Hindawi
Scientific Programming
Volume 2021, Article ID 6610655, 20 pages
https://doi.org/10.1155/2021/6610655

Research Article

FPGA Implementation of Improved Security Approach for Medical Image Encryption and Decryption

Amal Hafsa,[1] **Mohamed Gafsi**,[1] **Jihene Malek**,[1,2] **and Mohsen Machhout**[1]

[1]*Electronic and Micro-Electronic Laboratory, LR99ES30, Faculty of Sciences, University of Monastir, Monastir, Tunisia*
[2]*Higher Institute of Applied Sciences and Technology, Sousse University, Sousse, Tunisia*

Correspondence should be addressed to Amal Hafsa; hafsaamal12@gmail.com

Received 7 November 2020; Revised 2 January 2021; Accepted 20 January 2021; Published 8 February 2021

Academic Editor: Autilia Vitiello

Securing medical images is a great challenge to protect medical privacy. An image encryption model founded on a complex chaos-based Pseudorandom Number Generator (PRNG) and Modified Advanced Encryption Standard (MAES) is put forward in this paper. Our work consists of the following three main points. First, we propose the use of a complex PRNG based on two different chaotic systems which are the 2D Logistic map in a complex set and Henon's system in the key generation procedure. Second, in the MAES 128 bits, the subbytes' operation is performed using four different S-boxes for more complexity. Third, both shift-rows' and mix-columns' transformations are eliminated and replaced with a random permutation method which increases the complexity. More importantly, only four rounds of encryption are performed in a loop that reduces significantly the execution time. The overall system is implemented on the Altera Cyclone III board, which is completed with an SD card interface for medical image storage and a VGA interface for image display. The HPS software runs on μClinux and is used to control the FPGA encryption-decryption algorithm and image transmission. Experimental findings prove that the propounded map used has a keyspace sufficiently large and the proposed image encryption algorithm augments the entropy of the ciphered image compared to the AES standard and reduces the complexity time by 97%. The power consumption of the system is 136.87 mw and the throughput is 1.34 Gbit/s. The proposed technique is compared to recent image cryptosystems including hardware performances and different security analysis properties, such as randomness, sensitivity, and correlation of the encrypted images and results prove that our cryptographic algorithm is faster, more efficient, and can resist any kind of attacks.

1. Introduction

Currently, the fast growth of the Internet makes Electronic Healthcare (e-healthcare) feasible and popular. E-Healthcare refers to an internet-based system where the patient can contact an expert doctor for the diagnostic. Some medical images are stored and transmitted over the Internet. These images may contain much privacy of patients and are very confidential and sensitive. Therefore, the best significant way to protect this privacy issue is data encryption. Medical images have some characteristics, such as redundancy, big data volume, and great pixel correlation, compared to the normal images [1]. Medical image encryption algorithms require not only great security but also fast encryption speed. The Advanced Encryption Standard (AES) has been designed for different applications. However, it is inappropriate for securing large medical images. Thus, it is necessary to improve the AES making it suitable to secure medical images against attacks. A random number generator is used to generate a sequence of random numbers for encryption. When the generated number is more random, the encryption effect is better. Chaos systems are used in the designing of the Pseudorandom Number Generator (PRNG) to generate good keys for encryption. This technique has several significant advantages against other generators, such as the true random number generator (TRNG) and the Linear Feedback Shift Register (LFSR), It is very sensitive to initial conditions, characterised by a, long periodicity, and provides large keyspace. Thus, combining a chaotic system and improved AES can provide great performances in terms

of security and run time. Beyond algorithm strictness, an efficient implementation technique of one cryptosystem is required. In a software implementation, an algorithm is executed in a sequential way. This technique is not sufficient to provide good performance enough in real-time applications. In addition, the algorithm is vulnerable to software attacks. However, the hardware implementation is required to get good performance enough and protection against attacks from running an algorithm [2]. Increasing system performance is based on two basic concepts: increasing the processor clock frequency and using specific processors. In the hardware implementation, we have two choices: an ASIC and an FPGA. The first choice is the most expensive. The second choice is a promising solution. FPGAs allow the designer to create a custom circuit implementation of an algorithm using a standard component made up of basic programmable logic elements. An FPGA offers significant cost advantages over an ASIC development effort and offers the same level of performance in most cases. Another advantage of the FPGA against IC is its ability to be dynamically reconfigured. Based on a NIOS II softcore processor and a cyclone III FPGA, a strong prototype platform for medical image processing is designed in our work. The aim of this paper is to design a real-time medical image encryption system based on a strong cryptographic model with the image input from an SD card interface and an output to a VGA interface. We propose a chaotic encryption algorithm combined with high-dimensional chaotic mapping and improved confusion and diffusion of MAES and implemented on SoPC FPGA. We focus to gain an overall great performance and a high level of security.

In history, medical image encryption models have been reported. Laiphrakpam and Khumanthem [3] suggested the use of ElGamal encryption algorithm to encrypt medical images. In this paper, the data expansion problem was resolved. However, the use of an asymmetric algorithm to encrypt images was highly time-consuming. In 2018, Elhoseny et al. [4] propounded a hybrid encryption scheme that mixed both AES and Rivest–Shamir–Adleman (RSA) calculations. The cryptosystem started by encoding the mystery data; at that point, it concealed the outcome in a cover image employing 2D-DWT-1L or 2D-DWT-2L. Both shading and dark scale images were employed as cover images to disguise diverse content sizes. While the level of security was improved, the use of two cryptographic algorithms could increase the run time for image processing and could cause delays during transmission. Zhang et al. [5] proposed an image encryption system based on the combination of the AES-128 and the Cipher Block Chaining mode (CBC) standards. For this, the plain image was fragmented into subblocks sized 128 bit. After that, an initial vector, named IV with a size equal to 128 bit was generated by the Tent chaotic map and XORed with the initial plain subblock. Secondly, the AES-128 was applied to obtain the first ciphered subblock. Finally, the rest of the different subblocks were scripted sequentially following the same steps applied on the first one block. According to the results presented in [5], we notice that the encryption systems based on the existing AES algorithm caused a long execution time because of the multiple iterations, and it was not secure enough to protect image privacy because of predefined procedures. This disadvantage affected directly the global quality of the system in the case of online encryption. In the other case, the use of the CBC mode has many disadvantages such as its sequential architecture, which could cause a slowdown in encryption systems. Another disadvantage of the CBC standard was the propagation of an error may occur easily and could affect all blocks. Toughi et al. [6] used the Elliptic Curve Cryptography (ECC) operations as an initial number generator and proposed the encryption via a standard AES to create a novel pseudorandom to mask all pixels. However, the use of a sequential way to encrypt the image augmented the time complexity. Chaos-based encryption has been suggested as an efficient way to deal with the intractable issue of rapid and secure images. This is due to many strengths of chaos such as the deterministic pseudorandom number generation (PRNG), the long periodicity, the sensitivity to the initial conditions, and the large keyspace. Hu et al. [7] suggested an ameliorated cryptographic system based on chaotic map and Latin square. The parameter of the chaotic system was calculated by the original image. However, the keyspace was less than 2^{100}. Authors in [8] proposed cooperation between ECC and a chaotic system. In this paper, authors utilized cyclic elliptic curves with LFSR and a chaos system for the keystream sequences' generation. Then, image encryption was performed using the key streams. The suggested method was vulnerable to the Chosen Plain Text Attacks (CPA) [9]. Yu et al. [10] suggested an image cryptosystem based on a combination between the 3D orthogonal Latin squares (3D-OLSs) and a matching matrix. Firstly, the 3D sine map was used to generate three chaotic sequences. Next, a 3D orthogonal Latin square and a matching matrix were produced by using the chaotic sequences. Then, the 3D-OLSs and the matching matrix were jointly used to permute the original image. After that, all planes of the permuted matrix were divided into sixteen blocks of the same size. The chaotic sequence was sorted and a position matrix was generated. According to the position matrix, the blocks of each plane were linked and shifted by using a cyclic shift operation; then, a new matrix was generated. Finally, the encrypted image was generated by executing a diffusion operation for the new matrix. Xiuli et al. [11] proposed a medical image encryption model that combined Latin square and a chaotic system. Ben Sliman et al. [12] suggested an efficient technique to generate a novel chaotic system using the amalgamation between the Logistic map in a complex set, Julia's fractal process, and chaotic attractors. The Lyapunov exponents were calculated to demonstrate the chaotic state of the new behaviour. This approach, using the fractal process and Logistic map with chaotic attractors, could facilely be implemented and simulated. Then, they suggested a secure cryptosystem for image encryption based on the proposed chaotic system. The algorithm contained the Shannon principle of confusion and diffusion.

A new image encryption algorithm based on DNA sequence operations, Single Neuron Model (SNM), and chaotic map was proposed in [13]. A 512 bit hash value dependent to the original image was proposed for initial conditions; then, a confusion-diffusion was adopted as an architecture of the cryptosystem. The 2D Logistic-adjusted-Sine map (2D-LASM) was used to confuse the pixels of color components simultaneously, while SNM was utilized to create the keystream; otherwise, the hash value of the clear image was injected additionally in the diffusion procedure.

Ben Sliman et al. [14] suggested an image encryption model based on the 2D Logistic map in a complex set and nonuniform cellular automata using the secure hash algorithm SHA-2. The proposed algorithm adopted confusion-diffusion as architecture. An efficient image encryption scheme based on the nested chaotic map and deoxyribonucleic acid (DNA) was proposed in [15]. In this paper, the secure hash algorithm SHA-256 was used for the initial condition values' generation of the nested chaotic system. The cryptosystem consisted of two main layers: confusion and diffusion. In the first layer, the nested chaotic map was used to create a scrambled image. The scrambled image was obtained via the ascending sorting of the first component of the nested chaotic index sequence. For a high level of sensitivity, complexity, and security, DNA sequence and DNA operator were used additionally with the nested chaotic map and hash algorithm to modify the pixels values. Results showed improvement of NPCR, UACI, and entropy. Elgendy et al. [16] suggested an image encryption algorithm based on two-dimensional (2D) chaotic maps, including a standard map, baker map, and cat map. Findings showed a reduction in execution time, but the results of security analysis, such as correlation, entropies, and differential attacks, were not ideal values compared to other propounded models.

Our work makes the following contributions:

(1) Designing a complex chaos-based PRNG with the goal to generate high-quality encryption keys.

(2) Designing an improved cryptosystem for medical images encryption and decryption, which combines the complex PRNG and a modified AES (MAES), where the subbytes' operation is performed using four different s-boxes generated by the chaotic system. Then, both shift-rows and mix-columns are eliminated and replaced with a random permutation method. This increases the complexity of the system. Finally, only four rounds of encryption are performed in a loop that reduces significantly the execution time.

(3) Designing a strong prototype platform for secure medical images based on the NIOS II processor and FPGA.

(4) Undertaking in-depth experimental measurements in FPGA for several medical images with different types, contents, and sizes to evaluate the strength of the proposed cryptosystem against the new generation of attacks. In [17, 18], a scheme is proposed to verify the randomness of the image, named "Shannon's local entropy." We employ the Shannon local entropy analysis to validate the suggested method [19, 20].

(5) Undertaking in-depth evaluation study of the performance of the execution and comparing the results with other recent works.

This paper is structured as follows. Section 2 presents the designed complex chaotic system and the proposed image cryptosystem algorithm. Section 3 describes the implementation of the medical image encryption system on the FPGA followed by experimental results. Security analysis and evaluation are detailed in Section 4, and finally, Section 5 concludes the paper and recommends some future works.

2. Cryptosystem Design

In this section, we introduce the designed image cryptosystem based on MAES and chaos-key generator. The general view of the proposed image cryptosystem architecture is depicted in Figure 1. We firstly describe the chaos-based PRNG for the key generation, which is composed of two different chaotic systems: the Logistic map in a complex set (2D) and Henon's map (2D). Secondly, the MAES is clearly detailed.

2.1. Pseudorandom Number Generator. PRNGs are used to generate keys useful for encryption. Chaotic systems are an effective solution for good key generation. Chaos systems are very sensitive to the initial condition and have long periodicity, good entropy, and good statistical behaviour of randomness [21–25]. In the literature, several chaotic systems have been investigated for key generation. In our work, we have selected to use Henon's map and 2D Logistic map in the complex set since they have good chaotic behaviour [13, 21, 22].

Henon's map is defined by equation (1). The system has a state of two variables (X, Y) and two parameters a and b. It is under chaotic behaviour when $a = 1.4$ and $b = 0.3$ [28–30]. n represents the number of iteration. The initial state (x_0, y_0) of Henon's map is derived from the initial key ki:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n, \\ y_{n+1} = bx_n. \end{cases} \tag{1}$$

The 2D Logistic map in the complex set is defined by equation (2). The system has a state of two variables (x, y) and one parameter λ. For $\lambda \epsilon [0, 4]$, the system is under chaotic behaviour. The initial state (Xl, Yl) of the 2D Logistic map is derived from the initial key ki:

$$\begin{cases} x_{i+1} = yx_i(1 - x_n) + \lambda y_i^2, \\ y_{i+1} = \lambda y_i(1 - 2x_i). \end{cases} \tag{2}$$

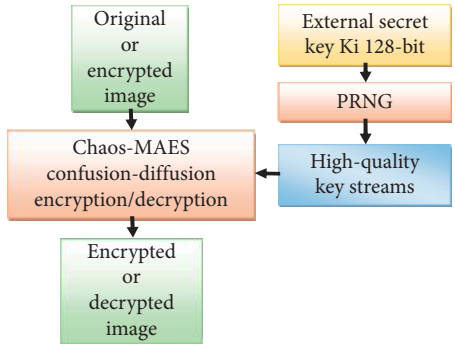


Figure 1: General view of the proposed cryptosystem architecture.

To generate high-quality keys, a complex architecture of PRNG is proposed which employs both Henon's map and 2D Logistic map in the complex set. The general architecture is depicted in Figure 2. It includes three data processing blocks: an Initial State Generator (ISG), a Complex Chaotic Design (CCD), and a Convertor block. The overall system has one input and one output each sized 128 bit, and it involves a state of four variables (Xh, Yh, Xl, Yl).

The ISG is employed to generate implicitly an initial state (Xh_0, Yh_0, Xl_0, Yl_0) for the chaotic system from its 128 bit initial secret key input. For that, the initial key ki is divided into 8 bit blocks as in equation (3). Therefore, the variables of the initial state ($Xh0$, $Yh0$, $Xl0$, $Yl0$) are computed separately using equations (4)–(7):

$$Ki = k_1|k_2|k_3|,\ldots,|k_{32}, \tag{3}$$

$$Xh_0 = \frac{(k_1 \oplus k_2 \oplus \cdots \oplus k_8)}{2^8}, \tag{4}$$

$$Yh_0 = \frac{(k_9 \oplus k_7 \oplus \cdots \oplus k_{16})}{2^8}, \tag{5}$$

$$Xl_0 = \frac{(k_{17} \oplus k_{12} \oplus \cdots \oplus k_{24})}{2^8}, \tag{6}$$

$$Yl_0 = \frac{(k_{25} \oplus k_{17} \oplus \cdots \oplus k_{32})}{2^8}. \tag{7}$$

The use of the same initial key permits obtaining the same random number sequence always. The converter block is employed to convert the underlying state of the chaotic design into 32 bit numbers suitable for encryption equations (8)–(11). Therefore, a sequence of 128 bit random numbers' PRNS is obtained which presents high statistical behaviour of randomness (equation (12)):

$$XH = \left(Xh_i \times 10^{12}\right) \bmod 2^{32}, \tag{8}$$

$$YH = \left(Yh_i \times 10^{12}\right) \bmod 2^{32}, \tag{9}$$

$$XL = \left(Xl_i \times 10^{12}\right) \bmod 2^{32}, \tag{10}$$

$$YL = \left(Yl_i \times 10^{12}\right) \bmod 2^{32}, \tag{11}$$

$$\text{PRNS} = \text{Concat}(YH, XL, YL, XH). \tag{12}$$

2.2. Modified AES. The AES is one of the most known encryption algorithms for data protection. Invented in 1998 by Joan Daemen and Vincent Rijmen and proved in 2000 by the NIST, the AES has been widely deployed, thanks to its high performance. It involves key sizes and block sizes. The size of the information block is 128 bits, and the length of the key can be 128, 192, or 256 bits [23]. The repetitions and size of the key determine the complexity of the algorithm. A higher repetition or an elevated key size provokes higher CPU usage and complexity. For 128 bits key, about 2^{128} attempts are needed to crack, but it is not appropriate in multimedia data because multimedia information is characterized by great redundancy. Thus, only utilizing the existing AES cryptosystem cannot attain good quality of encryption. To solve the issue of the AES encrypted images, we mix the features of a 4D chaotic system for good key generation and improvement in confusion and diffusion in the AES. Our method augments the complexity of encryption and enhances the security level.

Figure 3 depicts the flowchart of the image encryption algorithm using MAES and the proposed chaotic key generator. The decryption cryptosystem is the reverse procedure of the encryption algorithm.

For the encryption operation, we need 4 rounds. Each round transformation is performed as a set of iterations, which includes the subbytes' operation using four different S-boxes, a random permutation, and an add-round key operation.

(1)Process 1 (subbytes): consists of replacing each byte of the state matrix with another value. The substitution S-box guarantees Shannon's principle of confusion. Four different S-boxes:S-box1, S-box 2, S-box 3, and S-box 4, are used for the substitution that increases the complexity of the algorithm.

(2) Process 2 (random permutation): block's pixels are randomly permuted using two predefined methods. It guarantees the Shannon diffusion principle. Figure 4 illustrates the process of the random permutation. The condition of the parity of block position has been adopted which permits using the permutation method 1 or method 2:

(a) If the position of the block is odd, then, the block's pixels are permuted using method 1
(b) If the position of the block is even, then, the block's pixels are permuted using method 2

(3) Process 3 (add-round key): each byte in the matrix uses Xor to manipulate the round key. A subkey is obtained from the main PRNG. It guarantees the Shannon diffusion principle.

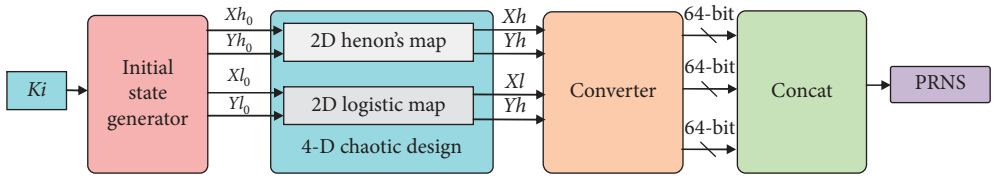


Figure 2: General view of the proposed PRNG.

3. FPGA Implementation

3.1. System Design Hardware Implementation. In this paper, the FPGA-based NEEK development board including Cyclone III (Altera) is required. The suggested System on Programmable Chip (SoPC) includes the NIOS II processor which is a 32 bit embedded processor specialized for the Altera family of FPGAs, internal memory controllers, a timer to perform the run time, a JTAG UART for the debug, and IPs for image storing and displaying which are, respectively, the SD card and the VGA monitor. The principal processing core of the embedded image system is the NIOS II processor. With the help of Qsys (System Integration tool of Quartus II), the CPU is connected with all modules via an Avalon bus, as depicted in Figure 5. Both SD card and VGA interfaces are connected to the processor, and the SRAM memory and remaining IPs' hardware are interfaced via the bus. The transmission of information between the SD card, VGA interface, and SRAM can be done by using the processor. The three required components are clearly described in this section.

3.1.1. NIOS II Processor. In this work, the FAST version of the CPU is used. It is a 32 bits scalar RISC architecture [24]. The extensibility, flexibility, and adaptability constitute the significant things, to be interested in, for this CPU. The NIOS II design is depicted in Figure 6.

3.1.2. SDI/O Card Interface. The SD card is portable which permits the information stored to be transmitted to other devices. The Altera board has SD card ports. It permits the SD card to be connected to the FPGA. The SD card FPGA is designed as a hardware IP with the use of the Qsys-implemented system. The overall system contains the NIOS II CPU and other modules. Information stored in the SD card can be processed by simple programs executed on NIOS II CPU. As depicted in Figure 7, the SD card interface is composed in the following blocks:

(1)SD Control block: it assures the transmission of the image to the FIFO (First-in First-out) with 32 bits data path. In fact, with the aim of employing the Avalon bus size totality (32 bit), every four bytes are treated at 32 bits words.

(2) FIFO module: it assures the memorization of the image line. It is considered as a buffer between both data writing and reading. Writing in the FIFO module is synchronized with the SD clock, while reading is synchronized with the clock of the overall system (50 MHz). In fact, reading data must be very rapid.

(3) DMA (direct memory access) module: it assures the data transmission from the FIFO to the SRAM by sending signals. The SD interface sends the image information and signals of control via the bus.

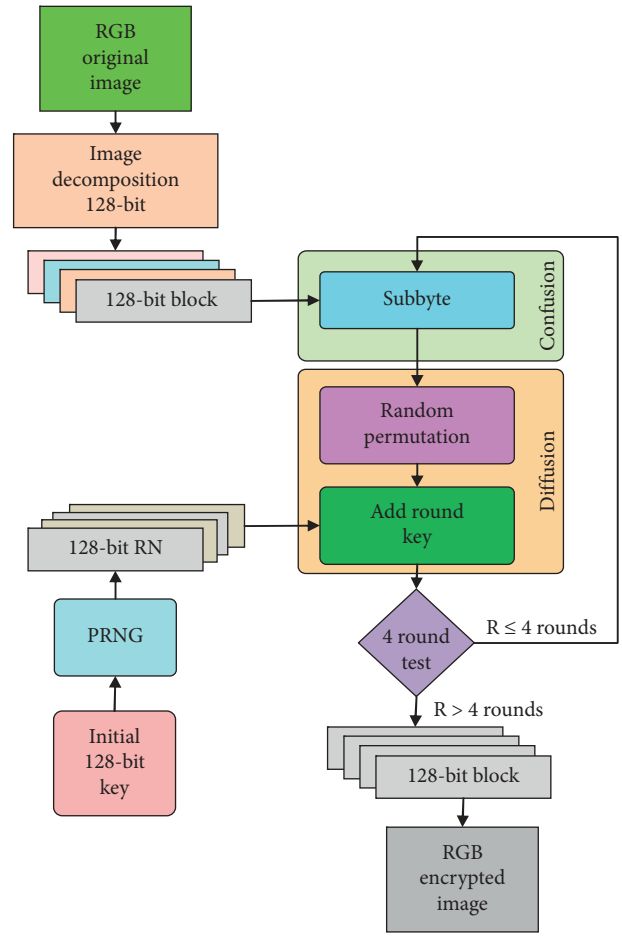


Figure 3: Flowchart of image encryption in this proposal method.

3.1.3. VGA Interface. Figure 8 presents the architecture of the VGA interface. It is responsible to transmit information from the bus into the VGA board to visualize images in the VGA monitor. It is structured by the following blocks:

(1)The DMA block: it assures the information transmission from the SRAM to the FIFO using both«-master_rd » and « master_addr»signals.

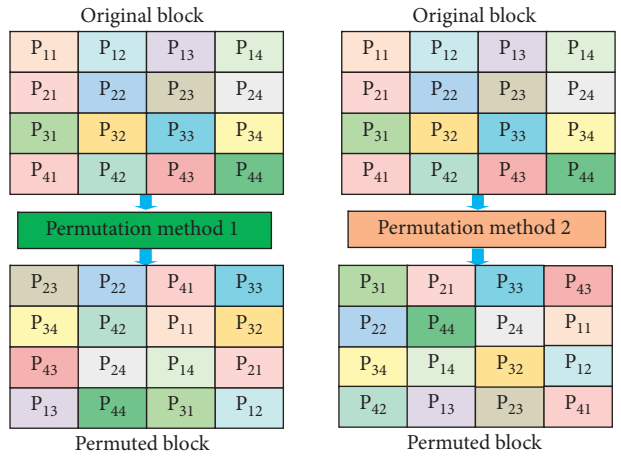


Figure 4: Description of the two permutation methods.

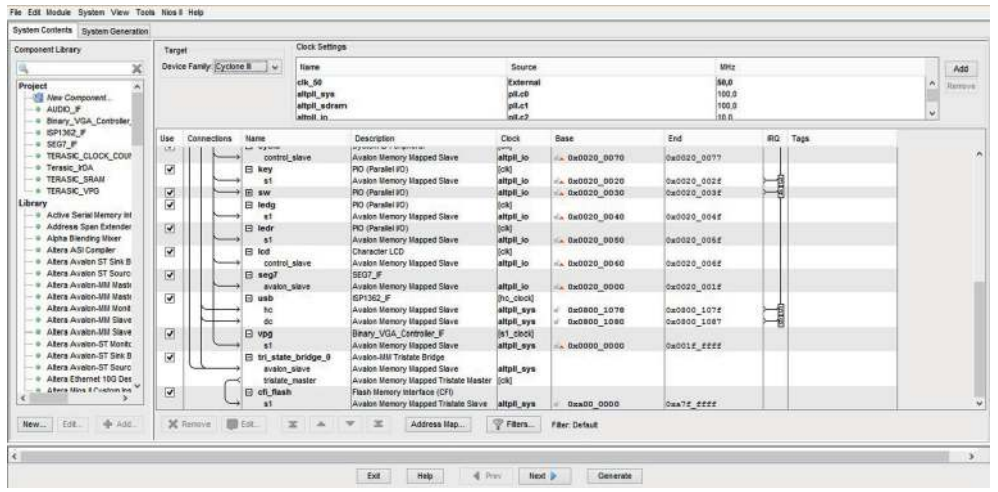


Figure 5: Connection in Qsys GUI.

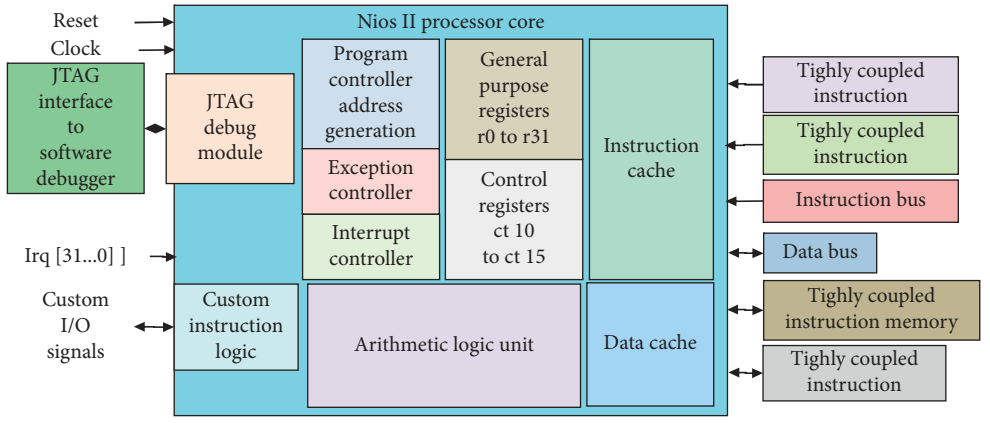


Figure 6: Chart flow of the NIOS II system design.

(2) The buffer block: two FIFO having the same size compose this module. In fact, when the writing is given by the DMA in the first FIFO, the VGA control block assures the reading of the information from the second FIFO. The writing on the FIFO is synchronized in 50 MHz while the reading is synchronized

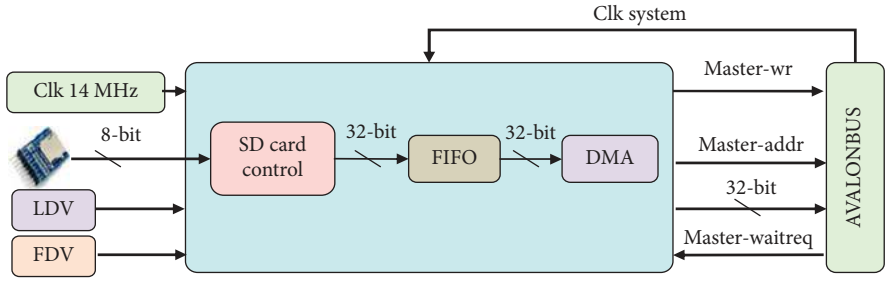


Figure 7: SD card interface.

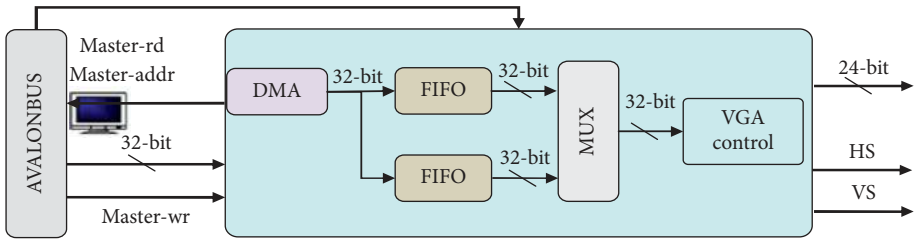


Figure 8: VGA interface.

with the VGA clock (25 MHz). The interface is given to assure the transmission of the 32 bits data via the bus to the visualization.

(3) VGA controller: it controls and transmits « R », « G », and « B » and synchronization signals to the VGA extension board.

All hardware IPs are developed in VHDL language in ALTERA Quartus tools. Once hardware is designed, we have implemented the application on the board. For this, we have firstly ported the derivative of Linux kernel (μClinux) on the processor to facilitate the implementation of the suggested image encryption on the chosen hardware platform.

3.2. Encryption System Architecture. Several AES hardware architectures have been reported in the literature [33]. In this paper, the goal is to design an improved architecture of the algorithm to speed up execution on 32 bit processors with memory constraints available in the embedded systems. The NIOS II 32 bit processor and the arithmetic logic unit (ALU) architectures are founded on the address buses, data buses, and registers of 32 bits data path. Every transformation of the AES cryptosystem maps a 128 bit as the input state and a 128 bit as the output state. To optimize the size of the MAES hardware conception, the 128 bit data block is split into four 32 bit blocks and is required at one column or at one row via the 32 bit data bus. Only the random permutation operation demands the accessibility of the totality of data (128 bits) before starting. Thus, four registers (32 bits) are required. On the contrary, four different S-boxes are needed in our proposed architecture. The encryption datapath processes a complete 32 byte block in parallel and the total round transformation is executed in a one-clock cycle. Thus, four clocks are needed for the entire encryption. The proposed architecture is depicted in Figure 9. It includes four components:

(1) The Input_Buffer and the Output_Buffer as well as many internal communication data paths are 32 bits in width and used to hold the plaintexts of 128 bits before being processed and to memorize cipher texts until processing the overall 128 bits

(2) Control unit is used to generate control signals for all components

(3) Key expansion PRNG unit is employed to generate a set of round keys

(4) MAES transformation round is employed to encrypt data input

The proposed cryptographic algorithm is interfaced with the SoPC as a hardware accelerator. The system designed is generated and downloaded successfully in Cyclone III FPGA NEEK developed board. The control part of the system is developed in C language in NIOS II IDE. In fact, a C code is downloaded on the soft processor to communicate with the proposed algorithm accelerator. The result of communication between the processor and the IP block is acquired. The ciphered image is forward to the PC via JTAG_URAT to perform findings in 32 bit frames.

Figure 10 presents the results of the suggested security system design (storage, processing (encryption/decryption), and display of the image signal) where the input is from the SD card interface and the output is on the VGA display interface. Both encryption and decryption procedures are implemented on the NEEK board. The encrypted result of the image is shown in Figure 10(a), whereas the decrypted result of the original image is as illustrated in Figure 10(b).

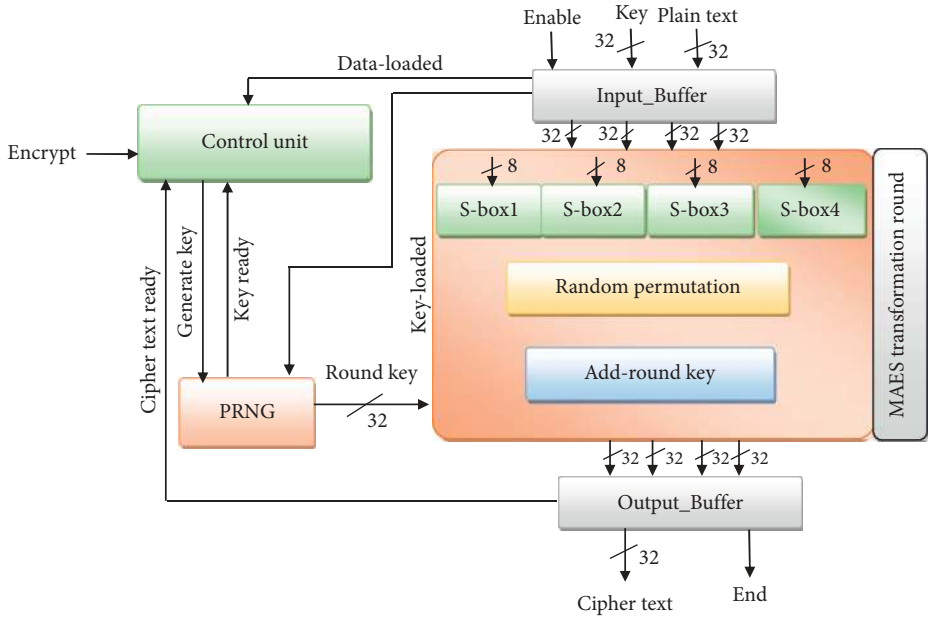
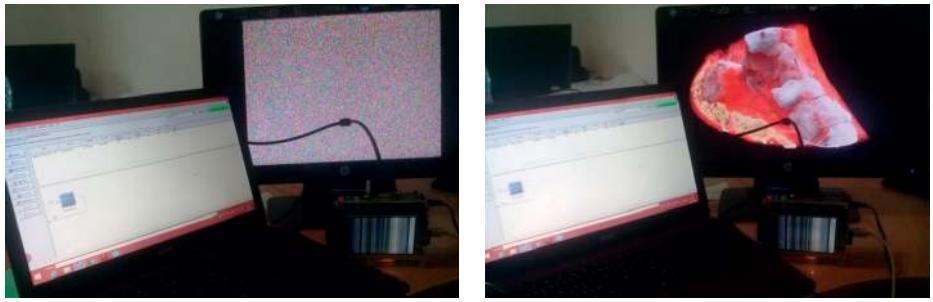


Figure 9: Proposed chaos-MAES architecture on FPGA.



(a) (b)

Figure 10: FPGA-based implementation of chaos-MAES-based secure image communications. Input from SD card interface and output on VGA display interface. (a) Encryption process. (b) Decryption process.

3.3. Hardware Performance. The proposed cryptosystem is implemented on the NEEK board featuring Cyclone III FPGA. Table 1 illustrates the performances utilization extracted from Quartus II implementation software. The system needs 14% of logic elements, 12% of combinational functions, 8% of logic registers, and 22% of memories. Finally, it runs at 167.83 MHz clock frequency, consumes 137.06 mW at the power, and can achieve a great throughput of 1.34 (Gbits/s).

The system throughput is an important metric that provides the number of bits processed in a second, which is computed using

$$\text{Throughput} = \frac{\text{nb\_bit} * \text{frequence}}{\text{latence}} \frac{\text{Mb}}{\text{s}}. \quad (13)$$

Concluding the obtained results, the proposed cryptosystem hardware design occupies a small hardware area and reaches 1.34 Gbits/s of throughput.

The execution time is a parameter that is significant to perform the real-time encryption processes. The proposed method has the aim to reduce the maximum processing time. Only four rounds of encryption are performed in a loop instead of 10 rounds that reduces significantly the execution time. The encryption datapath processes a complete 32 byte block in parallel and the total round transformation is executed in a one clock cycle. Thus, only four clocks are needed for the entire encryption.

Table 1: FPGA implementation of the proposed cryptosystem.

Hardware performances	Cyclone III
Total logic elements (LE)	3.216/24.624 (14%)
Total combinational function	2.860/24.624 (12%)
Dedicated logic registers	1.962/24.624 (8%)
Memories	131.616/608.256 (22%)
F Max	167.83 MHz
Total thermal power dissipation	137.06 Mw
Throughput	1.34 (Gbits/s)

From Table 2, the time required to encrypt Lena's $(512 \times 512 \times 3)$ standard test image using complex PRNG-

Table 2: Comparison of the proposed encryption model's run time with the existing AES and other works.

Execution time (s)	Proposed method	Existing AES	[34]	[35]	[36]
Lena ($512 \times 512 \times 3$)	0.02457	68.2218	15.268	0.3	0.0255

MAES is 0.02457 s, whereas, for the current standard AES implemented in the hardware device featuring a NIOS II softcore processor, it is 68,2218 s [37]. The suggested algorithm is about 97% faster compared to the standard AES. Similarly, a comparison of the execution time with other algorithms implemented in an FPGA is illustrated in the same table. The results prove that the processing time of the proposed model is much less than the existing works.

4. Security Analysis and Interpretation

In this part, we evaluate the system on FPGA for several ordinary and medical images with different types and sizes. For ordinary color images, we use the standard Lena, Peppers, and Baboon images of size ($512 \times 512 \times 3$) (Figure 11). For medical images, seven different types of images are selected which are depicted in Figure 12. Medical images are obtained by ultrasound device, 3D Scanner, magnetic resonance device MRI, X-ray, radiography, endoscopy, and computerized tomography (CT-scan). Simulation findings and performance analysis for the chosen images are given in this section highlighting the quality analysis of images, statistical analysis, key analysis, and algorithm performance.

4.1. Statistical Analysis. In this section, we use image histogram, information Entropy, 2D Normalized Correlation (NC), and correlation coefficient (ρ).

4.1.1. Histogram Analysis. The image histogram is a two-dimension statistical curve showing the distribution of Gray scales according to their values. Figure 13 shows the original images and their corresponding encrypted images and histograms of the original images and their corresponding encrypted images.

As seen in Figure 13, we note that the histogram of the resultant encrypted image is uniformly distributed and dissimilarly compared to the histogram of the original image in Figure 13 which contains large spikes. Therefore, the original image's pixels and the encrypted image's pixels are completely different.

4.1.2. NC Analysis. The normal correlation (NC) is a performance that evaluates the grade of similitude between two objects. If the original and the encrypted are different, therefore, the correlation factor of the cipher image is well low or highly close to zero. Results in Table 3 show that the NC values are reduced which proves that there is no correlation between original and ciphered images. As a consequence, the proposed system is safe against statistical attacks.

4.1.3. Global and Local Shannon Entropy Analysis. The global Shannon entropy is measured by applying equation (14) to the image. The entropy parameter is considered as the standard to test randomness. The entropy coefficient is utilized to obtain the incertitude performed in the ciphered image. If the entropy is elevated, the confidentiality is higher. Note that the utmost entropy value for a gray scale image is 8 bits/pixel. The average value for H (m) for numerous preceding works was between 7.90 and 7.99. This value is depending on the image, the size of the key, and the cryptographic model. Entropy is computed as

$$H(m) = \sum_{i}^{2N-1} P(mi)\, Log2\left(\frac{1}{P(mi)}\right), \tag{14}$$

where $H(m)$ is the Entropy image, $P(mi)$ is the probability mass function, and $2N - 1$ presents the number of gray levels.

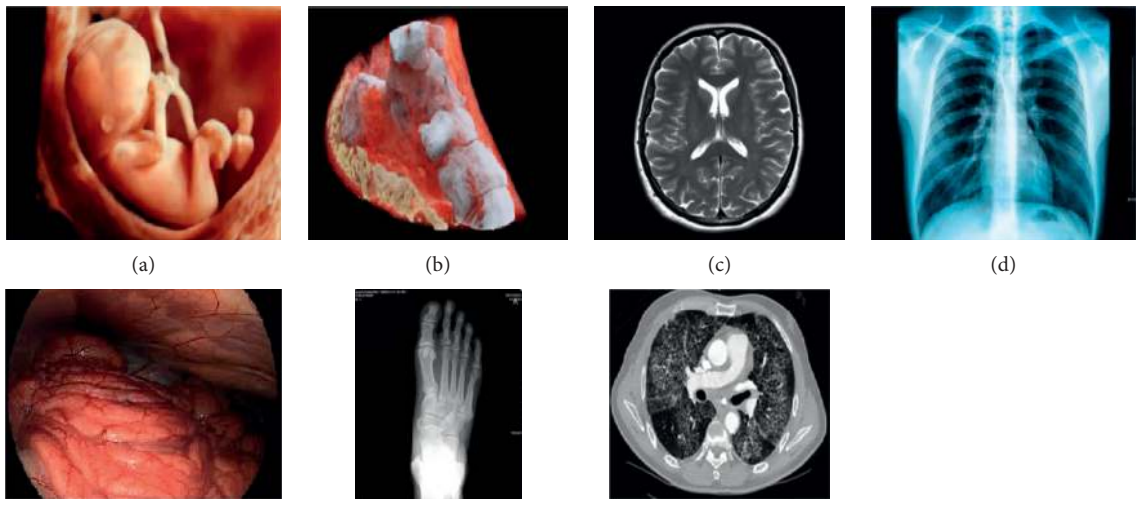
This technique fails to measure the real degree of randomness of an image. It has many weaknesses such as unfair random comparisons between images of different sizes, the inability to discern the randomness of images before and after image encrypting, and possible inaccurate scores for the synthesized images. However, it cannot be used for universal measures of randomness. To overcome this problem, local Shannon should be applied. The local entropy is measured by computing the mean of global Shannon entropies over all the nonoverlapping blocks of size 1936 pixels in the image. Table 4 introduces the simulation results of global and local Shannon entropy found for each image.

Analysing the results, the encrypted image's global entropy value is highly close to the ideal value 8 and the mean of local entropy is very important. This indicates that the pixels of the cipher image are random. As a result, the proposed system is safe against entropy and statistical attacks. Table 5 compares the global entropy value with the existing AES and other encryption algorithms. Our results are more successful than other works which prove the efficacity of the proposed cryptographic model.

4.1.4. Correlation Coefficient Analysis. In a clear image, the correlation of the adjacent pixels is close to one. Unlike in an encrypted image, the adjacent pixels must be not correlated [35]. Let x and y be two Gray scale values of two adjacent

(a) (b) (c)

Figure 11: Standard Lena, Peppers, and Baboon images used for the test. (a) Color Lena.jpg [512 × 512 × 3]. (b) Peppers.jpg [512 × 512 × 3]. (c) Color Baboon.jpg [512 × 512 × 3].



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

(e) (f) (g)

Figure 12: Seven different medical images chosen for the test. (a) 3D ultrasound baby [625 × 410 × 3]. (b) 3D scanner ankle [1080 × 1920 × 3]. (c) 1D MRI [800 × 600]. (d) 3D X-ray chest [3816 × 2832 × 3]. (e) 3D endoscopy [181 × 278 × 3]. (f) 3D radiography foot [2400 × 2956 × 3]. (g) 3D CT-scan chest image [800 × 600 × 3].

pixels in the image, and the correlation of the adjacent pixels is computed using equations (15)–(18):

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{15}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x_i)\right)^2, \tag{16}$$

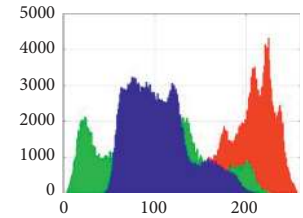
$$\operatorname{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\left(y_i - E(y)\right)\right), \tag{17}$$

$$r_{xy} = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{18}$$

where $E(x)$ is the expectation of x, $D(x)$ is the estimation of the variance in x, and cov (x, y) is the estimation of the covariance between x and y. Figure 14 shows the distributions of 2000 pairs which are randomly selected adjacent pixels of the original and encrypted 3D original medical scanner Ankle image, respectively, in each channel.

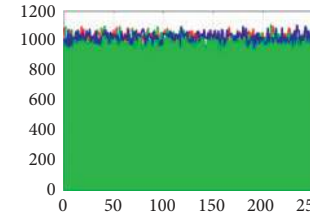
Table 6 shows the distributions of 2000 pairs which are randomly selected adjacent pixels of the original and encrypted images, respectively. The results clearly show that the correlation coefficient of the original images is close to 1, while the encrypted images are close to zeros. In addition, the distribution of adjacent pixels is inconsistent, i.e., there is no correlation between them. This indicates that the algorithm eliminates the correlation of adjacent pixels in the plain image, and it makes an encrypted image with no correlation. The proposed cryptographic method is


13.1



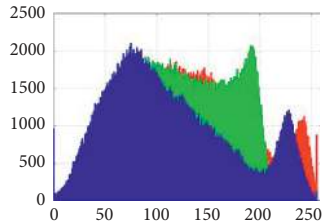
13.2


13.3



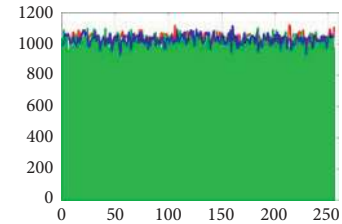
13.4


13.5



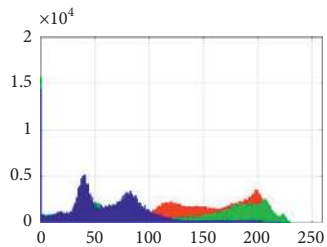
13.6


13.7

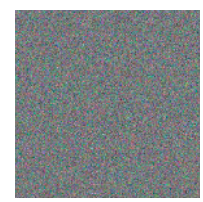


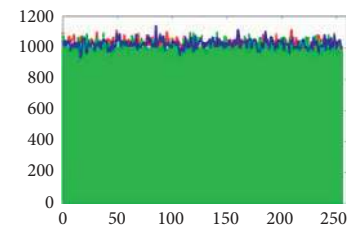
13.8


13.9



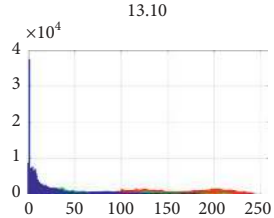
13.10


13.11



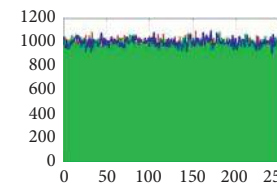
13.12


13.13



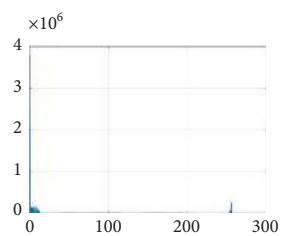
13.14


13.15



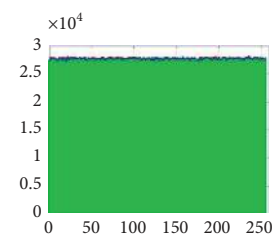
13.16


13.17



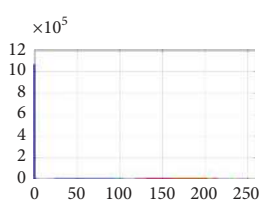
13.18


13.19



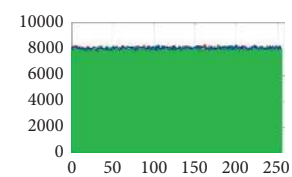
13.20


13.21



13.22

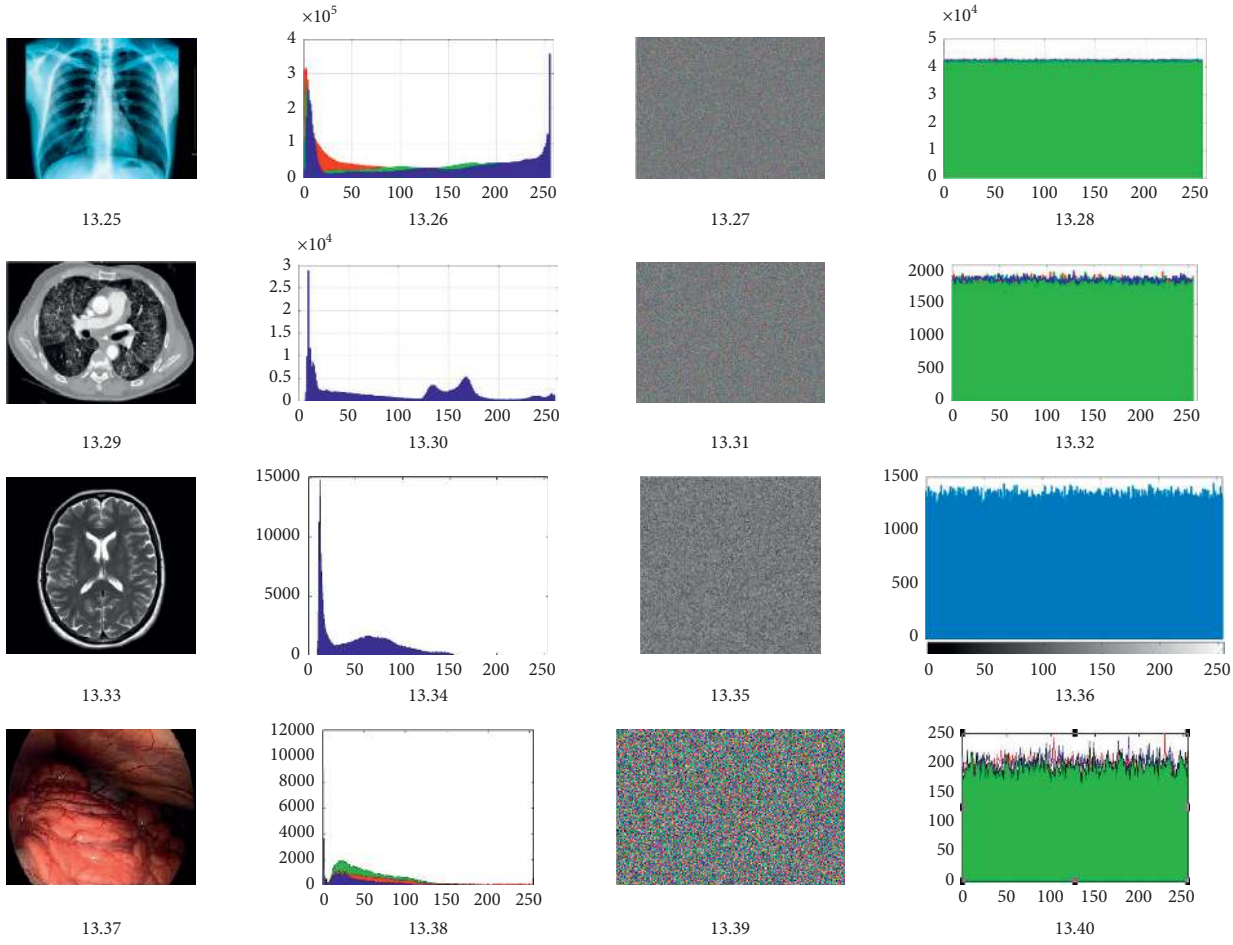

13.23



13.24

(a)

Figure 13: Continued.



(b)

Figure 13: Histogram of the original images and their corresponding encrypted images.

Table 3: NC results of encrypted images.

Image	NC		
	Red	Green	Blue
Lena	−0.00321	−0.00238	0.00065
Peppers	−0.00243	−0.00018	−0.00079
Baboon	0.00274	−0.001912	−0.01348
Ultrasound	0.00065	−0.00042	−0.00036
Scanner ackle	−0.0049	0.0035	−0.00276
Endoscopy	−0.00047	0.00024	−0.00046
MRI		−0.00082	

Table 4: Global and local Shannon entropy values of encrypted images.

Image	Local Shannon entropy			Global Shannon entropy		
	Red	Green	Blue	Red	Green	Blue
Lena	7.9548	7.9542	7.9546	7.99988	7.99989	7.99989
Peppers	7.9546	7.9544	7.9549	7.99989	7.99987	7.99986
Baboon	7.9554	7.9553	7.9557	7.99994	7.99989	7.99978
3D ultrasound	7.9557	7.9548	7.9552	7.99999	7.99999	7.99999
3D ankle	7.9563	7.9559	7.9559	7.99999	7.99999	7.99999
MRI		9.9553			7.99988	

Table 5: Comparative study of the average global entropy values.

Cryptosystem	Lena standard test image
Proposed model	7.99988
Existing AES	7.8693
Ref. [3]	7.9993
Ref. [38]	7.99932
Ref. [34]	7.9969
Ref. [35]	7.9989
Ref. [36]	7.9994
Ref. [9]	7.9975
Ref. [6]	7.9998
Ref. [8]	7.9973
Ref. [39]	7.9978
Ref. [40]	7.999329
Ref. [12]	Proposed 1: 7.998119 Proposed 2: 7.997349 Proposed 3: 7.997224 Proposed 4: 7.997189
Ref. [13]	7.9980
Ref. [14]	7.9980
Ref. [15]	Proposed 1: 7.9984 Proposed 2: 7.9985
Ref. [41]	7.99935
Ref. [42]	7.99935

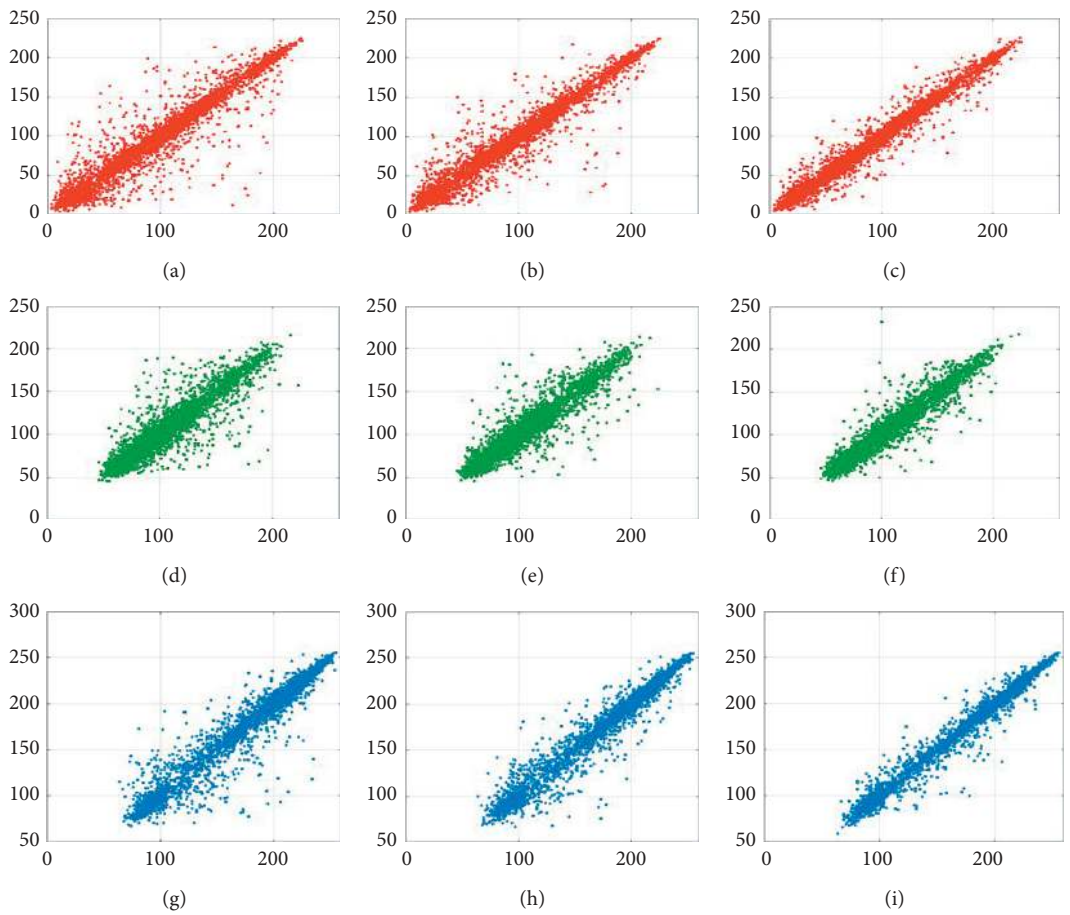


Figure 14: Continued.

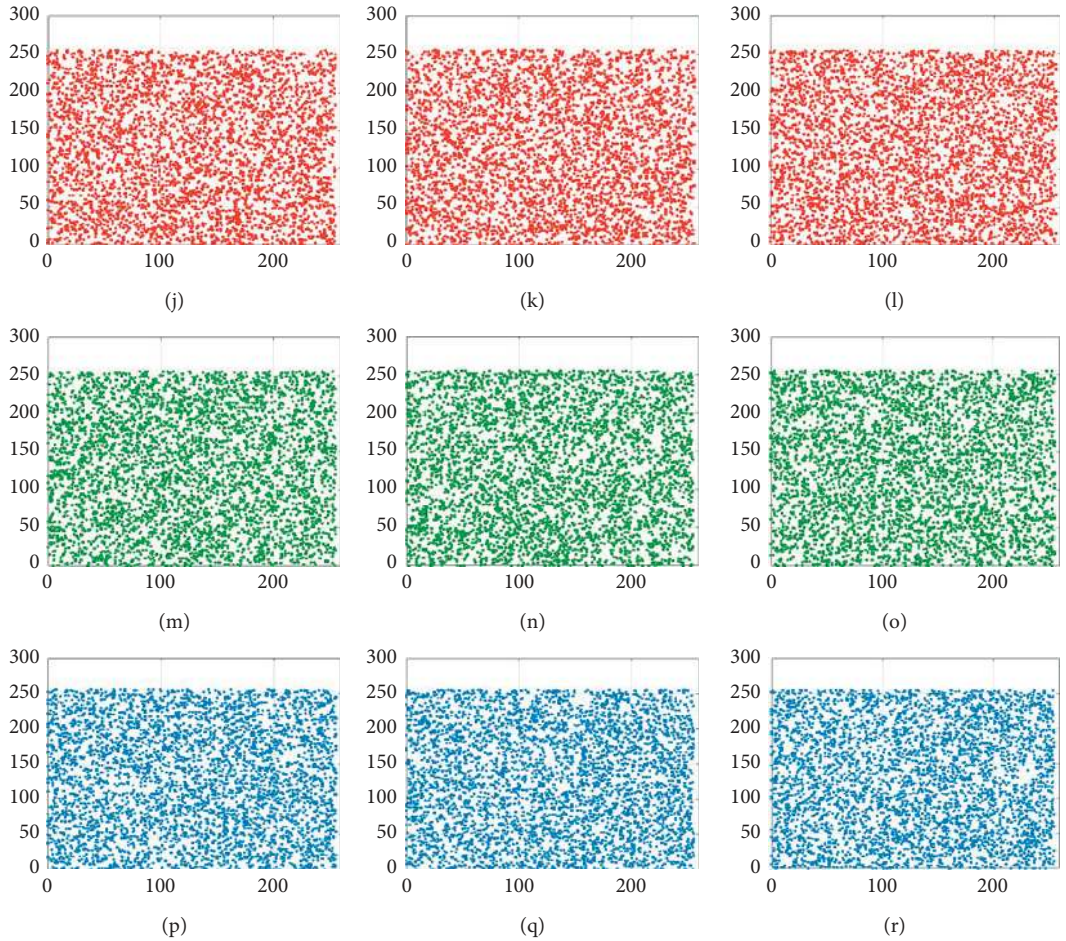


Figure 14: Correlation distribution of the original and cipher 3D original scanner ankle image with color image in horizontal, vertical, and diagonal directions: (a–i) correlation distribution of original images; (j–r): correlation distribution of cipher images.

Table 6: ρ values of original image and its corresponding encrypted image with chaos-MAES.

Image	Status	Horizontal			Vertical			Diagonal		
		Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena	Plain	0.989	0.984	0.957	0.979	0.966	0.935	0.967	0.952	0.918
	Cipher	0.0007	−0.001	−0.0006	−0.015	−0.008	0.0019	−0.025	0.015	0.0105
Peppers	Plain	0.969	0.976	0.948	0.963	0.973	0.952	0.950	0.965	0.921
	Cipher	−0.036	0.003	−0.034	0.001	−0.068	−0.007	0.013	0.002	0.006
Baboon	Plain	0.914	0.967	0.983	0.902	0.984	0.991	0.950	0.950	0.913
	Cipher	0.007	0.002	−0.082	−0.015	−0.002	−0.042	0.0019	−0.032	−0.035
Ultrasound	Plain	0.898	0.900	0.836	0.972	0.972	0.959	0.978	0.981	0.966
	Cipher	−0.002	−0.001	−0.009	−0.004	−0.003	−0.001	−0.002	−0.003	−0.002
Scanner ankle	Plain	0.998	0.998	0.996	0.997	0.998	0.995	0.999	0.999	0.998
	Cipher	−0.005	−0.002	−0.01	−0.031	−0.025	−0.006	−0.002	−0.005	−0.017
Endoscopy	Plain	0.988	0.988	0.988	0.987	0.986	0.987	0.983	0.982	0.982
	Cipher	−0.029	−0.076	−0.094	0.001	−0.007	−0.006	0.001	−0.005	0.021
Radiography foot	Plain	0.998	0.997	0.995	0.999	0.999	0.998	0.999	0.999	0.998
	Cipher	−0.031	−0.005	−0.016	−0.003	−0.003	−0.018	−0.004	−0.010	−0.033
3D X-ray	Plain	0.9981	0.9971	0.9995	0.9995	0.999	0.999	0.9995	0.9986	0.9987
	Cipher	−0.024	−0.016	−0.005	−0.007	0.018	0.003	−0.004	−0.033	−0.010

compared with the existing AES and other methods existing in the literature, and results in Table 7 prove that the propound cryptosystem has a better correlation with the smallest coefficients in all directions which prove the effectuality of the algorithm and its capability for resisting statistical attack.

4.2. Differential Attack Analysis

4.2.1. Keyspace. The keyspace of a safety encryption scheme should be very large to resist the brute-force attack. In the proposed algorithm, for an initial key *Ki*, there are 2^{128} dissimilar keys, which are very large. Certainly, the key brute-force attacks are computationally infeasible.

4.2.2. Key Sensitivity. The key sensitivity analysis warrants the safety of one cryptographic algorithm. An enhanced encryption model should be greatly sensitive to key changes. Similarly, the suggested model must be resistant to the brute-force attack obtained by large keyspace. To check the encryption process, the plain image is encrypted by three various keys: the first is the main key, the second is the same key with a small change in one bit, and the last is a variance between the two keys. The finding of three different ciphered images is presented in Figure 15. Similarly, the ciphered image is decrypted by two keys: one is the original key and the other is the modified key. The changed key does not allow retrieval of the clear image, as seen in Figure 16. As result, the suggested model is greatly sensitive to the key changes.

Both Number of Pixels' Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are utilized for the verification of the performance against differential attacks. According to [43], only one-bit modification over the clear image can result in a considerable modification in the encrypted picture. NPCR and UACI parameters are presented in equations (19) and (20):

$$\text{NPCR: } N(C1, C2) = \sum_{i,j} \frac{D(i,j)}{W * H} * 100\%, \tag{19}$$

$$\text{UACI: } U(C1, C2) = \frac{1}{W * H} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{225} * 100\%, \tag{20}$$

where $C1$ and $C2$ are the ciphered images, M is the size of images, and D presents the bipolar matrix determined from $C1$ and $C2$.

The NPCR measures the pixel number that modifies the value in differential attack. The elevated value is considered better. The UACI computes the average variance between two paired encrypted images where a minimal value is the best. Table 8 denotes the NPCR R, G, B and UACI R, G, B values for various medical color image sizes using the propound cryptographic method. Results prove that the encryption model has great performance, and it is characterized by high sensitivity to small modifications in the clear image. Table 9 compares both NPCR and UACI results using the suggested algorithm with the existing AES, and some existing works and findings prove that the propound cryptographic technique has met the desired objective for resisting differential attacks.

4.3. Randomness Analysis. Random analysis can be achieved using NIST 800-22. The test is useful to test random and Pseudorandom Number Generators [44] to determine whether or not a PRNG is appropriate for data encryption. The analysis contains 15 tests that assess key streams to meet important necessities. It focuses on different nonrandom aspects that can be found in a key sequence. The test results of 262,144 sequences of 128 bit generated by the proposed RNG are shown in Table 10. The sequences pass successfully all tests. This demonstrates that the generated pseudorandom numbers have good statistical properties such as highly unpredictable, random, independent, and uniformly distributed.

4.4. Know Plain Text (KPA) and Chosen Plain Text Attack (CPA). This kind of attack has been utilized to crack some of the cryptographic models. In general, an adversary utilizes whole black or whole white to discover the possible patterns in the cryptographic model. Thus, the whole white and whole dark images are ciphered utilizing the suggested method. Figure 17 presents the ciphered images and no pattern is apparent. The entropy value of images is self-same as other images and correlation coefficients are ideal. Table 11 illustrates the correlation between adjacent pixels and the entropy values of both images. Results prove that the system is greatly secure to these kinds of attacks.

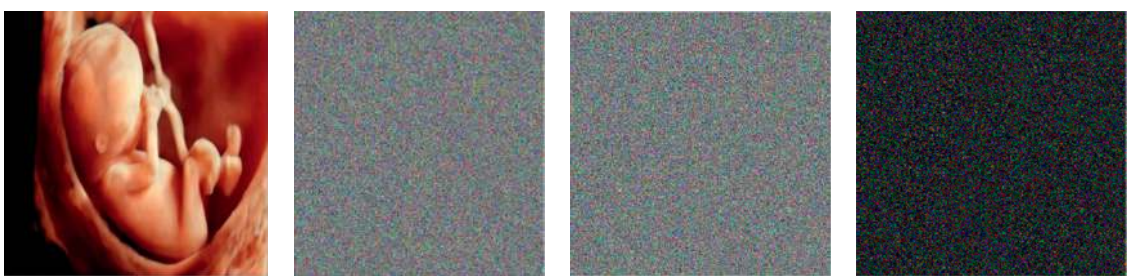
4.5. Robustness against Noise Attack. During the picture transmission via the network, the ciphered image can lose information or can be influenced by noise. Various cryptographic systems are sensitive to noise where a small change to the ciphered image can produce a strong distortion into the deciphered image. Figure 18 shows that the deciphered images keep the global clear image information for the person's eye when the ciphered image is affected by Salt and pepper noise with various percentages. Thus, the suggested method is robust and resist against noise attack.

5. Discussion

Through the experimental results, it is shown that the histogram of a ciphered image has uniform distribution and the correlation between pixels is reduced. The average entropy value of the cipher scanner ankle image with the proposed algorithm is 7.99999 (close to the ideal value). The variance of entropy between the propound model and the existing AES is 0.13069. Our method augments the entropy by about 18% compared to the standard one. Thus, more randomness can be created. Equally important is that the suggested cryptographic model has an efficient encryption effect, a large keyspace, and it is highly sensitive to key changes. Furthermore, findings prove that the proposed model can

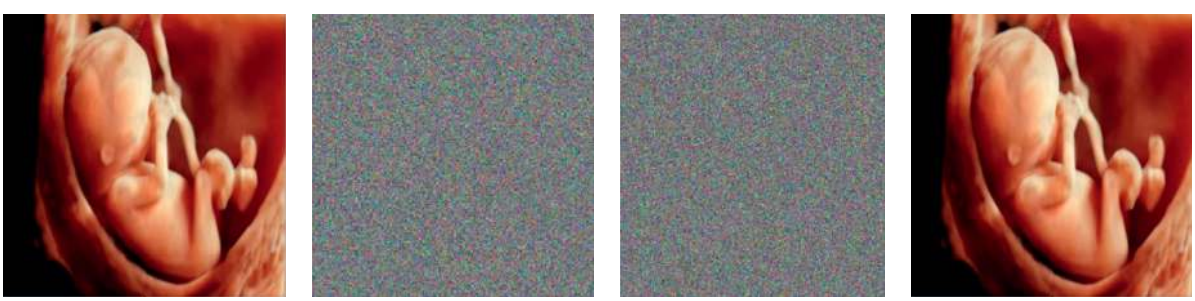
Table 7: Comparative study of average correlation coefficient for Lena image.

Model	Horizontal	Vertical	Diagonal
Proposed system	−0.0003	−0.006	0.00014
Existing AES	0.2724	0.2682	0.0765
Ref. [3]	−0.0008	0.0016	0.0043
Ref. [38]	−0.000483	−0.001001	−0.001015
Ref. [34]	0.0025	0.006207	0.003041
Ref. [35]	0.004639	0.006763	0.010818
Ref. [36]	0.000101	0.00000958	0.000131
Ref [9]	0.0070	−0.0102	0.0030
Ref. [6]	−0.000400	−0.0018	0.0001
Ref. [8]	0.001	0.0017	0.0125
Ref. [39]	0.0031	—	—
Ref. [40]	0.000751	0.001133	0.001253
Ref. [12]	Proposed 1 : 0.007950 Proposed 2 : 0.00987 Proposed 3 : 0.007768 Proposed 4 : 0.000914	Proposed 1 : 0.007422 Proposed 2 : 0.009145 Proposed 3 : 0.007773 Proposed 4 : 0.009525	Proposed 1 : 0.000139 Proposed 2 : 0.000697 Proposed 3 : 0.000143 Proposed 4 : 0.000711
Ref. [13]	0.01658	0.01235	0.014566
Ref. [14]	0.006150	0.006687	−0.007019
Ref. [15]	Proposed 1: −0.00093 Proposed 2: −0.0007	Proposed 1: −0.001 Proposed 2: −0.00059	Proposed 1: −0.00067 Proposed 2: 0.00093
Ref. [41]	0.0002	−0.0133	−0.0791
Ref. [42]	−0.1242	0.0027	0.0022



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

Figure 15: Test of the key encryption sensitivity. (a) Plain image of 3D ultrasound image, (b) cipher image by the main key, (c) cipher image by the modified key, and (d) the difference between image (b) and (c).



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

Figure 16: Test of the key decryption sensitivity: (a) original image of 3D ultrasound image, (b) cipher image by the right key, (c) decryption by 1 bit key change, and (d) decryption with the right key.

resist the noise attack with varied intensity, KPA, CPA, and differential attacks. The complex PRNG is tested by NIST, and the result proves that it generates a high-quality key. The run time of the proposed scheme is also executed, and findings prove that the proposed algorithm requires much less calculation time than the existing AES implemented in the hardware device. All in all, results show that a fast (1.34 Gbit/s) and highly secure data encryption is achieved with

Table 8: Results of NPCR and UACI for various color images.

Image	NPCR (%)			UACI (%)		
	Red	Blue	Green	Red	Blue	Green
3D ultrasound baby	99.896	99.746	99.799	33.776	33.723	33.697
3D scanner ankle	99.699	99.687	99.898	33.896	33.895	33.678
3D radiography foot	99.698	99.695	99.894	33.798	33.793	33.796
3D CT-scan chest image	99.793	99.659	99.763	33.805	33.898	33.891
Brain image		99.684			33.594	
Endoscopy	99.79	99.689	99.89	33.890	33.771	33.642

Table 9: Comparative study of NPCR and UACI tests for Lena image.

Image	NPCR (%)	UACI (%)
Proposed algorithm	99.69561	33.81015
Existing AES	0.0779	0.0097
Ref. [3]	99.62	33.41
Ref. [38]	99.6040	33.4614
Ref. [34]	99.6140	33.4805
Ref. [35]	99.6162	33.3979
Ref. [36]	99.61	33.48
Ref. [9]	99.62	33.56
Ref. [6]	99.60	33.48
Ref. [8]	99.50	33.30
Ref. [39]	99.6100	33.5000
Ref. [12]	Proposed 1 : 99.6253 Proposed 2 : 99.6271 Proposed 3 : 99.6188 Proposed 4 : 99.6253	Proposed 1 : 33.4565 Proposed 2 : 33.5589 Proposed 3 : 33.4468 Proposed 4 : 33.4565
Ref. [13]	99.6258	33.4586
Ref. [14]	99.6125	33.4164
Ref. [15]	Proposed 1 : 99.6208 Proposed 2 : 99.61	Proposed 1 : 33.4494 Proposed 2 : 33.4329
Ref. [41]	99.65950	33.83002
Ref. [42]	99.6315	33.8300

Table 10: Results of NIST 800-22 statistical test for the proposed PRNG.

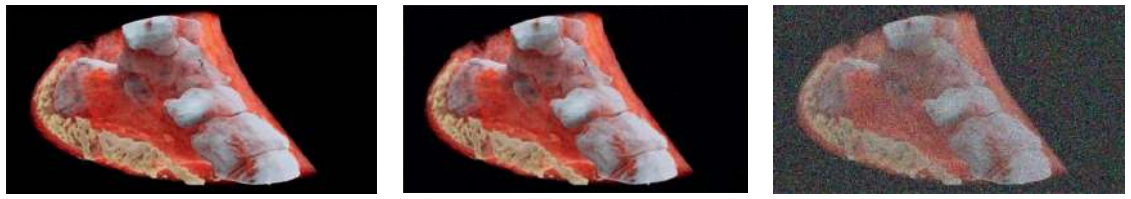
Statistical	P value	Status
Status frequency	0.9015	Pass
Block frequency ($m = 128$)	0.563	Pass
Forward cusum	0.648	Pass
Reverse cusum	0.672	Pass
Runs	0.672	Pass
Long runs of ones	0.644	Pass
Binary matrix rank	0.523	Pass
Spectral DFT	0.892	Pass
Nonoverlapping template ($m = 9$)	0.426	Pass
Overlapping template ($m = 9$)	0.619	Pass
Universal	0.473	Pass
Approximate entropy ($m = 10$)	0.456	Pass
Random excursions ($x = +1$)	0.924	Pass
Random excursions' variant ($x = -1$)	0.693	Pass
Linear complexity ($M = 500$)	0.586	Pass

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

Figure 17: (a) All black image, (b) all white dark image, (c) ciphered all black, and (d) ciphered all white.

Table 11: Results of entropy and NC for white and black images.

Image	Entropy	NC		
		Red	Blue	Green
All black	0	—	—	—
All black ciphered	7.99977	−0.0027	−0.0036	0.0015
All white	0	—	—	—
All white ciphered	7.99977	0.0065	−0.00145	0.00015



(a) (b) (c)

Figure 18: Decrypted 3D medical scanner ankle of size ($1080 \times 1920 \times 3$) with Salt and pepper noise: (a) $d = 0.005$, (b) $d = 0.1$, and (c) $d = 0.5$.

low power consumption (137.06 mw) and that the cryptosystem is robust, which makes it suitable to secure medical images in an embedded system. A comparison study is performed and the results prove that our algorithm outperforms other existing work in terms of speed of computation and safety level.

6. Conclusion and Future Work

An improved cryptographic system that mixes the use of a complex chaos-based PRNG and MAES is proposed in this paper. The complex chaos-based PRNG is put forward to generate a great-quality encryption key. The generated key presents high randomness, high entropy, and high complexity. In the MAES, the subbytes' operation is performed using four different S-boxes (S-box 1, S-box 2, S-box 3, and S-box 4) which increases the complexity. In addition, both shift-rows and mix-columns transformations are eliminated and replaced with a random permutation method for more complexity. Only four rounds of encryption are performed in a loop that reduces significantly the execution time. The encryption data path processes a complete 32 byte block in parallel, and the total round transformation is executed in a one clock cycle. Thus, only four clocks are needed for the entire encryption. The global cryptosystem is implemented in the NEEK board and great results are gained in terms of execution time, area occupation, power consumption, and throughput. However, the utilized NIOS II CPU is a relatively powerful one amongst embedded processors. The security analysis of our method proves that it is resistant to known attacks. The entropy, the correlation of adjacent pixels, and the histogram of encrypted images are performed successfully and findings are promising. As future work, we aim to propose a real-time video security approach that enhances the security of surgical telepresence during surgery between the site of surgery (local site) and the site that hosts the expert surgeon (remote site).

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare no conflicts of interest.

Authors' Contributions

All the authors helped to conceive these simulation experiments. Amal Hafsa and Mohamed Gafsi designed and

performed the experiments and have written the main part of the manuscript. Amal Hafsa, Mohamed Gafsi, Jihene Malek, and Mohsen Machhout contributed to the interpretation of the results as well as the revision and writing of the paper.

References

[1] J. Chen, L. Chen, L. Y. Zhang, and Z.-l. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 301–322, 2019.

[2] S. Kotel, M. Zeghid, A. Baganne, and R. Tourki, *FPGA-based Real-Time Implementation of AES Algorithm for Video Encryption, Recent Advances in Telecommunications, Informatics and Educational Technologies*, ResearchGate, Berlin, Germany, 2015, ISBN 978-1-61804-262-0.

[3] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved EIGamal encryption technique," *Optik*, vol. 147, pp. 88–102, 2017.

[4] M. Elhoseny, G. Ramírez-González, O. M. Abu-Elnasr, S. A. Shawkat, N. Arunkumar, and A. Farouk, "Secure medical data transmission model for IoT-based healthcare systems," *IEEE Access*, vol. 6, pp. 20596–20608, 2018.

[5] Y. Zhang, X. Li, and W. Hou, "A fast image encryption scheme based on AES," in *Proceedings of the 2th International Conference on Image, Vision and Computing*, IEEE, Chengdu, China, June 2017.

[6] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System," *Signal Processing*, vol. 141, p. 217, 2017.

[7] G. Hu, D. Xiao, Y. Wang, and X. Li, "Cryptanalysis of a chaotic image cipher using Latin square-based confusion and diffusion," *Nonlinear Dynamics*, vol. 88, no. 2, pp. 1305–1316, 2017.

[8] A. A. Abd El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 136–143, 2013.

[9] H. Liu and Y. Liu, "Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve," *Optics & Laser Technology*, vol. 56, pp. 15–19, 2014.

[10] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Journal of Optics and Laser Technology*, vol. 124, 2020.

[11] C. Xiuli, Z. Jitong, G. Zhihua, and Z. Yushu, "Medical image encryption algorithm based on Latin square and memristive chaotic system," *Multimedia Tools and Applications*, vol. 78, p. 3541935453, 2019.

[12] N. Ben Slimane, K. Bouallegue, and M. Machhout, "Designing a multi-scroll chaotic system by operating Logistic map with fractal process," *Nonlinear Dynamics*, vol. 88, no. 3, pp. 1655–1675, 2017.

[13] N. Ben Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30993–31019, 2018.

[14] N. Ben Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "Hash key-based image cryptosystem using chaotic maps and cellular automata," in *Proceedings of the 15th International Multi-Conference on Systems, Signals & Devices (SSD)*, Hammamet, Tunisia978-1-5386-5305-0/18/$31.00 ©2018, Hammamet, Tunisia, March 2018.

[15] N. B. Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "An efficient nested chaotic image encryption algorithm based on DNA sequence," *International Journal of Modern Physics C*, vol. 29, 2018.

[16] F. Elgendy, A. M. Sarhan, T. E. Eltobely, S. F. El-Zoghdy, H. S. El-sayed, and O. S. Faragallah, "Chaos-based model for encryption and decryption of digital images," *Multimedia Tools and Applications*, vol. 75, no. 18, pp. 11529–11553, 2015.

[17] X. Wang, Y. Zhao, H. Zhang, and K. Guo, "A novel color image encryption scheme using alternate chaotic mapping structure," *Optics and Lasers in Engineering*, vol. 82, pp. 79–86, 2016.

[18] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 995–1015, 2014.

[19] B. Radu, A. C. Dascalescu, and I. Priescu, "A new hyperchaotic map and its application in an image encryption scheme," *Signal Processing: Image Communication*, vol. 29, pp. 887–901, 2014.

[20] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A colour image encryption scheme using permutation-substitution based on chaos," *Entropy*, vol. 17, no. 6, pp. 3877–3897, 2015.

[21] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *The Journal of Supercomputing*, vol. 75, no. 10, pp. 6663–6682, 2019.

[22] W. Zhang, K.-w. Wong, H. Yu, and Z.-l. Zhu, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 8, pp. 2066–2080, 2013.

[23] S. Suri and R. Vijay, "An AES–CHAOS-based hybrid approach to encrypt multiple images," in *Proceedings of the International Conference in Recent Developments in Intelligent Computing, Communication and Devices*, pp. 37–43, Springer, Shenzhen, China, July 2017.

[24] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Journal of Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[25] Y. Qi and C. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *International Journal of Bifurcation and Chaos*, vol. 28, p. 1850047, 2018.

[26] M. Gafsi, N. Abbassi, M. Ali Hajjaji, J. Malek, and A. Mtibaa, "Improved chaos-based cryptosystem for medical image encryption and decryption," *Journal of Scientific Programming*, vol. 2020, Article ID 6612390, 22 pages, 2020.

[27] S. Ibrahim and A. Alharbi, *Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography*, IEEE Access, Piscataway, NJ, USA, 2020.

[28] J. Pratt, "Marshall medical center brings in new technology," 2012, https://www.mtdemocrat.com/special-sections/medical-guide-2012/marshall-medical-centerbrings-in-new-technology/.

[29] M. L. Mat Kiah, S. H. Al-Bakri, A. A. Zaidan, B. B. Zaidan, and M. Hussain, "Design and develop a videoconferencing framework for real-time telemedicine applications using secure group-based communication architecture," *Journal of Medical Systems*, vol. 38, no. 133, pp. 133–144, 2014.

[30] X. Zhang and W. Chen, "A new chaotic algorithm for image encryption," *International Conference on Audio, Language and Image Processing*, vol. 4, no. 3, pp. 889–892, 2008.

[31] FIPS PUB 197: Advanced Encryption Standard (AES). Computer Security Standard, Cryptography, 2001.
[32] A. Hafsa, N. Alimi, A. Sghaier, and M. Machhout, "A hardware-software Co-designed AES-ECC cryptosystem," in *Proceedings of the IEEE International Conference on Advanced Systems and Electric Technologies IC ASET*, Hammamet, Tunisia, January 2017.
[33] P. Hämäläinen, M. Hännikäinen, and T. D. Hämäläinen, "Review of hardware architectures for advanced encryption standard implementations considering wireless sensor networks," *SAMOS*, vol. 4599, pp. 443–453, 2007.
[34] J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, "New simple Chaotic System and its application in medical image encryption," *Multimedia Tools and Applications*, vol. 4, pp. 1–22, 2018.
[35] Z. Lin, J. Liu, J. Lian, Y. Ma, and X. Zhang, "A novel fast image encryption algorithm for embedded systems," *Multimedia Tools and Applications*, vol. 78, pp. 20511–20531, 2019.
[36] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua, "An improved image encryption algorithm for satelite application," *Advances in Space Research*, vol. 66, 2020.
[37] A. Hafsa, N. Alimi, A. Sghaier, and M. Machhout, "An improved co-designed AES-ECC cryptosystem for secure data transmission," *International Journal of Information and Computer Security (IJICS)*, vol. 13, 2020.
[38] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Information Sciences*, vol. 450, pp. 361–377, 2018.
[39] Y. Yao, W. Zhang, and N. Yu, "Inter frame distorsion drift analysis for reversible data hiding in encrypted H.264/AVC video bitstreams," *Signal Process*, vol. 132, pp. 19–28, 2017.
[40] C.-H. Yang, H.-C. Wu, and S.-F. Su, *Implementation of Encryption Algorithm and Wirless Image Transmission System on FPGA*, IEEE Access, Piscataway, NJ, USA, 2019.
[41] M. Gafsi, M. Ali Hajjaji, J. Malek, and A. Mtibaa, "Efficient encryption system for numerical image safe transmission," *Journal of Electrical and Computer Engineering*, vol. 2020, Article ID 8937676, 12 pages, 2020.
[42] M. Gafsi, S. Ajili, M. Ali Hajjaji, J. Malek, and A. Mtibaa, "High securing Cryptography system for digital image transmission," *Smart Innovation: Systems and Technologies*, Springer, vol. 146, pp. 311–322, 2020.
[43] Y. Wu, "NPCR and UACI randomness tests for image encryption, Cyber journals: multidisciplinary journals in science and technology," *Journal of Selected Areas in Telecommunications (JSAT)*, vol. 31–38, 2011.
[44] A. Melo, P. Bezerra, E. Cerqueira, and G. Antônio Jorge, "Abelém chapter 11: PriorityQoE: Atool for improving the QoE in video streaming," *Intelligent Multimedia Technologies for Networking Applications: Techniques and Tools*, IGI Global, Hershey, PA, USA, 2013.