IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 9, 2020, accepted August 27, 2020, date of publication August 31, 2020, date of current version September 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3020746

Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps

SALEH IBRAHIM[1,2], HESHAM ALHUMYANI[3], MEHEDI MASUD[3], (Senior Member, IEEE), SULTAN S. ALSHAMRANI[3], OMAR CHEIKHROUHOU[3], GHULAM MUHAMMAD[4], (Senior Member, IEEE), M. SHAMIM HOSSAIN[5], (Senior Member, IEEE), AND ALAA M. ABBAS[1,6]

[1]Department of Electrical Engineering, College of Engineering, Taif University, Al-Hawiya 21974, Saudi Arabia
[2]Computer Engineering Department, Faculty of Engineering, Cairo University, Giza 12613, Egypt
[3]College of Computer and Information Technology, Taif University, Al-Hawiya 21974, Saudi Arabia
[4]Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[5]Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[6]Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

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

This study was funded by the Deanship of Scientific Research, Taif University, Saudi Arabia, Research Project number: 1-440-6146.

ABSTRACT Protecting patient privacy and medical records is a legal requirement. Traditional encryption methods fall short of handling the large volume of medical image data and their peculiar statistical properties. In this paper, we propose a generic medical image encryption framework based on a novel arrangement of two very efficient constructs, dynamic substitution boxes (S-boxes) and chaotic maps. The arrangement of S-box substitution before and after chaotic substitution is shown to successfully resist chosen plaintext and chosen ciphertext attacks. Special precautions are taken to fend off the reset attack against pseudorandom number generators. We show how to implement the generic framework using any key-dependent dynamic S-box construction method and any chaotic map. Experimental results show that the proposed framework successfully passes all security tests regardless of the chaotic map used for implementation. Based on speed analysis, we recommend the use of the classical Baker map or Henon map to achieve encryption throughput approaching 90 MB/s on a modern PC without hardware acceleration.

INDEX TERMS Bijective substitution box, chaotic map, image encryption.

I. INTRODUCTION

The rapid development in networking and communication technology has led to significant advancement in multimedia and digital image communication. Medical images are important for assisting medical crews through diagnosis. Computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, and X-ray, provide a visual representation of body organs and tissue to help diagnosis and treatment planning. This valuable information includes the physical characteristics of the internal body organs such as size, shape, intensity, and position. With the global growth interest in patient records, all these important data including medical images are stored in Picture-and-Communication Servers. Moreover, many healthcare providers may need to exchange these records using convenient public networks to have access to the patients' health history. Medical images contain confidential information about patient health conditions. Therefore, there is a need to protect and secure patients' privacy when using storage and communication technologies with various applications platforms. As a matter of fact, medical images can be vulnerable to security threats including unauthorized data access and tampering. Encryption schemes are usually employed to protect stored and communicated images against these threats.

In addition to the high spatial correlation, medical images are characterized by their large volume. High resolution imaging and 3D imaging produce large volumes of data per second. Image data need to be encrypted in real time before storage or transmission. Therefore, medical images require more efficient encryption algorithms capable of handling high data transmission rates. The performance of recent medical image encryption schemes, such as [1]–[8] and generic image encryption schemes such as [9], [10] fall short of achieving real-time encryption speed.

The associate editor coordinating the review of this manuscript and approving it for publication was Giacomo Verticale.

In this paper, we take advantage of two of the most efficient encryption constructs, S-boxes and chaotic maps to propose a generic framework for medical image encryption. The proposed framework combines the desirable statistical properties and diffusion of chaotic maps and the confusion power of dynamic key-dependent S-boxes.

The special arrangement of S-box substitution before and after masking with the chaotic key stream is carefully designed to fend off chosen plaintext and chosen ciphertext attacks.

The proposed framework is especially designed to resist the very powerful PRNG-reset attack, to which most existing image encryption schemes are vulnerable. We provide detailed security analysis of the framework applicable to any chaotic map or dynamic S-box construction method.

Moreover, we demonstrate the applicability of the proposed framework to any chaotic map by studying the security and speed performance of the framework with a variety of classical and modern chaotic maps. Results show that the proposed framework achieves stronger security level and enhanced speed compared to existing medical image encryption schemes. We also show how the proposed framework can be easily adapted to take advantage of future efficient chaotic maps and key-dependent S-box construction methods.

The rest of the paper is organized as follows: Section 2 surveys existing medical image encryption schemes and covers in brief the necessary background and related work on dynamic key-dependent S-box construction techniques and image encryption schemes using chaotic maps. Section 3 describes the proposed image encryption framework and presents an implementation of the proposed framework using a new key-dependent S-box construction method. Section 4 evaluates the performance of the proposed image encryption framework using a variety of chaotic maps. Section 5 highlights the advantages of the proposed framework in comparison to related medical image encryption schemes. Finally, concluding remarks are drawn in Section 6.

II. BACKGROUND AND RELATED WORK

In this section, we present necessary background on the uses of dynamic key-dependent S-boxes and chaotic maps in image encryption schemes and review related medical image encryption schemes proposed in literature.

A. DYNAMIC KEY-DEPENDENT S-BOXES

An S-box can be viewed as a function $S : \{0, 1\}^m \rightarrow \{0, 1\}^n$, which substitutes m input bits with n output bits. S-boxes are used in encryption schemes as a simple and efficient way to introduce nonlinearity. A bijective S-box is an invertible $n \times n$ S-box. A dynamic S-box is a cryptographic block, with a variable substitution function that can be changed dynamically. If the substitution function can be controlled by a parameter, the parameter is called a key and the resulting dynamic S-box is called a key-dependent S-box.

Several key-dependent S-box construction methods can be found in literature. In [11], dynamic S-boxes are constructed by composing a random sequence of static S-boxes controlled by a chaotic map. In [12] a discrete chaotic system was proposed to drive the functional composition sequence, which is encoded into a key using Lehmer's code. The authors of [13], proposed a key-dependent S-box construction based on a complete order defined on the points of finite elliptic curves. The authors of [14] used a linear fractional transformation with randomized coefficients to transform an initial static S-box to a key-dependent dynamic S-box.

B. CHAOTIC SYSTEMS

Chaotic systems are dynamic systems that are highly sensitive to initial conditions and thus are ideal candidates for generating cryptographic pseudorandom sequences.

Chaotic sequences such as Henon map, Baker map, logistic map, and Arnold cat map, have been used in many encryption algorithms found in literature [6], [15]–[17]. There are several ways in which chaotic maps can be used in an image encryption scheme. Namely, chaotic sequences can control a scrambling process, a dynamic S-box construction, or a pixel value substitution using XOR or modular addition operations.

New chaotic maps with improved properties continue to be proposed in literature. In [18], a new 2D sine logistic modulation map is presented with wider chaotic range than the classical sine and logistic chaotic maps. In [19], the authors proposed a 2D sine-chaotification system to enhance the dynamic behavior of existing chaotic maps. They applied their system to enhance Henon map and 2D sine logistic map. Recently, [15] proposed a 2-dimensional logistic-modulated-sine-coupling-logistic (LSMCL) chaotic map. However, the composition of multiple simple chaotic systems to enhance chaotic performance usually comes at the cost of increased computation time.

C. COMBINING CHAOTIC MAPS AND DYNAMIC S-BOXES FOR IMAGE ENCRYPTION

Several image encryption schemes combine chaotic maps with S-boxes, to obtain the desirable properties of both components. In [20], the authors proposed an image encryption scheme based on a combination of chaotic maps and multiple dynamic S-boxes, along with block permutation. The image encryption scheme proposed by [21] also combines multiple dynamic S-boxes with a chaotic substitution. In [22], the authors combined a dynamic S-box with a 2D chaotic map for image encryption. The image encryption schemes in [23] and [24], also use dynamically constructed S-boxes, permutation and a chaotic key stream substitution. The scheme presented in [25], uses a similar structure to [24] but adds chaining of chaotic maps.

In [26], the authors proposed another encryption scheme combining permutation, S-box substitution and diffusion using chaotic maps. To improve diffusion, another scheme in [27] uses a few S-boxes and dynamically changes the S-boxes based on plain image pixels.

D. MEDICAL IMAGE ENCRYPTION SCHEMES

Several medical image encryption schemes have been proposed in literature. The authors in [5] introduced a medical image encryption system based on cosine number transform (CNT) defined over a chosen Galois field. Further in [4], the authors extended the use of CNT to 3D medical image method based and used 3 rounds of scrambling using Arnold cat map. In both schemes, the authors did not study the encryption speed, leaving the applicability of their methods to real-time encryption questionable.

An encryption system combining chaos and DNA was introduced by the authors of [6]. They used a scenario of two rounds with six steps to achieve the permutation, substitution and diffusion required for encryption. The main disadvantage of their system is the relatively low encryption speed.

In [28], the authors used tensor compressive sensing to combine 3D image compression and encryption and non-autonomous Lorenz system. Two main issues can be noted in this scheme. First, it is extremely slow due to its iterative nature. Second, the presented security analysis lacks some important tests such as plain image sensitivity analysis, which leaves it potentially susceptible to differential attacks.

The authors of [7] used an improved El-Gamal elliptic curve cryptosystem with multi-round of Arnold transformation for medical image encryption. To improve encryption speed and reduce the expansion of encrypted image size, they embedded multiple image pixels into a single point not necessarily on the elliptic curve. However, the use of multi-round Arnold transformation is time consuming and as a result, the speed of their scheme was very limited. Moreover, in their effort to save space, they reused the same random number for encrypting all image blocks, which leaves the door wide opens attacks against El-Gamal cryptosystem. In [1], the authors used the same EL-Gamal elliptic curve cryptosystem, but with Mersenne Twister pseudo-random number generator. Their improved system had a much better encryption speed. However, the issue with the reuse of the same random number for encrypting all image blocks persists.

In [29], the authors presented a medical image encryption scheme, denoted MIE-BX based on high-speed scrambling, insertion of random pixels and pixel-adaptive diffusion. Their simulation results showed that their encryption speed can exceed traditional encryption methods such as AES. However, [2] pointed out a potential vulnerability in MIE-BX to an attack against PRNG known as the reset attack. In this attack the adversary resets the PRNG state causing it to generate the same sequence of numbers every time. The authors of [2] used this vulnerability to launch a chosen-plaintext attack against MIE. To resolve this issue, they introduced a nonlinear operation on shuffled images. However, the computational overhead of the additional operation was not evaluated, and no speed analysis was presented by the authors.

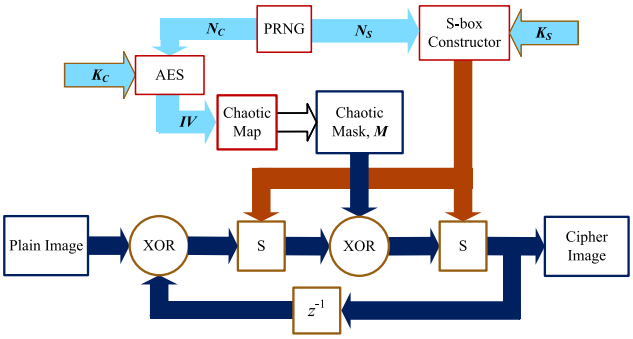

FIGURE 1. Proposed image encryption framework.

III. THE PROPOSED MEDICAL IMAGE ENCRYPTION FRAMEWORK

The purpose of medical images is to support medical diagnosis. Therefore, the slightest presence of noise may affect the accuracy of diagnosis. Therefore, the proposed medical image encryption framework assumes that the underlying channel is lossless. The main concern of the proposed framework is protecting patient privacy.

In this section, we first present the proposed image encryption generic framework and its associated encryption and decryption algorithms in detail. The implementation of this generic framework can be realized using a variety of chaotic maps and key-dependent S-box construction methods. Therefore, we dedicate the second subsection to specific implementations of the proposed framework.

A. GENERIC FRAMEWORK

The proposed image encryption framework is based on two generic components. The first generic component is a key-dependent S-box construction algorithm, denoted $\mathbb{S}_{K_S}$, where K_S is the key. Given an α-bit initialization vector, $N_S \in \{0,1\}^{\alpha}$, $\mathbb{S}_{K_S}(N_S)$ produces a bijective 8×8 S-box. The second generic component is a chaotic pseudo-random source, denoted $\mathbb{C}$. Given a β-bit initialization vector, $IV \in \{0,1\}^{\beta}$, $\mathbb{C}(IV)$ can generate a pseudorandom byte stream of arbitrary length. $\mathbb{S}$ and $\mathbb{C}$ can be realized by many existing key-dependent S-box construction methods and chaotic systems.

It is assumed that an encryption key is secretly shared by the communicating parties prior to the image communication session. The encryption key has two parts, K_S, which controls the S-box construction and K_C, which controls the generation of the chaotic sequence.

Given a plain image, I, to encrypt, the proposed framework works in two phases, as shown in Figure 1. During the preparation phase, a PRNG generates two nonce random numbers, N_S and N_C, then N_S is AES encrypted using key K_C to obtain the chaos initialization vector $IV = \text{AES}_{K_S}(N_C)$. $\mathbb{S}$ constructs a dynamic S-box, $S = \mathbb{S}_{K_S}(N_S)$ and the initialized chaos source $\mathbb{C}(IV)$ generates a pseudorandom byte stream, M, of the same size of the plain image, I.

During the encryption phase, the constructed S and M are utilized to transform plain image pixels to cipher

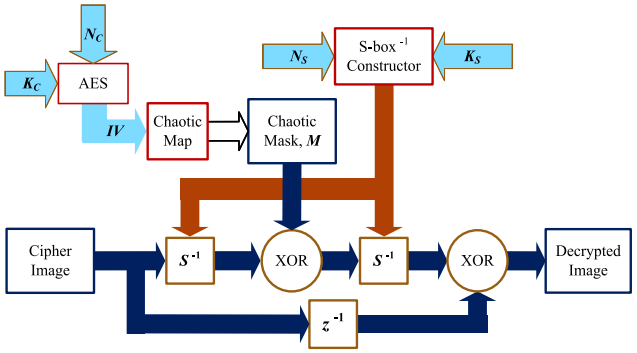

FIGURE 2. Proposed image decryption framework.

Algorithm 1 Image Encryption

Input: plain image, I, shared key (K_S, K_C), chaotic transient length N_T

Output: cipher message, (N_S, N_C, I_C)

1. Use the PRNG to generate two nonce, N_S and N_C.
2. Construct a dynamic S-Box $S = \mathbb{S}_{K_S}(N_S)$.
3. Initialize the chaotic source $\mathbb{C}$ using $IV = \text{AES}_{K_S}(N_C)$.
4. Iterate $\mathbb{C}$ for N_T times to skip the transient effect.
5. Use $\mathbb{C}$ to generate a chaotic sequence, M, of length $\#I$.
6. For each plain image pixel $I(i,j)$, calculate $I_C(i,j) = c_k = S(S(I(i,j) \oplus c_{k-1}) \oplus m_k)$, where $1 \le k \le \#I$, $c_0 = 0$.
7. Output the cipher message (N_S, N_C, I_C) ■

image pixels. A plain image pixel is first XORed with the previous cipher image pixel, indicated by the (z^{-1}) in the block diagram. The result is then substituted using the S-box, S, then XORed with the corresponding value of the chaotic sequence, M. The result is finally substituted again using the same S-box, S, to produce the corresponding cipher image pixel. The nonce numbers N_S and N_C are stored in the cipher image header to facilitate decryption.

As shown in Figure 2, to decrypt a cipher image, N_S and N_C are extracted from its header and used along with the shared secret keys, K_S and K_C, to construct the corresponding chaotic sequence, M, and inverse S-box (S^{-1}). Each cipher image pixel is substituted, XORed with the corresponding chaotic sequence value, substituted again, and finally XORed with the previous cipher image pixel. The encryption and decryption procedures are listed in Algorithm 1 and Algorithm 2, respectively.

B. FRAMEWORK REALIZATION

To demonstrate the application of the proposed generic framework, we present a sample implementation for the generic key-dependent S-box construction component, $\mathbb{S}$, and the generic chaotic source component, $\mathbb{C}$.

1) DYNAMIC S-BOX CONSTRUCTION COMPONENT

The proposed framework makes the following assumptions about the S-box construction component, $\mathbb{S}$: 1) $\mathbb{S}$ is

Algorithm 2 Image Decryption

Input: cipher message (N_S, N_C, I_C), shared key (K_S, K_C), chaotic transient length N_T

Output: decrypted image, I_D

1. Construct the inverse S-box $S^{-1} = inv(\mathbb{S}_{K_S}(N_S))$.
2. Initialize the chaotic source $\mathbb{C}$ using $IV = \text{AES}_{K_S}(N_C)$.
3. Iterate $\mathbb{C}$ for N_T times to skip the transient effect.
4. Use $\mathbb{C}$ to generate a chaotic sequence, M, of length $\#I_C$.
5. For each cipher image pixel $c_k = I_C(i,j)$, calculate $I_D(i,j) = S^{-1}(S^{-1}(c_k) \oplus m_k) \oplus c_{k-1}$, where $1 \le k \le \#I$, $c_0 = 0$.
6. Output the decrypted image I_D ■

key-dependent, i.e., the generated S-box is determined by K_S and N_S, so that the decryption process can generate the inverse S-box from the same key, 2) $\mathbb{S}$ must be able to generate an unlimited number of S-boxes, to increase the key-space, and 3) $\mathbb{S}$ must be able to generate a dynamic S-box reasonably fast, so that a new S-box is constructed for each image in real time. Any key-dependent dynamic S-box construction method satisfying these assumption, such as [12], [14], [25], [30]–[41], can replace the generic S-box component, $\mathbb{S}_{K_S}(N_S)$, where K_S and N_S map to the key of the S-box construction method. For example, the method in [11] uses repetitive functional composition to construct a dynamic S-box from of a set of initial static S-boxes. The choice of which S-box to compose in each iteration is controlled by a chaotic map. The initialization of the chaotic map and the number of compositions can be mapped to N_S and K_S, respectively.

To use any key-dependent S-box construction method which has only one initialization parameter, such as [42], we propose the following modification to convert it to a two-parameter function. Let $\mathbb{S}(K)$ be a key-dependent S-box construction method with one parameter, K. Define $\mathbb{S}'_{K_S}(N_S) = \mathbb{S}(AES_{K_S}(N_S))$. This introduces dependency on both K_S and N_S.

In this paper, we propose a new key-dependent S-box construction method based on Mersenne twister PRNG (MT19937) shown in Algorithm 3.

A sample S-box generated by the proposed method is shown in Figure 3. Standard security tests of S-boxes include nonlinearity (NL), linear approximation probability (LAP), differential uniformity (DU), strict avalanche criterion (SAC) and bit independence criterion (BIC) [43].

Cryptographic analysis of the sample S-box was verified using SageMath [44] and compared to recently proposed qualifying S-box construction methods in Table 1. The comparison shows that the S-boxes generated by the proposed method are similar to those generated by relevant methods. However, the proposed S-box construction method has two main advantages: 1) sufficiently large key space, since the internal state of the MT19937 consists of 19937 bits, and 2) the use of integer arithmetic allows faster construction of

TABLE 1. Cryptographic analysis of the sample S-box constructed by the proposed method in comparison to relevant methods.

	NL			BIC		SAC			DU	LAP
	Min	Max	Avg	NL	SAC	Avg.	Max	Min		
Proposed	106	110	108.00	104.29	0.4961	0.4990	0.5781	0.4063	10	0.1250
Ref. [25]	104	110	106.25	103.93	0.5070	0.5029	0.5938	0.4219	10	0.1328
Ref. [12]	106	108	106.75	103.79	0.4951	0.5034	0.6250	0.4219	10	0.1328
Ref. [30]	106	108	107.25	105.29	0.4980	0.5034	0.6094	0.4219	12	0.1328
Ref. [31]	106	110	107.75	105.07	0.5023	0.4976	0.5781	0.3906	10	0.1250
Ref. [32]	104	110	106.50	105.2	0.4984	0.5120	0.6406	0.4375	10	0.1172
Ref. [33]	102	110	105.50	104.3	0.4988	0.5010	0.6094	0.4063	12	0.1250
Ref. [34]	102	108	105.25	103.8	0.4971	0.5056	0.5781	0.4375	10	0.1563
Ref. [35]	106	108	106.50	104.2	0.5003	0.4978	0.5938	0.4375	10	0.1328
Ref. [14]	104	108	106.75	103.9	0.4997	0.5071	0.5938	0.4062	14	0.1406
Ref. [36]	104	110	106.00	104.21	0.5014	0.5197	0.6250	0.4375	10	0.1328
Ref. [37]	102	108	104.50	104.64	0.5013	0.4980	0.6406	0.4219	12	0.1250
Ref. [38]	106	110	108.50	104.00	0.4971	0.5017	0.5938	0.4062	10	0.1328
Ref. [39]	106	110	107.00	105.5	0.5010	0.5015	0.5625	0.4063	10	0.1250
Ref. [40]	106	108	107.00	103.5	0.5040	0.4970	0.5781	0.4219	10	0.1563
Ref. [41]	102	108	105.25	102.6	0.4994	0.5037	0.6094	0.4062	10	0.1328

245	227	89	216	101	124	88	182	217	64	158	197	236	74	35	30
248	102	132	108	103	155	194	237	209	193	68	122	142	252	59	169
22	164	99	125	42	9	134	198	175	247	107	203	43	225	106	123
240	191	4	168	255	15	221	138	170	165	151	54	133	52	140	233
0	117	188	100	109	23	13	38	36	139	26	3	19	201	174	58
55	229	146	204	98	121	154	143	113	115	73	84	34	189	127	254
171	212	215	76	110	222	94	195	46	8	235	118	28	40	2	150
244	156	179	27	190	5	186	67	120	230	80	238	242	29	61	214
41	220	185	86	78	92	148	176	111	181	205	31	85	145	47	70
128	166	16	95	208	77	210	116	223	37	144	75	21	196	126	7
12	10	173	60	20	49	11	97	184	65	183	177	202	149	218	69
178	137	224	114	90	161	157	66	226	82	136	6	25	206	192	232
1	167	163	32	172	44	83	119	159	18	56	91	207	45	180	253
112	57	81	130	246	50	187	51	200	62	152	105	239	211	219	53
129	131	249	87	71	153	160	147	79	251	199	243	141	63	96	231
135	17	241	213	33	228	93	14	39	250	72	24	104	48	162	234

FIGURE 3. Sample dynamic S-box constructed using the proposed method.

Algorithm 3 Construct Key-Dependent S-Box

Input: nonce, N_S, shared S-box key, K_S

Output: S-box, s (0: 255)

1. Calculate the seed $= AES_{Ks}(N_S)$.
2. Initialize the MT19937 PRNG, $\mathbb{R}$, using the seed.
3. Initialize collision vector a (0: 255) $\leftarrow$ false
4. **for** $i = 0$: 255
5. **repeat**
6. $j \leftarrow$ next random from $\mathbb{R}$ mod 256.
7. **until** $a\,(j) =$ false
8. $a\,(j) \leftarrow$ true, $s\,(i) = j$
9. **end for**
10. Output s (0: 255) ■

dynamic S-boxes and avoids potential implementation errors due to conversion from initialization bit vectors to floating point representation.

2) CHAOTIC SOURCE COMPONENT

The chaotic source component, $\mathbb{C}$, can be implemented using any classical or modern chaotic map. For example, Table 2 lists a sample of four classical chaotic maps and four modern chaotic maps that are used to implement the proposed framework. The mapping between the initialization vector, IV, and the initial state is shown next to each chaotic map. The specific mathematical expression for this mapping depends on the actual implementation of the chaotic map. When the state of the chaotic map is represented as double-precision floating-point numbers, the initial state can be expressed as

$$(x_0, y_0) = 2^{-53}\left(\sum_{i=0}^{53} 2^i b_i,\ \sum_{i=0}^{53} 2^i b_{i+64}\right), \qquad (1)$$

where b_i is the ith bit of the initialization vector, IV.

TABLE 2. Sample chaotic maps used to implement the proposed framework.

Map	Equations	IV
Arnold cat map	$x_n = (2x_{n-1} + y_{n-1}) \bmod 1,$ $y_n = (x_{n-1} + y_{n-1}) \bmod 1$	x_0, y_0
Baker map	$x_n = \begin{cases} \frac{x_{n-1}}{p}, & 0 \le x_{n-1} < p \\ \frac{x_{n-1}-p}{1-p}, & p \le x_{n-1} < 1 \end{cases}$ $y_n = \begin{cases} py_{n-1}, & 0 \le x_{n-1} < p \\ 1-(1-p)y_n, & p \le x_{n-1} < 1 \end{cases}$	x_0, y_0
Henon map	$x_{n+1} = 1 - ax_n^2 + y_n,$ $y_{n+1} = bx_n$	x_0, y_0
Standard map	$p_n = p_{n-1} + K\,sin(x_{n-1}),$ $x_n = (x_{n-1} + p_{n-1}, 2) \bmod 2\pi$	x_0, p_0
SLM [18]	$x_{n+1} = (\alpha \sin(\pi y_n) + \beta)x_n(1-x_n)$ $y_{n+1} = (\alpha \sin(\pi x_{n+1}) + \beta)y_n(1-y_n)$	x_0, y_0
SCSLM [19]	$x_{n+1} = \sin\big(\pi(\alpha\, sin(\pi y_n) + \beta)x_n(1-x_n)\big)$ $y_{n+1} = \sin\big(\pi(\alpha\, sin(\pi x_{n+1}) + \beta)y_n(1-y_n)\big)$	x_0, y_0
SCH [19]	$x_{n+1} = \sin\big(\pi(1 - \alpha x_n^2 + y_n)\big),$ $y_{n+1} = \sin(\pi\beta x_n)$	x_0, y_0
LSMCL [15]	$x_{n+1} = \big(\sin\big(4\pi\alpha y_n(1-y_n)\big) + \beta\big)x_n(1-x_n)$ $y_{n+1} = \big(\sin\big(4\pi\alpha x_{n+1}(1-x_{n+1})\big) + \beta\big)y_n(1-y_n)$	x_0, y_0

To generate the chaotic keystream, the floating-point representation of the chaotic map state, (x_k, y_k), is converted to an 8-bit integer number, m_k, using the equation

$$m_k = \left(2^{24} x_{N_T+k}\right) mod 256 \tag{2}$$

IV. PERFORMANCE ANALYSIS

To evaluate the security and performance of the proposed framework, we performed standard tests including statistical analysis, differential analysis, key sensitivity analysis, key space analysis, and speed analysis. Although necessary, these statistical tests are not sufficient and further analysis must be performed to show the resistance of the proposed framework to specific cryptanalysis scenarios [45], [46]. Therefore, we also analyzed the framework resistance to chosen-plaintext, chosen-ciphertext cryptanalysis, and the PRNG-reset attack. Figure 4 shows the sample medical images used for testing [47]–[49]. During the testing, we used the proposed S-box construction method based on MT19937 PRNG, whereas the chaotic map was varied among the list of maps defined in Table 2.

A. STATISTICAL ANALYSIS

Statistical analysis includes a set of tests which assess immunity to statistical ciphertext-only attacks.

1) HISTOGRAM TEST

The uniformity of an encrypted image histogram is a basic requirement for a strong encryption system to resist statistical attacks. For visual inspection, Figure 5 shows sample histograms of the encrypted CT scan image generated by the proposed framework for each of the evaluated maps. Histograms appear uniform indicating that the proposed framework passes this test. Histograms of the other medical images we tested exhibit similar uniformity.

As a numeric metric of the uniformity of a histogram, Chi-square variance test (χ^2) is utilized. The test compares the variance of the histogram to the histogram of a completely random image. The test starts by calculating

$$X^2 = \sum_{i=1}^{256} (f_i - E_k)^2 \Big/ E_k, \tag{3}$$

where f_i is the frequency of gray level i in the encrypted image and $E_k = N/256$, which is the expected frequency of gray level value for an image containing N pixels. Since the histogram of a gray level images has 255 degrees of freedom, the resulting X^2 is tested against the distribution $\chi^2(255, \alpha)$, where α is the significance level. The histogram passes the test if the p-value is greater than α, which indicates that the histogram uniformity is satisfactory.

Since chaotic maps are sensitive to the initialization vector, IV, which change with each encryption attempt, the quality of the resulting histogram may vary accordingly. To study this effect, the χ^2 test was repeated 1000 times for each of the chaotic maps. We reported the χ^2 test pass rate for each chaotic map in Table 3. Results indicate all the proposed framework passes the histogram χ^2 test with very high probability with all the considered chaotic maps.

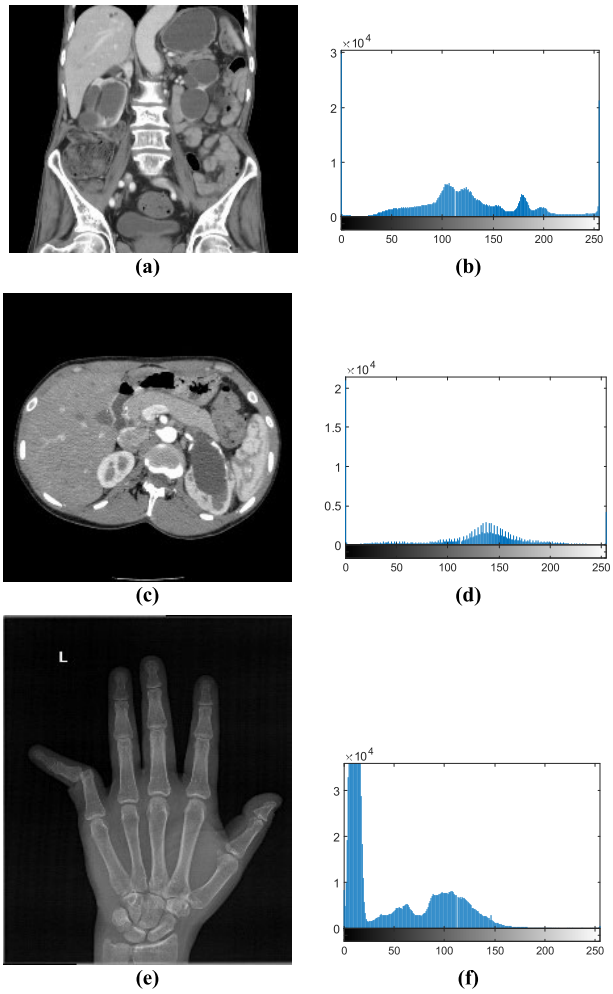

FIGURE 4. Sample medical images used for statistical testing. Sample 750 × 870 CT scan image (a), corresponding histogram (b), sample 512 × 512 MRI image (c), corresponding histogram (d), sample 1338 × 1094 X-ray image (e) and corresponding histogram (f).

TABLE 3. Histogram χ^2 test pass rate at $\alpha = 0.01$.

Map	CT scan	MRI	X-ray
Arnold	98.4%	99.2%	98.5%
Baker	99.0%	99.0%	99.0%
Henon	98.5%	98.8%	98.9%
Standard	98.7%	98.9%	98.9%
SLM	98.4%	98.7%	99.0%
SCSLM	98.4%	98.6%	98.8%
SCH	98.9%	98.9%	98.4%
LSMCL	98.6%	98.5%	99.2%

2) CORRELATION TEST

The cross-correlation test measures the disparity between the encrypted image and the plain image. Obviously, the optimal correlation is zero.

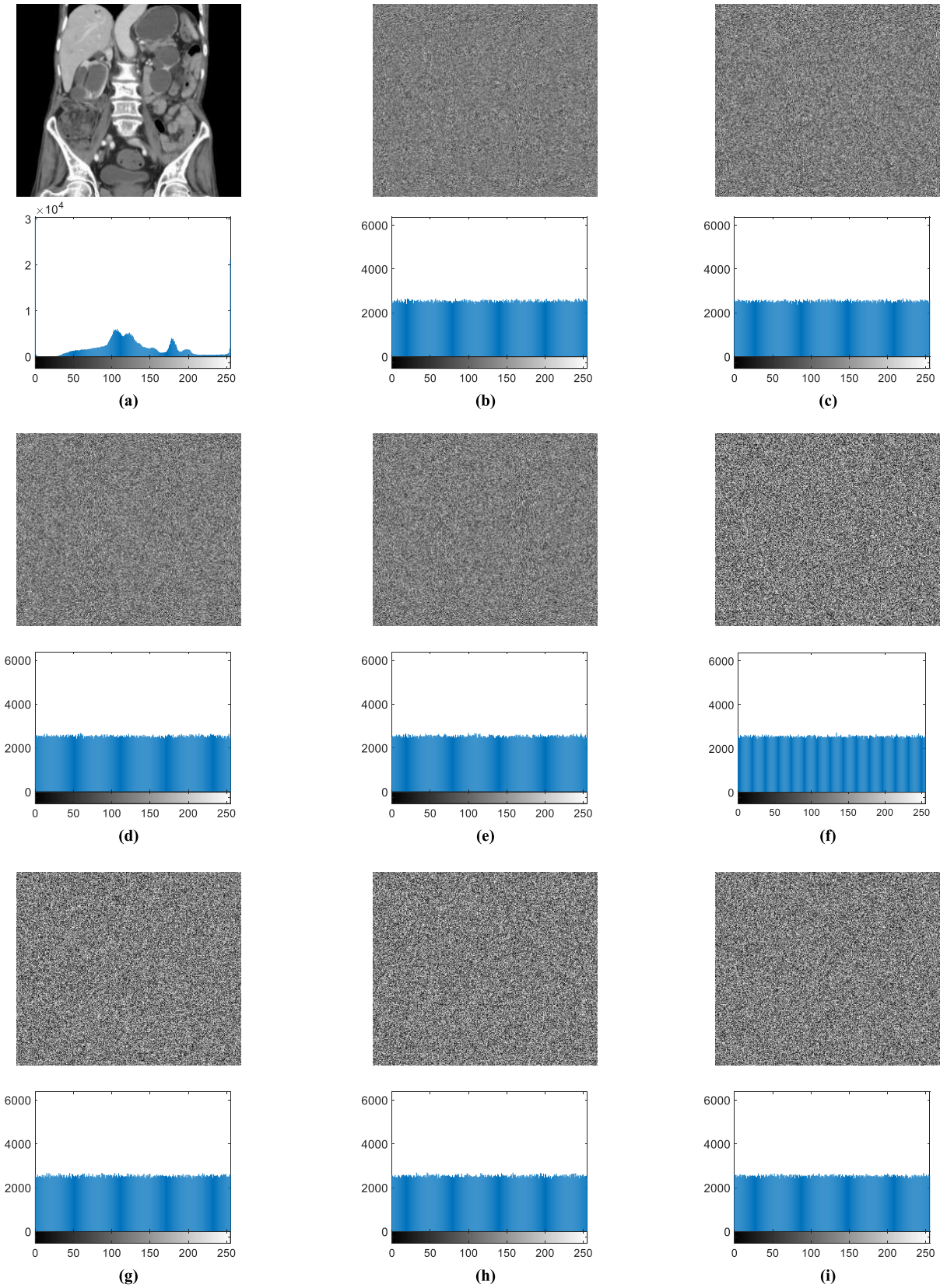

FIGURE 5. Sample CT scan image and corresponding histogram before encryption (a), and after encryption with the proposed framework using Arnold cat map (b), baker map (c), Henon map(d), standard map (e), SLM map (f), SCSLM map (g), SCH map (h) and LSMCL map (i).

TABLE 4. Cross correlation between pairs of plain and cipher images.

Map	CT scan	MRI	X-ray
Arnold	-0.0037	0.0008	-0.0008
Baker	0.0011	0.0012	0.0011
Henon	0.0010	0.0021	0.0006
Standard	0.0005	-0.0002	0.0000
SLM	0.0004	-0.0017	-0.0002
SCSLM	0.0006	0.0010	0.0005
SCH	-0.0004	-0.0013	0.0001
LSMCL	0.0002	-0.0011	-0.0018

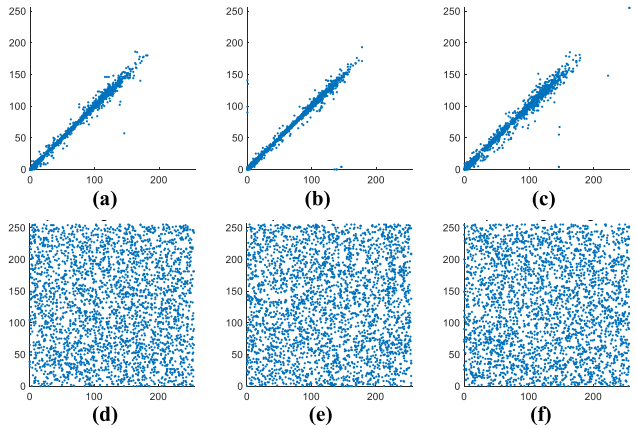

FIGURE 6. Spatial correlation distribution of a sample X-ray image encrypted with the proposed framework using Henon map. Plain image horizontal, vertical and diagonal correlation in (a), (b) and (c). Cipher image horizontal, vertical and diagonal correlation in (d), (e) and (f).

The cross-correlation coefficient is performed as follows:

$$C_{x,y} = \frac{\text{cov}(x, y)}{\sqrt{v(x)} \cdot \sqrt{v(y)}} \tag{4}$$

where x and y are the plain image and the encrypted image, respectively, N is the number of image pixels,

$$\begin{aligned} \text{cov}(x, y) &= \frac{1}{N} \sum_{j=1}^{N} \left(x_j - \bar{x}\right)\left(y_j - \bar{y}\right), \\ v(x) &= \frac{1}{N} \sum_{1j=1}^{N} (x_j - \bar{x})^2, \\ v(y) &= \frac{1}{N} \sum_{1j=1}^{N} (y_j - \bar{y})^2, \\ \bar{x} &= \frac{1}{N} \sum_{j=1}^{N} x_j, \text{ and } \bar{y} = \frac{1}{N} \sum_{j=1}^{N} y_j. \end{aligned}$$

Table 4 shows that the correlation between encrypted images and plaintext images is near zero indicating that our scheme achieves high confusion.

One of the characteristics of a plain image is spatial correlation, i.e., correlation between neighboring pixels. An adversary can use the correlation between neighboring cipher pixels to infer some information about the plain image. Therefore, any encryption system must minimize such correlation. The spatial correlation distribution is depicted in Figure 6 for the plain and encrypted X-ray image, encrypted using Henon map. Results illustrate how the plain image strong spatial correlation was removed in the cipher image.

Table 5 shows the values of correlation between the neighboring pixels in horizontal, vertical and diagonal directions for the encrypted images. The correlation coefficients for the encrypted images are almost zero, indicating that the proposed framework reduces the correlation between neighboring pixels to a satisfactory level.

3) ENTROPY TEST

A good encryption scheme must maximize randomness of the cipher image. To evaluate the randomness in the cipher image the global entropy test is carried out as follows

$$E(X) = -\sum_{j=0}^{255} P_j \log_2 P_j, \tag{5}$$

where P_j is the probability of occurrence of pixel intensity j. Table 6 shows that the global entropy for sample medical images encrypted with the proposed framework is near the value 8, which indicates a completely uniform distribution of pixel values.

The local Shannon entropy (LSE) test considers the mean entropy of a set of randomly selected blocks of the image, thus estimating local randomness. LSE is calculated as follows:

1- Randomly select N_B non-overlapping blocks, $B_1, B_2, \ldots, B_{N_B}$ from the cipher image, with block size T_B pixels.

2- Calculate the entropy $E(B_i), i = 1, 2, \ldots, N_B$ for each block using (5).

3- Compute the mean (LSE) as follows:

$$\overline{E_{N_B,T_B}}(B) = \frac{1}{N_B} \sum_{i=1}^{N_B} E(B_i) \tag{6}$$

According to [50], the mean value of LSE of a random image is 7.9024693 with $N_B = 30$ and $T_B = 1963$. The confidence interval for LSE, with confidence level $\alpha = 0.05$, is (7.901901305, 7.903037329).

The LSE results shown in Table 6 indicate that images encrypted with the proposed scheme satisfy the randomness hypothesis at confidence level $\alpha = 0.05$.

4) NIST RANDOMNESS TEST SUITE

A standard set of randomness hypothesis tests was proposed by NIST in [51]. When the p-value of each test is greater than α, we may conclude that the tested sequence appears to be random with confidence level α. We performed the tests on a sample of cipher images corresponding to the MRI-3D image encrypted with classical Baker map and enhanced sine-chaotified Henon map. The results of the tests listed in Table 7 shows that the cipher images pass all randomness tests at $\alpha = 0.01$ confidence level.

5) TEXTURE ANALYSIS

Image encryption quality can also be quantified through applying a set of texture analysis statistics to the resulting encrypted images [52]. First, we compute an 8×8 gray-level co-occurrence matrix (GLCM) of the encrypted image I_C using the following expression

$$p(i,j) = \frac{1}{\#I_C} \# \left\{ (x,y) \;\middle|\; \left\lceil \frac{I_C(x,y)}{32} \right\rceil = i, \left\lceil \frac{I_C(x,y+1)}{32} \right\rceil = j \right\} \tag{7}$$

TABLE 5. Spatial correlation coefficients of encrypted images.

Map	CT scan			MRI			X-ray		
	H	V	D	H	V	D	H	V	D
Arnold	0.0096	0.0235	-0.0258	0.0211	-0.0150	-0.0413	0.0433	-0.0433	0.0176
Baker	-0.0135	-0.0066	0.0135	-0.0100	-0.0035	-0.0156	-0.0156	0.0076	0.0126
Henon	-0.0096	0.0133	-0.0060	0.0247	0.0048	-0.0003	0.0167	0.0321	-0.0158
Standard	0.0179	-0.0094	0.0240	-0.0218	-0.0051	-0.0041	0.0314	0.0352	0.0149
SLM	0.0130	0.0040	0.0214	-0.0332	-0.0015	-0.0032	-0.0069	-0.0158	-0.0095
SCSLM	-0.0039	-0.0114	-0.0222	-0.0049	-0.0121	0.0124	0.0171	-0.0398	-0.0236
SCH	-0.0124	-0.0081	-0.0046	-0.0251	-0.0027	0.0076	0.0174	0.0164	-0.0012
LSMCL	0.0168	0.0042	0.0366	-0.0121	-0.0014	-0.0035	0.0224	0.0622	0.0114

TABLE 6. Global entropy and local Shannon entropy test results for encrypted images.

Map	CT scan			MRI			X-ray		
	Global	LSE		Global	LSE		Global	LSE	
Arnold	7.9998	7.9021	Pass	7.9992	7.9030	Pass	7.9999	7.9022	Pass
Baker	7.9997	7.9022	Pass	7.9992	7.9030	Pass	7.9999	7.9020	Pass
Henon	7.9997	7.9028	Pass	7.9994	7.9030	Pass	7.9999	7.9030	Pass
Standard	7.9997	7.9020	Pass	7.9994	7.9020	Pass	7.9999	7.9022	Pass
SLM	7.9997	7.9022	Pass	7.9993	7.9028	Pass	7.9999	7.9028	Pass
SCSLM	7.9997	7.9026	Pass	7.9993	7.9020	Pass	7.9999	7.9029	Pass
SCH	7.9997	7.9030	Pass	7.9992	7.9027	Pass	7.9999	7.9028	Pass
LSMCL	7.9997	7.9023	Pass	7.9993	7.9027	Pass	7.9999	7.9027	Pass

TABLE 7. NIST randomness test suite results for encrypted MRI 3D image.

Test	Baker		SCH	
	p-Value	Result	*p*-Value	Result
Frequency	0.86234	Pass	0.36877	Pass
Block frequency	0.62555	Pass	0.26817	Pass
Cumulative sums	0.28340	Pass	0.13903	Pass
Runs	0.69474	Pass	0.31571	Pass
Longest runs of ones	0.91141	Pass	0.71748	Pass
Rank	0.17827	Pass	0.10050	Pass
Spectral DFT	0.03268	Pass	0.69474	Pass
Overlapping template	0.03517	Pass	0.01791	Pass
Non-overlap. template	0.01421	Pass	0.01216	Pass
Universal	0.21330	Pass	0.03035	Pass
Approximate entropy	0.87980	Pass	0.93816	Pass
Random excursions	0.15376	Pass	0.01671	Pass
Rand. excursion variant	0.03080	Pass	0.00716	Pass
Serial	0.05816	Pass	0.31571	Pass
Linear complexity	0.97606	Pass	0.93816	Pass

Then, we calculate the contrast, correlation, energy, and homogeneity of $p(i, j)$,

$$\text{Contrast}\,(I_C) = \sum_{i,j} |i-j|^2\, p(i,j) \tag{8}$$

$$\text{Correlation}\,(I_C) = \sum_{i,j} \frac{(i-\mu_i)\left(j-\mu_j\right) p\,(i,j)}{\sigma_i \sigma_j} \tag{9}$$

$$\text{Energy}\,(I_C) = \sum_{i,j} p\,(i,j)^2 \tag{10}$$

$$\text{Homogeneity}\,(I_C) = \sum_{i,j} \frac{p\,(i,j)}{1+|i-j|} \tag{11}$$

High quality encryption should generate a pseudorandom-like cipher image with a uniform gray-level cooccurrence matrix. By applying (8–11) to a uniform cooccurrence matrix we obtain contrast = 10.5, correlation = 0, energy = 0.015625 and homogeneity = 0.389397. Results shown in Table 8 show that the proposed framework effectively increases contrast and lowers correlation, energy, and homogeneity to near optimal levels, indicating high encryption quality.

B. DIFFERENTIAL ANALYSIS

Differential attacks exploit the difference between cipher images to infer information about plain images. To resist differential attacks, an encryption scheme should produce widespread changes in the cipher images corresponding to a small change in the plain image.

To verify the resistance to differential attacks, we induce a change in one bit of the original image and measure the changes in the resulting encrypted image. We calculate the Unified Averaged Changed Intensity (UACI) and Number of Pixels Change Rate (NPCR) using the following formulae

$$UACI\,(I_{C1}, I_{C2}) = \frac{1}{MN} \sum_{i,j} \frac{|I_{C2}\,(i,j) - I_{C1}(i,j)|}{255} \times 100\%, \tag{12}$$

$$NPCR\,(I_{C1}, I_{C2}) = \sum_{i,j} \frac{D\,(i,j)}{MN} \times 100\%, \tag{13}$$

where I_{C1} is the cipher image corresponding to the original plain image, I_{C2} is the cipher image corresponding to the changed plain image, MN is the number of image pixels, and

$$D\,(i,j) = \begin{cases} 1, & if\ I_{C1}(i,j) \neq I_{C2}(i,j) \\ 0, & \text{otherwise.} \end{cases} \tag{14}$$

An encryption scheme shows immunity against deferential attacks if UACI value is close to 33.4635% and the NPCR value is close to 99.6094% [53]. We use the randomness test proposed in [54] to judge if the resulting NPCR and UACI are distinguishable from a random change, with significance

TABLE 8. Second-order texture analysis statistics of encrypted images.

Map	Contrast			Correlation			Energy			Homogeneity		
	CTS	MRI	X-ray	CTS	MRI	X-ray	CTS	MRI	X-ray	CTS	MRI	X-ray
Plain image	0.102	0.143	0.046	0.8997	1.2184	1.3818	0.16514	0.31315	0.40985	0.95384	0.93565	0.97884
Arnold	10.48	10.52	10.47	-0.0004	-0.0028	-0.0004	0.01559	0.01557	0.01560	0.38933	0.38830	0.38905
Baker	10.45	10.43	10.49	0.0005	0.0003	-0.0007	0.01559	0.01557	0.01560	0.38918	0.38911	0.38921
Henon	10.51	10.47	10.49	-0.0011	-0.0006	-0.0002	0.01559	0.01557	0.01560	0.38900	0.38921	0.38920
Standard	10.52	10.54	10.47	0.0005	0.0000	-0.0003	0.01559	0.01557	0.01560	0.38884	0.38745	0.38916
SLM	10.50	10.50	10.49	0.0003	0.0008	-0.0018	0.01559	0.01557	0.01560	0.38851	0.38827	0.38914
SCSLM	10.50	10.46	10.49	-0.0006	0.0011	0.0007	0.01559	0.01557	0.01560	0.38905	0.38880	0.38882
SCH	10.46	10.51	10.49	0.0014	-0.0015	0.0000	0.01559	0.01557	0.01560	0.38966	0.38860	0.38899
LSMCL	10.45	10.44	10.51	-0.0000	-0.0024	-0.0003	0.01559	0.01557	0.01560	0.38964	0.38913	0.38904

TABLE 9. NPCR and UACI confidence intervals for $\alpha = 0.01$ significance level.

Image	Size	$NPCR_{min}$	$UACI_{min}$	$UACI_{max}$
MRI	512×512	99.5810	33.3445	33.5826
CT scan	750×870	99.5914	33.3881	33.5390
X-ray	1338×1094	99.5974	33.4132	33.5139

level $\alpha = 0.01$. Table 9 shows the UACI and NPCR confidence intervals corresponding to each of the sample images used for testing.

We repeated the plain image sensitivity tests 1000 times for each image with each of the chaotic maps. For each test, the value of just one randomly chosen bit of the plain image is flipped. Table 10 lists the mean values of NPCR and UACI as well as the test pass percentage for $\alpha = 0.01$. The results indicate that the proposed framework is immune to differential cryptanalysis.

To visually inspect the difference between two cipher images I_{C1} and I_{C2}, we calculate the difference image using the following formula

$$\delta(i,j) = (I_{C1}(i,j) - I_{C2}(i,j)) \bmod 256. \quad (15)$$

As shown in Figure 7 (e), the difference image is random-like, which indicates that the proposed framework has strong diffusion capability and thus resists differential cryptanalysis.

TABLE 10. Summary of differential attack test.

Map	Image	UCAI		NPCR	
		Mean	Pass%	Mean	Pass%
Arnold	CT scan	33.4614	98.8%	99.6095	99.3%
	MRI	33.4559	99.1%	99.6086	99.8%
	X-ray	33.4644	99.5%	99.6091	99.3%
Baker	CT scan	33.4696	99.0%	99.6093	99.3%
	MRI	33.4603	99.2%	99.6098	98.9%
	X-ray	33.4694	98.7%	99.6094	99.6%
Henon	CT scan	33.4602	99.4%	99.6094	99.2%
	MRI	33.4644	99.2%	99.6094	99.2%
	X-ray	33.4676	99.0%	99.6093	99.2%
Standard	CT scan	33.4531	98.9%	99.6093	99.5%
	MRI	33.4459	98.7%	99.6094	98.7%
	X-ray	33.4693	98.6%	99.6092	99.0%
SLM	CT scan	33.4738	98.8%	99.6091	98.7%
	MRI	33.4574	98.9%	99.6095	99.4%
	X-ray	33.4684	99.3%	99.6096	99.4%
SCSLM	CT scan	33.4666	99.3%	99.6092	99.4%
	MRI	33.4457	99.1%	99.6093	99.0%
	X-ray	33.4654	99.4%	99.6093	98.8%
SCH	CT scan	33.4702	99.0%	99.6094	99.6%
	MRI	33.4520	99.4%	99.6093	99.0%
	X-ray	33.4623	99.2%	99.6095	99.2%
LSMCL	CT scan	33.4716	99.2%	99.6099	99.1%
	MRI	33.4904	99.4%	99.6099	98.9%
	X-ray	33.4560	98.6%	99.6090	99.0%

C. KEY SENSITIVITY ANALYSIS

To resist related-key attacks, an encryption scheme should be sensitive to changes in the encryption key. Both the encryption process and the decryption process should be sensitive to the key. To measure the key sensitivity of the proposed encryption process, we start with an initial encryption key, K, then make a slight one-bit change to the key to obtain a related encryption key, $K' = K \oplus 1$. A plain image, I, is encrypted with K and with K' to obtain I_{C1} and I_{C2}, respectively. We then calculate the correlation, the NPCR and the UACI for I_{C1} and I_{C2}.

The proposed framework has two encryption keys, the S-box construction key, K_S and the chaotic map key, K_C. Therefore, we test the scheme's sensitivity to each of them.

Results of encryption key sensitivity analysis, with respect to the dynamic S-box key are presented in Table 11. Results include correlation coefficient, UACI and NPCR for three medical images encrypted using two related dynamic S-box keys K_S and K'_S. Results indicate high sensitivity to changes in dynamic S-box key.

Results of chaotic map encryption key sensitivity analysis are presented in Table 12. Each row indicates the results for one of the investigated chaotic maps, including the correlation coefficient, the UACI and the NPCR for three medical images encrypted using two related chaotic maps keys K_C and K'_C such that $K_C \oplus K'_C = 1$. Results indicate high sensitivity to changes in chaotic map keys.

As shown in Figure 8 and Figure 9, the difference between the two images encrypted with related S-box keys or related chaotic map keys is a random image, which indicates that the proposed framework is highly sensitive to slight changes in encryption keys.

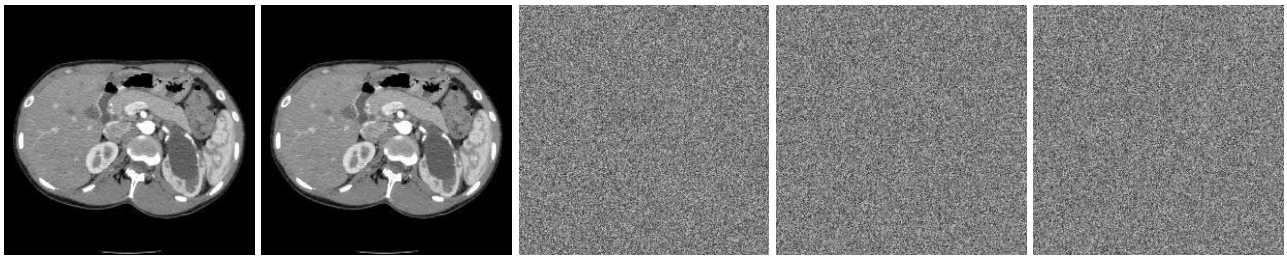

FIGURE 7. Visual results of plain image sensitivity analysis with Baker map showing (a) original image, (b) changed image, (c) original cipher image, (d) changed cipher image and (e) difference between cipher images.

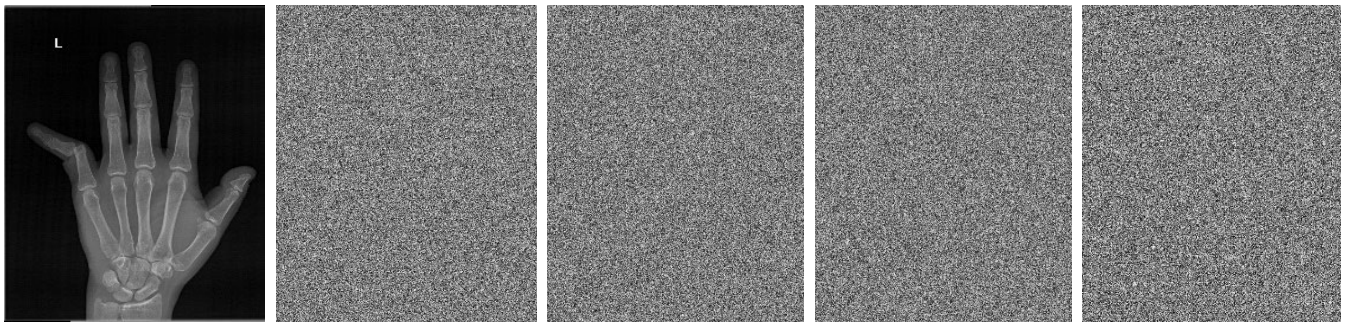

FIGURE 8. Visual results of S-box key sensitivity analysis, showing (a) original image, (b) image encrypted with S-box key, K_S, (c) image encrypted with related S-box key, K'_S, (d) difference between encrypted images, and (e) image decrypted with K'_S after encryption with K_S.

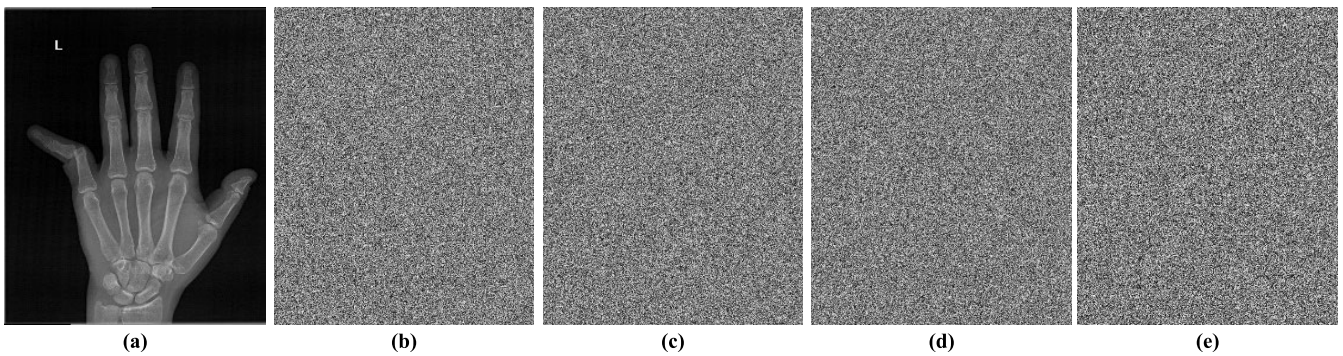

FIGURE 9. Visual results of chaotic map key sensitivity analysis, showing (a) original image, (b) image encrypted with chaotic map key, K_C, (c) image encrypted with related chaotic map key, K'_C, (d) difference between encrypted images, and (e) image decrypted with K'_C after encryption with K_C.

To illustrate the sensitivity of the decryption process to the key, we encrypt the plain image with key, K, then decrypt the resulting cipher image with K' to obtain the decrypted image I_D. Results of decryption shown in Figure 8 and Figure 9 appear random, which indicates that the decryption process is highly sensitive to both keys, K_S and K_C.

D. KEY SPACE ANALYSIS

The simplest cryptanalysis attack consists of a blind search for the encryption key in the set of all such possible keys. Therefore, it is necessary to make the key space large enough to deter brute-force attacks.

The encryption key of the proposed framework consists of two components, namely, the dynamic S-box key, K_S and chaotic map key, K_C. This composite encryption key gives our scheme a clear advantage in comparison with traditional chaotic encryption schemes, in which the encryption key is limited to chaotic map parameters. For the used 2D-chaotic maps, the initialization has at least 2×53 significant bits, giving a key space of 2^{106}.

Theoretically a dynamic S-box is chosen from a set of (256!) S-boxes. This increases the key space by a factor of $\sim 10^{1167}$. Practically the key space of the dynamic S-box is limited by its construction algorithm. The proposed S-box construction method uses a 128-bit key. Together with the chaotic map key, the resulting key space is beyond the reach of brute-force attacks. A powerful adversary with a classical computer capable of attempting 10^{12} keys per second would need more than 10^{50} years.

TABLE 11. Results of S-Box key sensitivity analysis $K_S = 75907410529288501092361216523777083 84$, $K'_S = 75907410529288501092361216523777083 85$.

Map	Image	Correlation	UACI	NPCR
Arnold	CT scan	0.0006	33.4672	99.6066
	MRI	-0.0023	33.5230	99.6057
	X-ray	-0.0001	33.4500	99.6051
Baker	CT scan	0.0002	33.4574	99.6093
	MRI	-0.0038	33.5639	99.6210
	X-ray	-0.0023	33.4951	99.5995
Henon	CT scan	0.0003	33.4374	99.6020
	MRI	0.0000	33.4446	99.6173
	X-ray	0.0005	33.4073	99.6136
Standard	CT scan	0.0020	33.4015	99.6223
	MRI	-0.0004	33.4726	99.6136
	X-ray	-0.0009	33.4834	99.6368
SLM	CT scan	-0.0007	33.4339	99.6334
	MRI	0.0024	33.3918	99.6143
	X-ray	0.0003	33.5065	99.6017
SCSLM	CT scan	-0.0003	33.4831	99.6052
	MRI	-0.0006	33.4767	99.6067
	X-ray	0.0010	33.4457	99.6131
SCH	CT scan	0.0018	33.4332	99.6126
	MRI	-0.0005	33.4692	99.6197
	X-ray	0.0011	33.4594	99.6082
LSMCL	CT scan	-0.0013	33.4858	99.6078
	MRI	0.0002	33.4567	99.6066
	X-ray	-0.0002	33.4658	99.6051

TABLE 12. Results of chaotic map key sensitivity analysis $K_C = 14521908243480811746592776770990164 3963$, $K'_C = 14521908243480811746592776770990164 3962$.

Map	Image	Correlation	UACI	NPCR
Arnold	CT scan	-0.0025	33.5011	99.6112
	MRI	0.0005	33.4554	99.6161
	X-ray	-0.0012	33.4755	99.5991
Baker	CT scan	0.0007	33.4452	99.6123
	MRI	0.0011	33.4375	99.6124
	X-ray	-0.0002	33.4265	99.6029
Henon	CT scan	0.0026	33.4046	99.6006
	MRI	0.0004	33.4326	99.5985
	X-ray	0.0000	33.5043	99.6197
Standard	CT scan	-0.0020	33.5082	99.6349
	MRI	-0.0008	33.4809	99.6090
	X-ray	0.0010	33.4661	99.5926
SLM	CT scan	-0.0038	33.5162	99.6181
	MRI	-0.0040	33.5440	99.6075
	X-ray	0.0025	33.4266	99.6181
SCSLM	CT scan	-0.0017	33.5153	99.5953
	MRI	-0.0007	33.4922	99.6050
	X-ray	-0.0009	33.4935	99.6015
SCH	CT scan	-0.0016	33.4865	99.6013
	MRI	0.0006	33.4490	99.6072
	X-ray	0.0003	33.4614	99.6006
LSMCL	CT scan	-0.0007	33.4722	99.6097
	MRI	0.0003	33.4687	99.6118
	X-ray	0.0002	33.4571	99.6085

E. RESISTANCE TO CHOSEN-PLAINTEXT AND CHOSEN-CIPHERTEXT ATTACKS

In a chosen-plaintext attack, the adversary has temporary access to the encryption oracle and can feed it with carefully chosen plaintext to reveal some information about the encryption key. Therefore, immunity against chosen-plaintext attacks precludes known-plaintext attacks, in which the adversary exploits knowledge of one or more plaintext-ciphertext pairs. In a chosen-ciphertext attack, the adversary gains temporary access to the decryption oracle and can feed it with carefully chosen ciphertext to infer some information about the encryption key.

A common chosen-plaintext attack uses an all-white or an all-black image and attempt to detect any non-random patterns in the cipher image or any non-uniformity in its histogram.

As shown in Figure 10, the resulting cipher images have no visible patterns and their histograms are uniform. Moreover, Table 13 demonstrates that the histogram χ^2-test, the spatial correlation, and the entropy of the encrypted all-black image match the characteristics of a pseudorandom image.

The rest of this subsection discusses the special precautions taken to make the proposed framework resist chosen-plaintext and chosen-ciphertext attacks.

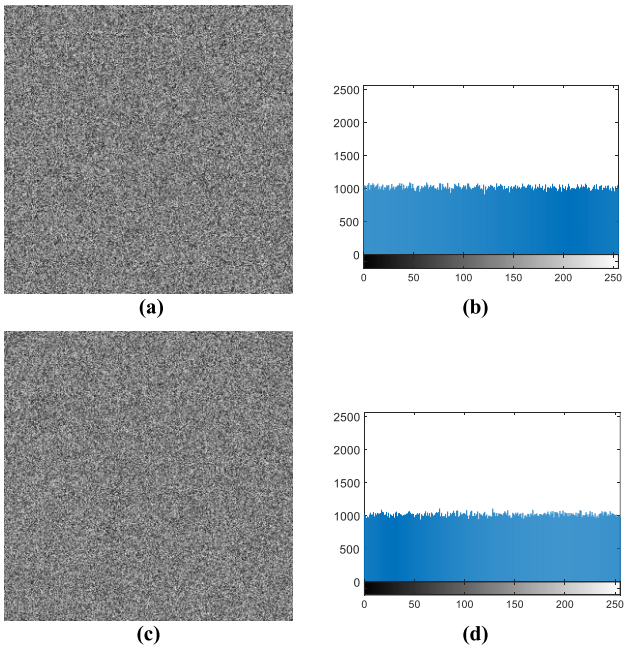

FIGURE 10. Results of chosen plaintext attack. All-white image encrypted with the proposed framework using Arnold cat map (a), and its corresponding histogram (b). All-black image encrypted with the proposed framework using SCSLM map (c) and its corresponding histogram (d).

TABLE 13. Statistical analysis of the encryption result of all-black image.

Map	Histogram	Correlation			Entropy
	p-Value	H	V	D	
Arnold	0.9879	-0.0016	0.0050	-0.0243	7.9994
Baker	0.5509	-0.0178	-0.0072	0.0040	7.9993
Henon	0.9021	0.0158	0.0073	0.0070	7.9994
Standard	0.5096	0.0011	-0.0017	-0.0277	7.9993
SLM	0.0556	0.0119	0.0229	-0.0271	7.9992
SCSLM	0.0219	0.0178	0.0183	-0.0034	7.9992
SCH	0.0338	-0.0155	0.0176	-0.0015	7.9992
LSMCL	0.0666	0.0345	-0.0015	-0.0002	7.9992

1) RESISTANCE TO CHOSEN-PLAINTEXT ATTACKS

As noted in [46], a chaotic map key, K_C, may be recoverable by an algebraic attack if the adversary gains access to the chaotic sequence. Therefore, the proposed framework employs four mechanisms to protect the chaotic sequence. First, the feedback mechanism complicates the form of plaintext needed to expose the chaotic mask. Second, the nonce initialization generates a different chaotic sequence for each encryption attempt. Third, AES encryption of nonce initialization enables resistance to the reset attack against the PRNG [2]. Fourth, the last S-box substitution adds another line of defense to the chaotic map.

To demonstrate the effectiveness of these mechanisms, let's assume that an adversary attempts a chosen-plaintext attack by choosing a plain image p_k, $\forall 1 \leq k \leq \#I$ and obtains the corresponding cipher image $c_k = S\left(S\left(p_k \oplus c_{k-1}\right) \oplus m_k\right)$. To cryptanalyze the chaotic mask, $m_k = S^{-1}\left(c_k \oplus S\left(p_k \oplus c_{k-1}\right)\right)$, an all-black image is not suitable to expose m_k, due to the feedback mechanism.

Instead, the adversary may use a special plain image satisfying $p_k \oplus c_{k-1} = \eta$ to obtain $m_k = S^{-1}(c_k \oplus S(\eta))$, such that $S(\eta)$ can be guessed as a constant $\epsilon \in \{0, 1, \ldots, 255\}$. In this case, the adversary would be left with $m_k = S^{-1}(c_k \oplus \epsilon)$, where both m_k and S^{-1} are still unknown. Since $c_k \oplus \epsilon$ has a uniform random distribution, the adversary must guess the entire S-box while simultaneously cryptanalyzing m_k. Therefore, the second S-box adds an extra layer of security to the chaotic map against cryptanalysis.

Under the conditions of a reset attack, if the adversary can reset the encryption PRNG during a chosen-plaintext attack, the resulting chaotic sequence m_k and S-box S may be fixed across multiple chosen-plaintext encryption attempts. This powerful attack may allow the adversary to recover m_k and cryptanalyze it to obtain the chaotic map initialization, IV. However, since $IV = AES_{K_C}(N_S)$, the secret key, K_C, remains protected by AES.

2) RESISTANCE TO CHOSEN-CIPHERTEXT ATTACKS

The first S-box protects the chaotic map against chosen-ciphertext attacks, in a way similar to the role played by the second S-box in protecting the chaotic map against chosen-plaintext attacks. For instance, if the adversary chooses an all-black cipher image $c_k = 0, \forall 1 \leq k \leq \#I$, and obtains a decrypted image, $p_k = S^{-1}\left(S^{-1}(0) \oplus m_k\right)$, the adversary needs to solve $m_k = S\left(p_k\right) \oplus S^{-1}(0)$, where both m_k and S are unknown. The adversary must cryptanalyze both the chaotic map and the S-box simultaneously, which strengthens the chaotic map against chosen-ciphertext attacks.

F. COMPUTATIONAL SPEED ANALYSIS

The time complexity of the proposed encryption algorithm (Algorithm 1) is $O\left(T_N + n\right)$, where T_N is the chaotic transient length and n is the image size. Namely, Steps 1 and 2 of are $O(1)$, Step 3 is $O(T_N)$ and Steps 4 through 6 are $O(n)$. Since, T_N is constant, Algorithm 1 is $O(n)$.

TABLE 14. Medical images used for speed testing.

Image set	Image size	Set size
X-Ray [48]	1338×1094	1
CT Scan [49]	750×870	35
MRI [47]	512×512	361

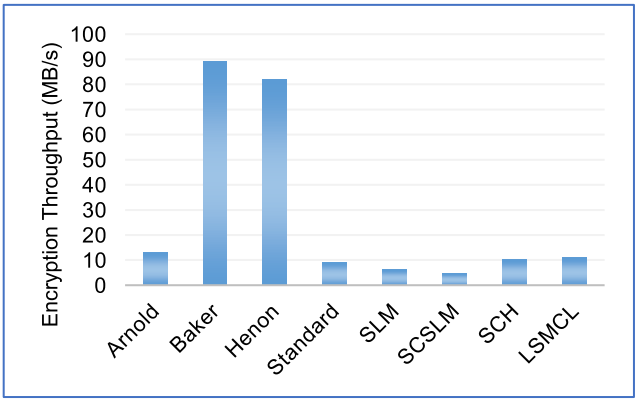

FIGURE 11. Encryption throughput of the proposed scheme.

To measure the speed of the proposed encryption framework, it was implemented in Java and run on JavaSE 1.8 virtual machine on a PC with Intel Core i7-4790 @ 3.6GHz base speed and 32GB of RAM. The encryption parameters were set to a 128-bit key, $\boldsymbol{K_S}$. The program was then used to encrypt the three medical image sets of varying sizes as specified in Table 14.

Encryption throughput is calculated as the size of data encrypted per second. Figure 11 shows the average encryption throughput for the proposed framework with each of the chaotic maps. As shown in Figure 11, the baker map achieves the best performance with encryption throughput averaging at 89 MB/s.

With such a throughput, the proposed encryption framework is well suited for real-time encryption and decryption of medical image data. For instance, the MRI image set consisting of three hundred and sixty-one images totaling 94.6 MB can be encrypted in less than 1.1 seconds. However, more sophisticated chaotic maps involving one or more sine operations, consume dramatically more time, which renders them unsuitable for real-time applications. For instance, the sine-chaotified sine-logistic 2D map (SC-SLM), the slowest among the evaluated chaotic maps, takes about 19.2 seconds to encrypt the 94.6-MB MRI image set.

Next, we study the effect of image size on the encryption throughput. For instance, in Figure 12, the encryption throughput for the proposed framework with Baker map is shown for images of varying size. The figure reveals that encryption throughput is almost constant regardless of the image size. This conforms with our earlier analysis that the complexity of Algorithm 1 is $O(n)$.

As shown in Table 15, the encryption time of the proposed framework with Baker map is broken down into three major components. The first component is the S-box construction

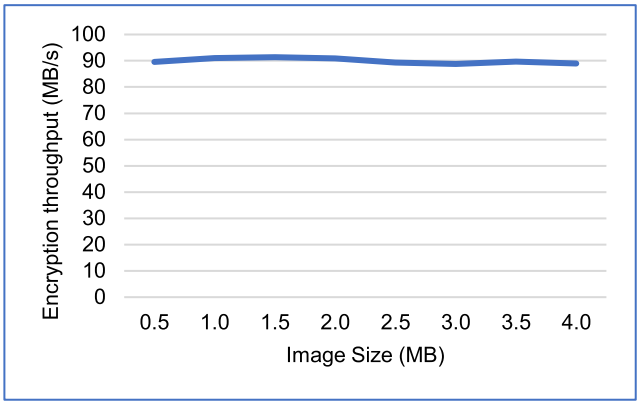

FIGURE 12. Encryption throughput of the proposed framework with Baker map with varying image sizes.

TABLE 15. Encryption time components for varying image size.

Image Size (MB)	Encryption time (ms)			
	S-box construction	Chaotic iteration	Pixel substitution	Total
0.5	0.024	3.649	2.160	5.833
1.0	0.028	7.502	4.403	11.932
1.5	0.027	10.920	6.434	17.380
2.0	0.027	14.557	8.640	23.225
2.5	0.027	18.048	10.703	28.777
3.0	0.028	21.927	12.973	34.929
3.5	0.028	25.992	15.337	41.357
4.0	0.028	29.542	17.375	46.945

TABLE 16. Comparison of entropy and spatial correlation of cipher images encrypted with related image encryption schemes.

Scheme	Entropy		Correlation		
	256×256	512×512	H	V	D
Proposed	7.9977	7.9995	-0.0054	0.0088	-0.0054
Ref. [1]	-	-	-0.0133	0.0058	0.0079
Ref. [2]	7.9976	-	-0.0187	-0.0182	0.0074
Ref. [3]	7.9577		0.0118	0.0107	0.0119
Ref. [5]	-	7.9992	0.0007	-0.0028	-0.0001
Ref. [6]	-	7.9993	0.0013	-0.0049	0.0057
Ref. [7]	-	7.9994	0.0035	0.0003	0.0034
Ref. [8]	7.9989	7.9993	-0.0002	-0.0024	0.0013

time, which approximately takes 28 μs, independent of the image size. The second component is the chaotic mask generation time, which takes a time linear in the size of the plain image. The last component is the substitution and XORing of pixels, which increases linearly with image size. The overhead of the proposed S-box construction method is relatively negligible, considering the additional security gained, which justifies the design of the proposed framework.

V. PERFORMANCE COMPARISON

To demonstrate the competitiveness of the proposed framework and highlight its advantages, we present comprehensive comparisons with related medical image encryption schemes. The comparisons presented here include statistical analysis, differential analysis, and encryption speed.

TABLE 17. Comparison of differential attack metrics with related image encryption schemes.

Scheme	Differential Analysis	
	UACI	NPCR
Proposed	33.4644	99.6095
Ref. [1]	33.4715	99.6073
Ref. [2]	33.4590	99.6100
Ref. [5]	33.4682	99.6082
Ref. [6]	33.4121	99.6536
Ref. [7]	33.4423	99.6071
Ref. [55]	33.41	99.79
Ref. [8]	33.42	99.58

TABLE 18. Comparison of encryption throughput with related image encryption schemes.

Scheme	Implementation	Throughput
Proposed	Java / Core i7 @ 3.6GHz	91.4 MB/s
Ref. [1]	Mathematica / Xeon @ 3.6 GHz	2.5 MB/s
Ref. [29]	— / Core i5 @ 2.6 GHz	9.6 MB/s
Ref. [7]	Mathematica / Core i7 @2.2 GHz	2.8 MB/s
Ref. [56]	MATLAB / Core i5 @ 3.4 GHz	0.1 MB/s
Ref. [27]	C++ / Core i5 @ 3.1 GHz	55.2 MB/s
Ref. [8]	— / —	0.2 MB/s

Table 16 compares the entropy and spatial correlation of cipher images generated by the proposed framework with those reported by other schemes. The results indicate that the proposed framework achieves a correlation value that is very close to the ideal value and in harmony with the results of the other schemes.

Table 17 compares the plain image sensitivity of the proposed framework with related schemes. Results show that the proposed framework achieves some of the best values of UACI and NPCR among related schemes. These results indicate that the proposed scheme offers high immunity against differential attacks.

Table 18 compares the encryption speed of the proposed framework with related image encryption schemes. For fairness, the software and hardware specifications reported by each of the schemes are indicated next to each scheme. Apparently, the proposed framework performs much faster than its competitors.

VI. CONCLUSION AND FUTURE WORK

By efficiently employing cryptographic primitives, the proposed medical image encryption framework achieves 1) an exceptional throughput suitable for real-time encryption, and 2) an enhanced resistance to chosen-plaintext, chosen-ciphertext and reset attacks. The security and efficiency advantages of the proposed framework can be extended to any classic, modern or future chaotic map. Moreover, the proposed framework can employ a class of efficient key-dependent S-box construction methods including the proposed key-dependent S-box construction method based on MT19937 PRNG, which offers a larger key space and faster construction times. When the proposed framework was tested with eight classical and modern chaotic maps, the best encryption throughput obtained was about 90 MB/s, achieved

with Baker map and Henon map. However, the proposed framework requires a lossless communication channel, which is desirable for accurate medical diagnosis. An interesting prospect for research extending this work is to investigate how the proposed framework may benefit from hardware acceleration for implementing cryptographic primitives. Developing efficient embedded implementation for medical imaging devices supporting DICOM standard is another proposed future work.

REFERENCES

[1] 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.

[2] 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.

[3] S. Heidari, M. Naseri, and K. Nagata, "Quantum selective encryption for medical images," *Int. J. Theor. Phys.*, vol. 58, no. 11, pp. 3908–3926, Nov. 2019.

[4] 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.

[5] 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.

[6] 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.

[7] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," (in English), *Optik*, vol. 147, pp. 88–102, Oct. 2017.

[8] 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.

[9] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, "Colour light field image encryption based on DNA sequences and chaotic systems," *Nonlinear Dyn.*, vol. 99, no. 2, pp. 1587–1600, Jan. 2020.

[10] Z. Gan, X. Chai, K. Yuan, and Y. Lu, "A novel image encryption algorithm based on LFT based S-boxes and chaos," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8759–8783, Apr. 2018.

[11] D. Lambić, "A novel method of S-box design based on chaotic map and composition method," *Chaos, Solitons Fractals*, vol. 58, pp. 16–21, Jan. 2014.

[12] D. Lambić, "A novel method of S-box design based on discrete chaotic map," *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, Mar. 2017.

[13] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Process.*, vol. 155, pp. 391–402, Feb. 2019.

[14] A. Zahid and M. Arshad, "An innovative design of substitution-boxes using cubic polynomial mapping," *Symmetry*, vol. 11, no. 3, p. 437, Mar. 2019.

[15] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019.

[16] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.

[17] J. A. P. Artiles, D. P. B. Chaves, and C. Pimentel, "Image encryption using block cipher and chaotic sequences," *Signal Process., Image Commun.*, vol. 79, pp. 24–31, Nov. 2019.

[18] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[19] Z. Hua, Y. Zhou, and B. Bao, "Two-dimensional sine chaotification system with hardware implementation," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 887–897, Feb. 2020.

[20] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[21] X. Wang, Ü. Çavu o lu, S. Kacar, A. Akgul, V.-T. Pham, S. Jafari, F. Alsaadi, and X. Nguyen, "S-box based image encryption application using a chaotic system without equilibrium," *Appl. Sci.*, vol. 9, no. 4, p. 781, Feb. 2019.

[22] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, Jan. 2018.

[23] P. Devaraj and C. Kavitha, "An image encryption scheme using dynamic S-boxes," *Nonlinear Dyn.*, vol. 86, no. 2, pp. 927–940, Oct. 2016.

[24] E. Hasanzadeh and M. Yaghoobi, "A novel color image encryption algorithm based on substitution box and hyper-chaotic system with fractal keys," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7279–7297, Mar. 2020.

[25] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[26] A. Belazi, A. A. A. El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Opt. Lasers Eng.*, vol. 88, pp. 37–50, Jan. 2017.

[27] X. Zhang, Y. Mao, and Z. Zhao, "An efficient chaotic image encryption based on alternate circular S-boxes," *Nonlinear Dyn.*, vol. 78, no. 1, pp. 359–369, Oct. 2014.

[28] 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.

[29] 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.

[30] Attaullah, S. S. Jamal, and T. Shah, "A novel algebraic technique for the construction of strong substitution box," *Wireless Pers. Commun.*, vol. 99, no. 1, pp. 213–226, Mar. 2018. [Online]. Available: https://link.springer.com/article/10.1007/s11277-017-5054-x

[31] L. Yi, X. Tong, Z. Wang, M. Zhang, H. Zhu, and J. Liu, "A novel block encryption algorithm based on chaotic S-box for wireless sensor network," *IEEE Access*, vol. 7, pp. 53079–53090, 2019.

[32] T. Farah, R. Rhouma, and S. Belghith, "A novel method for designing S-box based on chaotic map and teaching–learning-based optimization," *Nonlinear Dyn.*, vol. 88, no. 2, pp. 1059–1074, Apr. 2017.

[33] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, Feb. 2017.

[34] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017.

[35] D. Lambić, "S-box design method based on improved one-dimensional discrete chaotic map," *J. Inf. Telecommun.*, vol. 2, no. 2, pp. 181–191, Apr. 2018.

[36] X. Wang, A. Akgul, U. Cavusoglu, V.-T. Pham, D. V. Hoang, and X. Nguyen, "A chaotic system with infinite equilibria and its S-box constructing application," *Appl. Sci.*, vol. 8, no. 11, p. 2132, Nov. 2018.

[37] L. Liu, Y. Zhang, and X. Wang, "A novel method for constructing the S-box based on spatiotemporal chaotic dynamics," *Appl. Sci.*, vol. 8, no. 12, p. 2650, Dec. 2018.

[38] E. Al Solami, M. Ahmad, C. Volos, M. Doja, and M. Beg, "A new hyper-chaotic system-based design for efficient bijective substitution-boxes," *Entropy*, vol. 20, no. 7, p. 525, Jul. 2018.

[39] M. Ahmad, D. Bhatia, and Y. Hassan, "A novel ant colony optimization based scheme for substitution box design," *Procedia Comput. Sci.*, vol. 57, pp. 572–580, Jan. 2015.

[40] A. Zahid, M. Arshad, and M. Ahmad, "A novel construction of efficient substitution-boxes using cubic fractional transformation," *Entropy*, vol. 21, no. 3, p. 245, Mar. 2019.

[41] 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.

[42] Ü. Çavu o lu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons Fractals*, vol. 95, pp. 92–101, Feb. 2017.

[43] T. Shah and D. Shah, "Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over $\mathbb{Z}2$," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1219–1234, Jan. 2019.

[44] (Aug. 8, 2020). *SageMath*. [Online]. Available: http://www.sagemath.org

[45] F. Özkaynak, "Brief review on application of nonlinear dynamics in image encryption," *Nonlinear Dyn.*, vol. 92, no. 2, pp. 305–313, Apr. 2018.
[46] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102361.
[47] (May 5, 2020). *DICOM Library*. [Online]. Available: https://dicomlibrary.com?study=1.2.826.0.1.3680043.8.1055.1.20111102150758591.92402465.76095170
[48] (May 5, 2020). *Case Courtesy of Dr Mohammad A. ElBeialy, Radiopaedia.org*. [Online]. Available: https://radiopaedia.org/cases/5th-finger-pip-joint-fracture-dislocation-with-volar-plate-fracture
[49] (5-May-2020). *Case Courtesy of Dr Ammar Haouimi*. [Online]. Available: https://radiopaedia.org/cases/abdominal-aortic-aneurysm-37
[50] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[51] E. Barker and J. Kelsey, "NIST special publication 800-90: Recommendation for random number generation using deterministic random bit generators," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Mar. 2007.
[52] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "Generalized majority logic criterion to analyze the statistical strength of S-boxes," *Zeitschrift für Naturforschung A*, vol. 67, no. 5, pp. 282–288, May 2012.
[53] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[54] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *J. Sel. Areas Telecommun.*, vol. 2, no. 4, pp. 31–38, Apr. 2011.
[55] Z. M. Z. Muhammad and F. Özkaynak, "An image encryption algorithm based on chaotic selection of robust cryptographic primitives," *IEEE Access*, vol. 8, pp. 56581–56589, 2020.
[56] Z. Tang, J. Song, X. Zhang, and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Opt. Lasers Eng.*, vol. 80, pp. 1–11, May 2016.

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, Storrs, CT, USA, in 2010.

He is currently an Assistant Professor with the Electrical Engineering Department, Taif University, Saudi Arabia. He has been an Assistant Professor with the Computer Engineering Department, Cairo University, since 2011. He has published several research papers in high-impact journals and international conferences. He has co-advised. His current research interests include information security and computer networks.

HESHAM ALHUMYANI received the B.Sc. degree (Hons.) in computer engineering from Umm Al-Qura University, Makkah, Saudi Arabia, in 2009, and the M.Sc. and Ph.D. degrees in computer science and engineering from the University of Connecticut, Storrs, CT, USA, 2013 and 2016, respectively. He is currently an Assistant Professor with the Department of Computer Engineering, College of Computers and Information Technology, Taif University, Saudi Arabia. He is also the Dean of the College of Computers and Information Technology and a Teaching Staff Member with the Department of Computer Engineering, Taif University. He has published many research papers in international journals and conference proceedings. His current research interests include wireless sensor networks, underwater wireless sensor networks, image encryption, and the Internet of Things.

MEHEDI MASUD (Senior Member, IEEE) received the Ph.D. degree in computer science from the University of Ottawa, Canada.

He is currently a Professor with the Department of Computer Science, Taif University, Taif, Saudi Arabia. He has authored or coauthored around 70 publications, including refereed the IEEE/ACM/Springer/Elsevier journals, conference papers, books, and book chapters. His research interests include machine learning, distributed algorithms, data security, formal methods, and health analytics.

Dr. Masud has served as a Technical Program Committee Member in different international conferences. He was a recipient of a number of awards including, the Research in Excellence Award from Taif University. He is on an Associate Editorial Board of IEEE Access, the *International Journal of Knowledge Society Research (IJKSR)*, and an Editorial Board Member of the *Journal of Software*. He has also served as a Guest Editor for *ComSIS Journal* and the *Journal of Universal Computer Science (JUCS)*. He is a member of ACM.

SULTAN S. ALSHAMRANI received the bachelor's degree (Hons.) in computer science from Taif University, Saudi Arabia, in 2007, the master's degree in information technology, specialized in computer networks from The University of Sydney, Sydney, NSW, Australia, and the Ph.D. degree from the University of Liverpool, U.K.

He is currently working as an Assistant Professor with Taif University. He is also the Head of the Department of Information Technology and the Chairman of the Committee of Faculty Members Affairs.

OMAR CHEIKHROUHOU received the B.S., M.S., and Ph.D. degrees in computer science from the National School of Engineers, Sfax, in March 2012. His Ph.D. deals with security in Wireless Sensor Networks and more precisely with the Secure Group Communication in Wireless Sensor Networks.

He is currently an Assistant Professor with the College of Computer and Information Technology, Taif, Saudi Arabia. He is also a member of the CES Laboratory (Computer and Embedded System), National School of Engineers, University of Sfax. His current research interests include over several areas related to wireless sensor networks, cybersecurity, and multi-robot system coordination. He has several publications in several high-quality international journals and conferences.

Dr. Cheikhrouhou has received several me awards, including the Governor Prize from the Governor of Sfax in 2005.

GHULAM MUHAMMAD (Senior Member, IEEE) received the B.S. degree in computer science and engineering from the Bangladesh University of Engineering and Technology, in 1997, and the M.S. degree and the Ph.D. degree in electrical and computer engineering from Toyohashi University and Technology, Japan, in 2003 and 2006, respectively.

He is currently a Professor with the Department of Computer Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also involved in many research projects as a Principal Investigator and a Co-Principal Investigator. He is also affiliated with the Center of Smart Robotics Research, CCIS, King Saud University. He has authored or coauthored more than 200 publications, including the IEEE/ACM/Springer/Elsevier journals, and flagship conference papers. He has two U.S. patents. His research interests include image and speech processing, smart healthcare, machine learning, and AI.

Dr. Muhammad was a recipient of the Japan Society for Promotion and Science (JSPS) fellowship from the Ministry of Education, Culture, Sports, Science and Technology, Japan. He received the Best Faculty Award of the Computer Engineering Department, KSU, from 2014 to 2015. He has supervised more than 15 Ph.D. and Master Theses.

M. SHAMIM HOSSAIN (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada.

He is currently a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa. His research interests include cloud networking, smart environment (smart city, smart health), AI, deep learning, edge computing, the Internet of Things (IoT), multimedia for health care, and multimedia big data. He has authored or coauthored more than 250 publications, including refereed journals, conference papers, books, and book chapters. Recently, he co-edited a book on *Connected Health in Smart Cities* (Springer). He has one U.S. patent (in process).

Dr. Hossain is a Senior Member of ACM. He was a recipient of a number of awards, including the Best Conference Paper Award and the 2016 *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, the Nicolas D. Georganas Best Paper Award, the 2019 King Saud University Scientific Excellence Award (Research Quality), and the Research in Excellence Award from the College of Computer and Information Sciences (CCIS), King Saud University (three times in a row). He has served as the Co-Chair, the General Chair, the Workshop Chair, the Publication Chair, and the TPC for more than 12 IEEE and ACM conferences and workshops. He also is the Co-Chair of the Third IEEE ICME workshop on Multimedia Services and Tools for smart-health (MUST-SH 2020). He has served as a Guest Editor for *IEEE Communications Magazine*, *IEEE Network*, the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY IN BIOMEDICINE (also JBHI), the IEEE TRANSACTIONS ON CLOUD COMPUTING, the *International Journal of Multimedia Tools and Applications* (Springer), *Cluster Computing* (Springer), *Future Generation Computer Systems* (Elsevier), *Computers and Electrical Engineering* (Elsevier), *Sensors* (MDPI), and the *International Journal of Distributed Sensor Networks*. He is on the Editorial Board of several SCI/ISI-Indexed Journals/Transactions, including the IEEE TRANSACTIONS ON MULTIMEDIA, *IEEE Multimedia*, *IEEE Network*, the IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, the *Journal of Network and Computer Applications* (Elsevier), and the *International Journal of Multimedia Tools and Applications* (Springer). He also serves as a Lead Guest Editor for *IEEE Network*, the *ACM Transactions on Internet Technology*, the *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, and *Multimedia Systems* Journal.

ALAA M. ABBAS received the Ph.D. degree from Menofia University, Egypt, in 2008.

He is currently an Associate Professor with the Electronics and Electrical Communications Engineering Department, Faculty of Electronic Engineering, Menoufia University. He is also an Assistant Professor with the Electrical Engineering Department, College of Engineering, Taif University, Saudi Arabia. His areas of interest include image processing, watermarking, image encryption, and cryptography.