International Journal of Safety and Security Engineering
Vol. 12, No. 4, August, 2022, pp. 467-473
Journal homepage: http://iieta.org/journals/ijsse

Medical Image Encryption Based on Frequency Domain and Chaotic Map

Noor A. Yousif[1], Gaidaa S. Mahdi[2*], Ashwaq T. Hashim[1]

[1] Control and Systems Eng. Dept., University of Technology-Iraq, Baghdad 10066, Iraq
[2] Chemical Eng. Dept., University of Technology-Iraq, Baghdad 10066, Iraq

Corresponding Author Email: Gaidaa.s.mahdi@uotechnology.edu.iq

https://doi.org/10.18280/ijsse.120407

Received: 23 June 2022
Accepted: 20 August 2022

Keywords:
medical image, image encryption, IWT, chaotic map, AES, linear system, partial encryption

ABSTRACT

Medical images typically have diagnostic and confidential data and information about the patient and are usually sent using public networks. Due to the sensitivity of medical images, their security has become a challenging requirement that must be addressed. Traditional cryptographical algorithms are inadequate to ensure appropriate and fine security while encrypting them, because of the correlation between each pixel, high redundancy of the image and its major size. Chaotic systems with their properties and partial encryption based on frequency domain are the best candidates for securing the storage and transfer of digital images. The paper shows new criteria for encryption of medical image. It is designed to improve performance and meet the increasing need for better security for medical image encryption. At first, the pixel's correlation is eliminated by scrambling the input image and diffusing them using secret sharing based on polynomials. Various frequency domains of the image are accomplished by applying the integer wavelet transform of the scrambled image, namely, the associated detail of (HL, LH and HH) and the LL (approximation coefficient) through using the AES algorithm. The (LL) part is encrypted to originate the diffusion image and by using the inverse of the Haar wavelet transform to produce a reliable, unbreakable and secure form. The designed algorithm is used to reverse and shuffle every frequency sign of the transformed image before transformation image back to the pixel domain. The original image form is restored through the reverse decryption algorithm. The suggested algorithm is measured and evaluated in a statistical way and normal standard security; The outcome of the proposed algorithm shows a strong resistant to the familiar attacks and extra secure than the other algorithms in the domain of image cryptography.

1. INTRODUCTION

The fast evolution of the five generations (5G) technology causes tele-consultation and telemedicine to become a reality. In modern research, the process of telemedicine. Authentication matters of integrity, authenticity and medical information validity have become significant issues. Medical information is unlike any other data or digital information. Every small difference or change in medical data can cause medical controversies and disputes. That's why through the authentication process, no noise is added and only using the internal characteristics and inherent properties of the digital medical data information complete and finish copyright authentication to become an appropriate scheme for medical information authentication [1].

To obtain secure sensitive information, frequency transform methods like Discrete Cosine Transform (DCT), DWT based methods, machine learning and chaos theory can be used as encryption techniques [2, 3]. Before further processing, it is constantly necessary to transform each value of every pixel into confirmed frequency components in the frequency domain encryption. While, for encryption of the spatial domain, each encryption technique can be directly used and applied straightly to values of the pixel. The essential goal can be done using different approaches like direct scrambling, chaos theory and the substitution process [4, 5].

This paper is oriented by the chaos sequence and wavelet transform for the medical image encryption algorithm. Partial image encryption is vital as it reduces computational costs and time. Many existing complete image encryption algorithms may be more complex and uses traditional techniques. Securing medical imaging data depends on mechanisms that include Advanced Encryption Standard (AES) algorithm. However, implementation of this algorithm for medical images is time-consuming. An effective method has been developed to protect of medical data and images. A chaotic map and a wavelet transform are used. A scrambling method is applied by exploiting the features of chaotic maps suited for cryptography. The multimedia data is complicated to use directly, so it is ineffectual to encrypt the color images because the data of an image has very strong connections between neighboring pixels, which gives intelligible data and information. Because of the reduced correlation between the neighboring pixels, the understandable information will decrease. This paper uses chaos to mix the rows and columns of the plaintext image to provide every digital data with high safety and security. However, using a quadratic map to create a noisy image. Many algorithms for encryption the data are suggested and generally used, such as RC5, Blowfish, AES, IDEA and RSA. Many of them are applied for binary data or binary text in the proposed algorithm, and only the (LL) approximation coefficient is encrypted using the algorithm of

AES.

2. RELATED WORKS

In 2012, Al-Najdawi and Tedmori [6] presented a cryptography technique in which no image is lost. By using the (DCT) they developed an encryption algorithm to convert the original image to the frequency domain. The designed algorithm reverses the sign and shuffles off every frequency in the transformed domain.

In 2009, Liu et al. [7] the Fractional Fourier Transform is used to present an encryption method of a triple image. In 2012, Sastry and Samson [8] used wavelet transform as a proposed procedure of image encryption by lossy compressions. Encryption is achieved through a multilevel 2-D Haar by decomposing the compressed image. In the processing way of the frequency domain based on modifying and processing the image frequencies, every pixel of the image is restored and recovered totally through a reverse operation without losing data or information.

Thus, the approaches that are based on frequency are convenient. In 2014, Tedmori and Al-Najdawi [9] presented a technique using encryption/decryption without losing the symmetric key. Here, using the Haar wavelet transform every image is transformed into the frequency domain, and the subbands of the image are encrypted. The result guarantees a reliable, very secure and unbreakable format. This encryption technique includes diffusion of each frequency data, which are distinguishable in the desired image by using a reversible weighting factor between the remaining frequencies. In 2019, Guan et al. [10] proposed and demonstrated an encryption approach for a digital image that depends on dynamic deoxyribonucleic acid coding and chaotic process using hyper digital chaos in the frequency domain where the phase and amplitude factors in the frequency domain are scrambled and diffused. In 2020, Anand and Singh [11] combined the technology of singular value decomposition (SVD) and the discrete wavelet transform (DWT) to give an achievable scheme of a secure authentication of the patient information through embedding a watermark multi-level into the medical carrier image. In 2020, Saravanan and Sivabalakrishnan [12] introduced an enhanced image encryption model using n HCM. Various steps were composed, such as conversion of a frequency domain, image encryption and key generation using optimized HCM, and the decryption of an image. In 2021, Sun et al. [1] archived the medical image authentication by combining fractal dimension theory and the multi-scale wavelet transform.

3. THE ADVANCED ENCRYPTION STANDARD (AES)

AES considers a repeated rather than a Feistel cypher. The cypher is encrypted and decrypted data using two standard techniques substitution and permutation network (SPN). This network has many mathematical operations in block cypher algorithms [13]. The AES deals with 16 bytes (128 bits) as a fixed block-size plaintext. The AES works on a matrix of bytes, so those 16 are represented in a 4×4 matrix. Another essential feature of the AES is the number of rounds; this round number depends on the key length. Three different sizes of the key are used in the algorithm of AES to decrypt and encrypt data such as (256, 192 and 128 bits). The size of the key is responsible for deciding the number of rounds, like using ten rounds in 128-bit keys, 12 rounds in a 192-bit key and 14 rounds in a 256-bit key [14].

The phase of AES's encryption is divided into three stages: first initial, then main and finally the final round, as shown in Figure 1. Each of the three stages or steps uses the exact sub-procedure (works) in various combinations as below:

-Initial Round
Add the Round Key
-Main Rounds
Sub Bytes,
Shift the Rows,
Mix all Columns,
Add the Round Key,
-Final Round
Sub Bytes,
Shift every Rows,
Add the Round Key.

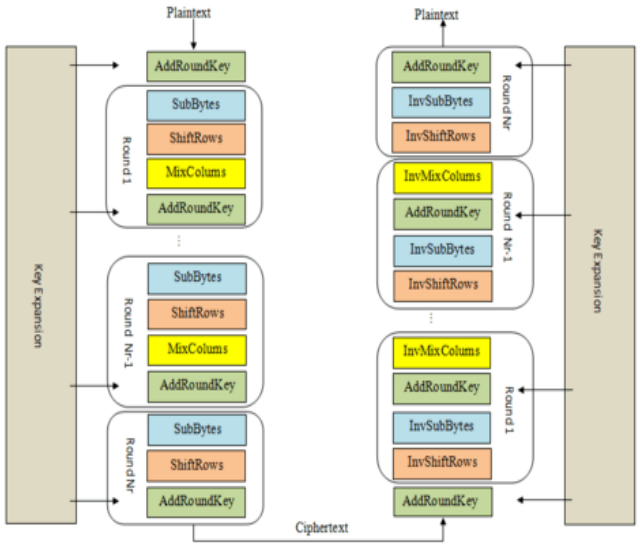

Figure 1. AES encryption and decryption structure

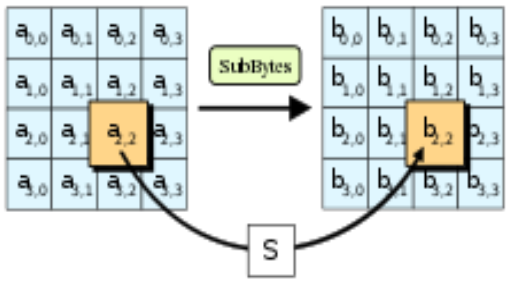

Figure 2. Step of subbytes

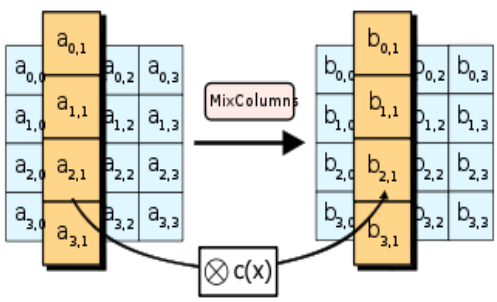

Figure 3. Step of the MixColumns

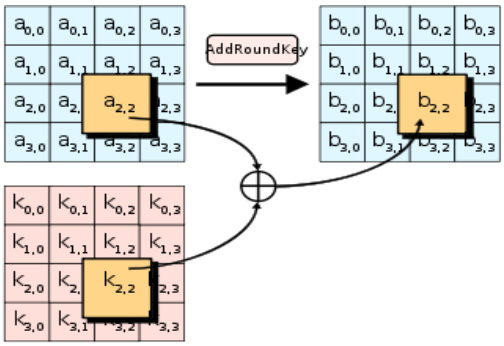

Figure 4. Step of the AddRoundKey

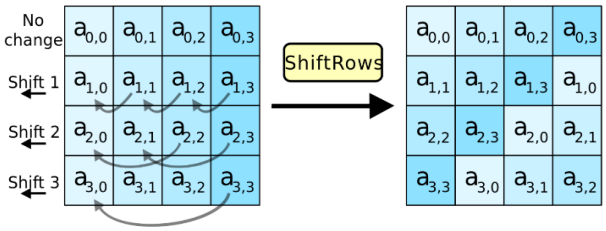

Figure 5. Step of the ShiftRows

Figure 2 shows that for every SubBytes move, every byte in each state is exchanged with its entrance in a lookup table with fixed 8-bit, S; bij = S(aij). As seen in Figure 3, MixColumns shows that a fixed polynomial c(x) is multiplied with every column in the state. Figure 4 shows the step of AddRoundKey where every byte of the state is merged with a round subkey byte using an XOR operation (⊕) [13]. Figure 5 shows manipulation of state's rows using ShiftRows Transform where each byte in the row is shifted using a particular offset. The first row stays constant through this process, while the other rows (2nd, 3rd and 4th) are subjected to 1 byte, 2 byte, and 3 byte circular shift operations. The first row stays untouched during the decryption process, while the other rows are moved to the right using the exact offset that has been used to shift them to the left during the encryption process.

4. THE CHAOTIC SYSTEM

The encryption using chaos-based shows a dominant rule and is crucial in modern multimedia cryptography rather than classical algorithms [15]. The system of chaos is scattered and very sensitive to initial conditions. There are many similarities with the usage of cryptography. In cryptography, as an outcome of encryption based on chaos, encryption using these methods has become one of the strong cryptosystem essential branches. At first, Fridrich used chaos maps for encryption algorithms using images very late. After that, the same maps were used for the vagueness of any image using the transformation in pixel location in 1997 [16].

When the researchers start to use the maps of MD chaotic, the images will be encrypted depending on chaotic maps of 2D and 1D. The MD chaotic maps are generally applied in encryption because of their comparatively complex parameters and structures. These characteristics and processes increase the difficulty and computations complexity and difficult implementation. Although 1D chaotic maps contain different distribution and choppy ranges, they contain a very structure that is superficial rather than the lower dimensional chaotic maps. Also, they are straightforward to use, implement and handle directly [17].

The Quadratic map is one of the actual examples of a chaotic system. A classical equation for a Quadratic map is [18]:

$$X_{n-1} = r - (X_n)^2 \quad (1)$$

where, r represents chaotic parameter, n represents the iterations number. Because the Quadratic map system is nonlinear, it is considered chaotic. It is considered deterministic because its equation determines the behaviour of the system, besides any little changes in the initial value of x0 causing a significant effect on the map's behaviour [18]. Figure 6 shows the Quadrate chaotic map.

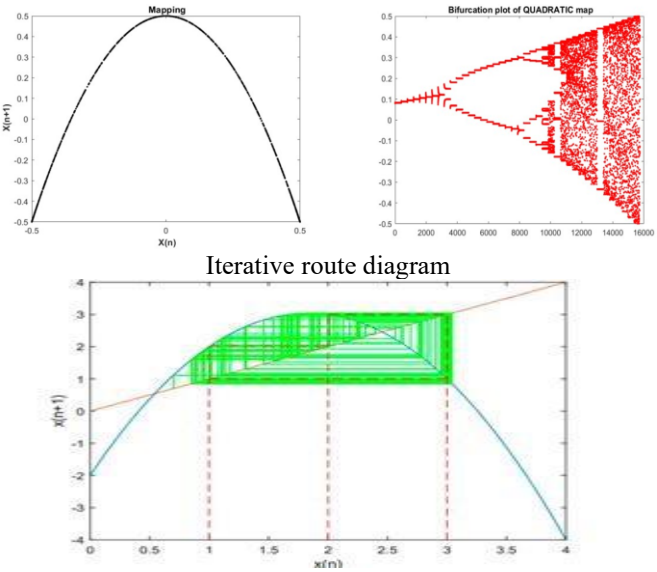

Figure 6. The map of quadratic chaotic

5. THE PROPOSED ALGORITHM

The proposed system first step is using the chaotic map is scrambling. Then Discrete Wavelet Transform (DWT) is used to lower the computational time of the encryption in such a way that only encrypted low frequency bands LL because most of the majority of information in the plaintext falls in these bands. Finally, applying the wavelet inverse to produce the cypher image. Figure 7 shows the block diagram of the suggested system.

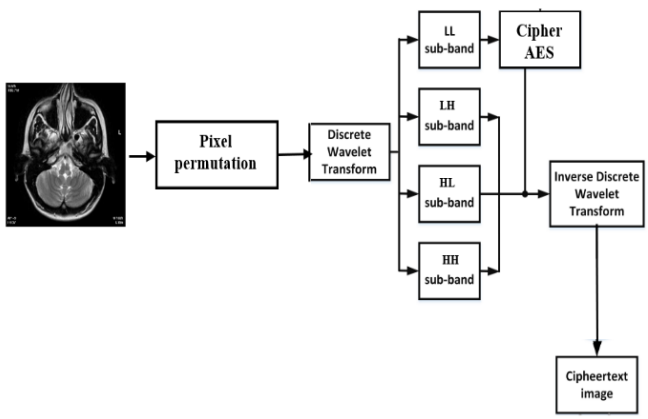

Figure 7. Suggested system diagram

Step1: Input the image of size (C × R) where C, R represent the columns and rows of the chosen medical image (MI), respectively.

Step2: Apply pixels permutation based on the linear system described in section 5.1.

Step3: Apply DWT on the permuted image to get the frequency subbands LL, HH, HL and LH.

Step4: Since every (sub-bands), the LL has very low-frequency components, this means that majority of the data information falls in the LL subband. So, to reduce the encryption computational time, and by using the AES encryption algorithm, the LL sub-band only is encrypted instead of the whole frequency sub-bands.

Step5: Use inverse wavelet transform to convert the manipulated frequency component to real data values and store those images inside an encrypted image.

5.1 Pixel permutation

The proposed algorithm uses the complicated reversible mixing permutation function. The necessary diffusion and confusion are being provided to the output pixel, where it's key-dependent permutation so that the additive differences are being destroyed.

A set of linear equations is used in the permutation process. The pixel correlation is detached by the linear transformation presented in Eq. (2)

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N = \begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N \qquad (2)$$

where, (x,y) is the original pixel position, (x′, y′) is the permuted pixel position and both (x,y), (x′,y′) ∈ [1, *N*] × [1, *N*]. Where *N* is the width or height of a square image. Modular algebra is used to manage the rising size of the total index size. Besides the use of linear equations. The field of indices values $\begin{bmatrix} x' \\ y' \end{bmatrix}$ is [0... *N*]. The Eq. (3) can be rewritten as follows:

$$\begin{bmatrix} K_1 & K_2 \\ K_3 & K_4 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N = \begin{bmatrix} x' + p_i \\ y' + p_i \end{bmatrix} \qquad (3)$$

where, pi represents an integer value that will not be considered as part of values of index, and during the retrieval phase, by using the specific integer division rules, its value will be compensated.

Using chaotic quadratic map to create subkeys through the following steps:

Step1: Let Len = R×C×4 (i.e., 4 keys K_1, K_2, K_3, and K_4)

Step2: Generate a sequence X in a random way by using Quadratic map

Assume r equal to 0.5, X_0 equal to 0.15

$X_0 = a \times X_0\text{^}2$

For i = 1 to Len

$X_i = r \times X_{i-1}\text{^}2$

End for

Step3: Change the domain of chaotic map X from [-0.5 0.5] to [1 R]

then Max =R and Min =1

For i = 1 to R

$Ti = (Max-Min)/(Max-Min) \times (X_i - Max) + Max$

Endfor

In a re-permutation process, the indices are fed to the inverse of re-permutation. At this stage, the indices $\begin{bmatrix} x' \\ y' \end{bmatrix}$ are applied to generate two sets of simultaneous linear equations (i.e., one for each index). So, by solving these sets of linear equations, the original indices can be revealed. Then, the proposed system used module algebra with the base N to minimize and reduce index range and maintain them between the range (0 and N). So is algebra needed to restore authentic indices $\begin{bmatrix} x \\ y \end{bmatrix}$ should consider the decreed range restriction of the indices.

6. EXPERIMENTAL RESULTS

Developed optimal image encryption in the frequency domain with the chaotic map was implemented in MATLAB 2018a and investigated on medical images of different types. It is achieved with a laptop containing the following characteristics: Intel (R) Core (TM) i5-4210U CPU @1.70 GHz 2.40 GHz, RAM 8 GB and Microsoft Windows 10 ultimate. All the images are MRIs having a dimension of various sizes. Figures 8 show the steps of the suggested system when applied to a brain image.

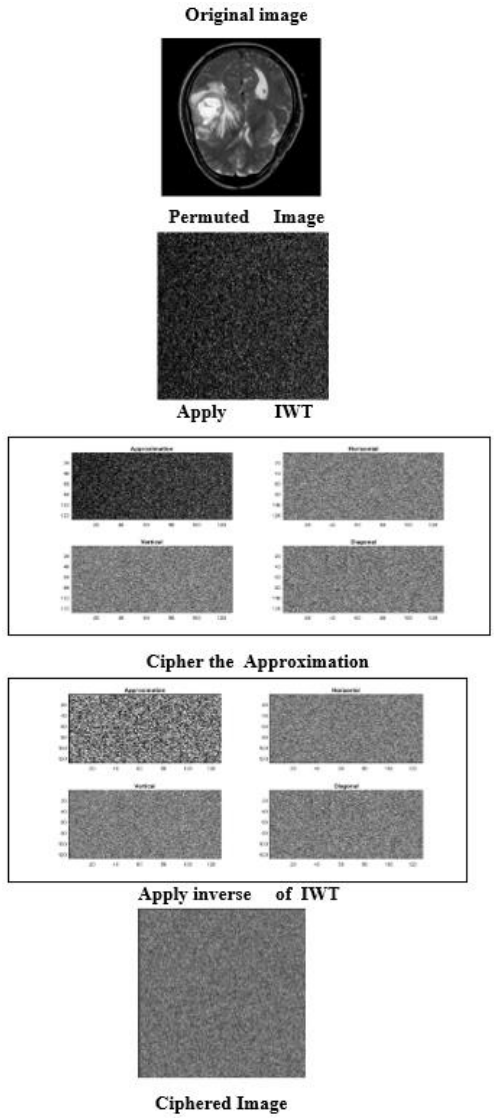

Figure 8. Example of proposed system implementation

The results of the encryption, original and cypher images, along with the histogram, are displayed in Figure 8. The pixel intensity values of the histogram of both the actual as well as the cipher images are generated by the histogram evaluations. The histogram is a graph present in the specific image and provides data about the pixel count of an image at every altered intensity value. This analysis is done between the actual images, and the corresponding cypher images are also graphically represented. As shown in Figure 9, the analysis revealed that the histogram of the actual images is entirely different for all images and the histograms are nearly similar in the cypher images.

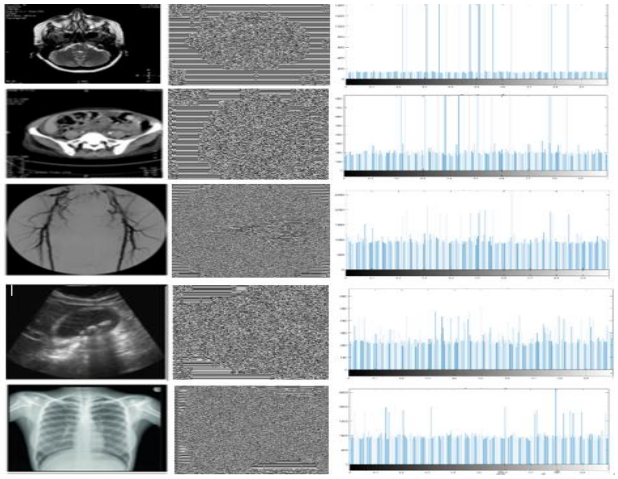

Figure 9. Samples of (a) Original image, (b) histogram of original image, (c) Cipher image, (d) histogram of cypher image and (e) Decrypted medical images

Figure 10 illustrates the test and encrypted histograms images using the AES basic algorithm. The histogram distribution of the for the AES original encrypted image is not identical; it is dose not match with an encrypted image.

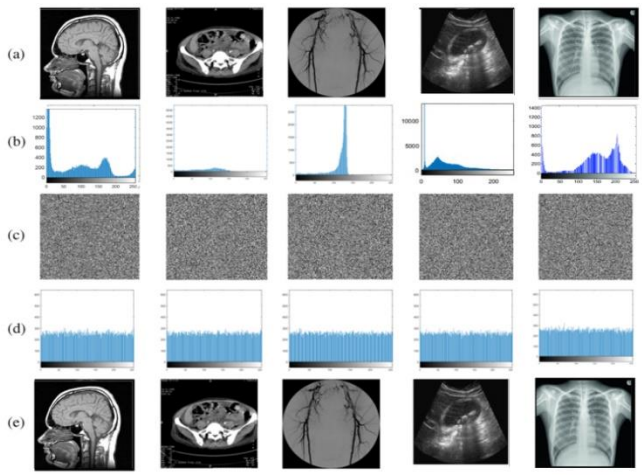

Figure 10. Samples of (a) Original image, (b) Cipher image by AES, and (c) The cypher image histogram

6.1 Analysis of the statistical security

In this section, the analysis of the Statistical security of the suggested technique and the comparison is done. These analyses include entropy, correlation, NPCR and UACI. Mathematically, these parameters can be computed using Eqns. (4)-(10) [19-21].

$$Entropy = -\sum im(pi)log2en(ci) \tag{4}$$

where: im(pi) is the potential of random variable occurrence p.

$$C_{xy} = \frac{COVR(x,y)}{\sqrt{V(x)}\sqrt{V(y)}} \tag{5}$$

where, $COVR(x,y)$ is the Covariance between x and y, it is given by:

$$COVR(x,y) = \frac{1}{n} \times \sum_{i=1}^{n} E[(x_i - \mu(x)(y_i - \mu(y))] \tag{6}$$

where, x and y are two adjacent pixels values in the image, V (x) is the variance of variable x and is given by [22]:

$$V(x) = \frac{1}{n} \times \sum_{i=1}^{n} [(x_i - \mu(x)]^2 \tag{7}$$

$\mu(x)$ is the mean of variable x.

$$\mu(x) = \frac{1}{n} \times \sum_{i=1}^{n} x_i \tag{8}$$

The varying number of pixels rate (NPCR) and the unified average change in intensity (UACI) is usually used for checking the sensitivity and avalanche effect of the plaintext, which are defined as:

$$NPCR = \frac{\sum_{i,j} W(i,j)}{M * N} \times 100 \tag{9}$$

where, N and M are the image height and width. $W(i,j)$ can be defined as:

$$W(i,j) = \begin{cases} 1, if\ Cip1(i,j) \neq Cip2(i,j) \\ 0, if\ Cip1(i,j) = Cip2(i,j) \end{cases}$$

where, $Cip1(i,j)$ Is the cypher image grey value and $Cip2(i,j)$ Grey value of new cypher image

$$UACI \frac{1}{M \times N} \times \sum_{i,j} \frac{abs(Cip1(i,j) - Cip2(i,j))}{255} \times 100 \tag{10}$$

As seen in Table 1, every 8-bit cipher image's local entropies are bigger than 7.998, close to the ideal value proves that our algorithm has a very good local randomness and can resist efficiently the entropy attacks. When the UACI and NPCR of the Ciphertext are larger than 99.60% and 33.46%, respectively [23], it shows very good security for the proposed algorithm.

Using the proposed encryption scheme, many different images are being tested to obtain UACI and NPCR. The test results show that our encryption scheme meets the strength requirements against various attacks.

The comparison of other methods with the proposed procedure while using analysis of an entropy correlation for the "Lena" image of the size (256 × 256) as shown in Table 2.

As seen in Table 2, Using the suggested algorithm, the correlation coefficients of the encrypted 'Lena' image are much closer to the value of zero than the authentic AES and other researchers, refers that the pixels of the image encrypted using the suggested algorithm are very unconnected with each

other and cannot foretell each other, which shows that this algorithm is very safe and secure. Table 3 gives the encryption time comparison. The encryption time represents the time required for encrypting the image by the proposed system and AES algorithm. From the comparison, we can conclude that the speed of the proposed system is very low compared AES algorithm.

Table 1. The analysis of the statistical security for the proposed system

Image Name	NPCR	UAC I	Correlation Horizontal	Vertical	Diagonal	Entropy
Image 1	99.6615	33.5172	-0.0020	0.0001	-0.0011	7.9988
Image 2	99.6576	33.5267	0.0013	0.0021	-0.0034	7.9986
Image 3	99.6223	33.5851	0.0023	-0.0019	0.0011	7.9995
Image 4	99.6369	33.6959	0.0061	-0.0116	0.0018	7.9992
Image 5	99.6544	33.6463	-0.0056	0.0037	0.0032	7.9996

Table 2. Performance comparisons with other methods

Measure	Li et al. [24]	Ahmad and Hwang [25]	Zhang and Xiao [26]	Xu et al. [27]	Wang et al. [28]	Hussain et al. [29]	Hashim et al. [30]	Proposed system
Horizontal Correlation	0.0327	0.9407	0.0018	−0.0230	0.0020	−0.0067	0.0064	−0.0026
Vertical Correlation	0.0219	−0.0273	0.0011	0.0019	−0.0007	−0.0137	0.0017	0.0027
Diagonal Correlation	0.0180	−0.0140	−0.0012	−0.0034	−0.0014	−0.0563	-0.0048	−0.0011
Entropy	7.9993	n/a	7.9994	7.9974	7.9970	n/a	7.9974	7.9991

Table 3. Time consumption for the proposed system compared to AES method

Image Name	Image Size	Encryption Time in Sec.	
		Proposed System	AES Method
Image2	128×128	3.2034	48.3384
Image1	256×256	20.4323	565.7291
Image4	512×512	203.1783	7872.1891

7. CONCLUSION

We suggested using the frequency domain and chaotic map to encryption and decryption the image. This proposed system offers much more efficient performance and security than traditional algorithms AES. It decreases the execution time of the encryption process by using a wavelet decomposition to focus the essential information of the image to the low part of frequency. Therefore, only the LL subband is ciphered, and any partial image encryption method should have much less time and complexity. Then by shuffling each pixel using a chaotic map, confusion and diffusion are accomplished. By using the entropy, correlation and histogram as a security measurement, the level of security of this system enhances the encrypted images by minimizing the value of correlation between elements of the image also decreasing standard information between the encrypted variable of the image, which increases its entropy value. Encryption in the frequency domain has many advantages. It is easier to identify the critical parts to be encrypted. It is hard to associate frequency domain values with spatial domain pixel values. This makes the image secure against many attacks, such as Ciphertext only, and known plaintext attacks. Because of the wavelet reconstruction step, it is impossible to distinguish between encrypted and unencrypted parts. The drawbacks of partial encryption are the lower security and the file size. To overcome the security issue, the permutation step is used to hide the correct locations of the image pixels.

REFERENCES

[1] Sun, T., Wang, X., Lin, D., Bao, R., Jiang, D., Ding, B., Li, D. (2021). Medical image security authentication method based on wavelet reconstruction and fractal dimension. International Journal of Distributed Sensor Networks, 17(4): 15501477211014132. https://doi.org/10.1177/15501477211014132

[2] George, L.E., Hassan, E.K., Mohammed, S.G., Mohammed, F.G. (2020). Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key. Iraqi Journal of Science, 61(4): 920-935. https://doi.org/10.24996/ijs.2020.61.4.25

[3] Ding, L., Ding, Q. (2020). A novel image encryption scheme based on 2D fractional chaotic map, DWT and 4D hyper-chaos. Electronics, 9(8): 1280. https://doi.org/10.3390/electronics9081280

[4] Wang, X., Chen, S., Zhang, Y. (2021). A chaotic image encryption algorithm based on random dynamic mixing. Optics & Laser Technology, 138: 106837. https://doi.org/10.1016/j.optlastec.2020.106837

[5] Wang, H., Wang, J., Geng, Y.C., Song, Y., Liu, J.Q. (2017). Quantum image encryption based on iterative framework of frequency-spatial domain transforms. International Journal of Theoretical Physics, 56(10): 3029-3049. https://doi.org/10.1007/s10773-017-3469-5

[6] Tedmori, S., Al-Najdawi, N. (2012). Lossless image cryptography algorithm based on discrete cosine transform. The International Arab Journal of Information Technology, 9(5): 471-478.

[7] Liu, Z., Dai, J., Sun, X., Liu, S. (2009). Triple image encryption scheme in fractional Fourier transform domains. Optics Communications, 282(4): 518-522. https://doi.org/10.1016/j.optcom.2008.10.068
[8] Samson, C., Sastry, V.U.K. (2012). A novel image encryption supported by compression using multilevel wavelet transform. International Journal of Advanced Computer Science and Applications, 3(9): 178-183. https://doi.org/10.14569/IJACSA.2012.030926
[9] Tedmori, S., Al-Najdawi, N. (2014). Image cryptographic algorithm based on the Haar wavelet transform. Information Sciences, 269: 21-34. https://doi.org/10.1016/j.ins.2014.02.004
[10] Guan, M., Yang, X., Hu, W. (2019). Chaotic image encryption algorithm using frequency-domain DNA encoding. IET Image Processing, 13(9): 1535-1539. https://doi.org/10.1049/iet-ipr.2019.0051
[11] Anand, A., Singh, A.K. (2020). An improved DWT-SVD domain watermarking for medical information security. Computer Communications, 152: 72-80. https://doi.org/10.1016/j.comcom.2020.01.038
[12] Saravanan, S., Sivabalakrishnan, M. (2020). Optimal image encryption in frequency domain using hybrid deer hunting with artificial bee colony with hybrid chaotic map. Appl. Math, 14(6): 1163-1174. https://doi.org/10.18576/amis/140622
[13] Al-Haj, A. (2015). Providing integrity, authenticity, and confidentiality for header and pixel data of DICOM images. Journal of Digital Imaging, 28(2): 179-187. https://doi.org/10.1007/s10278-014-9734-8
[14] Pramstaller, N., Gurkaynak, F.K., Haene, S., Kaeslin, H., Felber, N., Fichtner, W. (2004). Towards an AES crypto-chip resistant to differential power analysis. In Proceedings of the 30th European Solid-State Circuits Conference, pp. 307-310. http://dx.doi.org/10.1109/ESSCIR.2004.1356679
[15] Yasser, I., Mohamed, M.A., Samra, A.S., Khalifa, F. (2020). A chaotic-based encryption/decryption framework for secure multimedia communications. Entropy, 22(11): 1253. https://doi.org/10.3390/e22111253
[16] Fridrich, J. (1997). Image encryption based on chaotic maps. In 1997 IEEE international conference on systems, man, and cybernetics. Computational Cybernetics and Simulation, 2: 1105-1110. https://doi.org/10.1109/ICSMC.1997.638097
[17] Huang, L., Wang, S., Xiang, J., Sun, Y. (2020). Chaotic color image encryption scheme using Deoxyribonucleic Acid (DNA) coding calculations and arithmetic over the Galois field. Mathematical Problems in Engineering. https://doi.org/10.1155/2020/3965281.
[18] Moreira, F.J.S. (1992), Chaotic Dynamics of Quadratic maps. Master's thesis, University of Porto.
[19] Xu, X., Feng, J. (2010). Research and implementation of image encryption algorithm based on zigzag transformation and inner product polarization vector. In 2010 IEEE International Conference on Granular Computing, pp. 556-561. https://doi.org/10.1109/GrC.2010.11
[20] Ahmad, J., Larijani, H., Emmanuel, R., Mannion, M. (2018). Secure occupancy monitoring system for IoT using lightweight intertwining logistic map. In 2018 10th Computer Science and Electronic Engineering (CEEC), pp. 208-213. https://doi.org/10.1109/CEEC.2018.8674208
[21] Hashim, A.T., Jabbar, A.K., Hassan, Q.F. (2021). Medical image encryption based on hybrid AES with chaotic Map. In Journal of Physics: Conference Series, 1973(1): 012037. https://doi.org/10.1088/1742-6596/1973/1/012037
[22] Liu, G., Li, W., Fan, X., Li, Z., Wang, Y., Ma, H. (2022). An image encryption algorithm based on discrete-time alternating quantum walk and advanced encryption standard. Entropy, 24(5): 608. https://doi.org/10.3390/e24050608
[23] Wu, Y., Noonan, J.P., Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 1(2): 31-38. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.390.2127&rep=rep1&type=pdf.
[24] Li, Y., Li, X., Jin, X., et al. (2015). An image encryption algorithm based on zigzag transformation and 3-dimension chaotic logistic map. In International Conference on Applications and Techniques in Information Security, pp. 3-13. https://doi.org/10.1007/978-3-662-48683-2_1
[25] Ahmad, J., Hwang, S.O. (2016). A secure image encryption scheme based on chaotic maps and affine transformation. Multimedia Tools and Applications, 75(21): 13951-13976. https://doi.org/10.1007/s11042-015-2973-y
[26] Zhang, Y., Xiao, D. (2014). An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Communications in Nonlinear Science and Numerical Simulation, 19(1): 74-82. https://doi.org/10.1016/j.cnsns.2013.06.031
[27] Xu, L., Li, Z., Li, J., Hua, W. (2016). A novel bit-level image encryption algorithm based on chaotic maps. Optics and Lasers in Engineering, 78: 17-25. https://doi.org/10.1016/j.optlaseng.2015.09.007
[28] Wang, X.Y., Zhang, Y.Q., Bao, X.M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. Optics and Lasers in Engineering, 73: 53-61. https://doi.org/10.1016/j.optlaseng.2015.03.022
[29] Hussain, I., Shah, T., Gondal, M.A. (2012). Image encryption algorithm based on PGL (2, GF (28)) S-boxes and TD-ERCS chaotic sequence. Nonlinear Dynamics, 70(1): 181-187. https://doi.org/10.1007/s11071-012-0440-0
[30] Hashim, A.T., Jassem, A.H., Ali, S.A. (2021). A novel design of blowfish algorithm for image security. In Journal of Physics: Conference Series, 1818(1): 012085. https://doi.org/10.1088/1742-6596/1818/1/012085