Hindawi
Security and Communication Networks
Volume 2021, Article ID 3570904, 14 pages
https://doi.org/10.1155/2021/3570904

Research Article

A Novel Random Error Approximate Adder-Based Lightweight Medical Image Encryption Scheme for Secure Remote Monitoring of Health Data

Nagarajan Manikandan,[1] Rajappa Muthaiah,[1] Yuvaraja Teekaraman,[2] Ramya Kuppusamy,[3] and Arun Radhakrishnan[4]

[1]*School of Computing, SASTRA Deemed University, Thanjavur, Tamil Nadu 613 401, India*
[2]*Mobility, Logistics, and Automotive Technology Research Centre, Faculty of Engineering, Vrije Universiteit Brussel, Brussel 1050, Belgium*
[3]*Department of Electrical and Electronics Engineering, Sri Sairam College of Engineering, Bangalore City 562 106, India*
[4]*Department of Electrical & Computer Engineering, Jimma Institute of Technology, Jimma University, Jimma, Ethiopia*

Correspondence should be addressed to Yuvaraja Teekaraman; yuvarajastr@ieee.org and Arun Radhakrishnan; arun.radhakriahnan@ju.edu.et

Received 20 September 2021; Revised 14 October 2021; Accepted 27 October 2021; Published 23 November 2021

Academic Editor: Thippa Reddy G

In the present global scenario, social distancing is an inevitable one. The need for social distancing and advancements of technology to facilitate the patients and doctors around the world mandated the telemedicine and remote monitoring of patience details as the pivotal way to diagnose the disease. In this, it is essential to transmit the patient's information such as X-ray and scan images of them to the doctor in the remote location. Preventing the medical data from the technological adversaries is the need of the hour. Infinitesimal attacks in medical images may cost human lives. This work proposes a lightweight, secure medical image encryption scheme for the remote monitoring of health data. The proposed encryption scheme uses computationally less complex weighted shift approximate adder (WSAA)–based encryption logic. The scheme uses a 256-bit key for the encryption process that strengthens the encryption and robust against various attacks. The proposed encryption scheme deploys the WSAA for diffusing the pixel values. A unique way of key distribution for pixel-wise encryption within the image is proposed that avoids the need for separate logic for the pixel-wise confusion. The proposed Encryption scheme is evaluated for its entropy and horizontal, vertical, diagonal correlation, histogram, key space, and sensitivity. Experimental results affirm that the proposed scheme significantly good with less computational complexity. The peak signal-to-noise ratio (PSNR) value of the decrypted image is infinity, and this matches the ideal requirement of the medical encryption scheme.

1. Introduction

The recent technological development and advancement in the Internet of Things (IoT) facilitate the people to make use of resources available around the world. This rapid development of technology trends and enables the patients to get the support of doctors globally. The patient's information, such as clinical test reports, X-ray, and scan reports, are sent through the Internet medium. Most of the clinical data are in the form of an image [1]. The information over the Internet is more prone to vulnerabilities and attacks. Any corruption or misinterpretation of medical data due to the intermediate attack is nontolerable, and it may endanger to human lives. This necessitates the scheme for the secure remote monitoring of health data. There are many image encryption schemes presented in the literature for the general images, but when it comes to medical image, those methods may not be secure enough to preserve the information of the patients. This is due to the strong correlative nature of pixels with its adjacent pixels in the medical images and various modalities

of capture [2]. Most widely used modalities in the medicinal field are X-ray, magnetic resonance imaging (MRI), ultrasonography (US), computed tomography (CT), and positron emission tomography (PET) [3–6]. This triggered and motivated the researchers to develop various robust encryption schemes [2, 3, 7–19].

Recent research uses efficient techniques such as watermarking [7–10], Arnold mapping [11, 12], chaotic mapping [13, 14], permutation [14, 15], compression [15], scrambling [16], genetic algorithm [2], swarm optimization [17], elliptic curve cryptography [18], and neural networks [19] individually or as a combination for hiding the medical information or authenticating the information. Researchers developed their encryption schemes and validated for different modalities of medical images to defy against attacks. The generic need of any cryptosystem is to keep high computation cost and time of breaking the cipher [7]. The entire above encryption schemes are good enough to maintain the generic requirements. Nevertheless, the scenario has changed, and one more requirement is also needed to be considered along with those two generic requirements.

Nowadays, computing systems are getting smarter and almost all the devices which use the Internet are embedded and low power systems in nature. This demanded the lightness of computation and added the lightweight computation of the scheme in the requirement list [20]. Based on the need of the hour, many lightweight encryption schemes have been proposed for general images [21–25] and medical images [4, 5, 17, 26]. Various exciting and unique techniques are introduced for encryption to make it light. The logic used in moves of the knight pawn in the ancient Indian game chess along with a genetic algorithm is used to encrypt the image [21]. This approach attains the secured encryption in four stages with the moderate performance of entropy and PSNR. Mondal et al. formulated a lightweight scheme; two pseudorandom numbers (PRNs) are used. One is to permute the plain image, and another is to encrypt it by deoxyribonucleic acid (DNA) computation. This method achieves better performance at the expense of computation complexity [22].

Javeed et al. presented a chaotic-based lightweight system which uses the chaotic oscillator for generating random numbers to scramble the pixels. Authors claimed that their system withstands for plaintext attacks and brute-force attacks. This system has the complexity of solving and makes use of second-order differential equations for generating the random numbers [23].

A hybrid method of encryption after compression is developed by Almalkawi et al. [24]. Here, 2D logistic chaotic and Henon chaotic maps are used for bit scrambling and pixel shuffling of the compressed image, respectively. This method needs more number of rounds for better encryption. A partial encryption method of encrypting the region of interest area is proposed by the Khashan and AlShaikh [25]. Authors used the edge detection principle to locate useful information in the region of interest, and information of edges are encrypted. This obviously reduces the overhead of computation, but it reveals other regions explicitly. Mortajez et al. [26] developed a method of generating a key from the images and shuffling the pixel positions based the generated random numbers. The shuffled pixels are later encrypted by the sequence of logistic systems and XOR gates.

From the literature, it is evident that complex logics are needed to produce randomness. It also needs multiple rounds for achieving better encryption. In this work, we proposed a novel and unique scheme which avoids these overheads and attains good encryption.

1.1. The Significant Novelty and Contribution of Our Work in the Encryption and Decryption Process

(1) A unique method of deriving random numbers for shuffling bit positions of the pixels is proposed.

(2) Proposes a novel random error weighted (Hamming weight) shift approximate adder of less computational complexity for diffusing the bits in the pixel.

(3) An effective key distribution strategy is proposed among the pixels within an image to ensure the randomness of encryption.

(4) The two ways application of encryption process inherits itself the pixel confusion property and avoids the need for separate logic and computation complexity for the same.

(5) Uses very simple arithmetic and logical operations, which makes the encryption and decryption process a lightweight (based on computational complexity). Cryptanalysis of the implemented scheme proves that the proposed scheme defy various attacks.

1.2. Organization. The rest of the manuscript is presented as follows: related works are discussed in Section 2. Section 3 describes the proposed encryption and decryption schemes. Implementation of the proposed scheme and its outputs are presented in Section 4. Security analysis of the proposed schemes is detailed in Section 5. The suitability of the proposed scheme for medical application is justified by comparing PSNR with existing works in Section 6. Section 7 concludes the article with the consolidated research outcomes.

2. Related Works

The tremendous growth of the IoT triggered the researchers to focus on the concept of lightweight cryptography recently, even though it existed well before IoT. Most of the lightweight works are described for general images and not for medical images due to its close correlation of pixels. This motivates and challenges the researchers. The development of lightweight computation without accuracy loss has acquired major attention. In this section, we presented closely related latest works which involve less computation for the encryption process.

A lightweight encryption scheme for implantable medical devices is presented by Belkhouja et al. [27]. This encryption scheme targeted information transfer through

the wireless medium. Authors claimed that they had ensured the patient's information by encrypting the data using a lightweight chaotic system generated keys. Abd El-Latif et al. [28] developed the simple encryption protocol with the new logic called controlled-NOT image. They performed encryption based on the NOT image generated from the logistic map. In addition to that, the method of key matrix generation from the embedding process is suggested to improve the encryption process. The encrypted image can only be decrypted by having both the logistic map and the key matrix.

The idea of hardware-dependent [29, 30] encryption schemes has started to evolve recently for better compatibility and security. Ravichandran et al. [29] implemented a low power medical image encryption scheme in the field programmable gate array (FPGA) using the penta-layer approach. Encryption of the medical image is done in five different layers. Each layer uses a different scheme of shuffling and scrambling and attains a secured encrypted image. High security is attained by producing hardware-dependent encryption in the fourth layer. Janakiraman et al. [30] created the hardware-dependent lightweight steganography scheme by considering resource constraints in the hardware for embedded applications. The authors explored the device-dependent implementation of the cryptography schemes, which exhibits robustness against various attacks.

Encryption methods for the secure transmission of DICOM images are presented [26, 31]. A chaotic secure encryption scheme with dynamic secret keys is developed by Mortajez et al. [26]. The system uses a periodic confusion strategy to encrypt the DICOM images. The scheme first extracts the key from the medical image, and pixels position has been permuted using the periodic confusion strategy. Then, pixels are encrypted based on random sequences of the logistic map and XOR operator. Based on the cryptanalysis, authors claimed that their scheme is able to withstand against statistical attacks. Manikandan and Amirtharajan [31] formulated the new way of scrambling and used a RC6 cipher encrypted approximate coefficients of the Harr wavelet transform for encrypting the medical images to withstand various attacks. With the sufficient key space, the algorithm effectively withstands the key hack.

Venkateswarlu [9] has implemented a fast medical image security algorithm for color medical images using both watermarking and encryption schemes for better security in each color channel. In this scheme, the patient's information, along with the smoothened key image, is embedded into the image color channels to produce a watermarked image. In the second stage, each watermarked color channel is separately encrypted to generate a final encrypted image. The reverse process is done on the decryption side. The author claims that it shows better resistance against key guessing attacks. The key which made the scheme robust is the actual set back of this method. Here, the image of size less or equal to the plain image needs to be used as a key, and it needs more bandwidth for transmission and needs to have more storage for the computation.

Madhusudan and Sakthivel [12] developed the image encryption approach that first represents image pixels in binary form. The binary values of the pixels have been shuffled by the two random numbers generated by the Arnold map. The shuffled binaries are converted back to pixel integers and positions of the pixels are scrambled randomly with reference to the chaotic matrix to produce an encrypted image. The strength of the algorithm is justified by various security analyses. In this work pixels are not handled as an array; instead, it is converted into a sequence of numbers later diffusion and confusion are done. The shape conversion needs more logic to remember the indexes of each pixel when it is in the decryption stage, and it is an extra overhead.

Tamilarasi and Jawahar [17] designed a hybrid lightweight encryption algorithm with the swarm optimization technique (HLE-SO). HLE-SO combines the Paillier and KATAN methods to make it lightweight. The authors' utilized swarm optimization for managing key space which addresses the limitation of the key sizes of the lightweight encryption methods. They deployed the scheme for EEG medical data and simulated the algorithm using MATLAB. Authors mentioned that the KATAN algorithm used for lightweight features was subjected to 254 rounds.

Khashan and AlShaikh [25] presented a lightweight encryption scheme which encrypts a selected portion of the medical image. This scheme concentrates on the region of the interest portion of the medical image rather than useless black pixels around the actual medical image. To do that, this scheme first performs edge detection then encrypts the edges with the random keys generated by chaotic map using one-time pad algorithm. This method of selective portion encryption greatly reduces the computation overhead so that authors claim that it is a lightweight scheme. Authors claim their schemes robustness against various attacks. However, still, most of the portion is visible in the encrypted image that will lead to the guess of an image. Nevertheless, recovering entire information without the proper key is not possible.

Mubashar et al. [32] used a novel block chain based technique for the encryption of medical data along with the optimization algorithm to create a framework for the IoT based medical data archival system.

The existing works in the literature have its own merits and demerits. At the outset, frequent shuffling, more storage requirement, and a number of rotations are the major cons of the existing cryptosystems. Moreover, most of the works mentioned above are developed without considering hardware implementation complexities. Randomness and less complex computations are the desired pros of the cryptosystem. Our proposed architecture carefully handles the listed overheads and makes use of the novel weighted shift approximate adder to form a simple, lightweight, and secure encryption scheme.

3. The Proposed Scheme

This work is drafted to overcome the short comings of the existing lightweight cryptography schemes especially when they are implemented in portable devices. By carefully analyzing the needs, we proposed a scheme which has approximate adder as a core part and performs encryption and decryption process based on it. In this section, the research flow of the proposed scheme is explained from the design of

the novel proposed random error weighted shift approximate adder (WSAA) and its suitability for utilizing it in cryptography domain is analyzed. The encryption and decryption process are performed over various medical modality images using the MATLAB tool. Later, the strength of the proposed scheme is evaluated by applying various cryptanalysis methods and results of them are presented as proof of versatility of the proposed scheme with the less computation effort.

Our proposed random error approximate adder-based lightweight encryption and decryption scheme for securing remote medical data deploys the novel proposed random WSAA for bringing diffusion kind of property to the pixel values. In most of the cases, the diffused or permuted pixel and original pixel will have an equal Hamming weight. However, in our proposed scheme, weight after diffusion and before diffusion would not be equal. This gives additional security for the information in the diffusion phase.

3.1. Weighted Shift Approximate Adder. The proposed WSAA has two steps of computation. In the first step, an operand is circularly shifted toward right up to the number of positions equal to the Hamming weight of the given first operand. The weighted shift (WS) operand is added with the second operand and the shifted second operand in the second step. It can be observed that the Hamming weight of the sum is no way correlated to the source operand A or B. A sample calculation is presented in Figure 1.

The design expressions of the WSAA is given in the following equations (1)–(5):

$$\text{weighted shift}(A) = \text{circular shift}(A, \text{Hamming}(A)), \tag{1}$$

$$\text{Sum}_0 = \text{WS}_0(A) \oplus B_0 \oplus 0, \tag{2}$$

$$\text{Sum}_i = \text{WS}_i(A) \oplus B_i \oplus B_{i-1}, \tag{3}$$

$$\text{Carry}_{\text{in}} = \text{Carry}_0 = 0, \tag{4}$$

$$\text{Carry}_i = B_{i-1}. \tag{5}$$

In our propose, encryption scheme inputs for the WSAA is as follows:

$$A = \text{input pixel}, \tag{6}$$

$$B = \text{segmented key}, \tag{7}$$

$$\text{Carry}_i = \text{shifted segmented key}. \tag{8}$$

The segmented key is used as a second operand. The second operand is shifted toward left by one position. It is mentioned in equations (2), (3), and (7).

3.2. Error Characteristics of the Proposed WSAA. Error characteristics of the approximate adders describe the nature and accuracy of the results produced. In this work, the proposed WSAA is aimed to produce more errors in random so that it could be used in encryption schemes. For the proposed 8-bit WSAA, the following error metrics [33, 34] are calculated:

$$\text{MED} = \frac{1}{2^{2n}} \sum_{i=1}^{2^{2n}} \text{ED}_i,$$

$$\text{NMED} = \frac{\text{MED}}{D}, \tag{9}$$

$$\text{ER} = \frac{\text{number of erroneous results}}{\text{total number of results}},$$

where ED_i is the error distance which equals to the absolute difference of i^{th} actual and i^{th} approximate result. MED is the mean error distance and NMED is the normalized mean error distance. D denotes the maximum result of 8-bit accurate addition, and ER indicates the error rate.

The calculated error parameters of the proposed 8-bit WSAA are presented in Table 1. From the characteristics, it is clear that the proposed adder can be able to produce 99.7% erroneous results and its MED is also high. Moreover, the produced results are also random in nature.

3.2.1. Statistical Characteristics of the WSAA. The probability of each value of output is 1/256. Since 8-bit is only used to represent the result, the minimum value of the sum output is 0 and the maximum value of the output is 255. Each output value is produced by 256 unique combinations of inputs. This ensures the randomness of the produced output, and it minimizes the probability of guessing. Table 2 shows the few samples of combinations that produce 1 as the sum output.

In the conventional accurate adders, a specific number can be arrived as a sum result for a few related combinations and it is highly predictable. For instance, a resultant sum value 1 can be attained either by $0 + 1 = 1$ or by $1 + 0 = 1$. Similarly a bigger sum result may have "n" number of combinations to produce the sum as a result, yet it is easily predicted. However, in the proposed adder, the sum value is produced by various combinations of irrelevant numbers as shown in Table 2 and it is hard to predict the same.

Moreover, unlike the conventional and other approximate adders in the literature, the proposed WSAA has a peculiarity and it is noncommutative. Results of the same combination of inputs in a different order will give rise to different outputs, and the samples are given as proof in Table 3.

The proposed WSAA addition operation on a set S is said to be commutative if

$$\text{Input 1} + \text{Input 2} = \text{Input 2} + \text{Input 1}, \quad \text{for all Input 1} = \text{Input 2} \in S. \tag{10}$$

WSAA addition operation on a set S is said to be noncommutative if

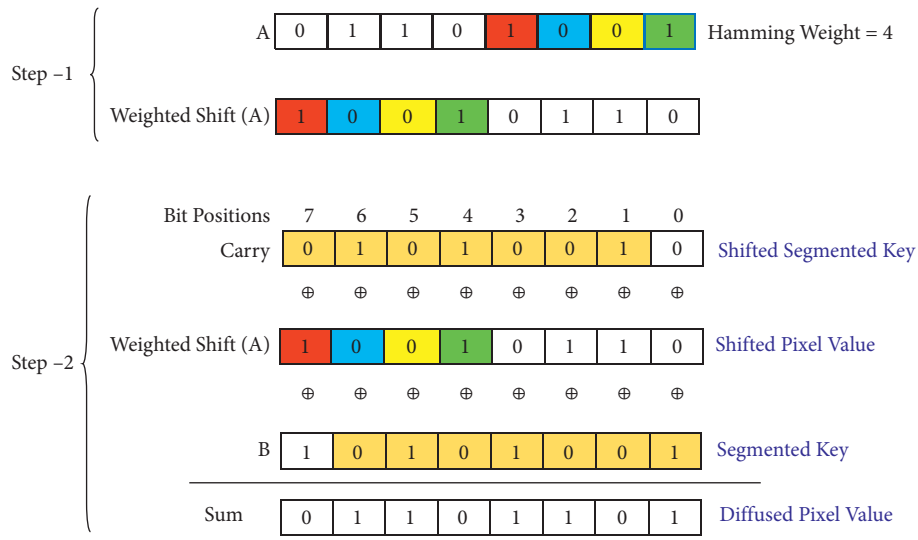

Figure 1: The proposed 8-bit weighted shift approximate adder (WSAA) steps with a sample calculation.

Table 1: Error characteristics of the proposed 8-bit WSAA.

Adder	ER	MED	NMED
Proposed 8-bit WSAA	0.997	149.25	0.293

Table 2: Samples of input combinations that produce the proposed WSAA sum output as 1.

Input1	Input2	Actual sum	Approximate sum of WSAA
0	255	255	1
1	1	2	1
2	3	5	1
3	251	254	1
4	7	11	1
5	243	248	1
6	247	253	1
7	23	30	1
8	15	23	1
9	227	236	1
10	231	241	1

Table 3: Proof for the noncommutative property of the proposed WSAA.

Input1	Input2	Actual sum	Approximate sum of WSAA
208	75	283	91
75	208	283	196
217	5	222	52
5	217	222	127
52	29	81	134
29	52	81	141
95	128	223	87
128	95	223	224
234	246	480	71
246	234	480	131

$$\text{Input 1} + \text{Input 2} \neq \text{Input 2} + \text{Input 1}, \quad \text{for all Input 1} \neq \text{Input 2} \in S. \tag{11}$$

The above statements are justified with a few sample inputs, and it is listed in Table 3.

The proposed approximate adder's error and statistical characteristics make this adder an excellent fit for the cryptography domain.

3.3. The Proposed Encryption Scheme. The proposed scheme uses a 256-bit key for the encryption process. This huge key is not directly used for encrypting a single pixel. Rather it is to be used as a keyspace to get the 8-bit segmented key for encrypting the 8-bit pixels of the medical images. Most of the modalities used in the medical imaging are in grayscale, so the size of the key for the encryption is chosen as 8-bit. For better encryption, pixels should undergo diffusion and confusion process. In our scheme, diffusion in the pixel bits is attained by means of the WSAA and confusion of the pixel position is done by proper distribution of the segmented keys to the pixel positions in a horizontal and vertical way. The distributed segmented keys (Sk) are used for encrypting the pixels in two rounds.

Steps involved in the proposed encryption scheme are given below.

Input: Plain Medical Image

Output: Encrypted (Ciphered) Medical Image

Step 1: A 256-bit secret private key (KEY) is taken for the encryption process, and it is circularly right-shifted to a certain number of bit positions equal to its Hamming weight.

Step 2: Key segmentation and distribution for the pixels in the medical image for the first round (horizontal) is done with a row number of pixels (Rn) using the following formula:

$$m = (\text{Rn}) \text{ modulus } 32, \tag{12}$$

$$\text{Sk}_{\text{Rn}}[7{:}\ 0] = \text{KEY}[(7 + m * 8){:}\ (m * 8)]. \tag{13}$$

Step 3: Each and every pixel in the specific row number will be passed along with its segmented key to the proposed WSAA and evaluated as per equations (1)–(8). This completes the diffusion process.

Step 4: Steps 1 to 3 are to be repeated till all the pixels in the medical image is covered. Once all the pixels are covered, then move to Step 5.

Step 5: Key segmentation and distribution for the row diffused pixels in the medical image for the second round (vertical) is done with a column number of pixels (Cn) using the following formula:

$$m = (Cn)\text{modulus}32, \tag{14}$$

$$\text{Sk}_{\text{Cn}}[7{:}\ 0] = \text{KEY}[(7 + m * 8){:}\ (m * 8)]. \tag{15}$$

Step 6: Each and every row diffused pixel in the specific column number will be passed along with its segmented key to the proposed WSAA and evaluated as per equations (1)–(8). This completes the confusion process. Repeat Steps 5 and 6 until all the pixels are processed.

The process from Step 1 to 6 outputs encrypted medical image with the best entropy and poor correlation between adjacent pixels.

3.4. The Proposed Decryption Scheme. The decryption process is the reverse process of the encryption process. Steps followed in the encryption scheme are carefully reprocessed with the valid 256-bit key to gain the original medical image back at the receiver end.

Input: Encrypted (Ciphered) Medical Image

Output: Plain Medical Image

Step 1: A 256-bit secret private key (KEY) is taken for the encryption process, and it is circularly right-shifted to a certain number of bit positions equal to its Hamming weight.

Step 2: Key segmentation and distribution for the pixels in the medical image for the first round (vertical) are done with the column number of pixels (Cn) using equations (14) and (15).

Step 3: Each and every column encrypted pixel in the specific column number will be passed along with its segmented key to the proposed WSAA and evaluated as per equations (16) and (20). This solves the confusion process and restores the pixel to supply for Step 6.

$$\text{WS}_0(A) = \text{Sum}_0 \oplus B_0 \oplus 0, \tag{16}$$

$$\text{WS}_i(A) = \text{Sum}_i \oplus B_i \oplus B_{i-1}, \tag{17}$$

$$\text{Carry}_{\text{in}} = \text{Carry}_0 = 0, \tag{18}$$

$$\text{Carry}_i = B_{i-1}, \tag{19}$$

$$A = \text{circular shift}(\text{WS}(A), \text{Hamming}(\text{WS}(A))). \tag{20}$$

Step 4: Steps 1 to 3 are to be repeated until all the pixels in the medical image are covered. Once all the pixels are covered, move to Step 5.

Step 5: Key segmentation and distribution for the restored pixels of the medical image for the second round (horizontal) are done with the row number of pixels (Rn) using equations (12) and (13).

Step 6: Each and every restored pixel in the specific column number will be passed along with its segmented key to the proposed WSAA and evaluated as per equations (16)–(20). This resolves the diffusion process. Repeat Steps 5 and 6 until all the pixels are processed.

The process from Step 1 to 6 outputs decrypted medical image with the best PSNR value that matches with ideal values and makes our scheme best fit for practical applications.

4. Implementation of the Proposed Scheme

The proposed WSAA-based lightweight medical encryption and decryption scheme has been implemented and validated using MATLAB 2019b. The scheme is applied and validated for different modalities medical images such as X-ray, CT, MRI, ultrasound, and PET. One sample image for each modality is taken for the evaluation. Our proposed scheme works well irrespective of the sizes of the images. For the fair evaluation and testing, two different sizes of images (512×512) and (256×256) are taken for testing the developed scheme.

The results of the encryption and decryption process, along with its histogram, are presented in Figures 2 and 3, respectively. The histogram of the encrypted image is given to prove the ability of the proposed scheme in distributing the pixels over the wide range equally. Among the images presented in Figure 2, X-ray chest, CT chest, MRI brain, and ultrasonography fetal images are of size 512×512, and the PET brain image is of size 256×256.

5. Security Analysis

The proposed cryptosystem is validated for its basic functionality, and cryptanalysis is done against various attacks. Our proposed scheme withstands for all the types of statistical attacks. The performance against various attacks is described in this section.

5.1. Histogram Analysis. Histogram of an image indicates the frequency of pixels in the image. An attacker with the histogram of an image can be able to guess the nature and some information of the image. For our proposed scheme, the histogram analysis was made and presented in Figures 2 and 3. Figure 2 compares the histogram of the original medical image and the encrypted medical image. From the figure, it is proved that pixels have been distributed in the encrypted image uniformly to the wide range. This nature

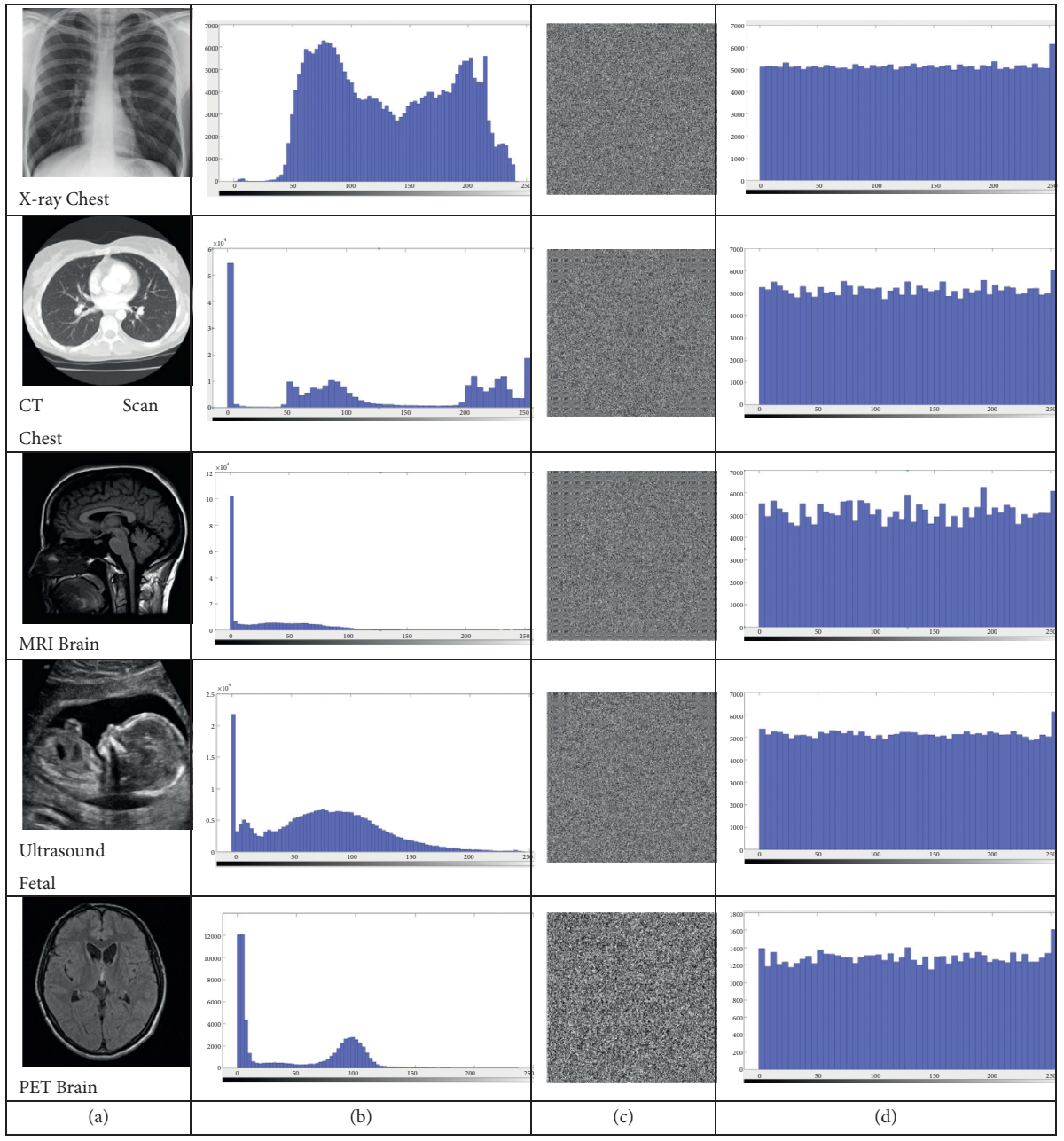

Figure 2: Implementation results of the proposed encryption scheme. From left to right column: (a) plain medical images subjected to encryption, (b) histogram of the plain medical images, (c) encrypted image of the plain images in the corresponding row, (d) histogram of the encrypted medical images.

creates a tough challenge for the attacker to gain any useful information from the encrypted image and makes statistical attack difficult.

5.2. Correlation Analysis. By nature, an adjacent pixel of any image has a close dependency with its neighbor pixels in all the direction. In fact, this property of an image only gives a smooth appearance to the image. This kind of adjacent pixel dependencies very high in the case of medical images having grayscale value, and it creates really a great challenge for the cryptosystem to overcome this and create ciphered images. These dependencies aid the attackers to regain the original image with few iterations of guessing easily. Hence, the robustness of any cryptosystem could be analyzed easily with this correlation measurement.

$$\mathrm{Cor}_{(a,b)} = \frac{\mathrm{Cov}(a.b)}{\sqrt{\sigma(a)}\sqrt{\sigma(b)}}, \tag{21}$$

where

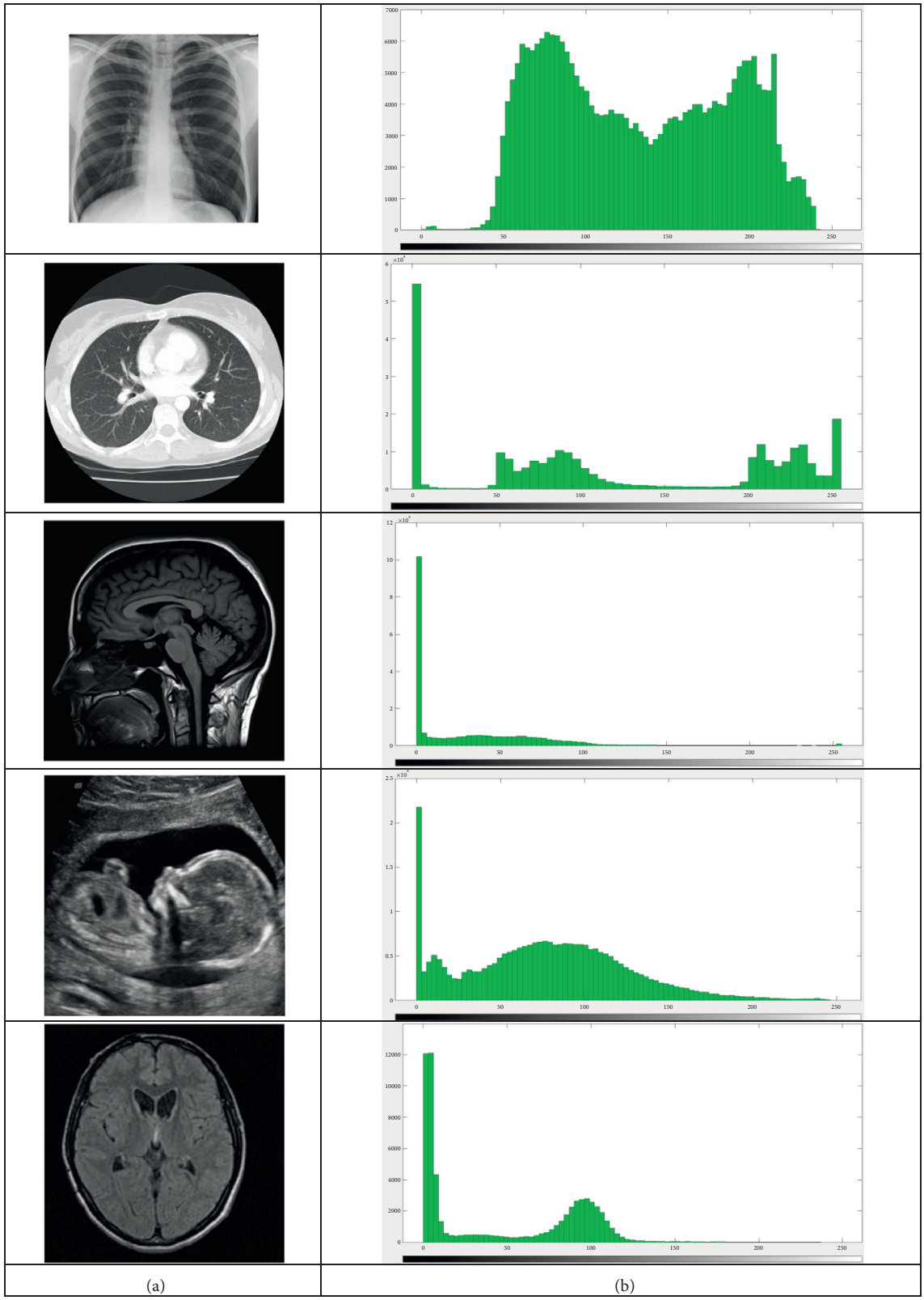

Figure 3: Implementation results of the proposed decryption scheme. (a) Decrypted medical images subjected to encryption, (b) histogram of the decrypted medical images.

$$\sigma(a) = \frac{1}{N}\sum_{i=1}^{N}\left(a_i - E(a)\right)^2,$$

$$\operatorname{cov}(a,b) = \frac{1}{N}\sum_{i=1}^{N}\left(a_i - E(a)\right)\left(b_i - E(b)\right), \quad (22)$$

$$E(a) = \frac{1}{N}\sum_{i=1}^{N} a_i.$$

In the above equation, a and b are the adjacent pixels in the plain or ciphered image and N represents the number of pixels. Adjacent pixels are taken in a horizontal, vertical, and diagonal direction, and correlation has been calculated. The measured correlations at different adjacencies for the plain and encrypted medical image sample X-ray chest image are listed in Table 1. Pixel distribution of X-ray chest image is plotted before and after encryption, and it is given in Figure 4.

From the results shown in Figure 4 and Table 4, it is evident that the proposed encryption scheme minimizes the correlation among the adjacent pixels and distributes the pixels values of all the ranges evenly throughout the image. This makes statistical analysis tough to crack the image.

5.3. Key Space Analysis. The availability of high-end complex systems with graphical processing units (GPU) supports the brute-force attack. Hence, it is required to increase the keyspace more than 2^{128} to avoid the attack. However, lightweight cryptography limits the increase of the key length up to 256-bits. In our work, we carefully handled the key length and the number of bits used for the computation. The proposed scheme uses 256-bits as a secret key to confuse the attackers, and it uses 8-bit key internally. This increases the key space of the proposed scheme to 2^{256} for a single round. The proposed system uses two rounds. Thus, the total key space enlarged to 2^{512}, which is more than enough to resist the brute-force attack.

5.4. Key Sensitivity Analysis. The robust encryption scheme needs to be very sensitive to the changes in the key values. Any minimum variations in the key need to produce a different encrypted image in the encryption process, and the minimum variations should not decrypt any portion of the image information. Our proposed scheme has been evaluated for both the conditions with a single-bit variation in the key.

Actual key K1 is 256′hF56C0062E818FFEA9F15E75DEF5EE81D-F656831C2C3E31B39C0C62BA5C51E B4

1-bit changed key K2 is 256′hF56C0062E818FFEA9F15E75DEF5EE81D-F656831C2C3E31B39C0C62BA5C51EB5

Encrypted image for different keys of 1-bit variation is shown in Figure 5. It is found that an encrypted image with key K2 is 98.458% different from the encrypted image with key K1. This proves that the proposed encryption scheme is robust in producing randomness even for single-bit variations.

Results of sensitivity analysis of the proposed scheme at the decryption side with keys K1 and K2 are presented in Figure 6. Column (a) is the decrypted image with the actual key K1. Column (b) is the decrypted image with the fake key K2 of 1-bit change. The results indicate even a single-bit change in the key is not accepted by the proposed scheme, and it is highly sensitive to the original key.

5.5. Entropy Analysis. The unpredictability of the information related to images can be measured with entropy. Entropy analysis verifies the randomness and uncertainty of the encrypted image information. Entropy information of the images is calculated using Shannon's formula [35] given in equation (23), and it is represented in a number of bits.

$$H(p) = -\sum_{i=0}^{2^N-1} P(p_i)\log_2\left(P(p_i)\right). \quad (23)$$

In the above equation, $P(p_i)$ represents the probability of the pixel (p_i) and number of bits in this is represented by N. For a grayscale image of 256 levels, an ideal value of the uniformly distributed information is $N = 8$ bits. Hence, it is always preferred to get the nearer entropy as that of the ideal case for the encrypted image. This ensures the uncertainty and randomness, and it is difficult to guess the encrypted pixel values. Deviation from this ideal value indicates the possibilities of disclosure of original information.

Measured entropy values of the plain images and encrypted sample images are listed in Table 5.

From Table 5, the entropy values of the ciphered images are very close to the ideal value 8. Since a fraction of information only available from the encrypted image, the proposed encryption scheme is secure against entropy attack.

5.6. Differential Attack Analysis. Differential attack is done to guess the key by analyzing the characteristics of the encrypted image, and this analysis corresponds to explore the strength of the encryption process against minute variations in the plain text or key [29]. Our proposed scheme is evaluated by the number of pixel change rate (NPCR) and unified average change in intensity (UACI). Analyzed values of various modalities of images are listed in Table 6.

5.7. Chosen Plain Text Attack Analysis. As the proposed encryption scheme uses xor logic gates in the adder circuits to encrypt the images, we attempted to do the chosen plain text attack to prove that our scheme is versatile and it is not revealing any information about the original image. The chosen plain text attack [29] is performed by following the equation

$$E_1(x,y) \oplus E_2(x,y) = I_1(x,y) \oplus I_2(x,y), \quad (24)$$

where I_1, I_2 are two plain images and E_1, E_2 are encrypted images of I_1, I_2, respectively. In the above equation, if the

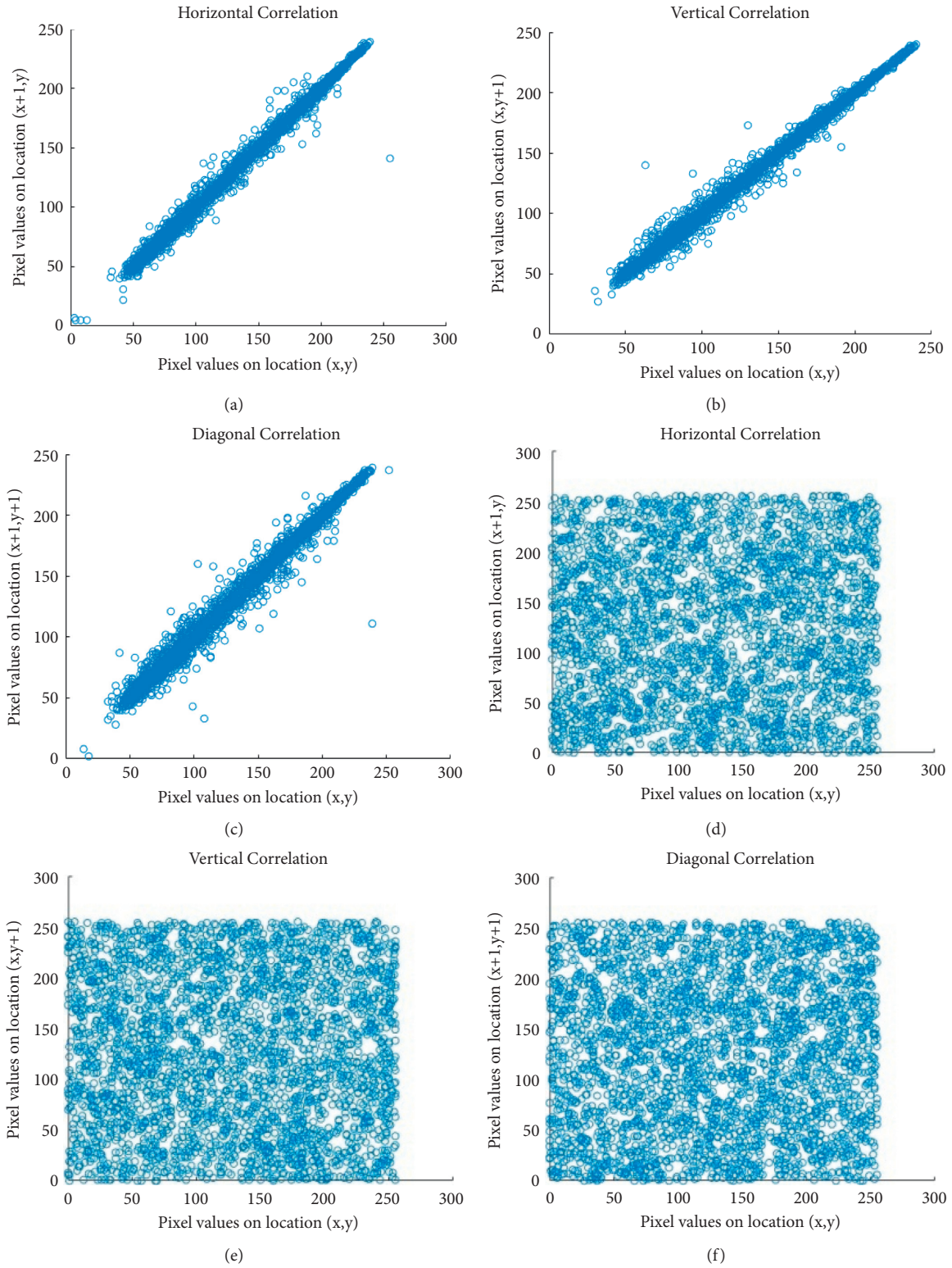

Figure 4: Correlation analysis results and plot of pixel distribution in the X-ray chest image sample. Pixel distributions plots are from left to right. For the plain image, (a) horizontal distribution, (b) vertical distribution, (c) diagonal distribution. Pixel distribution of encrypted image, (d) horizontal, (e) vertical, and (f) diagonal distributions.

statement is equal, then that encryption scheme is subjected to chosen plain text attack. Our encryption scheme successfully passed this analysis and produced unequal results.

5.8. PSNR Analysis and Comparison with Existing Works. This section presents the comparison of the peak signal-to-noise ratio of the decrypted image with the plain image.

Table 4: Correlation coefficients of different modality medical images.

Sample medical image	Horizontal		Vertical		Diagonal	
	Plain image	Ciphered image	Plain image	Ciphered image	Plain image	Ciphered image
X-ray chest	0.9965	−0.2898	0.9963	−0.0205	0.9928	−0.0109
CT scan chest	0.9943	−0.0570	0.9895	−0.0073	0.9873	0.0168
MRI brain	0.9777	−0.1135	0.9833	0.0156	0.9581	0.0219
Ultrasound fetal	0.9938	−0.0279	0.9863	−0.0122	0.9809	−0.0049
PET brain	0.9674	−0.0766	0.9768	0.0316	0.9426	0.0194

(a) (b) (c)

Figure 5: Key sensitivity test for single-bit variations in the key at encryption. (a) Plain X-ray chest image. (b) Encrypted image for actual key K1. (c) Encrypted image for 1-bit changed key K2.

Decrypted image and its histogram are shown in Figure 3. By comparing Figures 2 and 3, we can come to the conclusion that the decrypted image and its histogram exactly match the plain image and its histogram. This proves that no internal noises added during the encryption process. The PSNR value of the proposed scheme is calculated, and it is equal to the ideal value infinity. The PSNR value of the proposed work is compared with the average PSNR values of the existing works, and it is listed in Table 7.

6. Hardware Implementation

The proposed encryption scheme is implemented in a Field Programmable Gate Array (FPGA) to evaluate its lightweight and high-speed computation against various similar works in the literature. The proposed encryption architecture is deployed in verilog HDL as an encoder of block size 256-bit. Here, single block 32-pixels are to be encrypted in parallel by scheduling the 8-bit key for each pixel from the 256-bit key. The proposed encryption architecture is simulated and synthesized in Xilinx ISE 14.7 for the XC5VLX330T-2 FPGA. The resource utilization and performance factors in comparison with existing lightweight encryption schemes are listed in Table 8.

From the above table, it is evident that the proposed WSAA encryption scheme has 112% higher throughput per area and occupies moderate area (LUT) compared to LEA-256 and utilizes 5.2% and 23.61% less area compared to LEA-192 and LEA-256, respectively. This proves that the proposed WSAA scheme is a lightweight and high-speed encryption scheme.

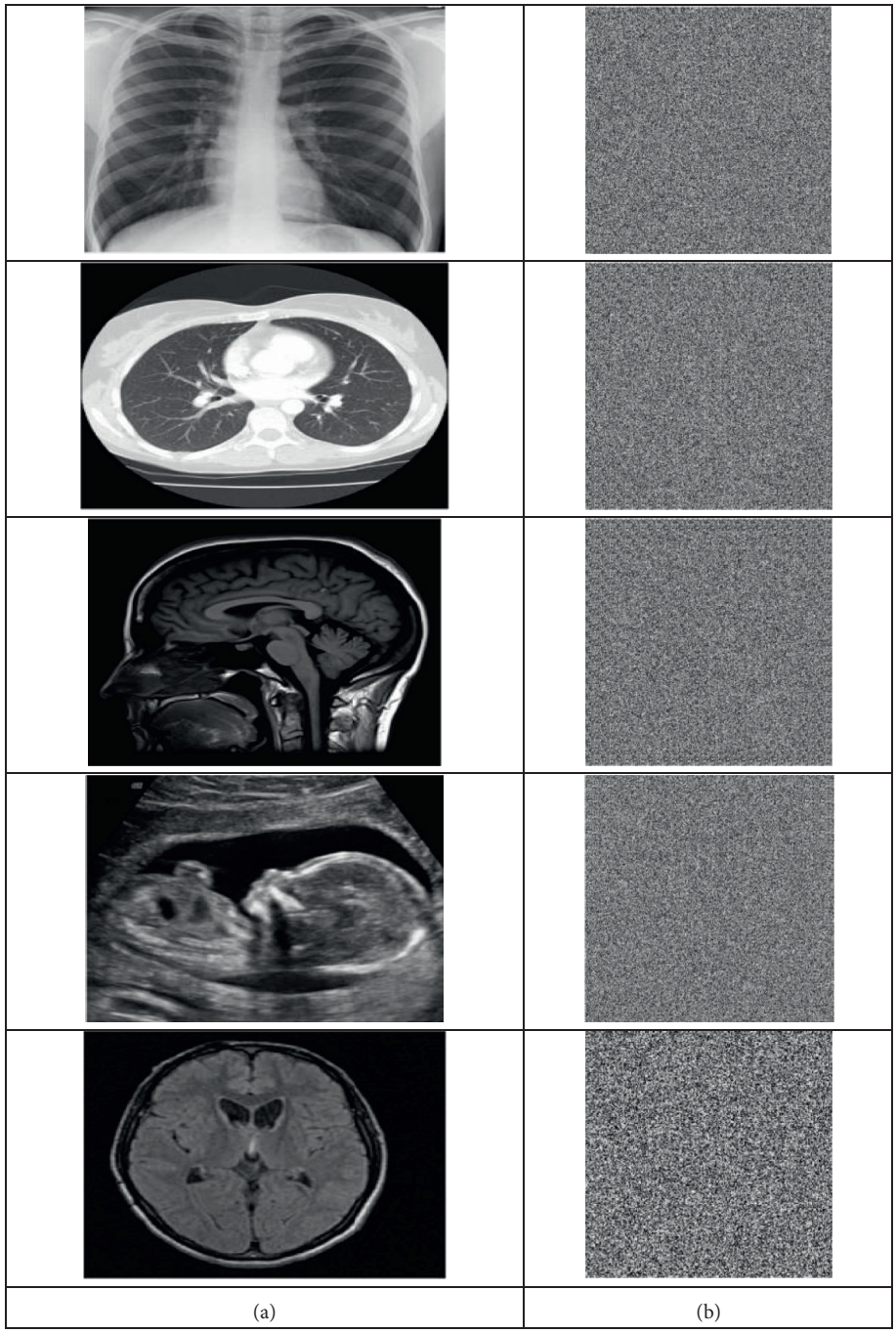

Figure 6: Key sensitivity test for single-bit variations in the key at decryption. (a) Decrypted image with actual key K1. (b) Decrypted image with 1-bit variation key K2.

Table 5: Measured entropy values of sample images before and after encryption.

Modality	Sample image	Size	Entropy	
			Plain image	Encrypted image
X-ray	Chest	512 × 512	7.5509	7.9913
CT scan	Chest	512 × 512	6.4985	7.9838
MRI	Brain	512 × 512	5.4162	7.9687
Ultrasound	Fetal	512 × 512	7.2543	7.9899
PET	Brain	256 × 256	5.9094	7.9850

Table 6: Measured entropy values of sample images before and after encryption.

Modality	Sample image	Size	NPCR (%)	UACI (%)
X-ray	Chest	512 × 512	99.615	33.653
CT scan	Chest	512 × 512	99.258	33.374
MRI	Brain	512 × 512	98.995	33.391
Ultrasound	Fetal	512 × 512	99.579	33.521
PET	Brain	256 × 256	99.571	33.518

Table 7: Comparison of average PSNR values of the decrypted image.

Scheme	Proposed	[9]	[15]
PSNR (in dB)	∞	78.35	36.78

Table 8: Comparison of FPGA implementation results of the proposed WSAA with other lightweight schemes.

Algorithm	Block size	Device name	LUT's	FFs	Slices	Cycle	Max. Frequency (MHz)	Throughput (Mbps)	Throughput per area
LEA-128 [36]	128	XC5VLX330T	713	386	—	24	217.806	1161.6	0.198
LEA-192 [36]	128	XC5VLX330T	911	508	—	28	218.250	996.57	0.153
LEA-256 [36]	128	XC5VLX330T	1131	645	—	32	126.23	505	0.071
Unified (sel-2'b0) [37]	128	XC5VLX330T	735	832	273	33	292	1152	0.186
LEA-256 [37]	256	XC5VLX330T	440	812	250	33	340	1367	1.092
Proposed WSAA	256	XC5VLX330T	864	864	437	32	500.25	4002	2.316

7. Conclusion

The technological advancement and the present scenario mandate the remote diagnosis and secure transmission of medical information in the form of an image over the Internet from the data centre to another or from patient to doctors. The disturbances and attacks on the medical images are non-tolerable. This work proposed a unique approximate adder-based lightweight encryption and decryption scheme which tolerates to various adversarial attacks. The lightness of the scheme is featured by the proposed novel random error weighted shift approximate adder. The inheritance of the key distribution and rounding scheme within the image pixels contribute to the robustness of the proposed scheme against various attacks. The proposed scheme is implemented and tested for different modalities of medical images such as X-ray, CT, MRI, ultrasound, and PET. The implemented system is analyzed for the histogram, correlation, entropy, and key sensitivity. The developed scheme defies the statistical attacks and able to produce infinite PSNR at the decryption stage. It satisfies the ideal condition for any medical transmission system. Thus, our proposed lightweight approximate adder-based encryption and decryption scheme is the best fit for real-time secure remote monitoring of medical data.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, 2017.

[2] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Optics and Lasers in Engineering*, vol. 110, no. October 2017, pp. 24–32, 2018.

[3] R. Thanki and S. Borra, *Medical Imaging and its Security in Telemedicine Applications*, Springer International Publishing, Berlin/Heidelberg, Germany, 2019.

[4] R. Tadeusiewicz and M. R. Ogiela, *Medical Image Understanding Technology*, pp. 470–479, Springer, Berlin/Heidelberg, Germany, 2004.

[5] A. B. Wolbarst and W. R. Hendee, "Evolving and experimental technologies in medical imaging," *Radiology*, vol. 238, no. 1, pp. 16–39, 2006.

[6] S. R. Cherry, "Multimodality imaging: beyond PET/CT and SPECT/CT," *Seminars in Nuclear Medicine*, vol. 39, no. 5, pp. 348–353, 2009.

[7] A. Mahmood, T. Hamed, C. Obimbo, and R. Dony, "Improving the security of the medical images," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 9, pp. 137–146, 2013.

[8] I. Jasmine Selvakumari Jeya and J. Suganthi, "RONI based secured and authenticated indexing of lung CT images," *Computational and Mathematical Methods in Medicine*, vol. 2015, pp. 1–9, 2015.

[9] I. B. Venkateswarlu, "Fast medical image security using color channel encryption," *Brazilian Archives of Biology and Technology*, vol. 63, pp. 1–8, 2020.

[10] A. Sivaprakash, S. N. E. Rajan, and S. Selvaperumal, "Privacy protection of patient medical images using digital watermarking technique for E-healthcare system," *Current Medical Imaging Formerly Current Medical Imaging Reviews*, vol. 15, no. 8, pp. 802–809, 2019.

[11] A. Umamageswari and G. R. Suresh, "Security in medical image communication with arnold's cat map method and reversible watermarking," in *Proceedings of the IEEE International Conference on Circuit, Power and Computing Technologies, ICCPCT*, pp. 1116–1121, Nagercoil, India, March 2013.

[12] K. N. Madhusudhan and P. Sakthivel, "A secure medical image transmission algorithm based on binary bits and Arnold map," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 5, pp. 5413–5420, 2020.

[13] J. Zhang, D. Hou, and H. Ren, "Image encryption algorithm based on dynamic DNA coding and chen's hyperchaotic system," *Mathematical Problems in Engineering*, vol. 2016, pp. 1–11, 2016.

[14] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on Latin square and memristive chaotic system," *Multimedia Tools and Applications*, vol. 78, no. 24, pp. 35419–35453, 2019.

[15] L. B. Zhang, Z. L. Zhu, B. Q. Yang, W. Y. Liu, H. F. Zhu, and M. Y. Zou, "Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach," *Mathematical Problems in Engineering*, vol. 2015, pp. 1–9, 2015.

[16] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.

[17] K. Tamilarasi and A. Jawahar, "Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm," *Wireless Personal Communications*, vol. 114, no. 3, pp. 1865–1886, 2020.

[18] M. Benssalah, Y. Rhaskali, and K. Drouiche, "An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2081–2107, 2020.

[19] A. Vizitiu, C. I. Niă, A. Puiu, S. Constantin, and L. M. Itu, "Applying deep neural networks over homomorphic encrypted medical data," *Computational and Mathematical Methods in Medicine*, vol. 2020, pp. 1–26, 2020.

[20] Z. Chen, "A lightweight encryption algorithm for images," *Advances in Intelligent and Soft Computing*, vol. 137 AISC, pp. 235–241, 2012.

[21] J. Kumar and S. Nirmala, "A new light weight encryption approach to secure the contents of image," in *Proceedings of the 2014 International Conference on Advances in Computing, Communications and Informatics, ICACCI*, pp. 1309–1315, Delhi, India, September 2014.

[22] B. Mondal and T. Mandal, "A light weight secure image encryption scheme based on chaos & DNA computing," *Journal of King Saud University - Computer and Information Sciences*, vol. 29, no. 4, pp. 499–504, 2017.

[23] A. Javeed, T. Shah, and A. Attaullah, "Lightweight secure image encryption scheme based on chaotic differential equation," *Chinese Journal of Physics*, vol. 66, no. July 2019, pp. 645–659, 2020.

[24] I. T. Almalkawi, R. Halloush, A. Alsarhan, A. Al-Dubai, and J. N. Al-karaki, "A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications," *Journal of Information Security and Applications*, vol. 49, p. 102384, 2019.

[25] O. A. Khashan and M. AlShaikh, "Edge-based lightweight selective encryption scheme for digital medical images," *Multimedia Tools and Applications*, vol. 79, no. 35-36, pp. 26369–26388, 2020.

[26] S. Mortajez, M. Tahmasbi, J. Zarei, and A. Jamshidnezhad, "A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images," *Informatics in Medicine Unlocked*, vol. 20, no. May, Article ID 100396, 2020.

[27] T. Belkhouja, A. Mohamed, K. Abdulla, A. Ali, X. Du, and M. Guizani, "Lightweight encryption of wireless communication for implantable medical devices using Henon chaotic system," in *Proceedings of the 2017 International Conference on Wireless Networks and Mobile Communications, WINCOM*, Rabat, Morocco, November 2017.

[28] A. A. Abd El-Latif, B. Abd-El-Atty, M. S. Hossain et al., "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018.

[29] D. Ravichandran, S. Rajagopalan, H. N. Upadhyay et al., "Encrypted biography of biomedical image - a pentalayer cryptosystem on FPGA," *Journal of Signal Processing Systems*, vol. 91, no. 5, pp. 475–501, 2019.

[30] 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, no. 22, pp. 31485–31513, 2019.

[31] V. Manikandan and R. Amirtharajan, "On dual encryption with RC6 and combined logistic tent map for grayscale and DICOM," *Multimedia Tools and Applications*, vol. 80, pp. 1–30, 2021.

[32] A. Mubashar, K. Asghar, A. R. Javed et al., "Storage and proximity management for centralized personal health records using an ipfs-based optimization algorithm," *Journal of Circuits, Systems, and Computers*, p. 2250010, 2021.

[33] M. Nagarajan, A. Sasikumar, D. Muralidharan, and M. Rajappa, "Fixed point multi-bit approximate adder based convolutional neural network accelerator for digit classification inference," *Journal of Intelligent and Fuzzy Systems*, vol. 39, no. 6, pp. 8521–8528, 2020.

[34] R. Jothin, M. P. Mohamed, and C. Vasanthanayaki, "High performance compact energy efficient error tolerant adders and multipliers for 16-bit image processing applications," *Microprocessors and Microsystems*, vol. 78, Article ID 103237, 2020.

[35] X. Hu, C. Jin, M. Alazab et al., "On the design of blockchain-based ECDSA with fault-tolerant batch verication protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, 2021.

[36] D. Lee, D.-C. Kim, D. Kwon, and H. Kim, "Efficient hardware implementation of the lightweight block encryption algorithm LEA," *Sensors*, vol. 14, no. 1, pp. 975–994, 2014.

[37] Z. Mishra, P. K. Nath, and B. Acharya, "High throughput unified architecture of LEA algorithm for image encryption," *Microprocessors and Microsystems*, vol. 78, Article ID 103214, 2020.