Data Hiding in 3D-Medical Image

https://doi.org/10.3991/ijoe.v18i03.28007

Balsam Abdulkadhim Hameedi[1(✉)], Muna Majeed Laftah[2], Anwar Abbas Hattab[1]
[1]University of Mustansiriyah, Baghdad, Iraq
[2]University of Baghdad, Baghdad, Iraq
balsamkadom278@uomustansiriyah.edu.iq

Abstract—Information hiding strategies have recently gained popularity in a variety of fields. Digital audio, video, and images are increasingly being labelled with distinct but undetectable marks that may contain a hidden copyright notice or serial number, or even directly help to prevent unauthorized duplication. This approach is extended to medical images by hiding secret information in them using the structure of a different file format. The hidden information may be related to the patient. In this paper, a method for hiding secret information in DICOM images is proposed based on Discrete Wavelet Transform (DWT). Firstly. segmented all slices of a 3D-image into a specific block size and collecting the host image depend on a generated key, secondly selected the block number and slice number, thirdly, the low-high band used for embedding after adding the generated number, fourthly, used the Hessenberg transform on the blocks that portioned the band (low-high) in a specific size. The secret information (image or text) is a binary value. It was embedded by setting the positive value in the diagonal to odd values if the embedded is one and setting it to even if the secret bit is zero. Several tests were applied, such as applying mean square error, peak signal to noise ratio PSNR, and structural similarity index measure SSIM. Some analyses such as adding noise, scaling, and rotation analysis are applied to test the efficiency. The results of the tests showed the strength of the proposed method.

Keywords—DICOM 3D-image, discrete wavelet transform, image watermark, key generation

1 Introduction

Cryptography and data hiding ensure that the data is being sent securely. The fact that the information hiding is different from cryptography that needs a cover media for embedded information [1]. Data hiding can be used for secret communication or to include additional visual information [2]. The data hiding method is used in some applications, such as those in the medical and military fields [3]. Important diagnostic information can be found in medical images [4]. Digital watermark technology has been developed for hiding copyright information in the image visually or invisibly [5]. The visible watermark consists of overlaying a proprietary logo in the original image, while for an invisible watermark that can perform copyright protection more robustness from many removable visible watermarking technologies [6, 7].

The key generation process is employed with encryption systems that are used in both symmetric and public-key cryptography methods or to map hiding information in data hiding methods [8, 9]. A random number generator (RNG) or a PRNG, which is a computer method that creates randomly examined results, are used to create keys. Linear recurrence, non-linear congruence, linear feedback shift registry (LFSR), cellular automata, the non-linear issue with logarithms, and other approaches are used to produce pseudo-random numbers [10, 11]. Pseudo-random number sequences are commonly used in communication and digital computing applications. Many applications demand the disappear random but predictable to the user [12]. The Linear Congruential Generator (LCG) which can be used to produce such sequences requires minimal memory (typically 32 or 64 bits) to retain state. This makes it valuable for simulating multiple independent streams [13]. Linear Feedback Shift Register (LFSR) is a shift register with a feedback path linearly related to the nodes using XOR gates. LFSRs are more popular because of their compact and simple design [14]. In [15], they proposed a color-medical copyright protection system based on a disorderly system and Quaternion Polar Harmonic Transforms (QPHT), which are quaternion orthogonal moment processes, that does not require any watermarking. Calculate QPHTs for the original medical color and determine accurate coefficients for producing a null and void image when inserting watermarks. In [16, 17], They use domain transformation technologies to provide a comprehensive and secure solution to watermarking for telehealth applications. For verification, annotation, and identification, the patient report/identity is incorporated in the host medical image. Apply a mess-based encryption technique to a watermarked image in a less difficult approach for improved secrecy. In [18], they presented a watermarking algorithm in the transform domain with two separate methods, the first one has combined the digital watermark and Electronic Patient Record (EPR) in the two regions: The Interest Regions (ROI) and the Non-Interest Region (RONI). In the second method, the digital watermark and EPR are hidden by the Non-Interest Region (RONI). Discrete Cosine Transform (DCT) was used in any 8 to 8 block algorithms.

This work presents an efficient method for hiding data in the wavelet domain using Hessenberg transform and DICOM image as a cover medium. The contributions of this work are represented by several points such as the hiding implemented in the collected matrix from 3-medical image depend on the proposed hybrid key generation method (LFSR-CG), the embedding implemented in the wavelet domain, adding generated number to a specific-band of the transform for more complexity, applying Hessenberg factorization, all these issues make the proposed method more efficiency and can be implemented in transfer the secret information in the medical image.

2 Discrete wavelet transform

Wavelet analysis is a technique for separating the information in an image into approximation and detailed sub-signals. The image's vertical, horizontal, and diagonal features or changes are revealed by three detailed sub-signals, while the approximation sub-signal reveals the overall trend of the pixel value. The first is the Continues wavelet transform, and the second is the Discrete wavelet transform [19, 20]. Wavelet analysis is calculated using filter banks. Filters are divided into two categories: **A high-pass filter** preserves high-frequency information while obliterating low-frequency information, and **Low pass filter**: high-frequency information is obliterated while law frequency data is preserved. The signal is split into two parts: a detailed part (high frequency) and a low-frequency approximation part (law frequency). Level 1 is the horizontal detail, level 2 is the vertical detail, and level 3 is the diagonal detail in the visual signal [21]. The methods used in [22–24] the frequency components to make an increased level of safety and make it more difficult for attackers to win.

3 Hessenberg transform

A Hessenberg matrix is a type of square matrix that is “nearly” triangular in linear algebra. A lower Hessenberg matrix has zero entries above the first super diagonal, while an upper Hessenberg matrix has zero entries below the first sub diagonal [25]. When applied to triangular matrices, many linear algebra procedures require substantially less computational effort, and this benefit often extends to Hessenberg matrices as well. If the constraints of a linear algebra issue prevent a general matrix from being reduced to a triangular one, the next best thing is generally reduction to Hessenberg form. Every matrix can be reduced to a Hessenberg form in a finite number of steps [26]. Iterative approaches, such as shifting QR-factorization, can be used to reduce the Hessenberg matrix to a triangular matrix. Shifted QR-factorization along with deflation stages can further decrease the Hessenberg matrix to a triangular matrix in eigenvalue methods.

4 Medical image (DICOM image)

The DICOM standard may be considered to have many support levels or various measures. Support for picture sharing for senders and receivers is the most basic, main level of support. Other measurements are handling of images, content planning for the patient, image quality, media storage, safety, etc. The information model for DICOM contains connections between the DICOM objects and a standard terminology [27]. The information objects of DICOM are descriptions to share the information. They can be seen as templates repeatedly reused when a mode produces a new image or other DICOM entity. There are basic characteristics of each image type and, thus, information object. The Digital Imaging and Communications in Medicine DICOM Standard. specifies a non-proprietary data interchange protocol, digital image format, and file structure for biomedical images and image-related information [28]. The DICOM standard is useful for integrating all modern imaging equipment, accessories, networking servers, workstations, printers, and picture archiving and communication systems (PACS) that may have been installed by multiple manufacturers.

5 Proposed method design

In this work, a method for hiding secret information (text or image) in the 3D-medical image (DICOM) is proposed. The method used key generation for specifying the location of hiding secret information. Linear feedback shift registers (LFSR) and linear congruential generators (LCG) are used to generated sequences of stream numbers appearance as random numbers. The block diagram of the process steps in the proposed method is shown in Figure 1 and the explanation of these steps are as follow:

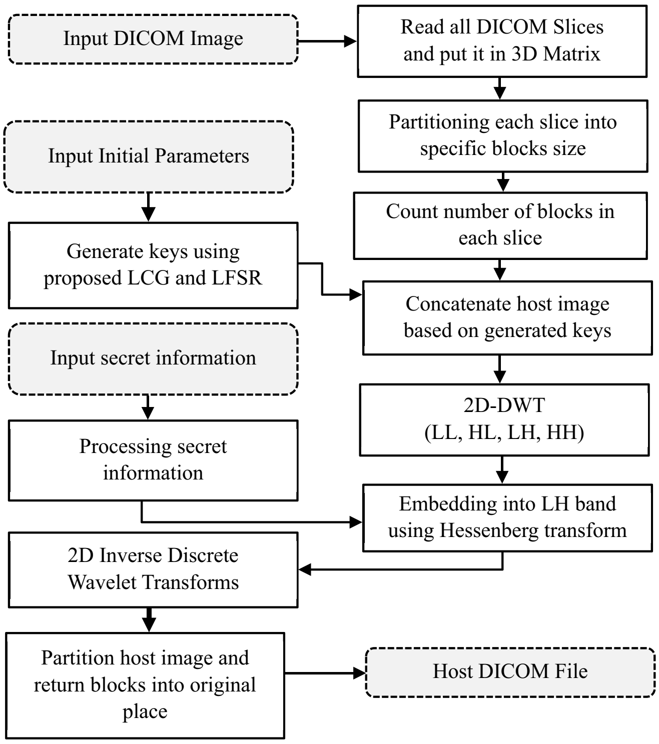
Input DICOM Image
Read all DICOM Slices and put it in 3D Matrix
Partitioning each slice into specific blocks size
Input Initial Parameters
Count number of blocks in each slice
Generate keys using proposed LCG and LFSR
Concatenate host image based on generated keys
Input secret information
2D-DWT (LL, HL, LH, HH)
Processing secret information
Embedding into LH band using Hessenberg transform
2D Inverse Discrete Wavelet Transforms
Partition host image and return blocks into original place
Host DICOM File

Fig. 1. The framework of proposed method

5.1 Read all DICOM slices in 3D matrix

This step is the first one in the proposal representing by reading all slices of the DICOM image and put them in three dimensions array.

5.2 Image partitioning

Each slice is partitioned into a specific block size (8×8) for example as shown in Figure 2. Each block is returned to the same place that takes it from before depend on the generated key.

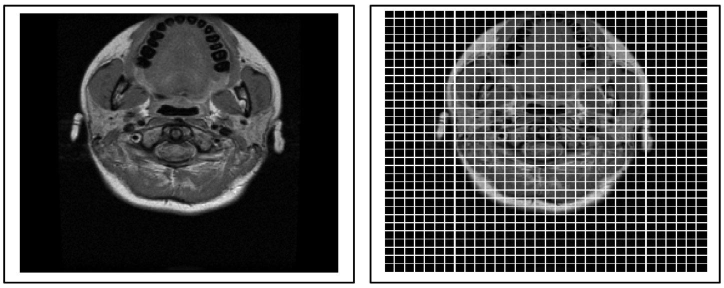

Fig. 2. Host image partitioning for each slice

5.3 Generate keys using LFSR-CG

The generated key in this proposal is represented by select blocks and select the slice number for concatenating the host image (cover medium). The block is indexed and the generated key is used to find the number of blocks and the slice number.

5.4 Concatenate host image based on generated keys

Each block is put in the new buffer to find the host image that will be used for embedding secret information. This step is explained in Figure 3.

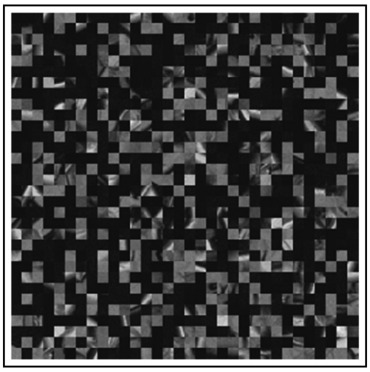

Fig. 3. The host image

5.5 Discrete wavelet transform (LL, HL, LH, HH)

The formation image (host image) is transformed using Discrete Wavelet Transform as shown in Figure 4 The results of four bands from the transform as the Low-Low band, High-Low, Low-High, and High-High band. For embedding the secret information key generation is used again by generating numbers in the specific range equal to the values in the selected band for embedding. These numbers will subtract after the embedding procedure.

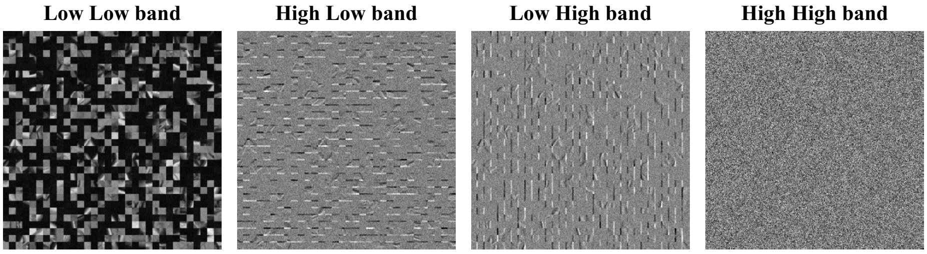

Fig. 4. Discrete wavelet transform of the host image

5.6 Processing secret information

The secret information hiding in the proposed method is either text or binary image. The text is converted to binary form and put in vector then padded with zeros and put into a two-dimensional array equal to the Low-High band as shown in Figure 5.

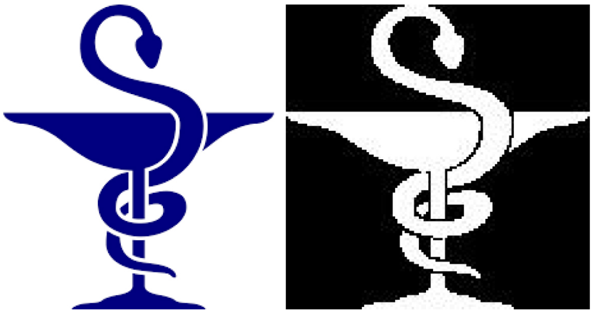

Fig. 5. Processing secret image

If information is an image, the process was converted to grey and then converted to binary form and then complimented the image to reduce the changes in the hosted image. The last step is to resize the secret image into a size equal to a Low-High band.

5.7 Embedding into LH band

The embedding process is represented by partitioning the selected band into 4×4-block. Each block is converted using Hessenberg transform that will produce a Hessenberg matrix H and a unitary matrix P so that A = P×H×P' and P'×P = Identity Matrix with size equal to size input matrix A. The diagonal of each block used for embedding make the number of positive value odd when the embedded bit was one and it is even when the embedded bit was zero. If the number of positive values is similar to the condition nothing will change otherwise a small change will occur. LH-band before and after embedding is shown in Figure 6.

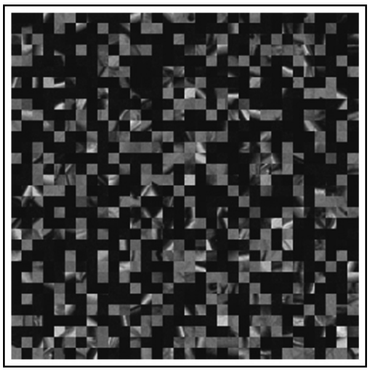

Fig. 6. The LH band before and after embedding process

5.8 2D-inverse discrete wavelet transforms

The three bands of the transformed hosted image are kept without any change and only the third band LH-band is updated for using them in inverse wavelet transform. The generated number that was added before is subtracted to return the blocks to the same position that got from. The hosted image after Inverse Discrete Wavelet transforms is shown in Figure 7.

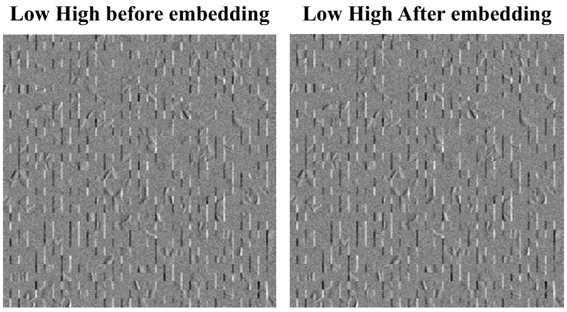

Fig. 7. Inverse DWT of the host image

5.9 Reorder hosted image into the original place

The updated image is again partitioned into the same size block (8×8) that was used before. Each block is returned to the same place that takes it from before depend on the generated key. Finally, for hiding secret images, the size of data is greater than text so the host image will resize to the dimension satisfying the embedding data size with the same procedure that applied to text data. at all the embedded data converted to binary form.

5.10 Proposed extraction method

The data extraction process includes applying the same steps that were previously included, which include reading the medical image (DICOM) and dividing it into blocks of the same size as before and performing the process of generating keys with the same initial values that were used in the first phase to generate the same numbers through which the same blocks are selected to assemble them elsewhere to configure the cover image) and get hidden information as explained in Figure 8. At first, concatenating the hosted image depending on key generation is shown in Figure 9.

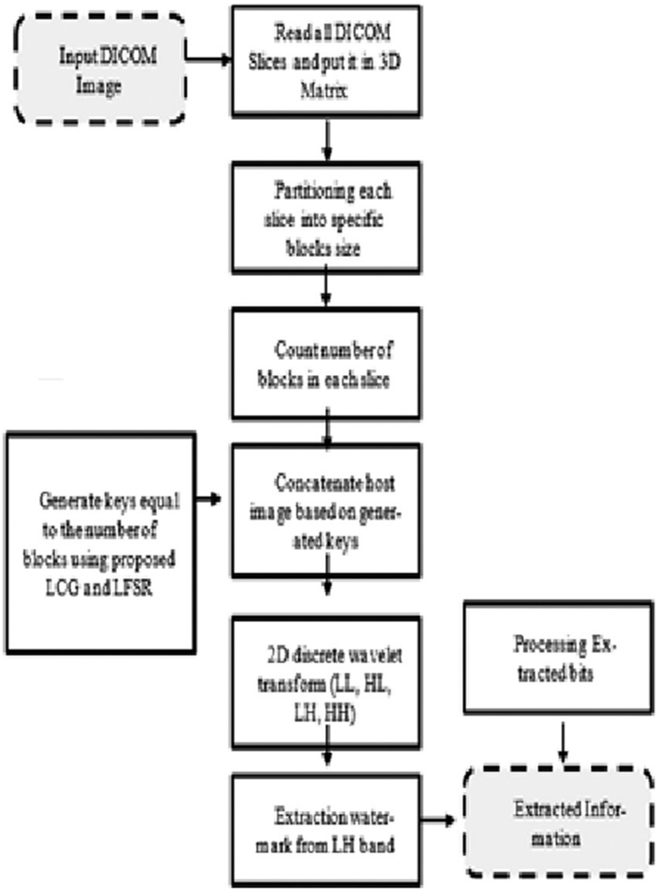
Input DICOM Image
Read all DICOM Slices and put it in 3D Matrix
Partitioning each slice into specific blocks size
Count number of blocks in each slice
Generate keys equal to the number of blocks using proposed LCG and LFSR
Concatenate host image based on generated keys
2D discrete wavelet transform (LL, HL, LH, HH)
Processing Extracted bits
Extraction watermark from LH band
Extracted Information

Fig. 8. Block diagram for proposed extraction method

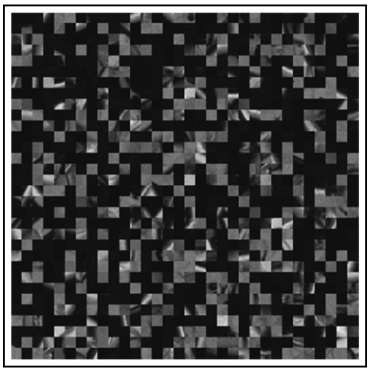

Fig. 9. Concatenating the block image

The cover image is transformed using discrete wavelet transform as shown in Figure 10 and produced four bands' Low-Low band, High-Low, Low-High, and High-High band.

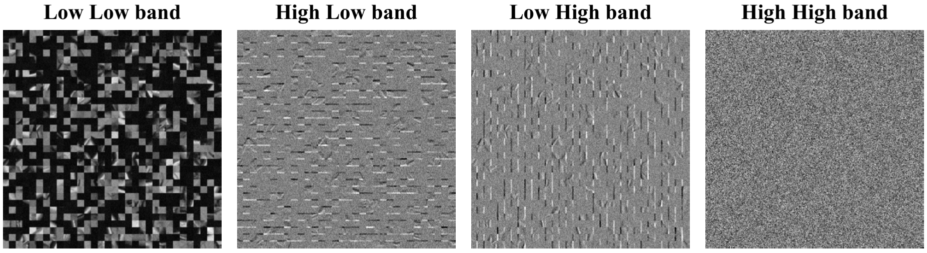

Fig. 10. Discrete wavelet transform of the host image

For extraction secret Information is either text or binary image. The bits are extracted by applying the same steps using in embedding for partitioning the used bands in hiding. On each block applying Hessenberg transform and find the positive value in the diagonal (count the number of positive values). If the number of positive is odd the embedding bit be one otherwise the bit will be zero. If the secret was text, the padded bit is neglected and get the only first specified bits.

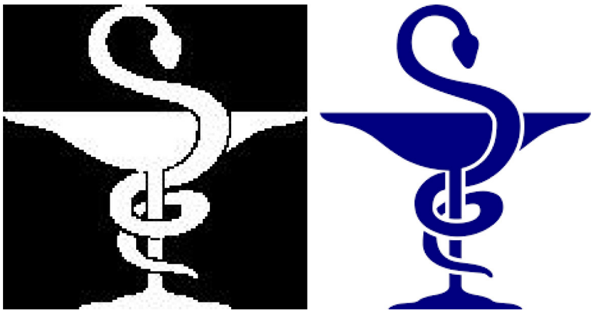

Fig. 11. Extraction secret image

If information is an image, the same process is applied and get the secret bits that are put in the image and it flipped to its complement form and resized to the same size as the original image as shown in Figure 11.

6 Experimental results

To implement the proposed methods, the MATLAB R2018b was used as a tool for programming language. A Windows10-based four-core Intel Core i7 MacBook Pro CPU @ 4.7G GHz Laptop with 8 Gigabyte-RAM has been used to perform all the experiments reported in this thesis. DICOM data object has several properties, such as name, ID, and so on, as well as one specific attribute that contains the picture pixel data. A DICOM object can only have one attribute that contains pixel data. This refers to a single image in several modalities. However, the property can have many "frames," allowing cine loops or other multi-frame data to be stored. Three- or four-dimensional data can be wrapped in a single DICOM object in certain instances. JPEG, lossless JPEG, JPEG 2000, and run-length encoding are some of the standards that can be used to compress pixel data (RLE). Figure 13 depicts slices of DICOM image that were used as DICOM images to conceal hidden information. The secret images used in proposed methods include a collection of images that are represented as logos. They exist several forms that will be used for hiding them in 3D medical images and then trying to extract them. Some samples of secret information (images) explain in Figure 12.

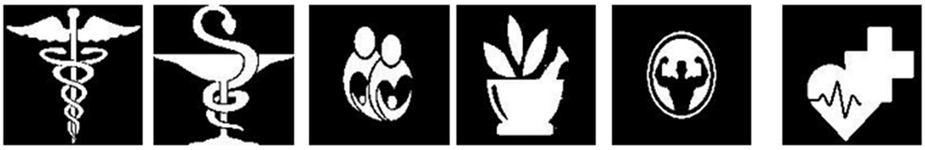

Fig. 12. Secret image samples

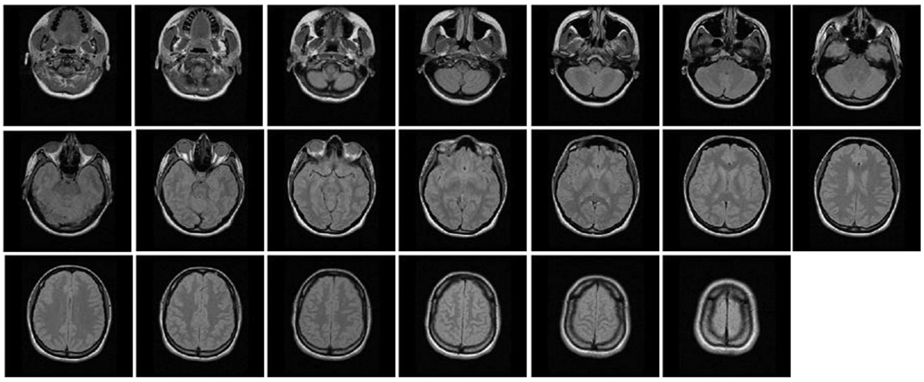

Fig. 13. DICOM image slices

Image quality is seen as a distinguishing feature of an image. Degradation is usually assessed in comparison to an ideal image known as image quality, which can be defined both technically and objectively to indicate the divergence from the ideal or reference model. Noise has an impact on image quality decrease. This noise is dependent on how it relates to the information in the image that the viewer is looking for. Acquisition, augmentation, compression, and transmission are only a few of the features that can be applied to visual data. After processing, some of the information offered by an image's features may be altered. As a result, the human view perceptron should be used to assess the quality. There are two types of appraisals in practice: subjective and objective. Subjective evaluation takes a long time and is costly to implement. Following that, objective image quality measurements are constructed based on several factors. For objective image quality assessment, a variety of methodologies and metrics are available.

6.1 Mean square error test

The MSE test is investigative the difference between the original image and the image carrying the hidden data. the test applied as confidential information and hidden in a set of DICOM slides, the results were as shown in Figure 14.

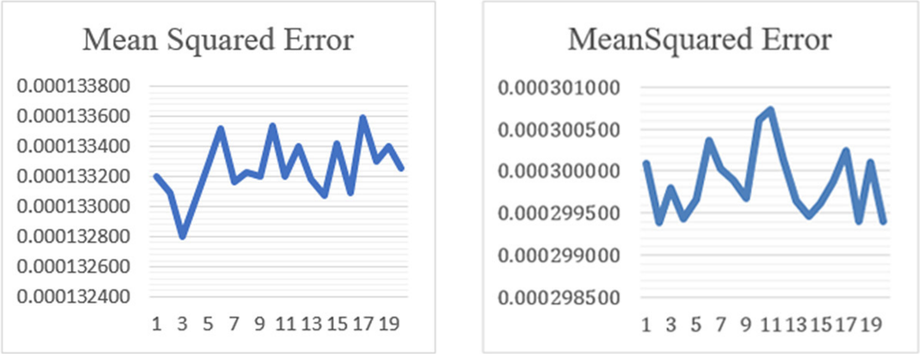

Fig. 14. A. Mean square error test (hiding text) B. Mean square error test (hiding image)

From the previous figures, the MSE rate is a low value that explains the similarity between host slices with original slices. the same test was applied to another type of hidden information (image) and the results explain in Figure 15. An average of six binary images was used for MSE testing and the MSE rate for image hiding is the low value that explains the similarity between host slices with original slices.

6.2 Peak signal to noise ratio test

PSNR test depends on MSE in the opposite order that the high value means the high similarity with the reference's images. It's applied the image results explained in Table 1 for the results of hiding texts in DICOM slices. And For hiding image in DICOM, Table 2 explain the result of hiding six binary images in the same slices respectively.

Tables 1 & 2. Peak signal to noise ratio test

Text#	Text1	Text2	Text3	Text4	Text5	Text6
Av.	38.745	38.759	38.756	38.753	38.754	38.751
image	Im. 1	Im. 2	Im. 3	Im. 4	Im. 5	Im. 6
Av.	35.229	35.227	35.234	35.225	35.233	35.233

From two previous tables, the mean value of PSNR is accurate in both tables which denoted the high similarity between the reference's images with host images.

6.3 Structural similarity index measure test

SSIM test applied on the host image with the references image to find the similarity between them. The SSIM test applied the same procedures for all cover mediums concerning the original status as explained in Tables 3 and 4 for hiding text.

Tables 3 & 4. SSIM test (hiding text)

Text#	Text1	Text2	Text3	Text4	Text5	Text6
Av.	0.8890	0.8893	0.8892	0.8891	0.8892	0.8891
image	Im. 1	Im. 2	Im. 3	Im. 4	Im. 5	Im. 6
Av.	0.8911	0.8905	0.8916	0.8905	0.8924	0.8911

6.4 Information hiding analysis

There several tests for analyzing the retrieval of secret information by making some changes to the images and find the extraction information quality such as:

A. Add noise analysis

This test was applied by adding noise to the DICOM slices and find the bit error rate of a secret image pixel. Several rates of noise are added to all slices in 3D-DICOM Image for all secret images that are used in testing and the results are explained in Table 5.

Table 5. Adding noise test

Image	Noise Rate				
	0.6%	0.7%	0.8%	0.9%	1.0%
1	0.0125	0.0586	0.0408	0.0862	0.0959
2	0.0261	0.0681	0.0867	0.1191	0.1492
3	0.0320	0.0435	0.0981	0.1125	0.1565
4	0.0544	0.0952	0.0645	0.0918	0.0723
5	0.0483	0.0625	0.1021	0.1074	0.1433
6	0.0071	0.0264	0.0459	0.0596	0.0955
Av.	0.0301	0.0591	0.0730	0.0961	0.1188

From the previous table, the minimum bit error rate when the added noise is less value in the experiment (0.6% added noise rate) and the maximum bit error rate when the highest value of noise rate in the experiment (1.0% added noise). Figure 16 explain the extraction binary image when added noise is 1.0%.

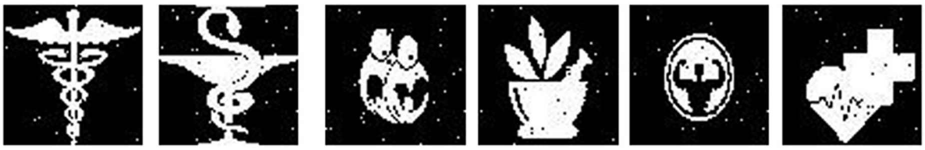

Fig. 15. The extracted secret images (noise)

B. Scaling analysis

This test was applied by scaling host image with different scaling factors such as 0.8 1.2 1.4 1.6, or 1.8 to find the effect of this factor on secret image retrieval. Several rates are tested and all retrieve the secret image in 100 per cent. Figure 17 explain the extraction binary image when tested with the scaling factor.

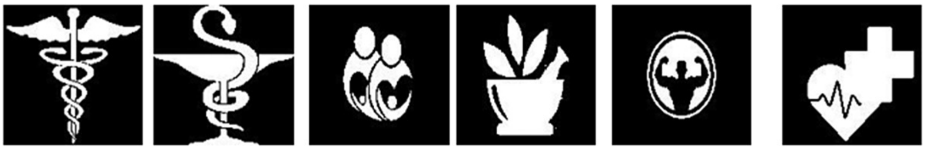

Fig. 16. The extracted secret images (scaling)

C. Rotation analysis

This test was applied by rotating the DICOM slices to a specific degree and again rotating them in reverse order and find the effect of this operation on the secret image retrieval. Several rates of rotation are applied to all slices in 3D-DICOM Image for all secret images that are used in testing and the results are explained in Table 6.

Table 6. Rotation test

Image	Degree of Rotate Angle				
	0.01	0.02	0.03	0.04	0.05
1	0.17646	0.22305	0.26055	0.28018	0.3083
2	0.15508	0.19316	0.22422	0.24238	0.26436
3	0.19375	0.24531	0.28604	0.30889	0.32119
4	0.14688	0.19785	0.22041	0.24209	0.26084
5	0.20049	0.24971	0.29131	0.32852	0.34141
6	0.14277	0.18203	0.20869	0.23564	0.25791
Av.	0.16924	0.21519	0.24854	0.27295	0.29233

From the previous table, the minimum bit error rate when the rotation is less value in the experiment (0.01%-degree rate) and the maximum bit error rate when the highest value of rotation rate in the experiment (0.05% rotation noise). Figure 18 explain the extraction binary image when rotation applied 0.01%.

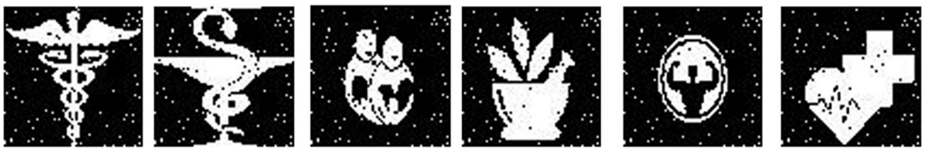

Fig. 17. The extracted secret images (rotation)

D. Visualization of secret images

The proposed method on six secret images and these images retrieved when applied extraction method as explained in Figure 19 for secret image 1, secret image 2. respectively.

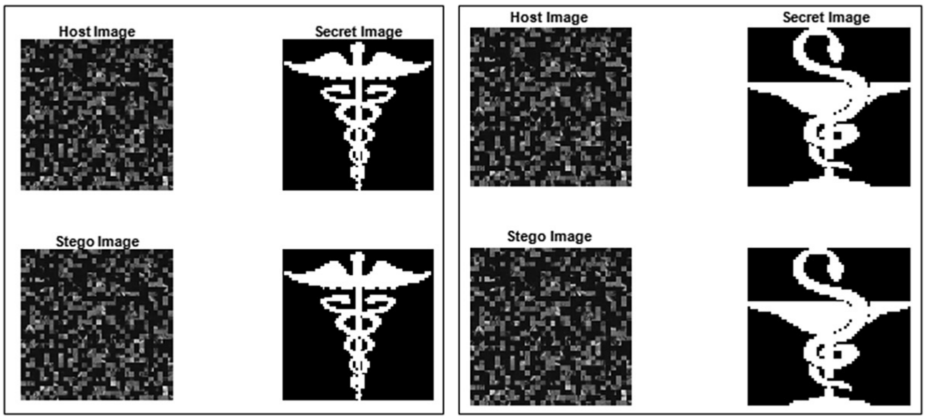

Fig. 18. Secret image 1 before and after extraction in scaling

7 Conclusions

According to the experimental results of using the proposed method, adding keys to the hiding process increases security and makes it more difficult for attackers to analyze confidential information, combining more than one method of key generation improves the randomness needed in the numbers generated in the keys, and using multiple types of information (text and image) in the hiding process demonstrates the flexibility for embedding information. Hiding in the wavelet domain is more resistant to attacks than hiding in the spatial domain Because transforming to another domain makes it difficult to extract information. Because the influence is spreading across a collection of pixels in the frequency domain, the quantity of degradation is more than in the spatial domain, but the altering is local in the spatial domain. Without knowing these values, adding produced numbers to the bands of DWT before embedding makes the extraction more difficult. One of the recommendations is that it is possible to scale by combining the proposed key generation with different methods. Using the proposed method in a different environment with a different sort of medical imaging. With the video stream, using the proposed concealing approach. Applying two proposals to the same collection of photos and treating them as two sections with a chosen indicator bit. Using another transform in the second proposed method, such as single value decomposition, to replace the Hessenberg transform.

8 References

[1] J. Selvakumari and S. Jeyaraj, “Using visible and invisible watermarking algorithms for indexing medical images,” *Int. Arab J. Inf. Technol,* vol. 15, no. 4, pp. 748–755, 2018.

[2] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, “Hiding clinical information in medical images: a new high capacity and reversible data hiding technique,” *Journal of biomedical informatics,* vol. 66, pp. 214–230, 2017. https://doi.org/10.1016/j.jbi.2017.01.006

[3] H. Agarwal, D. Sen, B. Raman, and M. Kankanhalli, “Visible watermarking based on importance and just noticeable distortion of image regions,” *Multimedia Tools Applications,* vol. 75, no. 13, pp. 7605–7629, 2016. https://doi.org/10.1007/s11042-015-2685-3

[4] K. Bhattacharjee, K. Maity, and S. Das, “A search for good pseudo-random number generators: Survey and empirical studies,” *arXiv preprint arXiv:.04035,* 2018.

[5] M. H. Ruslih, T. W. Purboyo, and A. S. R. Ansori, “A study of several algorithms for pseudo-random generator based on field programmable gate array (FPGA),” 2006.

[6] D. K. Mahto and A. Singh, “A survey of color image watermarking: State-of-the-art and research directions,” *Computers Electrical Engineering,* vol. 93, p. 107255, 2021. https://doi.org/10.1016/j.compeleceng.2021.107255

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

[8] S. Marwan, A. Shawish, and K. Nagaty, “Utilizing DNA strands for secured data-hiding with high capacity,” *International Journal of Interactive Mobile Technologies,* vol. 11, no. 2, 2017. https://doi.org/10.3991/ijim.v11i2.6565

[9] I. Sawaneh and Humanities, “DWT based image compression for health systems,”Journal of Advance Research in Social Science and Humanities, vol. 4, no. 9, pp. 01–67, 2018. https://doi.org/10.53555/nnmhs.v4i9.603

[10] H. Alrikabi, and H.Tauma, “Enhanced data security of communication system using combined encryption and steganography,” *International Journal of Interactive Mobile Technologies,* vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[11] D. Bucerzan, M. Crăciun, V. Chiş, and C. Raţiu, “Stream ciphers analysis methods,” *International Journal of Computers Communications Control,* vol. 5, no. 4, pp. 483–489, 2010. https://doi.org/10.15837/ijccc.2010.4.2506

[12] P. Kitsos, N. Sklavos, N. Zervas, and O. Koufopavlou, “A reconfigurable linear feedback shift register (LFSR) for the Bluetooth system,” in *ICECS 2001. 8th IEEE International Conference on Electronics, Circuits and Systems (Cat. No. 01EX483)*, 2001, vol. 2: IEEE, pp. 991–994.

[13] E. Matsuyama, D.-Y. Tsai, Y. Lee, and N. Takahashi, “Comparison of a discrete wavelet transform method and a modified undecimated discrete wavelet transform method for denoising of mammograms,” in *2013 35th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC)*, 2013: IEEE, pp. 3403–3406. https://doi.org/10.1109/EMBC.2013.6610272

[14] S. K. Mohanty, "I/O efficient algorithms for matrix computations," *arXiv preprint arXiv:.00733,* 2010.

[15] Z. Xia, X. Wang, W. Zhou, R. Li, C. Wang, and C. Zhang, "Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms," *Signal Processing,* vol. 157, pp. 108–118, 2019. https://doi.org/10.1016/j.sigpro.2018.11.011

[16] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimedia tools Applications,* vol. 78, no. 3, pp. 3457–3470, 2019. https://doi.org/10.1007/s11042-018-6263-3

[17] S. M. Najeeb, S. M. Ali, and H.Salim "Finding the discriminative frequencies of motor electroencephalography signal using genetic algorithm," *Telkomnika,* vol. 19, no. 1, pp. 285–292, 2021. https://doi.org/10.12928/telkomnika.v19i1.17884

[18] S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: a robust medical image watermarking system for E-healthcare," *Multimedia Tools Applications,* vol. 76, no. 8, pp. 10599–10633, 2017. https://doi.org/10.1007/s11042-015-3127-y

[19] P. Kumar, "Image denoising model based on wiener filter and a novel wavelet," *Image,* vol. 3, no. 6, 2018.

[20] I. A. Aljazaery, H. Alrikabi, and M. R. Aziz, "Combination of hiding and encryption for data security," *International Journal of Interactive Mobile Technologies,* vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[21] O. Abodena and M. Agoyi, "Colour image blind watermarking scheme based on fast walsh hadamard transform and hessenberg decomposition," *Studies in Informatics Control,* vol. 27, no. 3, pp. 339–348, 2018. https://doi.org/10.24846/v27i3y201809

[22] H. Th. ALRikabi, N. A. Jassim, "Design and implementation of smart city applications based on the internet of things," *iJIM,* vol. 15, no. 3, 2021. https://doi.org/10.3991/ijim.v15i13.22331

[23] M. Brundage *et al.*, "The malicious use of artificial intelligence: Forecasting, prevention, and mitigation," 2018.

[24] M. Al-dabag, H. S. ALRikabi, and R. Al-Nima, "Anticipating atrial fibrillation signal using efficient algorithm," *International Journal of Online and Biomedical Engineering (iJOE),* vol. 17, no. 2, pp. 106–120, 2021. https://doi.org/10.3991/ijoe.v17i02.19183

[25] Q. Su and B. Chen, "A novel blind color image watermarking using upper Hessenberg matrix," *AEU-International Journal of Electronics Communications in soil science plant analysis,* vol. 78, pp. 64–71, 2017. https://doi.org/10.1016/j.aeue.2017.05.025

[26] M. Rutherford *et al.*, "A DICOM dataset for evaluation of medical image de-identification," *Scientific Data,* vol. 8, no. 1, pp. 1–8, 2021. https://doi.org/10.1038/s41597-021-00967-y

[27] L. Yan, "DICOM standard and its application in PACS system," *Medical Imaging Process Technology,* vol. 1, no. 1, 2018. https://doi.org/10.24294/mipt.v1i1.221

[28] T. Cvija and K. Severinski, "Multiple medical images extraction from DICOM and conversion to JPG using Python," *Ri-STEM-,* p. 33, 2021.

9 Authors

Balsam Abdulkadhim Hameedi is presently master student in University of Mustansiriyah, Baghdad, Iraq/College education, computer Science department. She received his B.Sc. degree in computer science in 2000 from Mustansiriyah, Baghdad, Iraq/College education, computer Science department in Baghdad, Iraq.

Muna Majeed Laftah is presently Asst. Prof in Baghdad University/College education for women/Computer Science department. She received his B.Sc. degree in computer science in 1995 from the Al Technology University in Baghdad, Iraq. Her M.Sc. degree in computer science focuses on multimedia security from the Iraqi Commission for Computers and Informatics/Iraq in 2003. Her Ph.D. degree in computer science from Al technology University in Baghdad, Iraq/2017. Her current research interests include 3D security, encryption of multimedia. E-mail: muna.majeed@coeduw. uobaghdad.edu.iq

Anwar Abbas Hattab is presently Asst. Prof in University of Mustansiriyah, Baghdad, Iraq.

Article submitted 2021-11-11. Resubmitted 2021-12-20. Final acceptance 2021-12-22. Final version published as submitted by the authors.