Journal of Physics:
Conference Series



**PAPER** • **OPEN ACCESS**

# Medical Image Encryption Based on Hybrid AES with Chaotic Map

To cite this article: Ashwaq T. Hashim *et al* 2021 *J. Phys.: Conf. Ser.* **1973** 012037



# Medical Image Encryption Based on Hybrid AES with Chaotic Map

**Ashwaq T. Hashim[1]*, Amira K. Jabbar[2], Qussay F. Hassan[3]**

[1,2,3] Control and Systems Eng. Dept. University of Technology-Iraq, Baghdad, Iraq

60766@student.uotechnology.edu.iq

**Abstract.** Patient privacy and image protection is an obligation. Data privacy, data protection, and security must be provided by using encryption to ensure confidentiality. Currently, there are numerous standard traditional encryption algorithms. Most of these are suitable for a text file. It is challenging to employ these algorithms for images or videos directly because of strong adjacent pixels correlations. Decreasing the correlation among the surrounding pixels reduces the detail. An algorithm based on a quadratic map is applied as a preprocessing step to nullify the relationship between pixels and reduce the entropy. The AES image encryption is performed for confusion and diffusion, which are necessary for confidentiality. The security analysis findings indicate that the sensitive encryption and decryption techniques are highly dependent on any improvement in the key. The encryption solution is broad enough to avoid brute-force attacks. Thus, during the transfer of medical images over the network, protection can become an issue.

## 1. Introduction

During transmission over networks, data encryption is a solution to maintain confidentiality. These techniques, which protect information utilizing a secret code, are generally the result of mathematical problems that are very difficult to solve without this code. The data transmitted may be the entire patient record or only some clinical data such as images. One way to track the network is to use the "sniffers" that capture everything passing over the network and retain only the messages containing specific keywords [1]. The transmission process is performed over the Internet that makes the program vulnerable to hackers. Hackers can use smart software to take a photo, modify and save it. For example, someone who looks at any portion of the medical picture can send this to the doctor and re-arrange it as they wish. As a result, the doctor may currently make a wrong diagnosis [2].

Consequently, it was necessary to offer a technique for overcoming the challenges outlined above. The patients' right to privacy does not only protect personal information gathered by doctors. Nevertheless, it is also intended to safeguard the image/data transfer process against unauthorized individuals, whose intent would be to replicate these images to feed on or use them for medical purposes without patient's permissions and knowing the original owner [3].

In this paper, an encryption method is proposed using two of the best effective structures of encryption, AES and chaotic maps. They provided a general structure for ciphering medical images. The proposed system merges the required statistical features and chaotic maps diffusion with the confusion influence of the AES encryption algorithm.

The rest of the paper is organized as follows: Sections 2 and 3 describe the AES encryption algorithm and Quadrate chaotic map. Section 4 presents the existing medical image encryption approaches. In Section 5 the proposed image encryption system and an implementation of it are

presented. Section 6 evaluates the performance of the proposed image encryption system. Finally, concluding remarks are drawn in Section 7.

## 2. Advanced Encryption Standard

The Feistel structure is an iterative instead of an AES algorithm. Using these two well-known methods to encrypt and decrypt data, including encryption and permutation and substitution (SPN). Carrying out several mathematical operations in sequence by separate cyphers [4]. Since AES supports a fixed block size of 16 bytes of plaintext, this can handle 128 bits (16 bytes) A 16 bytes are depicted as four squares in a four-dimensional matrix, and AES acts on a byte matrix. In addition, a particularly important aspect of AES is the number of rounds, which can make a difference for speed. If you want to insert long keys, then the number of rounds required will increase. small, medium, and large (128, 192 or 256 bits). the key sizes decide on the number of rounds, including AES for 128-bit keys, must use ten rounds, twelve rounds for AES keys, and an additional two for 256-bit keys [5] and thus: To look at the process of AES encryption in three stages, the initial round, the middle rounds, and the end result are presented here in figure (1). The methods used in all of the model describe the different combinations of functions:

- Initial Round
  AddRoundKey
- Main Rounds
  SubBytes
  ShiftRows
  MixColumns
  AddRoundKey
- Final Round SubBytes
  ShiftRows
  AddRoundKey

As shown in Figure (2) the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S; bij = S(aij). In the MixColumns step, as shown in Figure (3), each column of the state is multiplied with a fixed polynomial c(x). In the AddRoundKey step, as shown in Figure (4), each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕) [5].

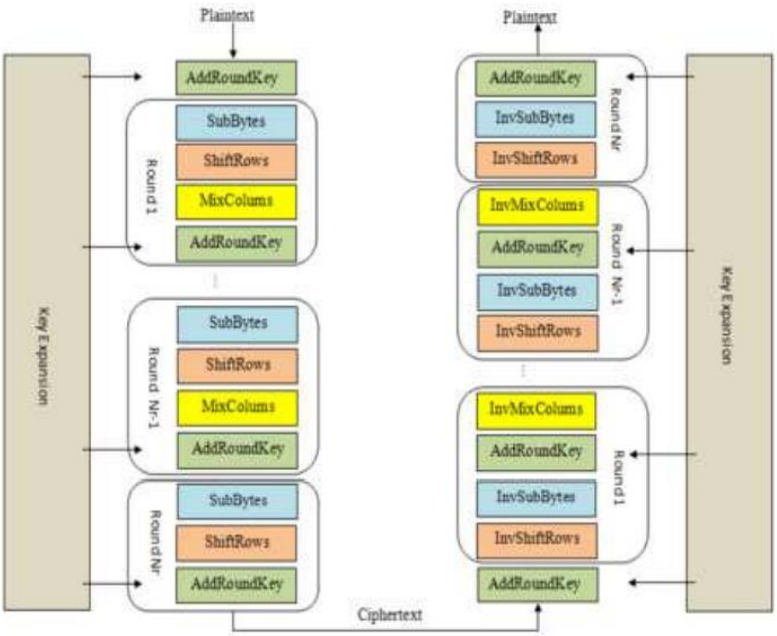



**Figure 1.** General steps of cipher and decipher in the AES.

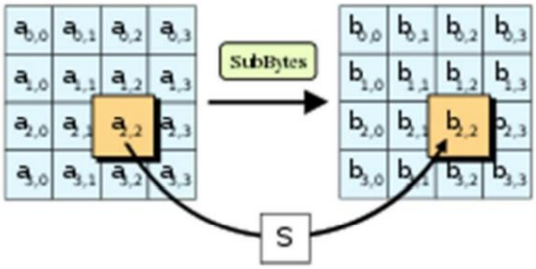



**Figure 2.** The SubBytes step.

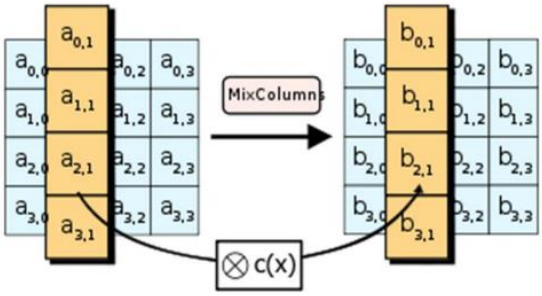



**Figure 3.** The MixColumns step.

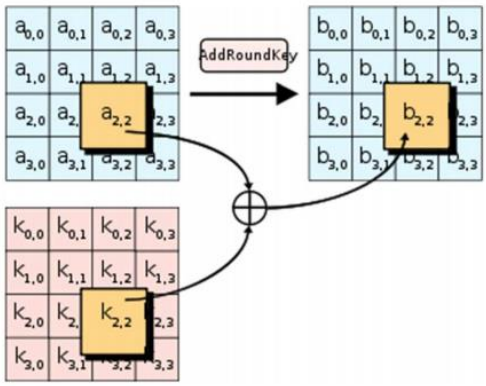



**Figure 4.** The AddRoundKey step.

## 3. Chaotic System

**Chaos-based encryption has introduced a progressively significant and dominant part in current multimedia cryptography than traditional algorithms [6]. The chaotic systems are ergodic, dispersive systems, and extremely sensitive to initial conditions. They have a lot of parallels with applying cryptography. In the field of cryptography, as a result of chaos-based encryption, the chaos-based encryption methods have become a key branch of the cryptosystem. Charlie Fridrich first applied chaotic maps to image encryption algorithms in the late. Then he set out to use the same maps for blurring any picture based on pixel location transformation in 1997 [7]. If researchers were to apply MD chaotic maps, they would start to encrypt images based on 1D and 2D chaotic maps. The MD chaotic maps are commonly used for encryption purposes due to their relatively intricate structures and parameters. But these processes and characteristics increase the complexity of computations and the difficulty of the implementation; despite the 1D chaotic maps having uneven distribution and discontinuous range, they have a more superficial structure than lower dimensional chaotic maps. They can also be straightforward to be handled**

**and used implemented [8]. The Quadratic map is a basic example of a chaotic system. The Equation of the classical Quadratic map is [9]:**

$$Xn\text{-}1 = r - (Xn)2 \quad (1)$$

**Where r is the chaotic parameter and n is the number of iterations. The system of the Quadratic map is chaotic, because it is nonlinear. It is deterministic since it has an equation that determines the behavior of the system. Also, a very slight change in the initial value x0 can significantly impact map behavior [9]. Figure (5) illustrates the Quadrate chaotic map.**

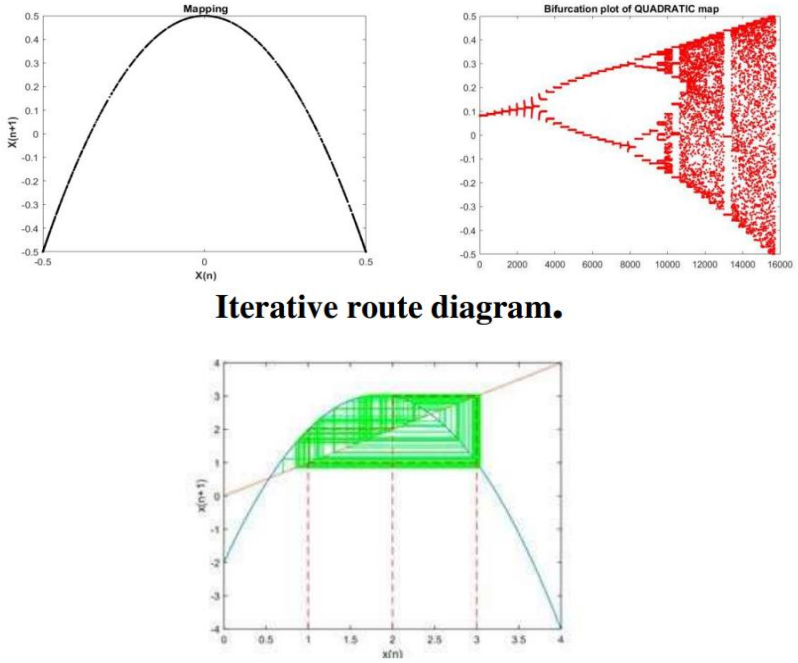



**Figure 5.** Quadratic chaotic map.

## 4. Related Works

Recently, a variety of methods have been developed to ensure the safety of medical images. The authors have included a comprehensive method for conducting a literature review on medical image protection in this section.. In 2014, V. Sunagar and C. Biradar [10] presented a secure method for encrypting all patient data in compliance with the organization's security policy, based on the advanced encryption standard (AES) algorithm. The AES encryption algorithm allows the safe initialization of data in a cloud environment. Finally, the framework included three modules: a module for the PHR owner/patient, a module for data confidentiality, and a module for cloud services that guarantees a high level of protection. In 2018,[11] Zhongyun and Shuang presented a method for encrypting medical images. To begin, some random data is inserted into the surrounding area of the image. Following that, two rounds of high-speed scrambling and pixel adaptive diffusion are used to randomly shuffle neighboring pixels and disperse the inserted random data across the image, resulting in an extremely effective and robust encryption scheme for medical images. It is composed of three components: random data injection, high-speed scrambling, and pixel-level adaptive diffusion. The random data injection function augments the image's surroundings with a random value. The aim of

the high-speed scrambling is to randomly scramble adjacent pixels. The adaptive diffusion at the pixel level distributes these inserted values across entire pixels, as the proposed encryption scheme can be directly applied to images in any representation format. In 2019, [12] Seyed and Yucheng present an algorithm based on chaotic systems to protect medical images against attacks. The proposed algorithm is composed of two major components: a high-speed permutation mechanism and adaptive diffusion. Study of noise and occlusion attacks demonstrates that the proposed algorithm is resistant to these forms of attacks. Moreover, it can be seen that the images after encryption and decryption are of good quality; the measures such as the correlation coe cients, the entropy, the number of pixel change rate (NPCR), and the uniform average change intensity (UACI) have suitable values; and the method is better than previous methods. In 2020, [13] Saleh and Hesham proposed a general medical image cipher structure based on a preparing of two very effective concepts, dynamic substitution boxes (S-boxes) and chaotic maps. It is demonstrated that the arrangement of S-box substitutions prior to and following chaotic substitution successfully resists chosen plaintext and chosen ciphertext attacks. By using powerful cryptographic primitives, the proposed medical image encryption system achieves 1) a high throughput suitable for real-time encryption and 2) increased resistance to chosen plaintext, chosen ciphertext, and reset attacks. The proposed framework's security and efficiency advantages can be applied to any classic, current, or future chaotic map. In 2020, [14] Qiu et al. suggested a security measure that takes advantage of the distributed nature of cloud storage and security keys. It employs a secret, randomly generated password. It is computationally impractical for attackers to have a large enough operational calculation (calculating a large enough number of passwords in a short period of time) to determine the password-the-user desired. This approach is based on a user-centric architecture that secures data on a trusted device, such as the end user's smartphone, and enables the end user to control the data sharing link. To demonstrate that the algorithm works on a smartphone, they evaluated the performance on one. In 2020, Manjula and Mohan [15] proposed using an encryption algorithm to encrypt patient data and conceal it inside medical images. It benefited from the use of an improved AES algorithm. The developers examined the Rijndael AES algorithm's overall structure. They discovered a new dynamic S-Box that provides robust security by using a hash function. In 2021, [16] Hanan and Parah presented a dual-layer security mechanism for securing electronic health records. They enhanced the proposed system's efficiency and security by incorporating steganography and cryptography. The method of interpolation is formulated first, followed by the analysis. The proposed self-adjusted confidence intervals are more accurate than the Nearest Neighbor Interpolation method's study confidence intervals. The variables are correctly predicted using the data set's other variables. The data that would be embedded in the proposed interpolation scheme's CIs was encrypted with a hyperchaotic framework. Additionally, it resulted in a highly stable device due to the large number of keys used (10110). EPR and a 128 128 authentication logo are embedded in the files. To ensure that no image is altered during the generation process, no embedding at the seed pixel location was performed.

## 5. Proposed System

Numerous standard data encryption algorithms are proposed and commonly used. Almost all of these are suitable for a text file. Since image data includes close associations between adjacent pixels, and these pixels have formed intelligible information. It is difficult to use multimedia data without decorrelated adjacent pixels. The amount of information that can be comprehended is reduced by minimizing the interaction between adjacent pixels. A preprocessing step depend on a chaotic map is used to reduce the high correlation between pixels and increase the entropy value. An image encryption algorithm is created by combining the chaos sequence and the AES algorithm. Figure 6 shows a block diagram of the proposed encryption process.

The sender generates a number between 1 and NM, where N and M are the medical image's dimensions. The permuted image is generated using the permutation algorithm. The image is then encrypted using the AES algorithm with a key, yielding an encrypted image. When the encrypted image is received, the receiver decrypts it using AES (using a previous key). The receiver generates a random number using the same hidden parameters X and an as the sender when it receives the decrypted image. The original text is then generated using the re-permuted image.

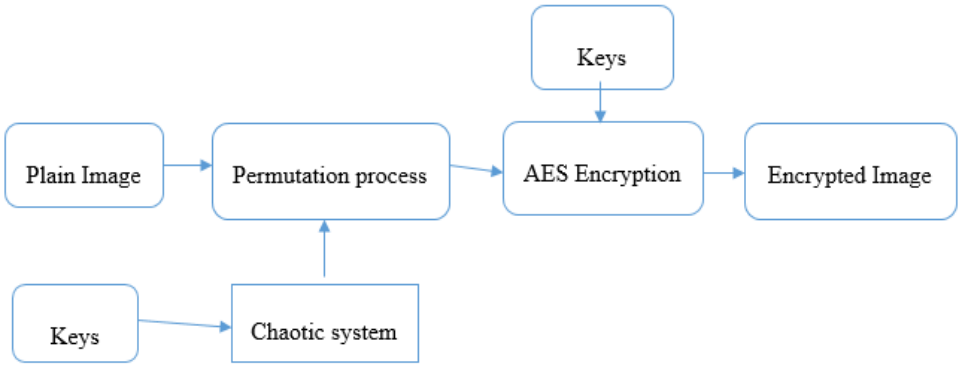



**Figure 6.** The block diagram of the proposed encryption method.

Algorithm (1) presents the proposed encryption system steps.

| **Algorithm 1: The encryption algorithm** |
|---|
| **Input:**<br>Mimg // medical image<br>$X_0$, a // secret parameters<br>**Output:**<br>EMimg //Encrypted medical image |
| **Step1:** Read medical image Mimg<br>**Step2:** Permute Mimg based on quadrate chaotic map by algorithm (2).<br>**Step3:** Perform the AES cipher algorithm to encrypt the permuted image.<br>**Step4:** Output the encrypted image EMimg. |

*5.1 The Permutation Process Based on Chaotic Map*

| **Algorithm 2: Image Permutation** |
|---|
| **Input:**<br>Mimg, // medical image<br>M, N, // medical image dimension<br>$X_0$, a // secret parameters<br>**Output:**<br>PMimg // Permuted medical image |
| **Step1:** Let Len = N×M<br>**Step2:** Construct a random sequence X by quadratic map<br>Let a =0.4, $X_0$ =0.15, $X_0$ = a × $X_0$^2<br>For i = 1 to Len<br>$X_i$= a ×$X_{i-1}$ ^2<br>End<br>**Step3: Mapping** the range of chaotic map X from [-0.5 0.5] to [1 Len]<br>Max =Len , Min =1<br>For i = 1 to L<br>$T_i$ = (Max–Min)/(Max-Min) × ($X_i$ –Max) + Max<br>End<br>**Step4:** Convert the Wimg from 2D to 1D |

**Step5:** Relocate the pixel positions of MI according to T
**Step6:** Reshape the 1D array to 2D permuted medical image PMimg.

*5.2 The AES Encryption Algorithm*

Today, almost all digital services like internet communication, medical and military imaging systems, and multimedia system require reliable security in storage and transmission of digital images. Due to the fast growth in multimedia technology, internet and cell phones, there is a need for digital photos security. Therefore, there is a need for image encryption techniques to hide images from such attacks. To protect valuable medical image information from undesirable readers, image encryption is essential. This thesis presents AES (Advanced Encryption Standard) operations in medical image encryption and decryption.

In the decryption process, the inverse of all steps is implemented to get the original image. Figure (7) shows the medical image encryption and decryption steps.

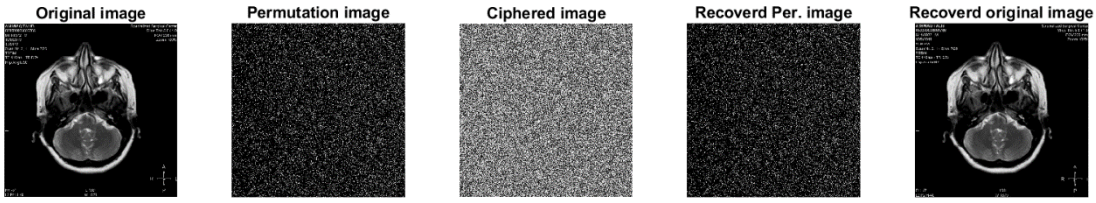



Figure 7: Medical image encryption and decryption.

## 6. Security of the Proposed System

Protecting medical image information is a legal requirement. Traditional encryption methods fall short of handling the large volume of medical image data and their peculiar statistical properties. Using generic medical image encryption framework based on a novel arrangement of two very efficient constructs, chaotic map and AES, provided image confidentiality of medical image. Figure (8) shows the test images after being permuted and then encrypted by the proposed algorithm.

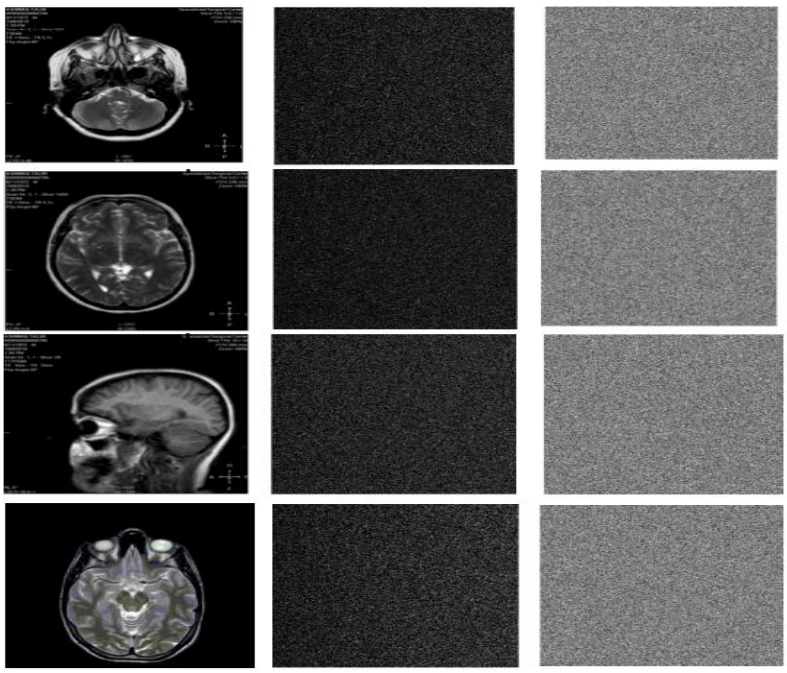
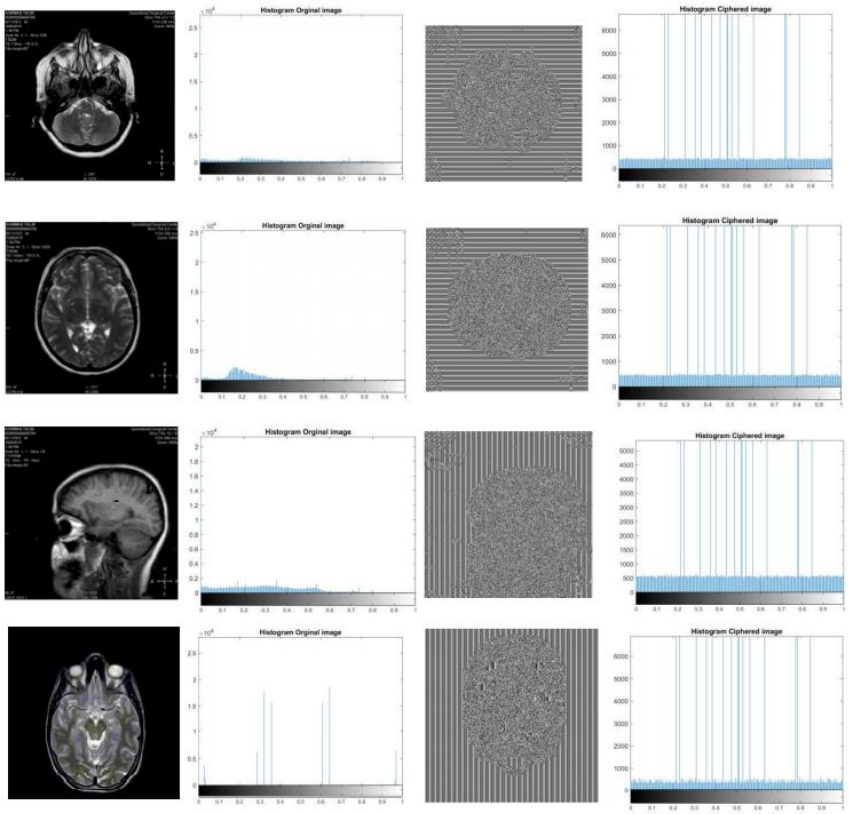


Figure 8: Medical image encryption. (a) Original image, (b) Permuted image, (c) Encrypted image

The analysis of the data of the image mainly consists of histogram analysis, pixels correlation and information entropy. After the algorithms review, the interpretation of the algorithm is used to function the assignment in this section.

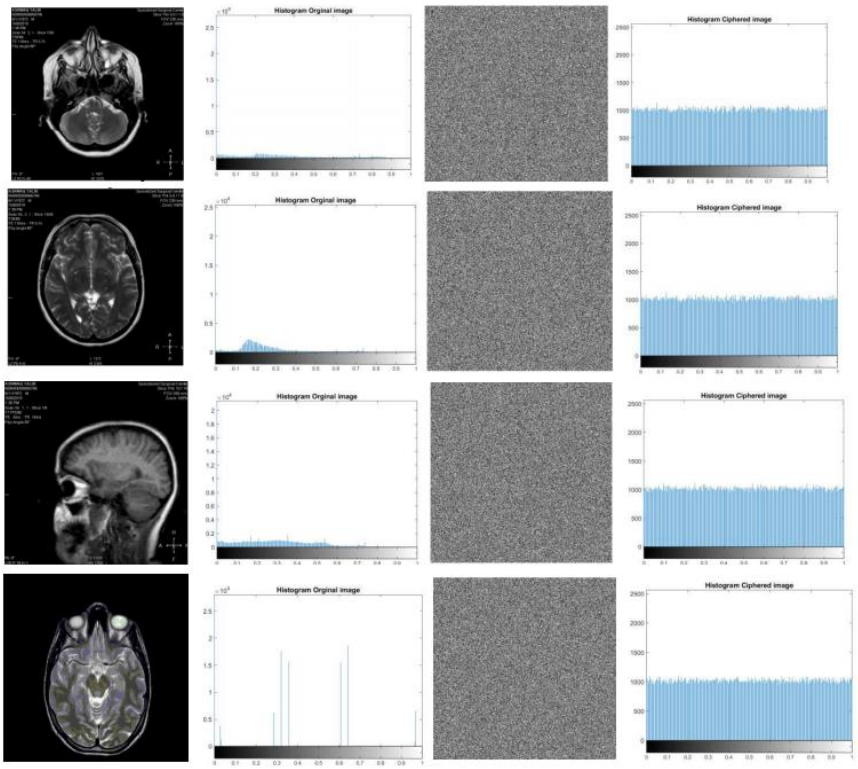
*6.1 Histogram Analysis*

A histogram depicts the distribution of image pixels of the image. Figure (9) shows the histograms of the test images and the encrypted images using the standard AES algorithm. In comparison, Figure (10) depicts the original test images' histograms and the encrypted images produced by the proposed method. We see how the probability distribution associated with the original image propagates as a single peak distribution. The probability distribution associated with the original image, which is further ciphered according to the proposed scheme, is closed to the equilibrium probability distribution. As a result, the machine generates a semi-random picture for each message its ciphers. Since the histogram distribution of the original AES encrypted image is not similar, it is incompatible with image encryption.




(a) (b) (c) (d)

Figure 9: Image encryption and decryption by AES. (a) Original image, (b) Histogram of original image, (c) Encrypted image (d) Histogram of the encrypted image.

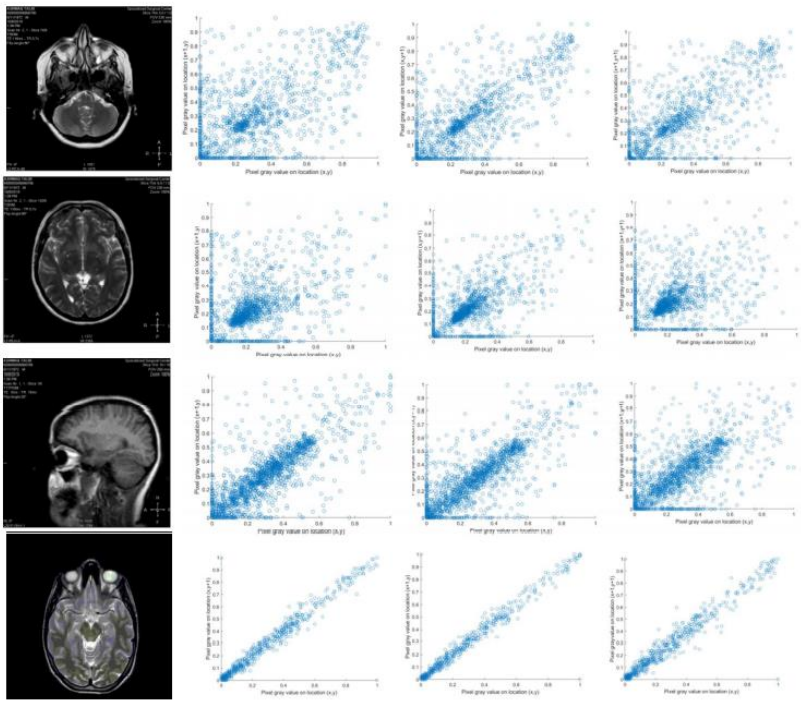



(a) (b) (c) (d)

Figure 10: Image encryption and decryption by the proposed system. (a) Original image, (b) Histogram of original image, (c) Encrypted image (d) Histogram of the encrypted image.

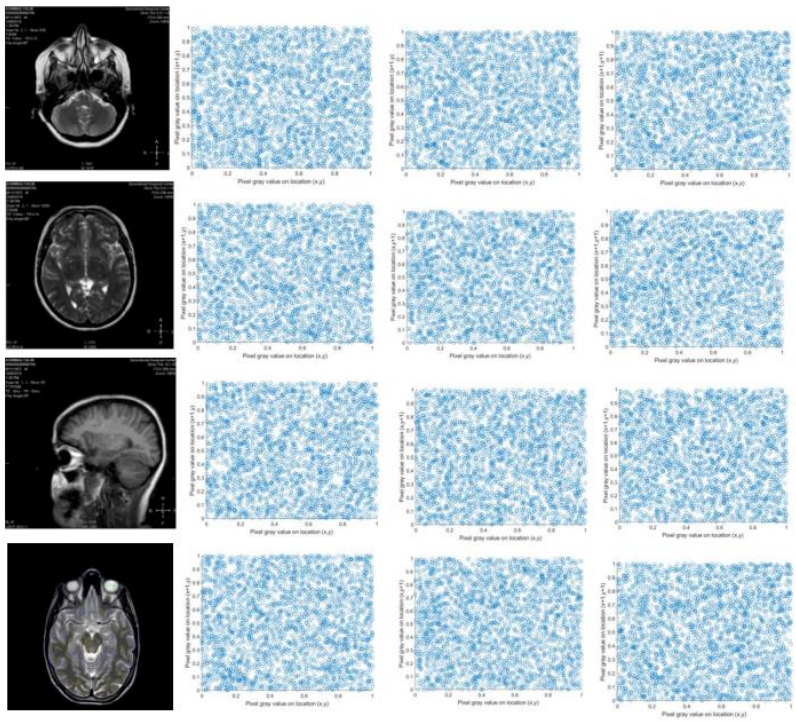
### *6.2 Correlation Coefficients Analysis*

The primary goal of image encryption is to reduce the connections between adjacent pixels. A standard image is densely sampled in all directions across the grid. One of the objectives of image encryption is to minimize associations between adjacent pixels in order to increase the apparent degree of protection. It is important to understand the relationship between horizontal, vertical, and diagonal pixels. Figure (11) illustrates the correlation density distribution maps for test images. The proposed relation map for the encrypted images by the device is depicted in Figure (12). Although the picture is highly associated in monochrome pictures, viewing a linear relationship, this correlation is significantly diminished when viewing ciphered images. This means that the latest technique for image encryption is extremely effective and secure. The accuracy relationship [17] between the proposed system and the AES method is shown in Table 1.



(a) (b) (c) (d)

Figure 11: Correlation coefficients of original images. (a) Original images, (b) Horizontal correlation,
(c) Vertical correlation,(d) Diagonal correlation.



(a) (b) (c) (d)

Figure 12: Correlation coefficients of original images. (a) Original images, (b) Horizontal correlation, (c) Vertical correlation, (d) Diagonal correlation.

**Table 1**: Comparison of correlation

| Images | AES algorithm | Proposed system |
|---|---|---|
| Image1 | -0.0188 | -0.0022 |
| Image2 | -0.0123 | -0.0019 |
| Image3 | -0.0168 | -0.0025 |
| Image4 | -0.0121 | -0.0016 |

*6.3 Entropy Analysis*

When the picture gives more sensory information, more entropy of information can occur. The information entropy [18] of original test images, ciphered images by AES algorithm, and encrypted image by the proposed method are computed and shown in Table (2). The entropy of the encrypted image shows that the proposed scheme for all test images is very strong and there is a greater superiority of the algorithm.

**Table 2**: Comparison of Entropy

| Images | Original images | AES algorithm | Proposed system |
|---|---|---|---|
| Image1 | 3.6285 | 6.9382 | 7.9906 |
| Image2 | 3.8132 | 7.0615 | 7.9995 |
| Image3 | 4.7443 | 7.3288 | 7.9980 |
| Image4 | 1.8632 | 6.7297 | 7.9994 |

*6.4 NPCR and UACI Analysis*

The NPCR and UACI tests [19] assess a cryptographic system's resistance to differential attack. The proposed system's NPCR and UACI results are summarized in Table (3). When the ciphertext's NPCR and UACI are greater than 99.60 and 33.46 percent, respectively [20], it means that the proposed algorithm is more secure than the standard AES algorithm. Thus, the proposed algorithm's values are closer to the theoretical value than the initial AES's values. As a result, the proposed algorithm is extremely resistant to differential attacks.

**Table 3**: Comparison of NPCR and UACI.

| Images | The Proposed systems | |
|---|---|---|
| | NPCR | UACI |
| Image1 | 99.62 | 44.25 |
| Image2 | 99.61 | 43.65 |
| Image3 | 99.64 | 41.56 |
| Image4 | 99.61 | 43.55 |

*6.5 Analysis of Key Space*

The key size should be larger than $2^{100}$ to prevent attacks like the brute force attack [21]. The large keyspace is also crucial to avoid a comprehensive search for a key (Solve the problem of detecting the exact key value by experimenting with the possible values until the correct key is found). The suggested approach is used Quadratic' map, that utilize two variables $x_0$ and a. Due to, the keyspace is $\{X_0, a\}$. Since $X_0$ and a are two numbers of double precision, the total number of various values for X0 and a is more than $10^{14}$. So, the keyspace for the proposed system is larger than $(10^{14})^2 = 10^{28} \approx 2^{93}$. The keyspace of the AES algorithm is $2^{256}$. The total keyspace of the proposed system is $2^{349}$. The keyspace between both the algorithm as well as the other implementations is compared to the keyspace given in Table 4. The main space of the used algorithm is larger than that of most

comparable algorithms. In this research, the keyspace for the improved encryption scheme is large, and thus, the brute force attack is impractical on the proposed algorithm.

**Table 4**. Comparisons of the keyspace.

| Encryption Algorithm | Keyspace |
|---|---|
| **Zhu et al. [ 64]** | $2^{339}$ |
| **Wang et al. [65]** | $2^{149}$ |
| **Guesmi et al. [66]** | $2^{256}$ |
| **Li et al. [67]** | $2^{299}$ |
| **Li et al. [68]** | $2^{375}$ |
| **Curiac et al. [69]** | $2^{128}$ |
| **Curiac et al. [70]** | $2^{357}$ |
| **The Proposed algorithm** | $2^{349}$ |

## 7. Conclusions

This article presents a novel algorithm for protecting these images from attacks that is based on AES and chaotic systems. By using powerful cryptographic primitives, the proposed medical image encryption scheme achieves the following: 1) a huge keyspace, making brute force attacks impractical. 2) Scrambling medical images prior to applying the AES algorithm provides greater protection than AES alone. The proposed system's ciphered images have a probability distribution that is similar to the equilibrium probability distribution; hence, the encrypted image is a semi-random image. Since the standard algorithm for image encryption is inefficient for use in authentication, it is substituted by a more effective algorithm. In comparison to the conventional AES algorithm, the proposed algorithm provides superior protection. Thus, the proposed algorithm's values for entropy, NPCR, UACI, and correlation coefficient are nearer to theoretic values than those of the traditional AES. As a result, the proposed algorithm is extremely resistant to differential attacks.

## 8. References

[1] Fernando Jorge S. Moreira, (1992), Chaotic dynamics of quadratic maps, Master's thesis, University of Porto.

[2]Tan, C.K., Ng, J.C., Xu, X. et al. Security Protection of DICOM Medical Images Using Dual-Layer Reversible Watermarking with Tamper Detection Capability. J Digit Imaging 24, 528–540 (2011).

[3] A. Ustubioglu and G. Ulutas, "A new medical image watermarking technique with finer tamper localization", J. Digit. Imag., vol. 30, pp. 665-680, Dec. 2017.

[4] G. Coatrieux, H. Maitre, and B. Sankur, "Strict integrity control of biomedical images," in Proceedings of SPIE, 2001, vol. 4314, pp. 229-240.

[5] B. Schneier, Applied cryptography: protocols, algorithms, and source code in C. Wiley, 1996.

[6] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, "A watermarking technique based on one-way hash functions," Consumer Electronics, IEEE Transactions on, vol. 45, no. 2, pp. 286-294, 1999.

[7] O. Tayan, M. N. Kabir, and Y. M. Alginahi, "A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents," Sci. World J., vol. 2014, pp. 1–14, Aug. 2014.

[8] Muhammad N, Bibi N, Mahmood Z, Akram T, Naqvi SR (2017) Reversible integer wavelet transform for blind image hiding method. PLoS ONE 12(5): e0176979. https://doi.org/10.1371/journal.pone.0176979

[9] A. K. Gulve and M. S. Joshi, "An image steganography method hiding secret data into coefficients of integer wavelet transform using pixel value differencing approach," Math. Probl. Eng., vol. 2015, 2015.

[10] Sunagar V, Biradar C. Securing public health records in cloud computing patient centric and fine grained data access control in multi owner settings. Int J Sci Appl Inf Technol (IJSAIT) 2014; 3(4):18–21.
[11] Z. Hua , S. Yi, Y. Zhou," Medical image encryption using high-speed scrambling and pixel adaptive diffusion" 144 (2018) 134–144.
[12] S. Moafimadani, Y. Chen, and C. Tang," A New Algorithm for Medical Color Images Encryption Using Chaotic Systems" 10 June 2019.
[13] S. Ibrahim, H.Alhumyani, M. Masud," A New Algorithm for Medical Color Images Encryption Using Chaotic Systems", 31, 2020, date of current version September 15, 2020.
[14] H. Qiu, M. Qiu, M. Liu and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0", IEEE J. Biomed. Health Informat., vol. 24, no. 9, pp. 2499-2505, Sep. 2020.
[15] Manjula G, Mohan H S, "A secure Framework for Medical Image Encryption Using Enhanced AES Algorithm", International Journal of Scientific & Technology Research, Vol. 9, No 2, February 2020.
[16] Hanan Aljuaid, Shabir A. Parah "Secure Patient Data Transfer Using Information Embedding and Hyperchaos", Sensors 2021, 21, 282.
[17] M. Najm , A.kamil ," Improved anti-noise attack ability of image encryption algorithm using de-noising technique", 2020, pp. 3080~3087.
[18] Ashwaq. T. Hashim, Ammar H, Suhad A," A Novel Design of Blowfish Algorithm for Image Security", 2021 J. Phys.: Conf. Ser. 1818 012085.
[19] Ashwaq. T. Hashim, Bahaa D. Jalil, "Color image encryption based on chaotic shit keying with lossless compression", International Journal of Electrical and Computer Engineering, Vol 10, No 6. 2020, pp. 5736~5748
[20] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber journals Multidiscip. journals Sci. Technol. J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.
[21] S. Zhang, X. Xie, and Y. Xu, "A Brute-Force Black-Box Method to Attack Machine Learning-Based Systems in Cybersecurity," *IEEE Access*, vol. 8, pp. 128250–128263, 2020.