.2022.63.5.35

[22] B. A. N. Nadiyya, K. Usman, S. Aulia, and B. C. Erizka, "X-ray images encryption analysis using arnold's cat map and bose chaudhuri hocquenghem codes," *Journal of Southwest Jiaotong University*, vol. 55, no. 6, 2020. https://doi.org/10.35741/issn.0258-2724.55.6.41

[23] M. M. Hashim, A. A. Mahmood, and M. Q. Mohammed, "A pixel contrast based medical image steganography to ensure and secure patient data," *Int. J. Nonlinear Anal. Appl.*, vol. 12, pp.1885–1904, 2021.

[24] M. S. Resen and M. M. Laftah, "A blind video copyright protection technique in maximum and minimum energy frames based on the fast walsh hadamard transform (FWHT) and discrete wavelet transform (DWT), and arnold map," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 16, no. 10, pp. 163–175, 2022. https://doi.org/10.3991/ijim.v16i10.30039

[25] S. H. Abbood, M. Rahim, and A. M.Alaidi, "DR-LL gan: Diabetic retinopathy lesions synthesis using generative adversarial network," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28005

[26] H. T. ALRikabi and H. T. Hazim, "Secure chaos of 5G wireless communication system based on IOT applications," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[27] M. K. Abdul-Hussein, "Evaluation of the interference's impact of cooperative surveillance systems signals processing for healthcare," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 03, pp. 43–59, 2022. https://doi.org/10.3991/ijoe.v18i03.28015

[28] N. Alseelawi, "A novel method of multimodal medical image fusion based on hybrid approach of NSCT and DTCWT," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 03, 2021. https://doi.org/10.3991/ijoe.v18i03.28011

[29] I. A. Aljazaery, H. T. Salim, and A. H. M. Alaidi, "Encryption of color image based on DNA strand and exponential factor," *International Journal of Online and Biomedical Engineering (iJOE)*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28021

[30] A. Al-zubidi, R. K. Hasoun, and S. H. Hashim, "Mobile application to detect Covid-19 pandemic by using classification techniques: Proposed system," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 16, pp. 34–51, 2021. https://doi.org/10.3991/ijim.v15i16.24195

[31] H. T. Hazim and H. Alrikabi, "Enhanced data security of communication system using combined encryption and steganography," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[32] H. A. Naman, N. A. Hussien, M. L. Al-dabag, and H. T. Alrikabi, "Encryption system for hiding information based on internet of things," *International Journal of Interactive Mobile Technologies (iJIM)*, vol. 15, no. 2, pp. 172–183, 2021. https://doi.org/10.3991/ijim.v15i02.19869

9 Authors

Nashwan Alsalam Ali is a member of the college of education for women, computer science department, University of Baghdad, Iraq. He received his B.Sc. degree in computer Science in 2003 from Technology University in Baghdad, Iraq. His M.Sc. degree in Computer Science focuses on Multimedia Security from Iraqi Commission for Computers and Informatics in Baghdad, Iraq. His Ph.D. in Computer Science, Technology University in Baghdad, Iraq. He can be contacted at (email: nashwan_alsalam60@coeduw.uobaghdad.edu.iq).

Iman I. Hamid is a member of the college of education for women, computer science department, University of Baghdad, Iraq. She received his B.Sc. degree in Computer Science in 2000 from Mustansiriyah University in Baghdad, Iraq. Her M.Sc. degree in Computer Science from Iraqi Commission for Computers and Informatics in Baghdad, Iraq. She can be contacted at (email: iman.hamid@coeduw.uobaghdad.edu.iq).

Article submitted 2023-01-12. Resubmitted 2023-02-17. Final acceptance 2023-02-24. Final version published as submitted by the authors.