IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 21 December 2023, accepted 25 February 2024, date of publication 5 March 2024, date of current version 14 March 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3374218

RESEARCH ARTICLE

A New 12-Bit Chaotic Image Encryption Scheme Using a 12 × 12 Dynamic S-Box

SALEH IBRAHIM[1,2], ALAA M. ABBAS[1,3], AYMAN A. ALHARBI[4], AND MARWAN ALI ALBAHAR[5]

[1]Department of Electrical Engineering, College of Engineering, Taif University, Taif 21944, Saudi Arabia
[2]Department of Computer Engineering, Faculty of Engineering, Cairo University, Giza 12613, Egypt
[3]Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[4]Department of Computer Engineering, College of Computers and Information Systems, Umm Al-Qura University, Makkah 21955, Saudi Arabia
[5]Department of Computer Science, College of Computer Science, Umm Al-Qura University, Makkah 21955, Saudi Arabia

Corresponding author: Saleh Ibrahim (saleh@eng.cu.edu.eg)

The authors extend their appreciation to the Deanship for Research and Innovation, Ministry of Education in Saudi Arabia for funding this research work through the project number: IFP22UQU4400257DSR031.

ABSTRACT The use of 12-bit levels of grayscale in medical image representation allows for more precise image analysis and diagnosis, and encrypting such images is essential for protecting patient privacy and security. Existing 8-bit image encryption schemes become inefficient when applied to 12-bit images. In this paper, we design a cryptographically strong encryption scheme to improve the efficiency of encrypting 12-bit medical images. The core of the proposed scheme is a key-dependent 12 × 12 S-box, which plays a crucial role in enhancing the security and efficiency of the encryption scheme. Most notably, test results show that 12 × 12 S-boxes offer significantly stronger confusion and key-sensitivity than their 8 × 8 counterparts. This finding enables the proposed 12 × 12 S-box-based scheme to process 12-bit images 3.3 times faster than an 8 × 8 S-box while passing all security tests. Experimental results show that the proposed scheme can encrypt 12-bit images at speeds up to 300MB/s. Moreover, the proposed scheme has also been shown to efficiently handle 8-bit images. Comparative results highlight the security and efficiency advantages of the proposed scheme over existing medical image encryption schemes.

INDEX TERMS Image encryption, key-dependent S-box, key-sensitivity, medical images, secure healthcare, 12-bit image encryption.

I. INTRODUCTION

Medical imaging is a crucial tool for medical diagnosis. Medical image pixel intensity values are frequently digitized into 4096 grayscale levels. The larger number of quantization levels facilitates more accurate diagnosis. Therefore, the DICOM standard medical image format [1] allows 12-bit or 16-bit pixel format to represent the 4096 levels. When medical images are stored or transmitted, they should be encrypted to protect patient privacy. Traditional image encryption schemes are often designed to deal with 8-bit pixel representing 256 grayscale levels. A straightforward application of those 8-bit schemes to a 12-bit image would only retain the 8 most significant bits of each pixel [2], thus causing a loss in contrast precision, which can lead to mistaken medical diagnosis. Alternatively, 12-bit medical image files may be treated as a sequence of 8-bit bytes, thus ignoring the difference between the least significant and the most significant pixel bits. However, the security and quality of encryption can be negatively affected, and the security analysis can be misleading. Moreover, this mismatch between the 8-bit architecture of the encryption scheme and the 12-bit data format of the image can require two 8-bit encryption operations per 12-bit pixel, which reduces the efficiency in terms of encryption speed.

The motivation for this work is to design an encryption architecture tailored for 12-bit medical images to achieve the following goals: 1) to retain the medical image information fidelity, 2) to enhance the security of encryption and the validity of security analysis, and 3) to improve the encryption speed.

Existing image encryption schemes often use a dynamic substitution box (S-box) as a building component that provides confusion. As a common building block of

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

cryptosystems, a bijective $n \times n$ S-box receives a group of n input bits and nonlinearly transforms them into a corresponding group of n output bits. The number of input bits is referred to as the width of the bijective S-box. Increasing the width of the S-box input and output from 8 bits to 12 bits enhances its confusion power by increasing the S-box key space from $(2^8!)$ to $(2^{12}!)$.

When chaotic maps are used in image encryption to generate random mask, the output of the chaotic map is traditionally truncated to 8 bits (mod 256) to match the pixel size. To deal with 12-bit images, the output of the chaotic map should be truncated to 12 bits (mod 4096) instead. Since the statistical properties of the generated random numbers is affected by the truncation length, the quality of the 12-bit truncated chaotic output should be verified.

Our contribution in this paper can be summarized as follows:

- Proposing a new 12-bit chaotic image encryption scheme to match the format of 12-bit medical images,
- Improving the security of chaotic image encryption using a 12×12 dynamic S-box construction method,
- Improving the throughput of the scheme to handle high resolution 3D medical images in real time by truncating chaotic sequences values at 12 bits.

In the rest of the paper, we first review the necessary background on dynamic S-boxes, and chaotic maps, and review medical image encryption literature in Section II. Then, we present the proposed medical image encryption scheme in in Section III. The security and speed analysis of the proposed scheme is reported in Section IV. The justification of the proposed scheme design and the role of each building block are presented in detail in Section V. Section VI compares the security and efficiency analysis of the proposed scheme to relevant medical image encryption schemes. Finally, we present our concluding remarks in Section VII.

II. BACKGROUND

A. CHAOTIC IMAGE ENCRYPTION

Chaos systems are a suitable choice for generating cryptographic pseudorandom sequences. Consequently, chaotic maps have been widely adapted and utilized in literature for various image encryption applications. Digital images in wireless communication systems have utilized chaotic maps to secure the transmission process [3], [4]. Authors in [4] developed a new scheme to enhance the randomness of chaotic maps designated for wireless communication applications. In [3] two chaotic maps have been developed using Logistic Map and Arnold's Cat map to secure real-time transmission of digital images in wireless communication. Thermal images can also be encrypted and secured using chaotic maps [5]. Many chaotic image encryption schemes, such as [6], exploit DNA coding technique to enhance security.

Authors in [7] developed an efficient 1-D fractional chaotic map to improve speed and key space. Using their new chaotic map, the authors constructed an image encryption scheme capable of 20 MB/s encryption throughput.

In [8], authors utilized a hybrid chaos system that combines more than one map to develop a grayscale image cryptosystem. In their system, Arnold's cat map is exploited to implement the confusion process while the diffusion process is achieved by the combination of sine map, logistic map, and tent map.

Recently, authors in [9] developed a secure image encryption scheme based on chaotic map and S-boxes method. The proposed approach uses 16 different S-boxes which are constructed based on 16 distinct primitive polynomials.

The performance of chaotic image encryption can be greatly improved through hardware acceleration. In [2], the authors implemented their encryption scheme on a digital signal processor to achieve encryption speed of 2 MB/s. On a smartphone, the same scheme achieved 8 MB/s encryption throughput. The authors of [10] proposed a fixed-point chaotic map composed of cascaded Logistic map, Lozi map, and Tent map and used FPGA for the implementation to achieve real-time encryption speed of 27 MB/s on a 27 MHz FPGA.

B. MEDICAL IMAGE CRYPTOSYSTEMS

Encryption of medical images have found considerable interest among researchers. A medical image cryptosystem has been presented in [11], which uses cosine number transform over a known Galois field. Another cryptosystem introduced in [12], applied the cosine number transform to the medial image in the three dimensions, by shuffling the image pixels three times using chaotic Arnold map. A downside of these cryptosystems is that they were not concerned with studying and reporting encryption time.

The authors of [13] proposed a cryptosystem which adds DNA encoding to chaos. They performed the permutation, substitution, and diffusion by using an encryption process with two rounds of six steps. The long encryption time of their system makes it not a good choice for real-time applications. Similarly, [14] utilized DNA encoding and crisscross diffusion to design a chaotic medical image encryption scheme with improved resistance to differential attacks.

A combination of 3D image encryption, compression, and non-autonomous Lorenz system was presented in [15]. Two points are noted about their system. Firstly, the encryption time is extremely long because of the employed iterative mechanism. Secondly, their scheme was not tested against differential attacks, which makes us suspect that it may not be immune to such attacks.

The medical image encryption scheme proposed in [16] used a four-dimensional chaotic system for iterative scrambling and bidirectional diffusion and introduced image-dependent key using the SHA-256 hash function. The multi-round process of permutation and diffusion slows down the performance of their scheme considerably.

In [17], the authors introduced a modified version of El-Gamal encryption systems combined with Arnold

transform multi-round to encrypt the medical images. Their cryptosystem decreases the size of the cipher images by using a single elliptic curve point with several image pixels to accelerate the encryption process. Despite this size reduction, the use of multiple rounds costs longer encryption time, and using the same random number for each block exposes the system to hacking. The authors in [18] improved the cryptosystem proposed in [17] with a different random number generator (Mersenne Twister). This modification led to decreasing the encryption time but did not resolve the issue of using an identical random number for encrypting all blocks of the image.

A medical image cryptosystem called MIE-BX is proposed in [19]. MIE-BX performed very fast permutation and diffusion. The authors claimed that their system can perform faster than AES. The authors in [20] reported a weak point in the system proposed in [19], namely its susceptibility to an attack called the PRNG reset attack, in which the attacker can reset the random number generator which leads to generating the same random number for the encryption process. The authors of [20] proposed a non-linear algorithm applied to the permutated image to overcome the reset attack. Unfortunately, the authors did not report any complexity analysis or encryption time results to evaluate the speed of their proposed scheme.

In [21], the authors proposed a medical image encryption generic framework with guarantees on security against various cryptanalysis attacks. The framework uses a PRNG to generate random nonces used for the encryption of each image. The framework was shown to achieve high encryption speeds of about 90 MB/s using Henon map or Baker map. The authors of [22] introduced a novel encryption scheme to secure the transmission of medical images and data in healthcare, particularly addressing the vulnerabilities of traditional digital watermarking methods. This scheme embeds encrypted medical images, physicians' fingerprints, and patient health records into a non-significant image, leveraging a chaotic encryption algorithm based on a permutation key and a hybrid asymmetric cryptography scheme that combines Elliptic Curve Cryptography (ECC) with AES. The proposed approach not only enhances the visual security of encrypted images but also improves the quality of medical image reconstruction, demonstrating significant advancements over existing secure image encryption methodologies in ensuring the integrity, authenticity, and confidentiality of transmitted medical data. Several existing medical image encryption schemes process 12-bit and 16-bit images. In [23], the authors address the critical balance between data security and image quality in healthcare watermarking schemes. Traditional methods often compromise image integrity, leading to security vulnerabilities. To counter this, they propose a novel reversible watermarking methodology, prioritizing both data embedding capacity and image imperceptibility without sacrificing security. This approach uses a uniquely generated key through a random path in a 4×4 block, ensuring robust security and minimal data distortion. The study tests data sizes ranging from 8 KB to 32 KB to evaluate image quality using metrics like PSNR, SSIM, and MSE. The findings demonstrate that their methodology significantly outperforms existing techniques, particularly in average PSNR (49.29), indicating a substantial improvement in embedding capacity and imperceptibility for MRI watermarked images. A 12-bit pixel is padded with zeros to form a 16-bit word, which is then processed by the encryption scheme. The scheme proposed in [2] was also applied to 12-bit medical images. The scheme presented in [12] encrypts 3D medical images with 16-bit pixels but the expected value of the differential analysis metric was not modified correctly to reflect the 16-bit nature of the data. The authors of [19] calculated the expected values of differential analysis metrics, but not the critical intervals for passing the tests.

C. BAKER MAP

The Baker map is a traditional chaotic map that can be used in scrambling an image, which changes pixels positions based on a key. The standard Baker map $\boldsymbol{B}$ splits a square into two rectangles as follows [24]:

$$\boldsymbol{B}(\boldsymbol{i},\boldsymbol{j}) = \begin{cases} \left(2\boldsymbol{i}, \dfrac{\boldsymbol{j}}{2}\right) & 0 \leq \boldsymbol{i} < 0.5 \\ \left(2\boldsymbol{i}-1, \dfrac{\boldsymbol{j}+1}{2}\right) & 0.5 \leq \boldsymbol{i} < 1 \end{cases}$$

As a generalization, the Baker map splits a square into vertical rectangles of different widths based on the key, then maps each rectangle to a horizontal slice of the output square. A discretized version of Baker can map image pixel positions to new output positions in a bijective way. The mapping process starts by splitting a square matrix of $\boldsymbol{H} \times \boldsymbol{H}$ pixels into rectangular slices of varying widths $\boldsymbol{w_k}$, such that each $\boldsymbol{w_k}$ divides $\boldsymbol{H}$. Each resulting slice of size $\boldsymbol{H} \times \boldsymbol{w_k}$ pixels is split into $\boldsymbol{w_k}$ horizontal rectangles of size $\boldsymbol{H_k} \times \boldsymbol{w_k}$ pixels, where $\boldsymbol{H_k} = \boldsymbol{H}/\boldsymbol{w_k}$. The $\boldsymbol{H}$ pixels within each rectangle are then output in column-major order from the bottom up into a corresponding row of the output. The number of input columns preceding the $\boldsymbol{k}$th slice is denoted $\boldsymbol{W_k} = \sum_{t=1}^{k-1} \boldsymbol{w_t}$. Each input pixel at column $\boldsymbol{x}$ and row $\boldsymbol{y}$ from the $\boldsymbol{k}$th slice such that $\boldsymbol{W_{k-1}} \leq \boldsymbol{x} < \boldsymbol{W_k}$ is transposed to output column $\boldsymbol{x'}$ and row $\boldsymbol{y'}$ using the following discretized Baker map formula [24]

$$(\boldsymbol{x'}, \boldsymbol{y'}) = \left((\boldsymbol{x} - \boldsymbol{W_k})\,\boldsymbol{H_k} + \boldsymbol{y}\ \boldsymbol{mod} \boldsymbol{H_k}, \boldsymbol{W_k} + \left\lfloor \frac{\boldsymbol{y}}{\boldsymbol{H_k}} \right\rfloor\right),$$

On the other hand, the Baker map can be used to change the pixel value (substitution) instead of changing its position. Starting from an initial state, $(\boldsymbol{x_0}, \boldsymbol{y_0})$, the process then applies Baker map to compute sequence of $\boldsymbol{L}$ points, where $\boldsymbol{L}$ is the number of image pixels. Each point, $(\boldsymbol{x_n}, \boldsymbol{y_n})$, is calculated from the last point using the following recurrence formula [21].

$$\boldsymbol{x_n} = \begin{cases} \dfrac{\boldsymbol{x_{n-1}}}{\boldsymbol{p}}, & 0 \leq \boldsymbol{x_{n-1}} < \boldsymbol{p} \\ \dfrac{\boldsymbol{x_{n-1}} - \boldsymbol{p}}{1 - \boldsymbol{p}}, & \boldsymbol{p} \leq \boldsymbol{x_{n-1}} < 1 \end{cases} \tag{1}$$

$$y_n = \begin{cases} py_{n-1}, & 0 \le x_{n-1} < p \\ 1-(1-p)y_n, & p \le x_{n-1} < 1 \end{cases} \quad (2)$$

Subsequently, the chaotic sequence $\langle (x_i, y_i) \rangle_{i=1}^{L}$ is transformed into a mask sequence $\langle m_i \rangle_{i=1}^{L}$ of 8-bit elements using the following formula:

$$m_i = \left(2^{24} x_i\right) mod 256 \quad (3)$$

XORing the resulting chaotic mask sequence with plain image pixels is useful for achieving histogram equalization.

D. CRYPTOGRAPHIC SUBSTITUTION BOXES

Substitution boxes are basic component of cryptographic schemes. It works as a function from m-bit input vector to an n-bit output vector. For bijective S-boxes, the size of input and output vectors is the same and the mapping must be invertible. In dynamic S-boxes, the mapping between input and output bit vectors changes dynamically for each encryption instance. A dynamic S-box is called key-dependent if the mapping is determined by a secret key to add an extra layer of confusion to the encryption scheme. Dynamic 8×8 S-boxes have a vast key space of $2^8! \cong 2^{1684}$, which is extended even further by dynamic 12×12 S-boxes to $2^{12}! \cong 2^{43250}$.S-boxes are usually implemented using lookup tables. Therefore, a 12×12 S-box can be stored in 8192 bytes of byte-oriented memory, which has become a negligible cost considering the state-of-the-art in computer architecture.

Several algorithms for constructing dynamic S-boxes appear in literature. The work presented in [25] compares five categories of algorithms for constructing dynamic bijective S-boxes from random sequences, namely, cleansing duplicates, sorting elements, Fisher-Yates shuffle, naïve shuffle, and random composition. The author concludes that the quality of the generated S-box is almost independent of the S-box construction algorithm. Earlier work in [26] showed that the choice of the chaotic map generating the random sequence doesn't affect the properties of the dynamic S-box either.

Although most of the literature is focused on generating 8×8 S-boxes, a few attempts at generating wider S-boxes have been reported. The authors of [27] used heuristic search to evolve bijective S-boxes of various sizes up to 12×12 S-boxes. In [28] the author used an algebraic structure to construct a highly nonlinear 12×12 S-boxes.

III. PROPOSED MODEL

A. SCHEME INITIALIZATION

The proposed scheme uses a PRNG component to generate random nonces that serve as ephemeral encryption keys. The PRNG must be initialized with a secret seed derived from a truly random source. The proposed scheme uses a public-key encryption for sharing the ephemeral encryption keys. To setup a secure communication channel between a sender and a receiver, the receiver uses elliptic curve ElGamal public key scheme, described in [29], to generate a pair of public and private keys, (K_A, K_B). The receiver then shares the public key, K_A, with the sender over the channel.

B. ENCRYPTION PROCESS

The encryption process takes a plain image, I, containing $L = n \times m$ pixels. The plain image pixels are taken in lexicographic order, denoted $\langle I_i \rangle_{i=1}^{L}$. For each plain image, two random nonces, N_S and N_C, are generated to serve as the image encryption keys. Using N_S, a dynamic key-dependent 12×12 S-box, S, is constructed by following the S-box construction algorithm described later in Section III-D. Using N_C, a Baker chaotic map is initialized, run for 512 iterations to increase key sensitivity, and then run for L iterations to generate a 2D chaotic sequence $\left\langle (x_i, y_i) \right\rangle_{i=1}^{L}$ using equations (1) and (2), and convert it to a sequence of 12-bit integer numbers $M = \langle M_i \rangle_{i=1}^{L}$ using the following equation.

$$M_i = \left(2^{24} x_i\right) mod 4096, \quad \forall i \in [L]$$

The sequence M is flipped to obtain M', i.e., $\left\langle M_i' \right\rangle_{i=1}^{L} = \langle M_{L+1-i} \rangle_{i=1}^{L}$.

Each pixel, I_i, of the plain image, I, is encrypted to produce a corresponding cipher pixel, C_i, of the cipher image, C, using the equation.

$$C_i = S\left(M_i' \oplus S\left(M_i \oplus S\left(I_i\right)\right)\right)$$

Using the receiver's public key, K_A, the encryption subkeys, N_S and N_C, are encrypted by the elliptic curve ElGamal cryptosystem [29], into N_S' and N_C', respectively. The encrypted subkeys, N_S' and N_C', are transmitted along with the cipher image C to the receiver. The encryption process is illustrated in Fig. 1.

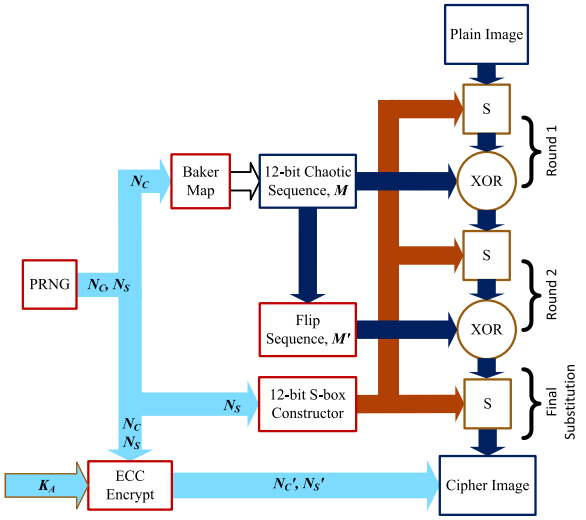

FIGURE 1. Proposed image encryption scheme.

C. DECRYPTION PROCESS

Using the private key, K_B, the decryption process recovers the encryption subkeys, N_S and N_C, from N_S' and N_C' extracted from the received cipher message.

The decryption process replicates steps 3, 4, and 5 of the encryption process to generate the key-dependent S-box, S, the chaotic mask, M, and the flipped chaotic mask M'.

The inverse S-box, S^{-1}, is obtained by calculating:

$$S^{-1}\left(S\left(x\right)\right) = x, \quad \forall x \in \{0, 1, \ldots, 4095\}$$

Each cipher pixel, C_i, of the received cipher image, C, is decrypted using the following equation, to produce a corresponding pixel, I_i, of the plain image, I.

$$I_i = S^{-1}\left(M_i \oplus S^{-1}\left(M_i' \oplus S^{-1}\left(C_i\right)\right)\right)$$

The decryption process is illustrated in Fig. 2.

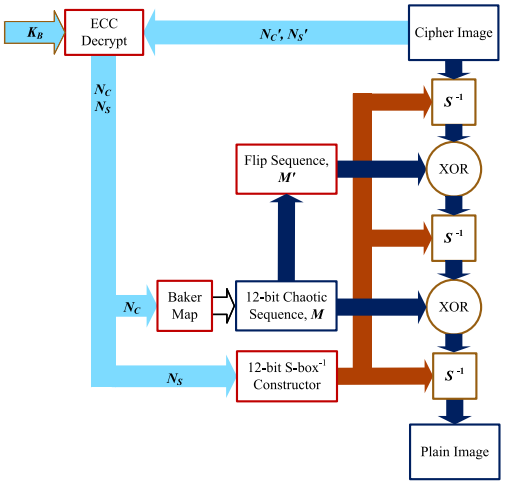

FIGURE 2. Decryption process.

D. DYNAMIC S-BOX CONSTRUCTION ALGORITHM

The proposed key-dependent S-box construction algorithm adapted from [31] combines two very efficient components, namely the Mersenne Twister pseudorandom number generator (MT19937 PRNG), and the Fisher-Yates shuffle algorithm [30]. The PRNG is initialized using a seed computed from the random nonce, N_S. Then the PRNG is queried to generate a pseudorandom sequence of 32-bit integers, which determine the two-round shuffling sequence. Two-round shuffling has the advantage of protecting the S-box against chosen plaintext cryptanalysis attacks as proven in [31].

IV. PERFORMANCE ANALYSIS

In this section, we analyze the security and efficiency of the proposed medical image encryption scheme. A set of three 12-bit medical plain images of size 512 × 512 pixels, shown in Fig. 3, is used for performing the different security tests.

A. STATISTICAL ANALYSIS

Statistical tests indicate the ability of the proposed scheme to resist statistical attacks. These tests include histogram, entropy, and correlation. The entropy of a 12-bit image I of size $N \times M$ pixels can be computed as follows:

$$E\left(I\right) = -\sum_{k=0}^{4095} \frac{f_k}{N \times M} log_2\left(\frac{f_k}{N \times M}\right),$$

where f_k is the frequency of the pixels of image I having a particular color intensity value k. Whereas the entropy of an ideal 8-bit random image is 8, the optimal entropy value of a 12-bit random image should be 12. Table 1 shows the entropy values for the variety of plain images and for their corresponding cipher images, making it evident that *our* scheme almost achieves the optimum value of the random 12-bit image.

TABLE 1. Entropy, histogram, and cross correlation.

Image (12-bit)	Entropy		Enc. Histogram Pass %		Cross Correlation
	Plain	Encrypted	α=0.05	α=0.01	
CT Scan	8.8250	11.9880	94.6%	98.8%	0.992665
MRI_1	10.795	11.9886	93.8%	98.9%	0.967772
MRI_2	10.1326	11.9888	95.6%	99.2%	0.985431

A flat histogram of an image means that each pixel value has the same frequency which is an expected result of good randomness. However, for a 12-bit random image, the histogram has a large dynamic range of levels (2^{12}), getting a visually flat histogram is challenging, due to the small number of pixels that fall within each of the 2^{12} bins. Fig. 3. shows the cipher images generated by the proposed scheme and their corresponding histograms. Although the histograms of the cipher images are more uniform than those of the plain images, it is difficult to judge the quality of the distribution visually.

For a more accurate judgment of the histogram, the Chi-squared (χ^2) test is used to compare the histogram variance of the resulting cipher images to that of perfectly random images. The χ^2 test is computed as follows:

$$\chi^2 = \sum_{k=0}^{4095} \left(f_k - E\right)^2 / E,$$

where f_k is the number of occurrence of pixels with color level equal to k in the cipher image, and $E = N \times M / 4096$ is the expectation of the number of pixels for each gray level in a uniformly random image. The histogram being tested is considered a uniform histogram if the p-value corresponding to the calculated value of χ^2 is greater than the significance level, α. To validate the randomness of cipher images generated by the proposed scheme, the χ^2 test is repeated for 1000 cipher images corresponding to each plain image with varying encryption keys. The results shown in Table 1 indicate that the proposed scheme produces a cipher image with a satisfactory histogram that is statistically indistinguishable from that of a uniformly random image that has 4096 gray levels.

The cross-correlation between the plain and cipher images is another widely used test that indicates the dissimilarity between the two images. In this test, a cross correlation value close to 0 means the two images are fully independent, whereas a value of 1 means linearly dependent images.

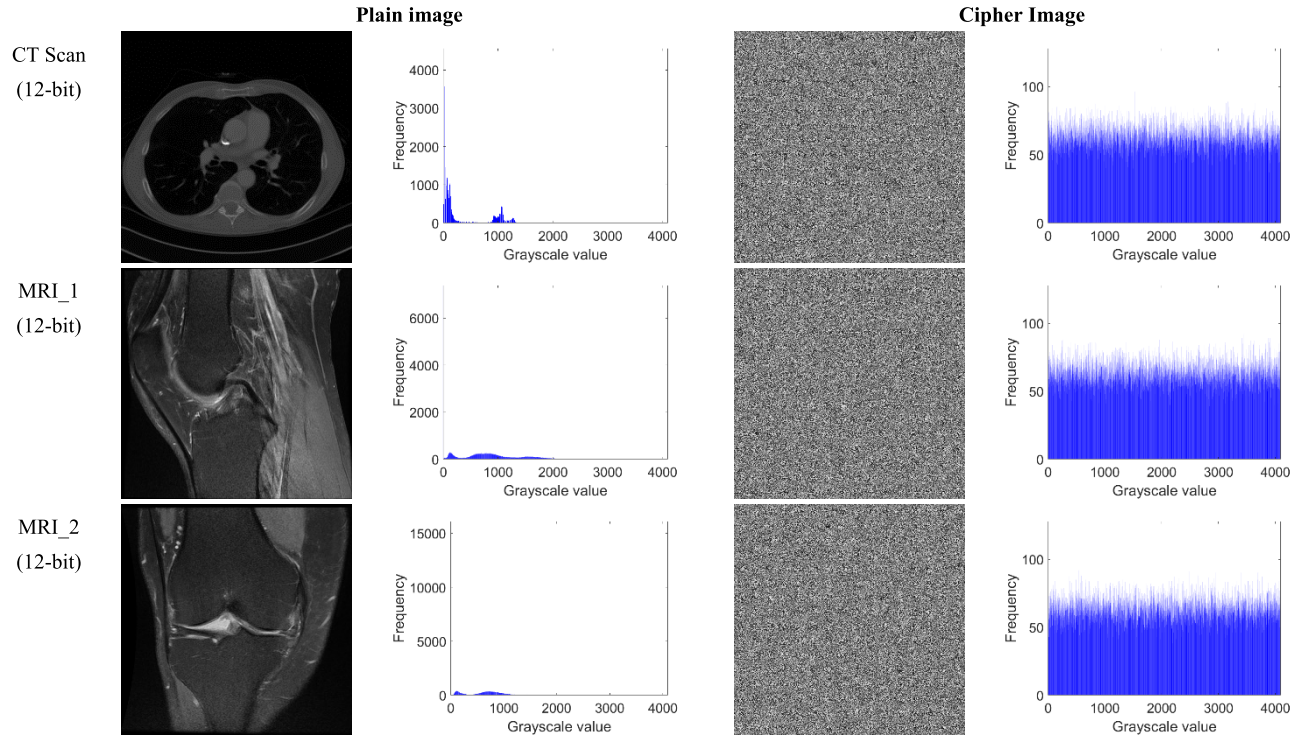

FIGURE 3. Effect of the proposed encryption scheme on image histogram.

Table 1 presents the cross-correlation values between the plain and cipher images, which reveal the proposed scheme success to generate a cipher image completely independent from the corresponding plain image.

Since adjacent pixels of an image are usually highly correlated, the plain image auto-correlation will be almost equal to 1 in all spatial directions (horizontal, vertical, and diagonal). If the proposed scheme can successfully cancel the spatial correlation in all direction, the auto-correlation value of the cipher image should be almost zero. As shown in Table 2, the auto-correlation values of the cipher images are close to zero.

TABLE 2. Spatial autocorrelation.

Image (12-bit)	Plain Image			Encrypted Image		
	H	V	D	H	V	D
CT Scan	0.9926	0.9864	0.9795	0.0013	0.0012	0.0015
MRI_1	0.9677	0.9875	0.9626	0.0007	0.0030	0.0001
MRI_2	0.9854	0.9738	0.9629	0.0013	0.0007	0.0004

B. DIFFERENTIAL ANALYSIS

In differential cryptanalysis, the adversary attempts to infer information about the secret key by observing how slight changes in the input plain image affect the corresponding cipher image. To ensure that the proposed encryption scheme can resist differential attacks, a slight change in the plain image should cause a dramatic change in the cipher image. In more rigorous terms, the difference between two cipher images corresponding to a one-bit change in the plain image should be indistinguishable from a random image. Two common measures of randomness used in differential analysis are the NPCR and UACI metrics. Given a 12-bit grayscale plain image, I, containing $N \times M$ pixels, a single bit change is introduced at a random location to obtain the modified plain image, I'. The corresponding cipher images are denoted C and C', respectively. The NPCR and UACI metrics are calculated using the following equations:

$$NPCR = \sum_{i=1}^{n}\sum_{j=1}^{m} \frac{\delta\left(C_{ij}, C'_{ij}\right)}{N \times M} \times 100\%$$

$$UACI = \sum_{i=1}^{n}\sum_{j=1}^{m} \frac{\left|C_{ij} - C'_{ij}\right|}{N \times M \times 2^{12}} \times 100\%$$

where

$$\delta(a, b) = \begin{cases} 1, & a = b \\ 0, & \text{otherwise} \end{cases}$$

For arbitrary 512×512 random 12-bit grayscale image, the mean and standard deviation of NPCR and UACI are calculated as follows [32].

$$\mu_{NPCR} = 1 - \frac{1}{2^{12}} \cong 99.975586\%$$

$$\sigma_{NPCR} = \sqrt{\frac{1}{512 \times 512}\left(\frac{2^{12}-1}{2^{2\times 12}}\right)} \cong 3.0514 \times 10^{-3}\%$$

$$\mu_{UACI} = \frac{1}{3}\left(1 + \frac{1}{2^{12}}\right) \cong 33.341471\%$$

$$\sigma_{UACI} = \sqrt{\frac{1}{512 \times 512}\frac{\left(2^{12}+1\right)\left(2^{2\times 12}+2\right)}{18\left(2^{12}-1\right)\left(2^{2\times 12}\right)}} \cong 4.6047 \times 10^{-2}\%$$

Table 3 shows the acceptable values for NPCR and UACI randomness tests for 512×512-pixel 12-bit images at different significance levels.

TABLE 3. NPCR and UACI randomness test limits.

Significance	$NPCR_{min}$	$UACI_{min}$	$UACI_{max}$
$\alpha = 0.05$	99.970567	33.251221	33.431721
$\alpha = 0.01$	99.968487	33.222862	33.460080

The results of the NPCR and UACI randomness tests, based on 1000 encryption attempts, are shown in Table 4. The results indicate that our scheme resists differential cryptanalysis.

TABLE 4. Differential analysis and pass rate.

Image (12-bit)	NPCR			UACI		
	mean	Pass rate		mean	Pass rate	
		α=5 %	α=1 %		α=5 %	α=1 %
CT Scan	99.97567	95.1 %	98.9 %	33.353	96.2 %	99.7 %
MRI_1	99.97556	94.7 %	98.6 %	33.331	95.8 %	99.1 %
MRI_2	99.97562	94.3 %	99.1 %	33.347	95.4 %	99.3 %

C. KEY SENSITIVITY

An encryption scheme should be highly sensitive to changes in the encryption key to thwart related-key attacks. In this type of attacks, two keys which are closely related are used for encrypting the same image to analyze the effect of each bit of the key on the encryption process. A slight change in the encryption key of a secure encryption scheme should produce a change in the cipher image that is indistinguishable from a random image. To test the key sensitivity of the proposed encryption scheme, we apply the NPCR and UACI randomness tests when the least significant bit of each of the encryption keys, N_S or N_C is changed. The test is based on 1000 encryption attempts and the pass rates are reported in Table 5.

The proposed scheme is highly sensitive to changes in the S-box construction key, N_S.

Similarly, Table 6 indicates that the proposed system is just as sensitive to the Baker map key, N_C

TABLE 5. S-Box-key sensitivity analysis.

Image (12-bit)	k-NPCR			k-UACI		
	mean	Pass rate		mean	Pass rate	
		α=5 %	α=1 %		α=5 %	α=1 %
CT Scan	99.975507	94.5 %	98.5 %	33.3405	94.0 %	98.9 %
MRI_1	99.975542	94.8 %	99.1 %	33.3399	96.3 %	99.1 %
MRI_2	99.975541	94.6 %	98.6 %	33.3398	95.2 %	99.5 %

TABLE 6. Chaotic-map-key sensitivity analysis.

Image (12-bit)	k-NPCR			k-UACI		
	mean	Pass rate		mean	Pass rate	
		α=5 %	α=1 %		α=5 %	α=1 %
CT Scan	99.975573	95.2 %	98.3 %	33.3398	94.2 %	99.3 %
MRI_1	99.975640	95.9 %	99.1 %	33.3431	94.2 %	99.0 %
MRI_2	99.975624	95.5 %	99.4 %	33.3422	94.8 %	98.9 %

D. RESISTANCE TO CHOSEN PLAINTEXT ATTACKS

To resist chosen-plaintext attacks (CPA), a PRNG is used to generate two random nonces, N_S and N_C, for each image being encrypted. N_S and N_C serve as encryption subkeys to initialize the MT19937 PRNG for dynamic S-box construction and the Baker map for chaotic mask generation. Each invocation of the encryption process generates a one-time-use S-box and chaotic mask. Therefore, the potential damage of any cryptanalysis attempt that could discover the chaotic mask or the S-box or even go further to reveal the corresponding encryption subkeys, N_S and N_C, is limited to the attacked image alone. Furthermore, the adopted two-round S-box shuffling procedure has the advantage of protecting the S-box against chosen-plaintext cryptanalysis attacks as proven in [31], which adds another obstacle to chosen-plaintext attacks against our scheme.

E. KEY SPACE ANALYSIS

Although the proposed dynamic 12 × 12 bijective S-boxes used by the proposed encryption scheme allows a key space of $2^{12}! \cong 2^{43250}$, the actual key space of the S-box is determined by the size of the key, N_S, allowed by the S-box construction algorithm. The proposed dynamic S-Box construction algorithm based on Mersenne Twister allows a key of size up to 19937 bits.

Similarly, the key space of the proposed encryption scheme is determined by its most vulnerable component, which is the public key encryption stage used for exchanging the image-dependent shared encryption keys, N_S and N_C. The elliptic curve ElGamal cryptosystem guarantees a higher

security per key bit compared to its RSA counterpart [33]. To guarantee security against elliptic curve discrete logarithm cryptanalysis, the size of the public key, K_A, must be sufficiently large, for instance by utilizing a standard 256-bit Curve25519.

F. SPEED ANALYSIS

Efficiency is a major design objective of image encryption schemes. The 12-bit data path feature of the proposed image encryption scheme enables faster encryption of 12-bit medical images. To demonstrate the advantage of the 12-bit data path over the traditional 8-bit data path, 12-bit medical images of different sizes are encrypted using the proposed scheme using 8-bit and 12-bit data paths. The scheme was coded in Java and executed on Java virtual machine version 1.8 on a Core-i7-8565U processor with base frequency of 1.8 GHz and 12GB of RAM.

Table 7 shows the encryption speed up obtained by using a 12-bit data path. The speed up is defined by:

$$\text{Speed up} = \frac{\text{Encryption time using } 8-\text{bit data path}}{\text{Encryption time using 12-bit data path}}$$

When a 12-bit image is encrypted by an 8-bit data path, each pixel is zero-extended to 16 bits and treated as two 8-bit words. The results in Table 7 indicate that a 12-bit data path increases the encryption speed by at least 44% for images of size 1024×1024 pixels.

TABLE 7. Encryption speed for 12-bit images.

Image Size (12-bit)	Encryption time (ms)		Speed up
	8-bit data path	12-bit data path	
256×256	0.9206	0.4814	1.91
512×512	2.3898	1.4754	1.62
1024×1024	8.4761	5.8892	1.44

Therefore, our scheme operating in 12-bit data path mode exhibits superior speed in encrypting 12-bit medical images, which have a higher dynamic range that facilitates more accurate medical diagnosis. Moreover, the results in Table 8 show that the proposed 12-bit data path can handle 8-bit images faster than the 8-bit data path. To achieve this speed, our scheme packs every three 8-bit pixels into two 12-bit words.

TABLE 8. Encryption speed for 8-bit images.

Image Size (8-bit)	Encryption time (ms)		Speed up
	8-bit data path	12-bit data path	
256×256	0.8414	0.5009	1.68
512×512	1.7052	1.4792	1.15
1024×1024	5.6649	5.5782	1.02

V. JUSTIFICATION FOR PROPOSED SCHEME DESIGN

The proposed scheme includes four effective design elements that facilitate the achievement of its security objectives with high computational efficiency. Namely, the scheme includes 1) a 12-bit key-dependent S-box, 2) two rounds of S-box substitution and XOR masking, 3) chaotic mask flipping, and 4) a final round of S-box substitution. To justify these design elements, we test a variety of potential configurations and measure S-box key sensitivity to determine which configurations are sufficiently secure. Subsequently, we compare the encryption throughput of proven configurations and choose the most efficient configuration. A configuration is determined by four factors:

- The number of S-box-XOR rounds which is varied between 1 and 3.
- The mode used for generating the XOR mask for each round. The first mode uses the same chaotic mask for all rounds. The second mode generates a different mask for each round. The third mode flips the first-round mask and use the flipped mask for the second round.
- The key-dependent S-box can either be an 8×8 S-box or a 12×12 S-box.
- The final stage of S-box substitution can be implemented or removed.

Table 9 summarizes the key sensitivity and throughput results for each of the 4×7 configurations. The encryption key sensitivity is tested with respect to changes in the S-box key using the UACI and NPCR randomness tests with $\alpha = 0.01$ significance level. The test is repeated 100 times for each configuration and the configuration is said to pass the key sensitivity test when both the UACI and the NPCR tests are passed at least 96 times. Otherwise, the configuration is considered to fail the key sensitivity criterion. The results

TABLE 9. Throughput (MB/s) with various design elements.

		8×8 S-box		12×12 S-box	
	Final S-box	No	Yes	No	Yes
1 Round	N/A	×	×	×	×
2 Rounds	Same Mask	×	×	×	×
	Different Mask	×	×	×	200
	Flipped Mask	×	×	×	**300**
3 Rounds	Same Mask	×	×	×	×
	Different Mask	91	90	134	133
	Flipped Mask	×	×	275	272

× The configuration fails the UACI or the NPCR key sensitivity tests (pass percentage < 96% at $\alpha = 0.01$)

In the remainder of this section, we investigate the effect of individual design choices on security and efficiency.

in Table 9 show that only 8 configurations pass the key sensitivity tests, in which case its encryption throughput is reported. The configuration with the highest throughput uses 12-bit S-box in two rounds plus a final substitution with mask flipping, thus justifying the configuration proposed in Fig 1.

In the remainder of this section, we investigate the effect of individual design choices on security and efficiency.

A. THE EFFECT OF THE NUMBER OF ROUNDS

Existing chaotic encryption schemes which use a chaotic sequence to mask the plain image through an XOR often use key-dependent dynamic S-boxes to increase the key space and introduce further confusion into the encryption process. The schemes presented in [9], [34], and [35] use one S-box substitution in addition to the XOR operation. Alternatively, the scheme in [21] use two dynamic S-box substitutions: one before the XOR operation and another afterwards. The proposed scheme performs two rounds of S-box substitutions and XOR masking in addition to a final substitution. To avoid related key attacks, such encryption schemes should pass the key sensitivity test with respect to the dynamic S-box key. To isolate the effect of the number of the rounds, the remaining configuration parameters are fixed. Namely, we use a 12 × 12 S-box, with mask flipping and include a final substitution. The results in Table 10 show the effect of the number of rounds of S-box substitutions on the sensitivity tests with respect to the S-box key. Clearly, one round of S-box substitution is potentially vulnerable to related key attacks, whereas two or more rounds are secure. However, applying two or more rounds reduces encryption throughput. Therefore, the proposed scheme applies two rounds of substitution.

TABLE 10. S-box key sensitivity for different number of rounds.

Number of rounds	UACI pass% ($\alpha = 0.01$)	NPCR pass% ($\alpha = 0.01$)	Throughput (MB/s)
1	28.0	73.8	329
2 (proposed)	**99.2**	**99.1**	**300**
3	98.8	98.7	261

B. EFFECT OF MASK FLIPPING

When using 2 rounds, the two masks must be statistically independent. Instead of generating two different masks, we can exploit the low autocorrelation of the mask by reusing a flipped or shifted version of the mask in the second round. As shown in Table 11, mask flipping improved UACI test results from 25% to 99.2%. Moreover, mask flipping achieves a 150% increase in throughput in comparison to using a different mask for the second round. Therefore, mask flipping improves key sensitivity significantly while avoiding the extra cost of generating a different mask for the second round.

TABLE 11. Effect of mask flipping on security and throughput.

Mask	UACI pass% ($\alpha = 0.01$)	NPCR pass% ($\alpha = 0.01$)	Throughput (MB/s)
Same mask	25.0	69.6	-*
Different mask	99.3	98.5	200
Flipped mask (proposed)	**99.2**	**99.1**	**300**

* *The throughput is intentionally omitted since this case is insecure.*

C. EFFECT OF FINAL SUBSTITUTION

When using 2 rounds, the presence of the final substitution significantly affects the sensitivity to the S-box key avoiding the need for an extra round. The results in Table 12. demonstrate the significant improvement in sensitivity to the S-box key due to adding a final substitution after the second round. Adding a third round would have also fixed the key sensitivity issue, but at a higher toll on the throughput.

TABLE 12. Effect of final substitution on S-box key sensitivity.

Rounds	Final Substitution	UACI pass% ($\alpha = 0.01$)	NPCR pass% ($\alpha = 0.01$)	Throug h-put
2 Rounds	No	32.5	73.3	-
2 Rounds (proposed)	**Yes**	**99.2**	**99.1**	**300 MB/s**
3 Rounds	No	99.2	98.5	264 MB/s
3 Rounds	Yes	98.3	98.9	261 MB/s

D. EFFECT OF 12 × 12 S-BOX

The use of the proposed 12 × 12 S-box improves the sensitivity of the scheme to the S-box key when the number of rounds is set to two with mask flipping engaged. Under these circumstances the 8×8 S-box counterpart fails the UACI test at $\alpha = 0.01$ as shown in Table 13. A scheme based on 8×8 S-box only passes the UACI test after the third round provided that different masks are applied at each round. Consequently, the proposed 12-bit encryption scheme performs three times faster than an 8-bit scheme of similar security.

VI. COMPARISON WITH OTHER SCHEMES

To highlight the advantages of the proposed medical image encryption scheme, we compare its security and efficiency

TABLE 13. S-box key sensitivity with different S-box size.

S-box Size	# Rounds	Mask mode	UACI	NPCR	Throughput
8×8	2	Flipped	89.4 %	97.8 %	-
12×12 (proposed)	**2**	**Flipped**	**99.2 %**	**99.1 %**	**300 MB/s**
8×8	3	Different	99.2 %	98.7 %	102 MB/s

analysis to similar existing schemes. Unless otherwise stated, all 8-bit and 12-bit images used in the subsequent analysis are of size 512 × 512 pixels.

Table 14 shows the results of the entropy and spatial correlation properties of the cipher images generated by the proposed scheme in comparison to other schemes. The results indicate that the proposed scheme produces cipher images competitively close to the values expected of a random image.

TABLE 14. Statistical analysis for 8-bit cipher images.

Scheme	Entropy	Correlation		
		H	V	D
Proposed	**7.9992**	**0.000779**	**0.003016**	**0.000136**
Ref. [11], 2015	-	0.0012	0.0003	0.0087
Ref. [12], 2020	-	0.00500	0.00057	0.00017
Ref. [13], 2019	7.9993	0.0025	0.0028	0.0027
Ref. [15], 2018	-	0.0002	0.0006	0.0003
Ref. [16], 2019	7.9993	0.0002	0.0024	0.0013
Ref. [17], 2017	7.9993	0.0008	0.0016	0.0043
Ref. [18], 2019	7.9999	0.01317	0.00136	0.00224
Ref. [20], 2020	7.9973	0.0026	0.0051	0.0264
Ref. [21], 2020	7.9992	0.0100	0.0035	0.0165
Ref. [36], 2021	7.999	0.00215	0.00595	0.00412
Ref. [2], 2017	7.9995	0.0090	0.0080	0.0083
Ref. [23], 2016	7.995	0.00593	-	-

The differential analysis results for the proposed scheme are compared to those of other schemes in Table 15. The results indicate that the proposed scheme is highly immune to differential cryptanalysis.

TABLE 15. Differential analysis for 8-bit and 12-bit images.

Scheme	NPCR		UACI	
	8-bit	12-bit	8-bit	12-bit
Proposed	**99.6082**	**99.9755**	**33.4657**	**33.3311**
Ref. [2]	99.4	99.96	–	33.39
Ref. [23]	99.43	99.996	33.7	23.603
Ref. [11]	99.6082	-	33.4682	-
Ref. [13]	99.6173	-	33.4755	-
Ref. [16]	99.61	-	33.38	-
Ref. [17]	99.62	-	33.41	-
Ref. [18]	99.6073	-	33.4715	-
Ref. [20]	99.6100	-	33.4590	-
Ref. [21]	99.6098	-	33.4603	-
Ref. [37]	99.723	-	36.568	-
Ref.[36]	99.68	-	33.66	-

Table 16 presents a comparison of key-sensitivity analysis results. The proposed scheme passes the NPCR and UACI tests with high probability.

TABLE 16. key-sensitivity analysis comparison.

Scheme	k-NPCR		k-UACI	
	8-bit Image	12-bit Image	8-bit Image	12-bit Image
Proposed	**99.6083**	**99.9757**	**33.4562**	**33.3435**
Ref. [16]	99.61	-	-	-
Ref. [20]	99.6127	-	-	-
Ref. [21]	99.6124	-	33.4375	-

TABLE 17. 12-bit image encryption time comparison.

Scheme	Image size		
	512×512	1024×1024	512×512×100 (3D)
	Encryption time (ms)		
Proposed	**2.16**	**8.5**	**217**
Ref. [21]	5.6	22.2	529
Ref. [2]*	7.6×4=30.4	375.4/5=75.1	-

**Results given in Ref* [2] *were for 256x256 and 2570x2048 12-bit images, from which the listed encryption times were estimated.*

To facilitate the comparison of the proposed scheme with related schemes, we used the same test environment used in [Ref. 21], i.e., Java virtual machine version 1.8 on a 3.6GHz quad-core Intel®Core™i7-4790 with 32GB RAM.

In **Table 17**, we compare the encryption time of 12-bit image. As the results show, the proposed scheme reduced the encryption time of a 512 × 512-pixel 12-bit image from 5.6 ms down to 2.16 ms. For the other images, the proposed scheme consistently saves more than half of the encryption time.

VII. CONCLUSION

In this paper, we proposed a 12-bit architecture for medical image encryption based on a 12 × 12 dynamic key-dependent S-box. The proposed scheme handles 12-bit medical images with high efficiency using the dynamic S-box for substitution and a Baker chaotic map for diffusion. We investigated 28 potential configurations and concluded that the best configuration that satisfies all security requirements efficiently consists of two rounds of substitution-diffusion with mask-flipping followed by a final substitution.

Our experiments also showed that 12 × 12 key-dependent S-boxes are more immune to related-key attacks compared to 8 × 8 S-boxes. The proposed scheme passes key-sensitivity tests where the corresponding configuration based on 8 × 8 S-boxes fails. The proposed scheme achieves a 300 MB/s encryption throughput for encrypting 12-bit encoded DICOM medical images, which is three times faster than the equivalently secure 8 × 8-based configuration.

In addition to its superior efficiency in handling 12-bit images, the proposed scheme still handles 8-bit images slightly more efficiently than its counterparts with an 8-bit data path. A crucial design decision that enabled the proposed scheme to reap the performance benefits of the 12 × 12 S-box is the use of the extremely efficient Fisher-Yates shuffle and Mersenne twister PRNG to construct a dynamic 12 × 12 S-box in 0.1 ms which is negligible with respect to the image encryption time.

The proposed scheme passes all the security tests in electronic code book (ECB) mode without the need for chaining. This enables straightforward parallelization of the scheme once the Baker map is replaced by a parallelizable chaotic map such as the EC-based map found in [35]. Parallelization will enable the proposed scheme to take advantage of readily available parallel processing capabilities such as multicore and multithreading processors available on modern computing platforms.

CONFLICT OF INTEREST

The authors declare that there are no conflicts of interest regarding the publication of this study.

DATA AVAILABILITY STATEMENT

The Dataset used in the analysis of the encryption scheme is publicly available in the following link https://dicomlibrary.com/

REFERENCES

[1] DICOM Standards Committee. (2021). *DICOM PS3.5 2021e—Data Structures and Encoding*. Accessed: Nov. 30, 2023. [Online]. Available: https://dicom.nema.org/medical/dicom/current/output/html/part05.html

[2] M. Boussif, N. Aloui, and A. Cherif, "Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition," *IET Image Process.*, vol. 11, no. 11, pp. 1020–1026, Nov. 2017, doi: 10.1049/iet-ipr.2017.0229.

[3] K. Kumar, S. Roy, U. Rawat, and S. Malhotra, "IEHC: An efficient image encryption technique using hybrid chaotic map," *Chaos, Solitons Fractals*, vol. 158, May 2022, Art. no. 111994, doi: 10.1016/j.chaos.2022.111994.

[4] E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via ZigBee channels," *Chaos, Solitons Fractals*, vol. 133, Apr. 2020, Art. no. 109646, doi: 10.1016/j.chaos.2020.109646.

[5] S. Beg, F. Baig, Y. Hameed, A. Anjum, and A. Khan, "Thermal image encryption based on laser diode feedback and 2D logistic chaotic map," *Multimedia Tools Appl.*, vol. 81, no. 18, pp. 26403–26423, Jul. 2022, doi: 10.1007/s11042-022-12724-3.

[6] N. Iqbal, M. Hanif, Z. U. Rehman, and M. Zohaib, "On the novel image encryption based on chaotic system and DNA computing," *Multimedia Tools Appl.*, vol. 81, no. 6, pp. 8107–8137, Mar. 2022, doi: 10.1007/s11042-022-11912-5.

[7] M. Z. Talhaoui and X. Wang, "A new fractional one dimensional chaotic map and its application in high-speed image encryption," *Inf. Sci.*, vol. 550, pp. 13–26, Mar. 2021, doi: 10.1016/j.ins.2020.10.048.

[8] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 2753–2772, Jan. 2021, doi: 10.1007/s11042-020-09648-1.

[9] T. A. Al-Maadeed, I. Hussain, A. Anees, and M. T. Mustafa, "A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes," *Multimedia Tools Appl.*, vol. 80, pp. 24801–24822, Apr. 2021, doi: 10.1007/s11042-021-10695-5.

[10] F. S. Hasan and M. A. Saffo, "FPGA hardware co-simulation of image encryption using stream cipher based on chaotic maps," *Sens. Imag.*, vol. 21, no. 1, pp. 1–22, Dec. 2020, doi: 10.1007/s11220-020-00301-7.

[11] J. B. Lima, F. Madeiro, and F. J. R. Sales, "Encryption of medical images based on the cosine number transform," *Signal Process., Image Commun.*, vol. 35, pp. 1–8, Jul. 2015, doi: 10.1016/j.image.2015.03.005.

[12] V. S. Lima, F. Madeiro, and J. B. Lima, "Encryption of 3D medical images based on a novel multiparameter cosine number transform," *Comput. Biol. Med.*, vol. 121, Jun. 2020, Art. no. 103772, doi: 10.1016/j.compbiomed.2020.103772.

[13] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[14] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools Appl.*, vol. 81, no. 5, pp. 7253–7270, Feb. 2022, doi: 10.1007/s11042-021-11812-0.

[15] Q. Wang, M. Wei, X. Chen, and Z. Miao, "Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 1715–1734, Jan. 2018, doi: 10.1007/s11042-017-4349-y.

[16] X. Chai, J. Zhang, Z. Gan, and Y. Zhang, "Medical image encryption algorithm based on Latin square and memristive chaotic system," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 35419–35453, Dec. 2019, doi: 10.1007/s11042-019-08168-x.

[17] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017, doi: 10.1016/j.ijleo.2017.08.028.

[18] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *J. Inf. Secur. Appl.*, vol. 49, Dec. 2019, Art. no. 102398, doi: 10.1016/j.jisa.2019.102398.

[19] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018, doi: 10.1016/j.sigpro.2017.10.004.

[20] Y. Chen, C. Tang, and R. Ye, "Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 167, Feb. 2020, Art. no. 107286, doi: 10.1016/j.sigpro.2019.107286.

[21] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad, M. S. Hossain, and A. M. Abbas, "Framework for efficient medical image encryption using dynamic S-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020, doi: 10.1109/ACCESS.2020.3020746.

[22] F. Castro, D. Impedovo, and G. Pirlo, "A medical image encryption scheme for secure fingerprint-based authenticated transmission," *Appl. Sci.*, vol. 13, no. 10, p. 6099, May 2023.
[23] S. Kanwal, F. Tao, A. Almogren, A. Ur Rehman, R. Taj, and A. Radwan, "A robust data hiding reversible technique for improving the security in e-Health care system," *Comput. Model. Eng. Sci.*, vol. 134, no. 1, pp. 201–219, 2023.
[24] F. Pichler and J. Scharinger, "Finite dimensional generalized baker dynamical systems for cryptographic applications," in *Computer Aided Systems Theory—EUROCAST* (Lecture Notes in Computer Science), vol. 1030, 1st ed. Berlin, Germany: Springer, 1996, pp. 465–476. [Online]. Available: http://link.springer.com/content/pdf/10.1007/BFb0034782.pdf
[25] S. Ibrahim, "Performance analysis of dynamic bijective S-box construction algorithms," in *Proc. Nat. Comput. Colleges Conf. (NCCC)*, Mar. 2021, pp. 1–4, doi: 10.1109/NCCC49330.2021.9428859.
[26] F. Özkaynak, "On the effect of chaotic system in performance characteristics of chaos based S-box designs," *Phys. A, Stat. Mech. Appl.*, vol. 550, Jul. 2020, Art. no. 124072, doi: 10.1016/j.physa.2019.124072.
[27] S. Picek, R. Santana, and D. Jakobovic, "Maximal nonlinearity in balanced Boolean functions with even number of inputs, revisited," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Jul. 2016, pp. 3222–3229, doi: 10.1109/CEC.2016.7744197.
[28] T. Ul Haq and T. Shah, "12 × 12 S-box design and its application to RGB image encryption," *Optik*, vol. 217, Sep. 2020, Art. no. 164922, doi: 10.1016/j.ijleo.2020.164922.
[29] A. Menezes, *Elliptic Curve Public Key Cryptosystems*. New York, NY, USA: Springer, 1993, doi: 10.1007/978-1-4615-3198-2.
[30] S. Ibrahim and A. M. Abbas, "Efficient key-dependent dynamic S-boxes based on permutated elliptic curves," *Inf. Sci.*, vol. 558, pp. 246–264, May 2021, doi: 10.1016/j.ins.2021.01.014.
[31] F. P. Miller, A. F. Vandome, and M. B. John, *Fisher–Yates Shuffle*. Saarbrücken, Germany: VDM Publishing, 2010.
[32] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J.*, vol. 2, no. 4, pp. 31–38, 2011.
[33] R. Harkanson and Y. Kim, "Applications of elliptic curve cryptography: A light introduction to elliptic curves and a survey of their applications," in *Proc. 12th Annu. Conf. Cyber Inf. Secur. Res.*, Apr. 2017, pp. 1–7, doi: 10.1145/3064814.3064818.
[34] S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using Henon map, dynamic S-boxes and elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 194289–194302, 2020, doi: 10.1109/ACCESS.2020.3032403.
[35] A. M. Abbas, A. A. Alharbi, and S. Ibrahim, "A novel parallelizable chaotic image encryption scheme based on elliptic curves," *IEEE Access*, vol. 9, pp. 54978–54991, 2021, doi: 10.1109/ACCESS.2021.3068931.
[36] I. B. Parlak, *A New Method for Medical Image Archival Based on Chaotic Maps*, vol. 58. Singapore: Springer, 2021, doi: 10.1007/978-981-15-8049-9_66.
[37] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A robust chaos-based technique for medical image encryption," *IEEE Access*, vol. 10, pp. 244–257, 2022, doi: 10.1109/ACCESS.2021.3138718.

SALEH IBRAHIM received the B.Sc. and M.Sc. degrees in computer engineering from Cairo University, Egypt, in 2000 and 2004, respectively, and the Ph.D. degree in computer science and engineering from the University of Connecticut, USA, in 2010. He has been an Associate Professor with the Computer Engineering Department, Cairo University, since 2011. He is currently an Assistant Professor with the Electrical Engineering Department, Taif University, Saudi Arabia. He has published several research papers in high-impact journals and international conferences. His current research interests include information security and computer networks.

ALAA M. ABBAS received the Ph.D. degree from Menoufia University, Egypt, in 2008. He is currently a Professor with the Department of Electronics and Electrical Communications Engineering, Menoufia University, and an Assistant Professor with the Electrical Engineering Department, Taif University. His research expertise spans image processing, watermarking, image encryption, and cryptography, contributing significantly to these fields in the academic community.

AYMAN A. ALHARBI received the B.Sc. degree from Umm Al-Qura University, Saudi Arabia, in 2006, and the M.Sc. and Ph.D. degrees in computer science and engineering from the University of Connecticut in 2012 and 2015, respectively. He is an accomplished academic and researcher with a distinguished background in computer science and engineering. Throughout his academic journey, he has demonstrated leadership capabilities by serving as the Head of the Computer Engineering Department. His commitment to academic excellence extended to administrative roles, as he took on the position of Vice-Principal of the Department of Investment at Umm Al-Qura University. Currently, he holds the position of an Associate Professor with Umm Al-Qura University. His multifaceted background, combining academic leadership, administrative roles, and research contributions, underscores his commitment to advancing knowledge in computer science and engineering, making him a notable figure in the academic community.

MARWAN ALI ALBAHAR received the B.S. degree in computer science from King Faisal University, Saudi Arabia, in 2011, the M.Sc. degree (Hons.) in computer science from Frostburg State University, USA, in 2015, and the Ph.D. degree from the University of Eastern Finland, in 2018. He has been involved within the information security field for the last 3+. He is a Senior Information Security, Privacy, and Risk Management Professional with a solid technical background and a highly analytical mind. His main research interests include computer networks and security, cybersecurity, and artificial intelligence.