Lightweight digital imaging and communications in medicine image encryption for IoT system

Muntaha Abdulzahra Hatem[1], Balsam Abdulkadhim Hameedi[2], Jamal Nasir Hasoon[3]
[1]Department of Missions and Cultural Relations, Ministry of Higher Education and Scientific Research-Iraq, Baghdad, Iraq
[2]Lecturer of Computer Science, Ministry of Education-Iraq, Baghdad, Iraq
[3]Department of computer sciences, Faculty of Science, Mustansiriyah University-Iraq, Baghdad, Iraq

Article Info

Article history:

Received Nov 04, 2022
Revised Feb 21, 2023
Accepted Mar 01, 2023

Keywords:

Five-dimensional chaotic map
Information entropy
Intensity
Lightweight present algorithm
Mean square error
Peak-to-signal noise ratio
Unified average changing

ABSTRACT

Diagnosis in healthcare systems relies heavily on the use of medical images. Images such as X-rays, ultrasounds, computed tomography (CT) scans, magnetic resonance imaging (MRIs), and other scans of the brain and other internal organs of patients include private and personal information. However, these images are vulnerable to unauthorized users who unlawfully use them for non-diagnostic reasons due to the lack of security in communication routes and the gaps in the storage systems of hospitals or medical centers. Image encryption is a prominent technique used to protect medical images from unauthorized access in addition to enhancing the security of communication networks. In this paper, researchers offer a lightweight cryptosystem for the secure encryption of medical images that makes use of the present block cipher and a five-dimensional chaotic map. More than 25 images from the open science framework (OSF) public database of patients with coronavirus disease 2019 (COVID-19) were used to evaluate the proposed system. DICOM stands for "digital imaging and communications in medicine". The efficiency of the proposed system is proved in terms of adjacent pixels' correlation analysis, National Institute of Standards and Technology (NIST) analysis, mean square error, information entropy, unified average changing intensity, peak-to-signal noise ratio, entropy, and structure similarity index image.

Corresponding Author:

Muntaha Abdulzahra Hatem
Department of Missions and Cultural Relations, Ministry of Higher Education and Scientific Research-Iraq
Al-Rusafa-Baghdad, Iraq
Email: muntaha.hatem@scrdiraq.gov.iq

1. INTRODUCTION

The Internet of Things (IoT) is a hybrid network that combines the internet with low-bandwidth networks so that inanimate things may send and receive data. Integrating many forms of technology and methods of communication, it is a promising area. Multiple industries may benefit from several IoT applications, including e-health, e-commerce, e-home, and so on [1]. Sensitive information is included in healthcare data, most notably in digital imaging and communications in medicine (DICOM) images, which have been communicated, stored, and preserved in unsecure ways to facilitate telemedicine [2]. Therefore, protecting DICOM images from being seen by the wrong people is a pressing concern. There are a variety of methods, such as encryption [3], [4] and watermarking [5], for safeguarding sensitive images. In e-health, the Internet of Things revolution will boost service quality while lowering costs [6]. Modern IoT cryptography categorization [7] considers the fact that some cryptographic approaches have been picked and tailored to meet the e-health system's restricted resources. These methods are known as lightweight cryptography (LWC).

The low power, high performance, cheap cost, and low energy consumption of the lightweight algorithms make them suitable for use in embedded systems and applications, which is regarded as ultralight [7]. Bits of fixed length and symmetric keys are used by lightweight block ciphers to define a transformation. This resilient primitive applies through substitution and the Feistel network [8] or permutation networks (SPN) [9], which requires more elementary operations [10]. For devices with little resources, the present is a simple cipher block that may be implemented in a 1000 gate equivalent (GE). It represents a turning point in the study of lightweight ciphers and acts as a standard for contemporary ciphers. The benefits of data encryption standard (DES) and advanced encryption standard (AES) are combined. It contains keys with sizes of 80 or 128 bits and blocks of 64 bits. It consists of 31 cycles of the permutation and substitution network [11]. Designing a good and safe cipher requires consideration of both confusion and dissemination. All block ciphers generate ciphers, i.e., they rely on diffusion and confusion operations that come after. While the diffusion is often associated with a permutation or mixing layer, the misunderstanding is frequently associated with a substitution layer (S-boxes) [12].

In 2016, a study was carried out by Natsheh *et al.* [13], provides a simple and effective encryption approach for pixel data for multi-frame DICOM medical images. The main goal of the proposed approach is to reduce the encryption and decryption time of these images. The method represented by applying the AES for encryption one slice of DICOM image. The other slices are diffusion by an exclusive-or operation with the encrypted image. Only one image is encrypted and excusive-or operation cipher for encrypting the remaining multi-frame DICOM images. The encrypted image is evaluated in computational time for complexity, check the normalized correlation, calculate the entropy before and after encryption, find peak-signal-to-noise-ratio (PSNR) for similarity and histogram analysis.

Ravichandran *et al.* [14] proposed a hybrid encryption algorithm based on deoxyribonucleic acid (DNA) and multiple chaotic maps for encrypting the cooler DICOM images. This hybrid algorithm can be adaptable for both partial/selective and full medical image encryptions. The algorithm comprises three phases, namely, permutation, encoding, and diffusion. The acquired results have proved that the developed DNA-chao cryptic scheme useful in several real-time medical applications namely mobile health care services and wireless medical networking for protecting medical images.

Janakiraman *et al.* [15] created the hardware-dependent lightweight steganography scheme by considering resource constraints in the hardware for embedded applications. Janakiraman *et al*. [15] explored the device-dependent implementation of the cryptography schemes, which exhibits robustness against various attacks. The fact that the scheme exhibits robustness against various attacks is significant, as it suggests that the method is secure and can protect the hidden data from potential attackers.

Boussi *et al.* [2], presents a novel encryption method for securing DICOM images used in medical applications. The proposed algorithm splits the original image into blocks of 16×16 pixels and then encrypts it through three steps. Firstly, the keys $k1, k2, k3$, and $k4$ are transformed from four vectors of 16 pixels to a matrix of 16×16 pixels. Then, the proposed algorithm encrypts the image block-by-block using the Vigenère cipher algorithm. For each block, the proposed algorithm modifies the key using Arnold transform. The proposed encryption algorithm is scalable with color images and joint photographic experts group (JPEG) compression.

Raj *et al.* [16], presents a lightweight image encryption scheme for medical image security feasible to realize as concurrent architectural blocks on reconfigurable hardware like field programmable gate array (FPGA) to achieve higher throughput. Lorentz attractor's chaotic keys perform the diffusion process in the proposed encryption scheme. Simultaneously, the pseudo-random memory addresses obtained from a linear feedback shift register (LFSR) circuit accomplish the confusion process.

Manikandan and Amirtharajan [17] designed a remote embedding of patient information into encrypted medical images. The encryption process involves the Bülban map, Le Gall 5/3 transform, confusion, and diffusion. The algorithm was tested on over 30 DICOM images taken from open science framework (OSF), a public database for coronavirus disease 2019 (COVID-19) patients.

Therefore, this paper focuses on a new methodology for enhancement privacy and reduce the computational time of multi frames DICOM images encryption and decryption by using the five-domination chaotic map with present lightweight cipher algorithm. Statistical analysis of the proposed approach is performed on the cipher image to assess the encryption/decryption performance. Overall, the approach proposed in the paper could have important implications for the field of medical imaging, where privacy and security are critical concerns. By reducing computational time and improving encryption/decryption performance, the proposed approach could make it easier and more efficient to secure medical images and protect patient privacy.

The remaining of the paper is organized as: section 2 explains the design and algorithms of the proposed approach. Sections 3 explain the simulation proposed method, the evaluation metrics, and experimental results and discussion respectively. Section 4 explain the experimental test result about implementing the proposed method. Finally, section 5 conclusion of the proposed approach.

2. METHOD

Proposed lightweight DICOM image encryption aims to enhancement security of the multi frame DICOM medical image by using hybrid encryption method of five-dimensional chaotic map and present lightweight encryption algorithm. The proposed method encrypts multi frame securely and quickly by applying the proposed Algorithm 1. The proposed method could have important implications for medical image security, as DICOM images often contain sensitive patient information that needs to be protected from unauthorized access. By utilizing a hybrid encryption approach that leverages both a chaotic map and a lightweight encryption algorithm, the proposed method may provide a strong level of security while also being computationally efficient.

Algorithm 1. Proposed lightweight DICOM medical image

```
Input: multi frame DICOM medical Image; 5D chaotic map parameters
Output: cipher image
Begin
Step 1: read DICOM image
Step 2: find $(n)$ the number of slices in DICOM
Step 3: find the dimension of slice
Step 4: generated five dimensions' chaotic map seq$(x)$, seq$(y)$, seq$(z)$, seq$(k)$, and seq$(p)$ using (5), (6), (7), (8), and (9)
Step 5: used seq$(x)$ for slices permutation from 1 to $n$
Step 6: used seq$(y)$ for row permutation in each slice
Step 7: used seq$(z)$ for column permutation
Step 8: divide each slice into specific size block with index (ind)
Step 9: used seq$(k)$ for permutation blocks $NewBlock(ind) = block(k(ind))$
Step 10: each $NewBlock$ divide into sub-block with size 64-bit
Step 11: used seq$(p)$ for generating numbers equal to number of sub-blocks with the 80 bits size
Step 12: used present algorithm for encrypt all sub-blocks
Step 13: merge the sub-blocks into one block equal to input block
Step 14: concatenate all blocks into new encrypted slice
Step 15: merge all slices into encrypted DICOM image
End algorithm
```

As shown in Figure 1, the proposed algorithm encrypts image block-by-block going through seven steps: key generation, DICOM slice permutation, row permutation of DICOM slice, columns permutation of DICOM slice, block dividing, block selection, present encryption. It appears that the proposed algorithm for lightweight DICOM image encryption involves a block-by-block encryption process that consists of seven steps, as illustrated in Figure 1. The first step is key generation, where a secret key is generated to be used in the encryption process. The second, third, and fourth steps involve permuting the DICOM slice by scrambling the order of the slices in the image, the rows within each slice, and the columns within each row, respectively. This permutation step is likely included to add an additional layer of complexity to the encryption process and to help prevent unauthorized access to the image, In the fifth step, the image is divided into smaller blocks, which are then selected for encryption in the sixth step. This block selection process may be necessary to optimize the encryption process and to ensure that the image is encrypted efficiently, and finally, the present lightweight encryption algorithm is applied to each selected block in the seventh step, to provide a strong level of encryption to the DICOM image. The proposed algorithm appears to be a comprehensive and multi-step approach to DICOM image encryption, designed to enhance the security of medical images while also ensuring that the encryption process is efficient and computationally feasible.

2.1. Key generation

The key generation is used in all stages in proposed method, the five-dimension chaotic map are used to generate five sequences of numbers. The first sequence used in slices permutation, the second sequence used in row permutation, the third sequence used in columns permutation, the fourth sequence used for block selection, and the fifth dimension used as key of present encryption algorithm. It appears that the key generation process is an important part of the proposed algorithm, as it is used in all stages of the encryption process and helps to ensure that the encryption is both secure and efficient.

A branch of mathematics called chaos theory. It concentrated on the dynamics of nonlinear dynamical systems that are sensitive to the beginning state. The outcome might be impacted by even a little modification to the input parameters. Numerous researchers exploit chaotic systems' output to boost cryptographic security [18]. Wireless key exchange is prevented by using pseudo-random generators. The identical encryption key will only be provided by the generating seed. Secure pseudo-random number generators are created by chaos.

The same pseudo-random sequence cannot be produced if the initial requirements are not met. Device-to-device communications that are encrypted are secured by this feature. Even if the attacker has the generation equations for the system, they are unable to produce the right pseudo-random sequence [19]. The following equations are those that describe the recommended system:

$$X = X + (-S \times X + Y \times K - R \times P) \tag{1}$$

$$Y = Y + (-Y - X \times Z + R \times X - U \times P) \tag{2}$$

$$Z = Z + (Z \times X \times Y - 1.5 \times S \times P - K) \tag{3}$$

$$K = K + (S \times X + (U \times Y - R \times K)) \tag{4}$$

$$P = P + (B \times ((X + K)/Z) + Y) \tag{5}$$

Where s = 0.95, r = 0.5, b = 0.01, and u = 1.1. The vectors that depict the behavior of the system are x, y, z, k, and p [20].

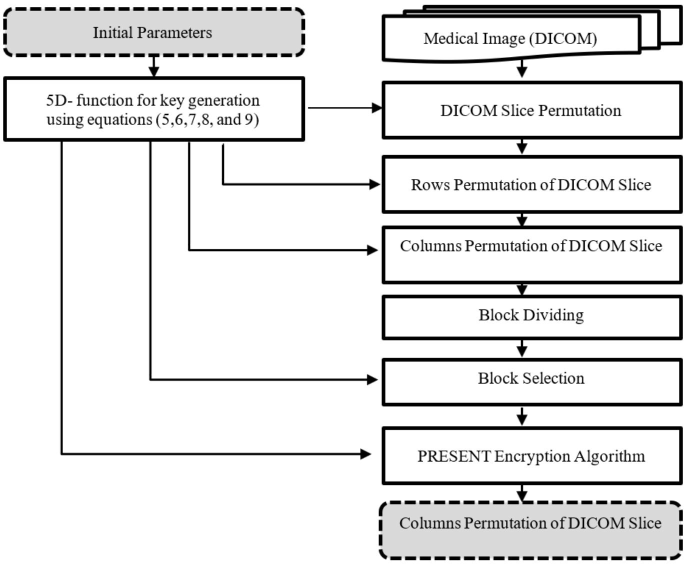

Initial Parameters
5D- function for key generation using equations (5,6,7,8, and 9)
Medical Image (DICOM)
DICOM Slice Permutation
Rows Permutation of DICOM Slice
Columns Permutation of DICOM Slice
Block Dividing
Block Selection
PRESENT Encryption Algorithm
Columns Permutation of DICOM Slice

Figure 1. Block diagram of proposed encryption method

2.2. DICOM slice permutation

The first dimension of generated sequence of the 5D chaotic map are used for DICOM slice permutation. The method is applied by selection a set of numbers equal to the number of slices in DICOM image and sorting in ascending or descending order and used the index of sorted number as permutation keys. This step is likely included to further obfuscate the order of the DICOM slices, making it more difficult for an attacker to understand the structure of the image. By using a sequence of numbers generated by a chaotic map, the permutation keys are randomized and hard to predict, which adds an additional layer of security to the encryption process. This step appears to be a key part of the algorithm, as it helps to ensure the security of the DICOM image by further complicating the order of the slices.

2.3. Rows permutation of DICOM slice

The second dimension of 5D chaotic map is used for row permutation of DICOM slices which is useful in confusion of input data as shown in Figure 2. The row permutation step involves scrambling the order of the rows within each DICOM slice using the second sequence of numbers generated by the chaotic map. This step is likely included to add an additional layer of confusion to the input data, making it more difficult for an attacker to understand the structure of the DICOM image. By using a sequence of numbers generated by a chaotic map for row permutation, the permutation keys are randomized and hard to predict, further enhancing the security of the encryption process. The row permutation step appears to be a useful technique for adding additional complexity and confusion to the DICOM image, thereby enhancing the security of the encryption process.

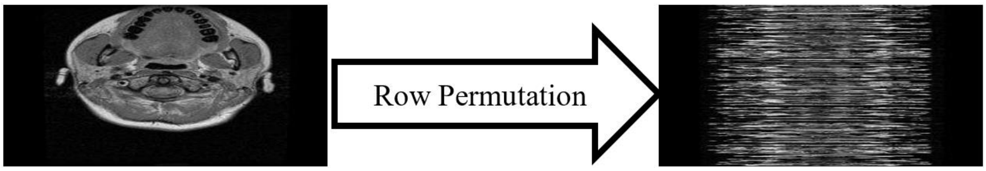


Figure 2. Example of rows permutation of the DICOM slice

2.4. Columns permutation of DICOM slice

The third dimension of 5D chaotic map is used for columns permutation of the output of the previous steps, this process applied on all the DICOM Slices as shown in Figure 3. Like the row permutation step, the column permutation step adds an additional layer of confusion to the output of the previous steps, further enhancing the security of the encryption process. By using a sequence of numbers generated by a chaotic map for column permutation, the permutation keys are randomized and hard to predict, making it more difficult for an attacker to understand the structure of the encrypted DICOM image. It appears that the column permutation step is a useful technique for enhancing the security of the encryption process, and it builds upon the previous row permutation step to further obfuscate the order of the data within the DICOM image.

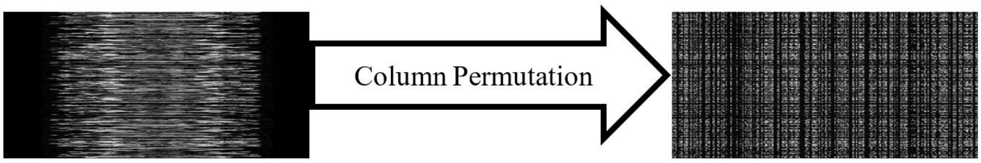


Figure 3. Example of the column’s permutation of DICOM slice

2.5. Block Dividing

This step applied on all slices of DICOM by specifying the block size which will divide them. The process applied on horizontally such row of block one by one, each block will label and be a 3D matrix. The third dimension be the index of block as shown in Figure 4.

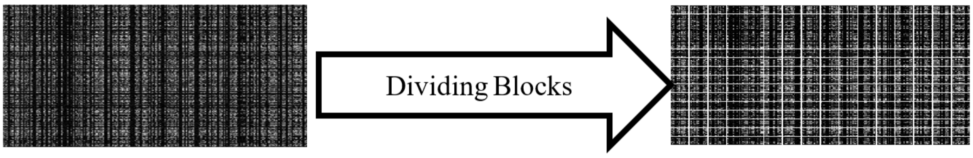


Figure 4. Example of the block dividing

2.6. Block Selection

The fourth dimension of the chaotic map is used for the selection of the block that is input to the encryption process. Which is satisfied by a selecting a set of generated numbers from the corresponding chaotic dimension, then sorting and using the index of sorted numbers as a key index for selecting the block that is input to the encryption process. This step is likely included to further enhance the security of the encryption process by adding an additional layer of randomness to the selection of the blocks that are encrypted. By using a sequence of numbers generated by a chaotic map for block selection, the key index is randomized and hard to predict, making it more difficult for an attacker to determine the structure of the encrypted DICOM image.

3. PRESENT ENCRYPTION ALGORITHM

The present algorithm applied on each selected block by partition blocks into 64-bits sub-block size, and the key into 80-bit sub-key. The used key is differed in each block which make it as dynamic key for more securing process. The result of each block is merged into new block equal to the input block as shown in Figure 5.

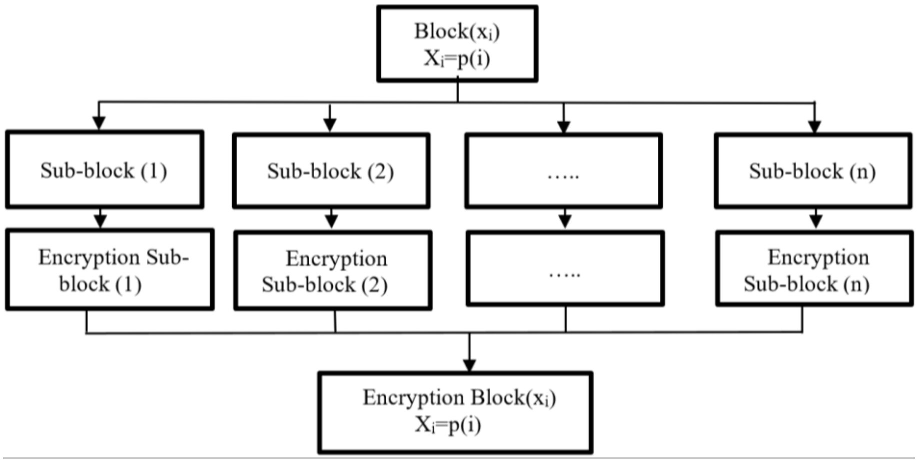


Figure 5. Block diagram of the present encryption algorithm

Present was designed by Bogdanov *et al.* [21]. The encryption algorithm of present is a lightweight symmetric-key block cipher. It has a block length of 64 bit with a key length of 80-bit or 128-bit, and it uses the structure of substitution permutation network (SPN) [22], [23]. The algorithm has 31 rounds and the last round of key addition, as shown in Figure 6. The three functions that make up the round are as: add round key, substitution box layer, and permutation layer should all be included [24].

- Adding the round key: merely the exclusive-or (XOR) operation of the state data block with the round key [23].
- Substitution box (SBoxlayer): is a nonlinear substitution layer that converts a four-bit input to a four-bit output using an equivalent Substitution Box (S-Box). The input-output relationship of a single S-box is shown in Table 1. For both indexes, the bit value in the index m is shifted to the index $n = P\ (m)$ in the permutation layer.
- Permutation (p-layer): the bit permutation used in the present is given by the Figure 7. Bit i is transferred to bit position $P\ (i)$.
- The key schedule: present can take keys of either 80 or 128 bits. However, we focus on the version with 80-bit keys. The user-supplied key is stored in a key register K and represented as $K_{79}K_{78}\ldots\ldots K_0$. At around i the 64-bit round key $K_i = K_{63}K_{62}\ldots\ldots K_0$ consists of the 64 leftmost bits of the current contents of register K. Thus, at round will have that:

$$K_{i=}k_{63}k_{62\ldots}k_0 = k_{79}k_{78\ldots}k_{16} \quad (6)$$

After extracting the round key K_i the key register $k_{79}k_{78\ldots}k_0$ is updated as shown in Figure 8 and the (7), (8), and (9) [21].

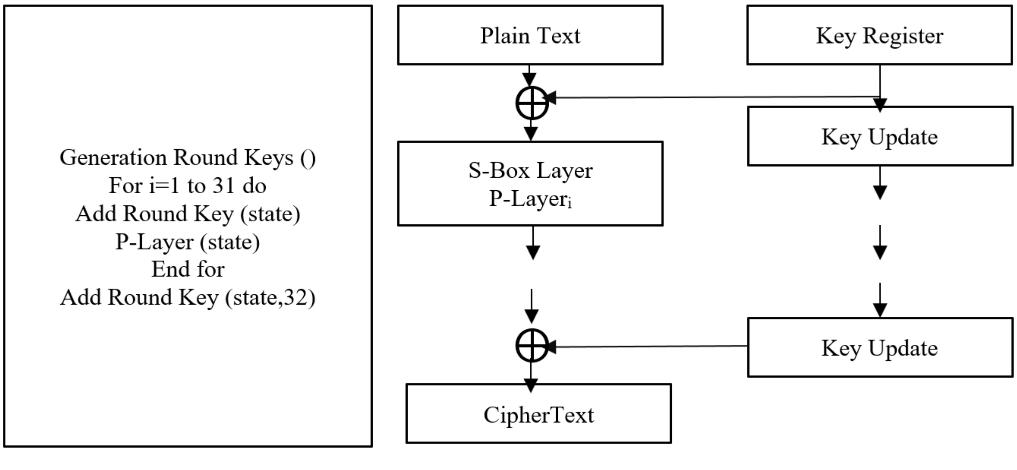


Figure 6. A block diagram of the present algorithm [24]

Table 1. Substitution box layer [21]

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[X]	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

i	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
P(i)	0	16	32	48	1	17	33	49	2	18	34	50	3	19	35	51
i	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	**31**
P(i)	4	20	36	52	5	21	37	53	6	22	38	54	7	23	39	55
i	**32**	**33**	**34**	**35**	**36**	**37**	**38**	**39**	**40**	**41**	**42**	**43**	**44**	**45**	**46**	**47**
P(i)	8	24	40	56	9	25	41	57	10	26	42	58	11	27	43	59
i	**48**	**49**	**50**	**51**	**52**	**53**	**54**	**55**	**56**	**57**	**58**	**59**	**60**	**61**	**62**	**63**
P(i)	12	28	44	60	13	29	45	61	14	30	46	62	15	31	47	63

Figure 7. Permutation layer [21]

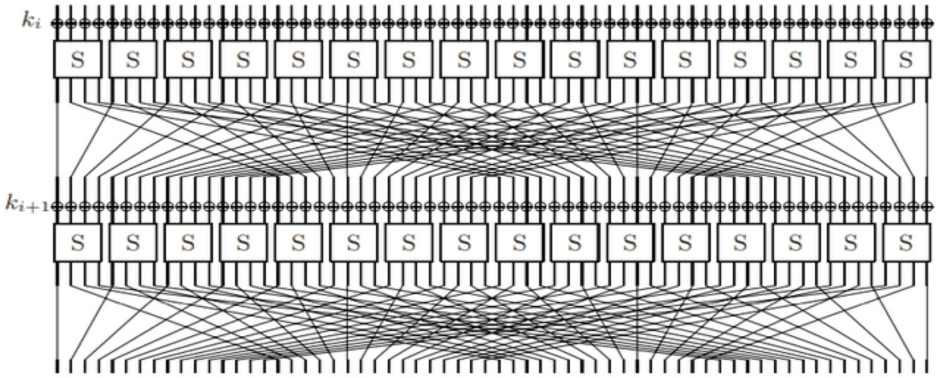


Figure 8. Present SP network [21]

$$[K_{79}K_{78} \ldots\ldots K_0K_1] = [K_{18}K_{17} \ldots\ldots K_{20}K_{19}] \tag{7}$$

$$[K_{79}K_{78}K_{77}K_{76}] = S[K_{79}K_{78}K_{77}K_{76}] \tag{8}$$

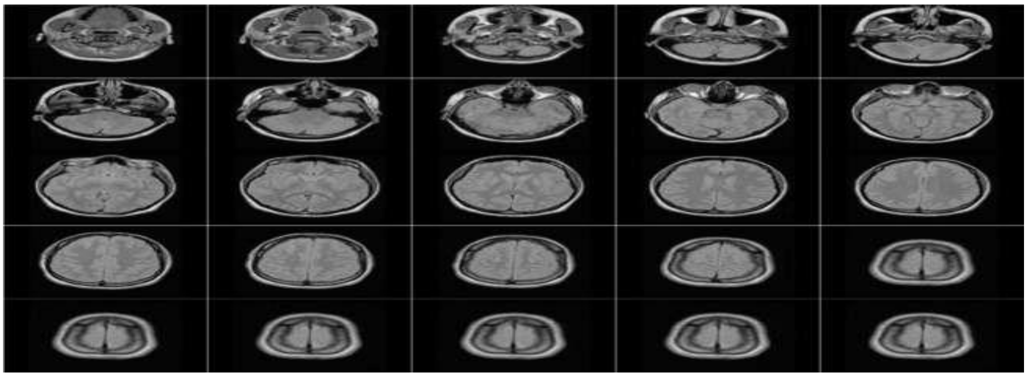
$$[K_{19}K_{18}K_{17}K_{16}K_{15}] = [K_{19}K_{18}K_{17}K_{16}K_{15}] \oplus Round - Counter \tag{9}$$

As a result, the key register is rotated 61 bits to the left, the left-most 4 bits are passed through the current S-box, and the value of the round counter (I) is exclusive-ored with bits $k19, k18, k17, k16,$ and $k15$ of K, with round counter's least significant bit on the right [21]. By using the present algorithm as a component of the proposed DICOM image encryption method, the authors are able to take advantage of the speed and efficiency of the present cipher while also adding an additional layer of security through the use of the chaotic map-based permutation and selection steps.

4. RESULTS

The proposed method applied on DICOM image of brain that consists of 25 slices, each slice consists of 2d matrix (256×256), each pixel represented by integer (16-bits). Figure 9 explain all DICOM slices of used image. The use of DICOM images is common in medical imaging, and the encryption of these images is important for ensuring patient privacy and data security. By applying the proposed method to a DICOM image of the brain, the authors demonstrate the effectiveness of their approach in encrypting complex and sensitive medical data.

The row permutation of the all slices explain in Figure 10 wich explain the steps are useful in confusion the input image. Row permutation is a process that changes the order of the rows in each DICOM slice, which helps to add an additional layer of confusion to the input image. By permuting the rows of the image, the location of each pixel is effectively randomized, making it more difficult for unauthorized users to decipher the encrypted data. The use of a five-dimensional chaotic map in this process further enhances the level of randomness and confusion in the resulting image, making it more secure against attacks.



Figur 9. An example of DICOM slicse

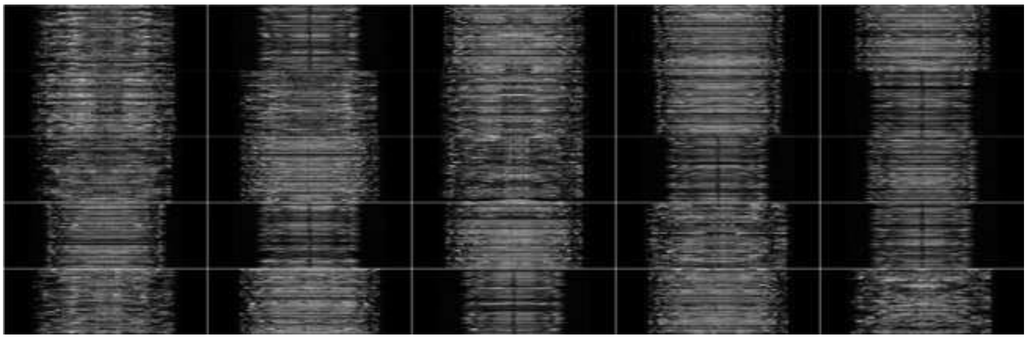


Figure 10. Results of row permutation

Columns permutation of the all slices explain in Figure 11 wich explain the steps are useful in confusion the input image. Column permutation is a process that changes the order of the columns in each DICOM slice, which further adds to the confusion and randomness of the resulting image. By permuting the columns of the image, the position of each pixel is effectively randomized in a different way than the row permutation process, making it more difficult for unauthorized users to decipher the encrypted data. The use of the third dimension of the five-dimensional chaotic map in this process further enhances the level of randomness and confusion in the resulting image, making it more secure against attacks.

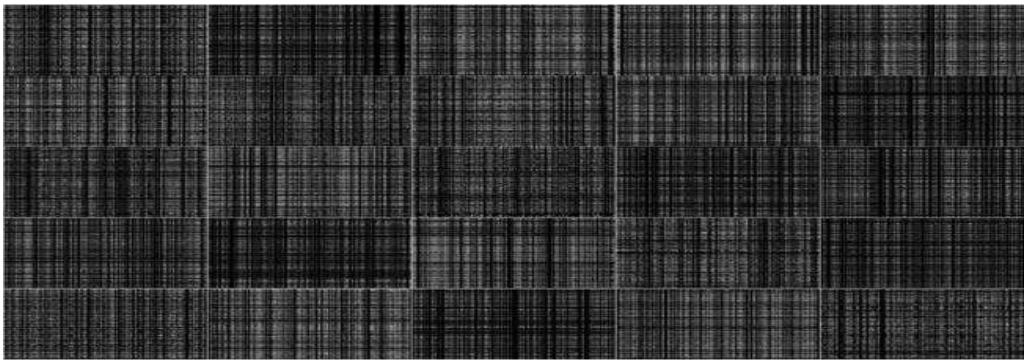


Figure 11. Results of the columns permutation

The five-dimension key generation are used in the proposed method all dimension samples explain in Figure 12. The five dimensions of the key generation are generated using a five-dimensional chaotic map. Each dimension of the chaotic map is used for a specific purpose in the encryption process. By using different dimensions of the chaotic map for different purposes, the proposed method achieves a high level of randomness and security in the encryption process, making it more difficult for unauthorized users to decipher the encrypted data.

Guidelines for data security were developed by the US-based National Institute of Standards and Technology (NIST). The NIST recommends fifteen tests for determining the robustness and unpredictability of an encryption algorithm [1], [25]. Table 2 shows that the proposed system has passed all fifteen tests suggested by the NIST, indicating that it is secure enough for digital encryption of medical images.

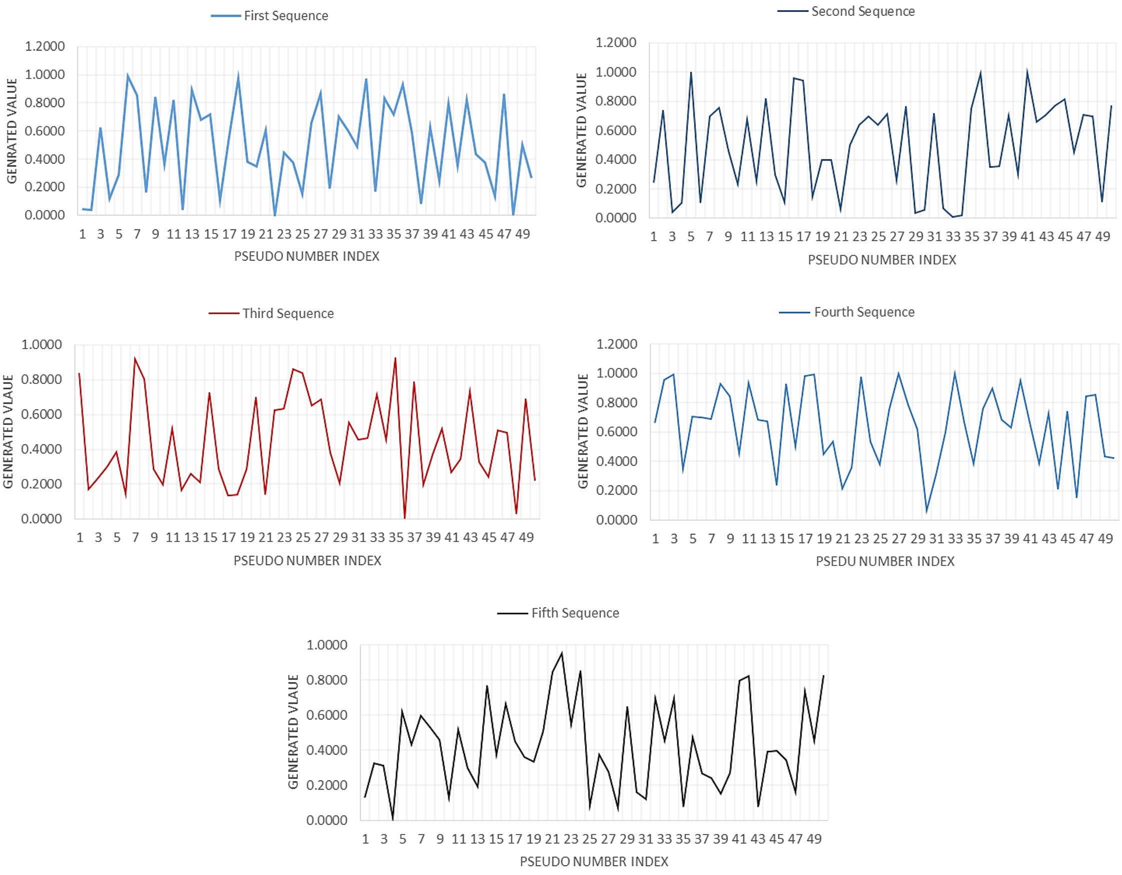


Figure 12. Five-dimension key generation

Table 2. Results of running NIST tests

No	Test name	P-value				
		X	*Y*	*Z*	*P*	*K*
1	Frequency	0.568	0.651	0.604	0.652	0.661
2	Frequency within a block	0.201	0.376	0.462	0.420	0.432
3	Run	0.749	0.505	0.572	0.569	0.552
4	Longest run of ones in a block	0.340	0.417	0.409	0.411	0.408
5	Binary matrix rank	0.567	0.332	0.398	0.336	0.390
6	Discrete fourier transform	0.636	0.667	0.639	0.621	0.660
7	Non-overlapping template matching	0.596	0.621	0.691	0.687	0.564
8	Overlapping template matching	0.313	0.571	0.346	0.336	0.376
9	Linear complexity	0.525	0.544	0.762	0.666	0.623
10	Serial	0.554	0.639	0.560	0.692	0.684
11	Approximate entropy	0.523	0.549	0.588	0.535	0.589
12	Cumulative sums forward	0.623	0.622	0.671	0.613	0.630
13	Cumulative sums reverse	0.711	0.622	0.771	0.716	0.754
14	Random excursions	0.549	0.709	0.760	0.70	0.711
15	Random excursions variant	0.599	0.580	0.599	0.560	50.598

The good encryption algorithm should have the capability to strive against statistical attack. This can be determined by analyzing correlation coefficients [14], entropy [13], mean absolute error (MAE) [6], PSNR [6], structure similarity index image (SSIM) [26], universal quality image index (UQII) [27], unified averaged changed intensity (UACI) [28], and Spatial correlation coefficient [28] of the encrypted image. By analyzing these metrics, we can evaluate the performance of an encryption algorithm and determine its effectiveness in providing security and confidentiality to the encrypted data.

The correlation is tested in three direction horizontal, vertical, and diagonal Figure 13 explains a sample of one slice in DICOM image. Correlation coefficients: correlation coefficients measure the degree of linear dependence between two variables. A good encryption algorithm should have a low correlation coefficient between the original and encrypted images.

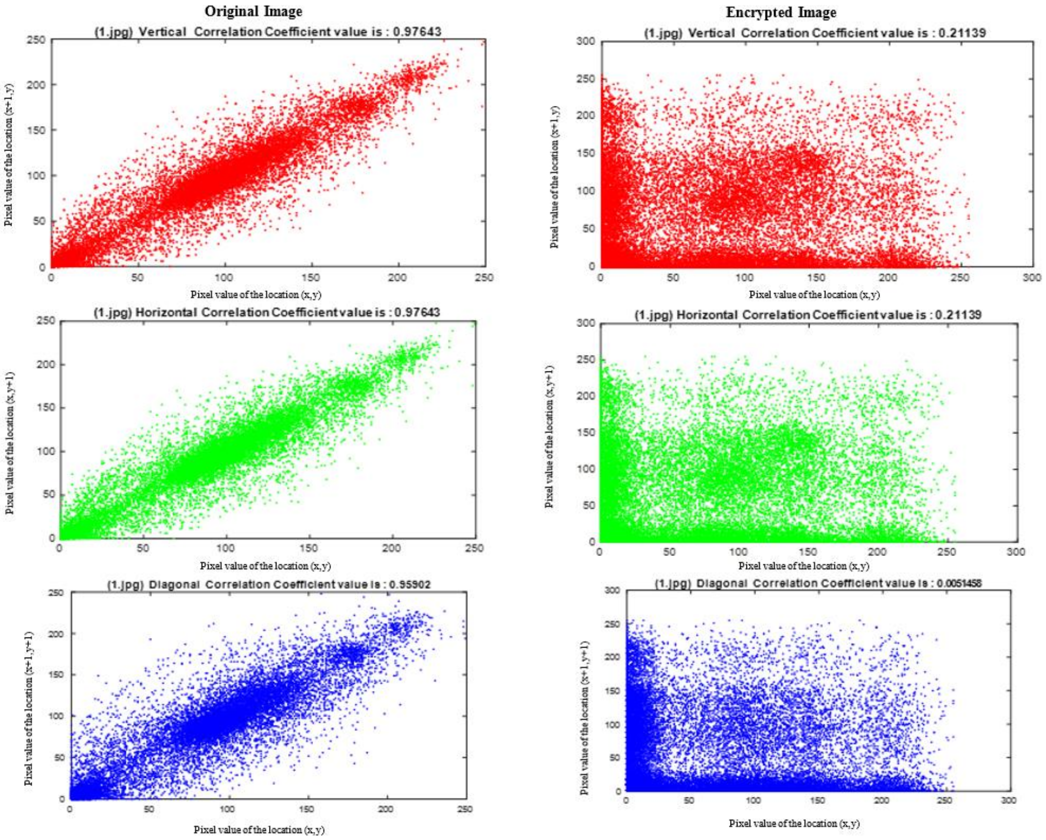


Figure 13. Correlation coefficient results

Table 3. Compare between proposed approach and previous works

Ref	Encryption method	Image type	Results

[13]	XOR encryption approach	Multi-frame DICOM	PSNR = 28.20
			Entropy = 7.3687

[14]	Hybrid encryption algorithm based on DNA and multiple chaotic maps	Multi-frame DICOM	Vertical correlation = -0.0025 Horizontal correlation = -0.0016 Diagonal correlation = 0.0116 Unified average change of intensity = 33.44 Entropy = 8
[15]	Hardware-dependent lightweight steganography scheme	Color image	PSNR of over 46 dB structural similarity index measure (SSIM) being 0.9999 and 0.9998

[16]	New encryption algorithm using Arnold transform and Vigenère cipher	Multi-frame DICOM	UACI = 33.20
			Entropy = 7.99
			Correlation = 0.0037

[17]	A lightweight image encryption scheme based on FPGA and Lorentz attractor's chaotic	Multi-frame DICOM	PSNR = 5 dB
[18]	Bülban chaotic map	Multi-frame DICOM	PSNR = 7.084 dB Entropy = 15.9815 bits Vertical correlation = 0.0275 Horizontal correlation = -0.0027 Diagonal correlation = 0.018

	Proposed hybrid PRESNET lightweight encryption and 5D chaotic maps	Multi-frame DICOM	PSNR = 5.2356
			Vertical correlation = 0.00123
			Horizontal correlation = -0.117
			Diagonal correlation = 0.0753
			SSIM = 0.1853
			Entropy = 15.789
			UACI = 33.2341

Figure 14 results of the correlation coefficients, entropy, MAE, PSNR, SSIM, UQII, UACI, and spatial correlation coefficient measurements. The proposed method efficiency is compared with previous works based on set of parameters such as PSNR test, entropy test, correlation, and UACI as explain in Table 3 and it proved the proposed approach has the best performance for encryption medical image. These comparisons are evaluating the proposal and convidence it to be applicable in medical application.

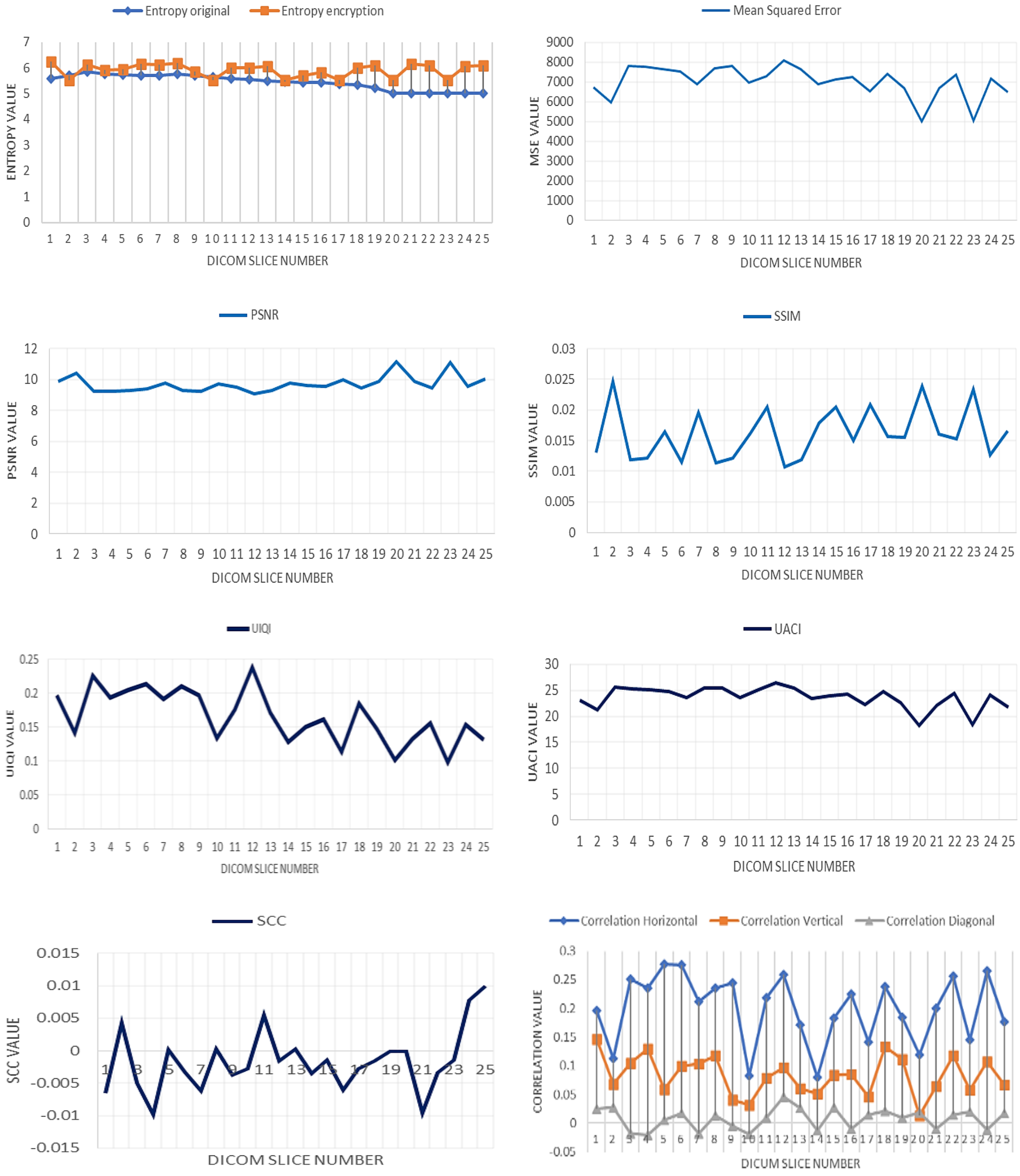


Figure 14. Performance test results

5. CONCLUSION

The need of using a reliable encryption method to safeguard sensitive medical image data was brought to light in this article. Five-dimensional chaotic maps and the lightweight presents block cipher are offered as a new method for improved image encryption. The suggested technique was applied to a 256×256 DICOM medical image, which utilized 25 frames. The suggested approach uses a five-dimensional chaotic map with row and column permutation to produce confusion and diffusion. In addition, the suggested system's dependability and security are evaluated and compared to those of already-existing methods using the following metrics. Measures of NIST and entropy may be acquired via a randomization test, while those of consistency and variance can be derived from a coefficient of correlation applied to pixel similarities.

Mean square error, peak to signal noise ratio, unified average changing intensity, and the structural similarity index picture are some more metrics that may be used for performance analysis. The results demonstrate the superior security of the suggested technique compared to the state-of-the-art image encryption technologies. Further, the suggested system may be used in real-time encryption since it consumes less computer resources while providing quick processing.

REFERENCES

[1] L. Yehia, A. Khedr, and A. Darwish, "Hybrid security techniques for internet of things healthcare applications," *Advances in Internet of Things*, vol. 5, no. 3, pp. 21–25, 2015, doi: 10.4236/ait.2015.53004.

[2] M. Boussif, N. Aloui, and A. Cherif, "Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher," *IET Image Processing*, vol. 14, no. 6, pp. 1209-1216, 2020, doi: 10.1049/iet-ipr.2019.0042.

[3] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu, and S. Miao, "Image block encryption algorithm based on chaotic maps," *IET Signal Processing*, vol. 12, no. 1, pp. 22–30, 2018, doi: 10.1049/iet-spr.2016.0584.

[4] S. K. Bhopi, N. M. Dongre, and R. R. Gulwani, "Binary key based permutation for medical image encryption," in *2016 International Conference on Inventive Computation Technologies (ICICT)*, 2016, pp. 1-6, doi: 10.1109/INVENTIVE.2016.7830180.

[5] A. Shehab *et al.*, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[6] H. Shin, H. K. Lee, H. -Y. Cha, S. W. Heo, and H. Kim, "IoT Security Issues and Light Weight Block Cipher," in *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2019, pp. 381-384, doi: 10.1109/ICAIIC.2019.8669029.

[7] S. B. Sadkhan and A. O. Salman, "A survey on lightweight-cryptography status and future challenges," in *2018 International Conference on Advance of Sustainable Engineering and its Application (ICASEA)*, 2018, pp. 105-108, doi: 10.1109/ICASEA.2018.8370965.

[8] M. A. Philip and Vaithiyanathan, "A survey on lightweight ciphers for IoT devices," *2017 International Conference on Technological Advancements in Power and Energy (TAP Energy)*, 2017, pp. 1-4, doi: 10.1109/TAPENERGY.2017.8397271.

[9] Z. M. J. Kubba and H. K. Hoomod, "A Hybrid modified lightweight algorithm combined of two cryptography algorithms PRESENT and Salsa20 using chaotic system," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019, pp. 199-203, doi: 10.1109/CAS47993.2019.9075488.

[10] S. M. Kareem and A. M. S. Rahma, "A novel approach for the development of the Twofish algorithm based on multi-level key space," *Journal of Information Security and Applications*, vol. 50, 2020, doi: 10.1016/j.jisa.2019.102410.

[11] R. Chatterjee and R. Chakraborty, "A modified lightweight PRESENT cipher for IoT security," in *2020 International Conference on Computer Science, Engineering and Applications (ICCSEA)*, 2020, pp. 1-6, doi: 10.1109/ICCSEA49143.2020.9132950.

[12] E. A. Al-Kareem and R. S. Mohammed, "A review of the most effective cryptography techniques based on conventional block cipher and lightweight," in *2021 1st Babylon International Conference on Information Technology and Science (BICITS)*, 2021, pp. 257-262, doi: 10.1109/BICITS51482.2021.9509903.

[13] Q. N. Natsheh, B. Li, and A. G. Gale, "Security of Multi-frame DICOM Images Using XOR Encryption Approach," *Procedia Computer Science*, vol. 90, pp. 175–181, 2016, doi: 10.1016/j.procs.2016.07.018.

[14] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Transactions on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017, doi: 10.1109/TNB.2017.2780881.

[15] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Indicator-based lightweight steganography on 32-bit RISC architectures for IoT security," *Multimedia Tools and Applications*, vol. 78, pp. 31485–31513, 2019, doi: 10.1007/s11042-019-07960-z.

[16] V. Raj, S. Janakiraman, and R. Amirtharajan, "Optimal concurrency on FPGA for lightweight medical image encryption," *Journal of Intelligent & Fuzzy Systems*, vol. 40, no. 6, pp. 10385–10400, 2021, doi: 10.3233/JIFS-200203.

[17] V. Manikandan and R. Amirtharajan, "A simple embed over encryption scheme for DICOM images using Bülban Map," *Medical & Biological Engineering & Computing*, vol. 60, pp. 701–717, 2022, doi: 10.1007/s11517-021-02499-4.

[18] F. Yu *et al.*, "Chaos-based engineering applications with a 6D memristive multistable hyperchaotic system and a 2D SF-SIMM hyperchaotic map," *Complexity*, 2021, doi: 10.1155/2021/6683284.

[19] N. Bagheri, R. Ebrahimpour, and N. Ghaedi, "New differential fault analysis on PRESENT," *EURASIP Journal on Advances in Signal Processing*, 2013, doi: 10.1186/1687-6180-2013-145.

[20] H. K. Hoomod, J. R. Naif, and I. S. Ahmed, "A new intelligent hybrid encryption algorithm for IoT data based on modified PRESENT-Speck and novel 5D chaotic system," *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 4, pp. 2333–2345, 2020. [Online]. Available: http://pen.ius.edu.ba/index.php/pen/article/view/1738/714

[21] A. Bogdanov *et al.*, "PRESENT : An ultra-lightweight block cipher," *International Workshop on Cryptographic Hardware and Embedded Systems (CHES 2007)*, 2007, pp. 450–466, doi: 10.1007/978-3-540-74735-2_31.

[22] J. Wang *et al.*, "A logistic mapping-based encryption scheme for wireless body area networks," *Future Generation Computer Systems*, vol. 110, pp. 57–67, 2020, doi: 10.1016/j.future.2020.04.002.

[23] Z. M. J. Kubba and H. K. Hoomod, "Modified PRESENT Encryption algorithm based on new 5D Chaotic system," *IOP Conference Series: Materials Science and Engineering*, 2020, vol. 928, doi: 10.1088/1757-899X/928/3/032023.

[24] L. Ding, "Improved Related-Cipher Attack on Salsa20 Stream Cipher," *IEEE Access*, vol. 7, pp. 30197–30202, 2019, doi: 10.1109/ACCESS.2019.2892647.

[25] A. Varici *et al.*, "Fast and efficient implementation of lightweight crypto algorithm PRESENT on FPGA through processor instruction set extension," in *2019 IEEE East-West Design & Test Symposium (EWDTS)*, 2019, pp. 1-5, doi: 10.1109/EWDTS.2019.8884397.

[26] S. Salunke, B. Ahuja, M. F. Hashmi, V. Marriboyina, and N. D. Bokde, "5D Gauss map perspective to image encryption with transfer learning validation," *Applied Sciences*, vol. 12, no. 11, 2022, doi: 10.3390/app12115321.

[27] Y. Byun, Y. Han, and T. Chae, "Image fusion-based change detection for flood extent extraction using bi-temporal very high-resolution satellite images," *Remote Sensing*, vol. 7, no. 8, pp. 10347–10363, 2015, doi: 10.3390/rs70810347.

[28] W. Zhang, Z. Zhu, and H. Yu, "A symmetric image encryption algorithm based on a coupled logistic-Bernoulli map and cellular automata diffusion strategy," *Entropy*, vol. 21, no. 5, 2019, doi: 10.3390/e21050504.

BIOGRAPHIES OF AUTHORS

Muntaha Abdulzahra Hatem received the Master and BSc degree in Computer Science (Mustansiriyah University, Iraq) in 2020 and 2009 respectively. his research interested in networkes, information security and artificial intelligence algorithms. She can be contacted at email: muntaha.hatem@scrdiraq.gov.iq.

Balsam Abdulkadhim Hameedi received a master's degree from University of Mustansiriyah, Baghdad, Iraq /College of education, computer Science department in 2022. She received his B.Sc. degree in computer science in 2000 from University of Mustansiriyah, Baghdad, Iraq/College of Education, computer Science department. His research interested in information security. She works in the Ministry of Education. She can be contacted at email: Balsam119@res-rus2.edu.iq.

Jamal Nasir Hasoon received the PhD degree in Computer Science (university of technology, Iraq) in 2020 and finished his Master and BSc degree in (Mustansiriyah University, Iraq) 2014 and 2006 respectively. his research interested in machine leaning, computer vision, pattern recognition and information security. He can be contacted at email: jamal.hasoon@uomustansiriyah.edu.iq.