IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received August 30, 2020, accepted October 5, 2020, date of publication October 20, 2020, date of current version November 5, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3032403

Efficient Image Encryption Scheme Using Henon Map, Dynamic S-Boxes and Elliptic Curve Cryptography

SALEH IBRAHIM[1,2] AND AYMAN ALHARBI[3]
[1]Electrical Engineering Department, College of Engineering, Taif University, Al-Hawiya 21974, Saudi Arabia
[2]Department of Computer Engineering, Faculty of Engineering, Cairo University, Giza 12613, Egypt
[3]Department of Computer Engineering, Umm Al-Qura University, Makkah 21955, Saudi Arabia

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

ABSTRACT Image encryption schemes can be vulnerable to a variety of cryptanalysis attacks. The use of key-dependent dynamic S-boxes has been shown to improve security. Threats of chosen-plaintext and chosen-ciphertext attacks still linger. In this paper, we present an efficient algorithm for constructing secure dynamic S-boxes derived from Henon map. We use the proposed dynamic S-box to construct an image encryption scheme that includes a novel combination of security features to resist chosen-plaintext and chosen-ciphertext attacks. Namely, a hash verification step at the end of the decryption procedure effectively thwarts chosen-ciphertext attacks. The hash also serves as an image dependent initialization for the keystream, which together with using an image dependent S-box resist known-plaintext attacks. Furthermore, encryption keys are protected against cryptanalysis using elliptic curve cryptography (ECC).Therefore, the recovery of secret keys is as hard as the elliptic curve discrete logarithm problem even in the unlikely case of the recovery of the temporary S-box or keystream. Our evaluation of the proposed image encryption scheme reveals that it achieves a higher security standard than existing techniques. Moreover, the proposed scheme is computationally efficient with encryption throughput approaching 60 MB/s.

INDEX TERMS Chaotic map, elliptic curve cryptography, image encryption, substitution box.

I. INTRODUCTION

The process of securing images content and preventing it from potential malicious access has become an integral part for various applications such as securing users' images when sharing data through social media, secure cloud environment and copyright protection. Encryption techniques transform a plaintext message to corresponding ciphertext message such that only an authorized user, who has access to a confidential decryption key, can recover the original message.

A secure encryption scheme must satisfy certain criteria such as confusion, diffusion and key-dependence requirements [1]. However, the high correlation between adjacent image pixels presents a special challenge. An adversary can exploit such correlation to launch various statistical attacks and infer some information about the content of the original image. Therefore, additional criteria must be met by image encryption schemes to guarantee immunity to such attacks. A common technique to overcome this problem is complementary addition with a pseudorandom number (PRN) sequence. The image encryption method proposed by [2] uses a PRN sequence, which is generated using a complete order defined on the points of an elliptic curve (EC) with secret parameters. Another well-studied PRN complementary padding method uses Henon chaotic map [3], which yields extremely efficient implementations [4].

Another peculiar feature of image encryption is the large volume of data and the subsequent requirement for efficient algorithms for encrypting image data. Asymmetric key encryption techniques, such as RSA and ECC are known for their relatively high computational cost. Therefore, symmetric key encryption algorithms are preferable for encrypting image data. A variety of symmetric key image encryption schemes have been proposed in literature [4]–[6]. Symmetric key techniques based on a cryptographically secure substitution box (S-box) have received special attention in literature such as [7], [8], because of their superior performance advantage.

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

In this paper, we propose a novel image encryption scheme that utilizes elliptic curve cryptography and secure hash algorithms to fend off chosen-plaintext and chosen-ciphertext attacks. The proposed encryption combines the efficiency and desirable statistical properties of Henon map with the additional security provided by dynamic S-box confusion. Our contribution can be summarized in the following points

1) proposing an efficient dynamic S-box construction method based on Henon map,
2) using an elliptic curve cryptosystem technique to protect encryption keys, and
3) using secure hash algorithm to identify malformed cipher message to resist chosen ciphertext attacks.

The rest of the paper is organized as follows: Section 2 covers the necessary background and related work on S-box construction techniques, elliptic curve cryptography and Henon map. Section 3 describes the proposed image encryption approach, including the new dynamic S-box construction algorithm. Section 4 evaluates the performance of the S-box construction algorithm and the strength of the generated S-boxes. Section 5 evaluates the performance of image encryption scheme. Section 6 highlights the advantages of the proposed image encryption scheme in comparison to related schemes. Finally, concluding remarks are drawn in Section 7.

II. BACKGROUND AND RELATED WORK

A secure encryption scheme must achieve Shannon's objectives of confusion and diffusion. To satisfy the confusion objective of cryptographic systems, symmetric key schemes often use substitution boxes as a basic building block. An $n \times m$ S-box carries out a substitution function which transforms a set of n input bits into a corresponding set of m output bits. The proposed encryption scheme uses invertible $n \times n$ S-boxes.

A. S-BOX BASED ENCRYPTION

Two main categories of S-boxes are used in encryption methods: static S-boxes and dynamic S-boxes [9]. A dynamic S-box has an advantage over a static S-box due to the former's additional key space. Consequently, dynamic S-boxes harden a cipher against potential brute-force attacks by increasing the key space [10]. In order to measure the strength of an S-box, researchers compare their S-box performance against available benchmark including Nonlinearity (NL), Linear Approximation Probability (LAP), Differential Approximation Probability (DAP), Strict Avalanche Criterion (SAC) and Bit Independence Criterion (BIC) [2], [7], [10]–[17]. Efficient methods for S-box construction, such as [7], [11], [14], generate a single or a limited number of static S-boxes. To address this limitation, several dynamic S-box construction methods have been developed such as [1], [2], [10], [12], [13], [16].

A dynamic S-box was utilized in [1]. The algorithm consists of five steps in order to construct a randomized S-box. However, one of the proposed steps depends on brute-force method to calculate all points of the chosen finite elliptic curve, which has the limitation of using small parameters. Therefore, the algorithm may be vulnerable to brute-force attacks. Reference [18] offers a similar construction algorithm, which shares the same limitation.

Reference [16], presents a secure dynamic S-boxes based on linear fractional transformations with randomized coefficients. Although their proposed algorithm is efficient, it has just about 2^{32} key space, which is within the reach of brute-force attacks.

In [10], authors proposed a new dynamic S-box, which utilizes chaos and the composition of basis S-boxes. The main drawback of this method is its relatively high computational cost for large key sizes.

Soft-computing methods have been applied to the problem of S-box construction. Reference [13] uses a genetic algorithm optimization to gradually improve the constructed S-box to achieve the nonlinearity and other strength objectives. However, soft-computing methods are not fast enough to allow real-time construction of dynamic S-boxes.

B. CHAOTIC SYSTEMS

Chaos systems are dynamic systems which are highly sensitive to initial conditions. Therefore, they are ideal candidates for generating cryptographic pseudorandom sequences. Chaotic sequences such as Henon map, Baker map, logistic map, Arnold cat mat, etc., have been used in many encryption algorithms that are found in literature.

Reference [19], proposes a new chaos map and a corresponding S-box-based encryption scheme with chaotic block permutation. In [14], the proposed S-box is applied along with a chaotic map for image encryption.

Recently, Hegui Zhu *et al.* in [20] proposed a 2-dimensional logistic-sine-modulated sine-coupling-logistic (LSMCL) chaotic map with two round of diffusion and permutation. The proposed system exhibits high security against standards attacks. However, the composition of multiple simple chaotic systems to enhance chaotic performance comes at an increased computational cost.

In [21], the authors introduced a new 1-D chaotic map by exponential chaotic model. They used the exponential arithmetic operation for nonlinearity. Their system can produce a new chaotic map from base maps (two maps) and exponent maps. In addition, the produced chaotic map shows a better performance in the presence of noise. The authors in [22] proposed a hybrid chaos system that combines more than one map in a cascading manner to produce new chaotic maps with improved chaos complexity.

C. HENON MAP

M. Henon proposed this classical dynamic system in discrete time domain [3]. Henon map transforms a point (x_p, y_p) into (x_{p+1}, y_{p+1}) as follows:

$$x_{p+1} = 1 - ax_p^2 + y_p, \quad y_{p+1} = bx_p \tag{1}$$

where a and b are the Henon map parameters. The behavior of the map depends on the value of a and b. When $a = 1.4$

and $b = 0.3$, the map is guaranteed to be chaotic [4]. Cryptologists leveraged the powerful features of Henon map in cryptographic systems. For image encryption, Henon map can provide confusion and histogram uniformity.

Henon chaotic map is computationally efficient and exhibits near optimal randomness properties. Pseudo-randomness tests, including balance test, run test and auto-correlation test, were performed on Henon map sequence and the reported results were very close to the theoretical optimal [23]. In [24], Henon-based permutations were shown to be closer to a random permutation than those based on Standard map and Arnold Cat map, and thus images scrambled with 3-round Henon map permutation don't contain any visible texture patterns.

D. ELLIPTIC CURVE PRELIMINARY

A finite elliptic curve (FEC) over a prime field is defined by the equation

$$E(p,a,b) = \left\{(x,y) | x,y \in \mathbb{Z}_p, y^2 = x^3 + ax + b \,(\bmod\, p)\right\} \cup \{\mathcal{O}\}, \quad (2)$$

where p is a prime number, $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$, a and $b \in \mathbb{Z}_p$ which satisfy the following criteria

$$4a^3 + 27b^2 \neq 0 \,(\bmod\, p). \quad (3)$$

$\mathcal{O}$ is called "the point at infinity" and serves as a special additive identity element, as will be shown shortly in Equation (4). In practice, $\mathcal{O}$ is represented by a pair of coordinates $\notin \mathbb{Z}_p$.

The inverse of a point $P = (x, y) \in E(p, a, b)$, is

$$-P = \begin{cases} \mathcal{O}, & P = \mathcal{O} \\ (x, p-y), & \textit{otherwise}. \end{cases} \quad (4)$$

For each pair of points $P, Q \in E(p, a, b)$, the sum point $R = P + Q$ is defined as the inverse of the third intersection point of the line $\overleftrightarrow{PQ}$ with the curve E. When $P = -Q$, the result of the addition is defined as the additive identity point $\mathcal{O}$.

$$P + Q = \begin{cases} P, & Q = \mathcal{O} \\ Q, & P = \mathcal{O} \\ \mathcal{O}, & P = -Q \\ R(x_R, y_R), & \textit{otherwise} \end{cases} \quad (5)$$

where $x_R = \lambda^2 - x_P - x_Q \,(\bmod\, p)$, $y_R = \lambda(x_P - x_R) - y_P \,(\bmod\, p)$ and

$$\lambda = \begin{cases} (y_Q - y_P)/(x_Q - x_P), & P \neq Q \\ (3x_P^2 + a)/2y_P, & P = Q \end{cases}$$

For a point $P \in E(p, a, b)$ and a multiplicand $k \in \mathbb{Z}_p$, scalar-point multiplication is defined as

$$kP = \begin{cases} O, & k = 0 \\ P + (k-1)P, & \textit{otherwise} \end{cases} \quad (6)$$

In practice, multiplication is implemented using a variation of the efficient double-and-add algorithm.

According to Hasse's theorem, the number of points on a FEC, $E(p, a, b)$, is bounded by

$$p + 1 - 2\sqrt{p} \leq \#E(p, a, b) \leq p + 1 + 2\sqrt{p}. \quad (7)$$

The elliptic curve discrete logarithm problem (ECDLP) aims to find $k \in \mathbb{Z}_p$, given $P, G \in E(p, a, b)$ such that $kG = P$. There is no efficient algorithm to find k and the hardness of this problem forms the basis of elliptic curve cryptography. Namely, a secret k can be hidden in the structure of $P = kG$.

Since its introduction in 1985 by Koblitz [25] and Miller [26], ECC has been increasingly used in applications to replace the less efficient RSA alternative. A preliminary on elliptic curves and EC cryptosystems can be found in [25]–[28].

E. CHAOS-BASED IMAGE ENCRYPTION

A plethora of chaos-based image encryption schemes have been proposed in literature in the past two decades. The role chaotic sequences play in image encryption varies from controlling pixel location permutation, pixel value substitution or application as an additive mask to pixel values. In this subsection, we review recent chaotic image encryption work most relevant to the proposed scheme. Namely, we focus on chaotic image encryption schemes employing dynamic S-boxes, Henon map, elliptic curve cryptography (ECC) or a combination thereof.

1) S-BOX-BASED CHAOTIC IMAGE ENCRYPTION

Several recent image encryption schemes depend on dynamic S-boxes. Reference [29], proposes an image encryption scheme, which starts by constructing three dynamic S-boxes. Image pixels are XORed with a keystream derived from a chaotic pseudorandom number generator, then each pixel is substituted using a randomly chosen S-boxes.

The scheme proposed in [30] uses a single dynamically constructed S-box for two rounds of chained substitution followed by one round of pixels permutation.

The authors of [31] apply a pixel location permutation, then chaotically choose one of multiple dynamically generated S-boxes, to substitute pixel values.

The schemes in [32] and [14], start with a permutation stage, followed by a dynamic-S-box-based substitution and finally a diffusion stage using a chaotic keystream.

On the other hand, the scheme in [33] starts by a dynamic-S-box-based substitution, then a permutation using a chaotic sequence, and finally a diffusion stage using a fractal image as a keystream.

An image encryption scheme, which starts by a diffusing stage with a chaotic keystream, followed by a substitution stage with 8 dynamic S-boxes, was proposed by [19]. Finally, another chaotic diffusion stage and a block permutation function are applied. A chaotic map was used as a source of the dynamic S-box construction parameters.

In [34], the authors used a similar dynamic S-box construction method to propose an image encryption scheme based on block permutation, substitution and diffusion with chaotic keystream.

The scheme in [35] tries to improve the computational efficiency by keeping few S-boxes and tries to improve security by using the plain image pixels to dynamically modify the S-boxes.

In [36], the authors proposed a novel synchronous chaining structure employing two dynamic S-boxes.

2) HENON MAP-BASED IMAGE ENCRYTION

Recently, several image encryption schemes employing Henon map appeared in literature. The scheme proposed in [37] integrated fractal and 3D Henon maps, with image based initialization, to generate keystreams, which control the a permutation phase, followed by an XOR diffusion phase. The scheme proposed in [24] performed three rounds of permutation-diffusion driven by a 2D Henon map. The initialization of chaotic maps was also derived from the image to resist chosen plaintext attacks.

Another Henon map-based scheme was proposed in [38], in which a modified Henon map controls pixel row and column permutation, whereas diffusion is performed using Sine map. A modified Henon-sine map was proposed in [39] to generate chaotic keystreams which control a DNA-based diffusion phase and a pixel permutation phase. However, the initial values of maps in both schemes are directly derived from secret keys, which make the scheme susceptible to chosen plaintext attacks.

3) ELLIPTIC CURVE-BASED IMAGE ENCRYTION

Several attempts to use ECC for image encryption have been presented in literature. Most recently, the scheme in [40] embeds the pixels of the scrambled image into an elliptic curve to apply ECC, then uses chaos game with DNA for diffusion. SHA-512 of the image was used to generate the initialization of chaotic maps to resist chosen plaintext attacks. However, the use of ECC for actual pixel encryption leads to high computational cost.

The scheme of [2] used EC to construct an S-Box and a pseudorandom keystream. The image dependent initialization was calculated using a simple sum operation, which may be vulnerable to chosen-plaintext attacks.

In [41], an EC public key cryptosystem was employed for the generation of shared encryption key. For actual image encryption, a self-invertible key matrix is multiplied by each image block. However, results of differential analysis expose some weakness.

An earlier scheme in [42] used public key ECC to encrypt diffused image pixels, which again is computationally taxing.

The scheme proposed in [43] combines public key ECC and AES to reduce the number of EC point multiplications and hence provide more efficient image encryption. Although this scheme uses two of the strongest encryption constructs, i.e. ECC and AES, the strength of the resulting scheme is questionable due to the lack of image-dependent initialization.

A comprehensive review of recent image encryption schemes can be found in [44].

Algorithm 1 Precondition Initial Point

Input: Key point (x_K, y_K).
Output: Initial system state (x_0, y_0)

$x_0 \leftarrow \text{abs}(x_K)$, $y_0 \leftarrow \text{abs}(y_K)$
while $x_0 > 0.5$ do
  $x_0 \leftarrow x_0/2$
end while
while $y_0 > 0.5$ do
  $y_0 \leftarrow y_0/2$
end while

III. THE PROPOSED IMAGE ENCRYPTION SCHEME

Prior to the commencement of the proposed scheme, the communicating parties are configured to use an elliptic curve $E(p, a, b)$ and a generating point $G \in E(p, a, b)$. They agree on a shared composite encryption key (K_1, K_2), such that K_1 and $K_2 \in \mathbb{Z}_2^{256}$. The proposed image encryption scheme generates a dynamic S-box modulated by K_1, and an image-dependent chaotic keystream modulated by K_2, which enables the proposed scheme to resist chosen plain-text attacks. Both the construction of the S-box and the generation of the keystream are derived from a Henon map pseudorandom sequence generator.

A. HENON MAP PSEUDORANDOM SEQUENCE GENERATOR

Given an initialization point (x_0, y_0), and a desired output length, t, we propose the following algorithm to generate a sequence of pseudorandom integers modulo-256, denoted $\mathcal{S}^{L,t}_{(x_0,y_0)} = (r_0, r_1, \ldots, r_{t-1})$. Using (1), calculate the next $t + L$ points (x_i, y_i), where $0 \le i \le t + L$, and L is the a constant number of initial iterations to get rid of the transient effect and improve key sensitivity. A pseudorandom integer r_i is obtained from a point (x_i, y_i) using the formula

$$r_i = 2^{24} x_{L+i+1} \; mod \; 256 \tag{8}$$

To avoid sequence divergence, the components of the initialization point (x_0, y_0) are limited in the interval $0 \le x_0, y_0 \le 0.5$. Since the given key point (x_K, y_K) may not fall in this domain, Algorithm 1 is performed to derive the initialization point from the key point.

B. DYNAMIC S-BOX CONSTRUCTION

To construct a bijective 8×8 S-box, the S-box key, K_S, is represented as a pair of double values (x_S, y_S), preconditioned using Algorithm 1. Then the Henon map pseudorandom sequence generator $(r_i) = \mathcal{S}^{L,t}_{(x_0,y_0)}$ is calculated, where $L = 100$, $t = 256\,\omega$, and ω is a parameter determining the number of permutation rounds. The sequence (r_i) is used to

Algorithm 2 Construct S-Box

Inputs: Key point $K_S = (x_S, y_S)$, number of rounds, ω.
Output: S-box $\Pi_{K_S,\omega} = (s_0, s_1, \ldots, s_{255})$.

$s_i \leftarrow i, \forall 0 \leq i \leq 255$ // identity mapping
$(r_0, r_1, \ldots, r_{t-1}) \leftarrow \mathcal{S}^{100,t}_{(x_S,y_S)}$
for $i = 0 : 256\,\omega - 1$, **do**
  swap($s_{i \bmod 256}, s_{r_i}$)
end for

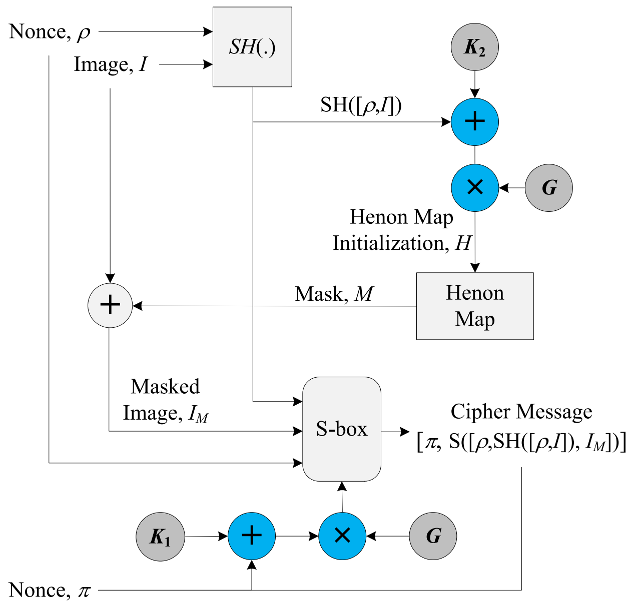


FIGURE 1. Proposed image encryption procedure.

construct the S-box by repeatedly swapping S-box elements guided by the pseudorandom sequence. The details of the S-box construction process are shown in Algorithm 2.

C. IMAGE ENCRYPTION AND DECRYPTION PROCEDURES

During the image encryption/decryption phase, each image passes through three main operations at the sender: 1) hash calculation of the plain image, 2) calculation and application of Henon map mask, 3) application of S-box. The main corresponding three inverse operations are then applied in reverse order at the receiver.

1) ENCRYPTION ALGORITHM

As shown in the block diagram in Figure 1, the encryption procedure starts with a plain image, I. First, two random nonce values π and $\rho \in \mathbb{Z}_2^{256}$ are generated. The nonce, π, along with key K_1 control the construction of a dynamic S-box with key point $K_S = (\pi + K_1)\,G$, where G is generator point of the elliptic curve used for encryption. In this paper, we used a standard elliptic curve known as Curve25519 [45]. For higher levels of security, larger curves such as Curve448 may be used. The important role of elliptic curve multiplication in securing the key, K_1, against cryptanalysis will be discussed in Section 5. Next, we compute the secure hash of the plain image concatenated with random

Algorithm 3 Image Encryption

Input: plain image, (I), session key (K_1, K_2), number of permutation rounds, ω.
Output: cipher message, C.

1, $\rho \xleftarrow{R} \mathbb{Z}_2^{256}$, $\pi \xleftarrow{R} \mathbb{Z}_2^{256}$.
2. $K_S \leftarrow (\pi + K_1)\,G$
3. $(x_S, y_S) \leftarrow$ precondition (double (K_S))
4. $S \leftarrow \Pi_{(x_S,y_S),\omega}$ using Algorithm 2
5. $K_H \leftarrow (SH\,([\rho, I]) + K_2)\,G$
6. $(x_H, y_H) \leftarrow$ precondition(double (K_H))
7. $I_M \leftarrow \mathcal{S}^{100,\#I}_{(x_H,y_H)} \oplus I$
8. $C = [\pi, S\,([\rho, SH\,([\rho, I])\,, I_M])]$ ■

nonce ρ, using the SHA-256 algorithm. The notation $SH(.)$ is short for $SHA256\,([\rho, I])$. The other key point, H, is obtained by adding $SH\,([p, I])$ to key, K_2, and multiplying by the generator point G. Then H is used to seed another Henon map sequence generator to generate an additive chaotic mask. This formulation ensures that the chaotic mask is sensitive to changes in the plain image and thus resistant to chosen plaintext attacks.

The Henon map key point (x_H, y_H) is derived from the elliptic curve point K_H by taking the least significant 52 bits of each coordinate and converting it to a floating-point, i.e.

$$\text{double}(H) = 2^{-52}\left(x_{K_H} mod 2^{52}, y_{K_H} mod 2^{52}\right). \quad (9)$$

Henon pseudorandom sequence generator is used to generate the sequence, $M = \mathcal{S}^{100,\#I}_{x_H,y_H}$, where $\#I$ denotes the number of pixels in image I. The mask M is then XORed with plain image pixels to introduce confusion and histogram uniformity into the resulting masked image, I_M. The S-box substitution is applied byte-by-byte to ρ, $SH\,(I)$, and I_M to produce the cipher message $C = [\pi, S\,([\rho, SH\,([\rho, I])\,, I_M])]$. The detailed steps of the encryption algorithm are listed in Algorithm 3.

2) DECRYPTION ALGORITHM

The block diagram of the decryption procedure is shown in Figure 2. First, we extract π from the cipher message and use it along with K_1 to construct the inverse S-box S^{-1}. We then apply the inverse S-box to the remaining part of the cipher message to obtain the random nonce, ρ, the hash of the nonce and image, $SH\,([\rho, I])$ and the masked image, I_M. Using $SH\,([\rho, I])$ and key, K_2, we obtain the pseudorandom mask, M, by following the same steps used during encryption. The decrypted image I_D is the XOR of I_M with M. If the decryption is successful, then $SH\,([p, I_D])$ must match the $SH\,([p, I_D])$ extracted from the cipher message. To resist chosen-ciphertext attacks, the algorithm withholds I_D if this integrity check fails. The detailed steps of the decryption algorithm are listed in Algorithm 4.

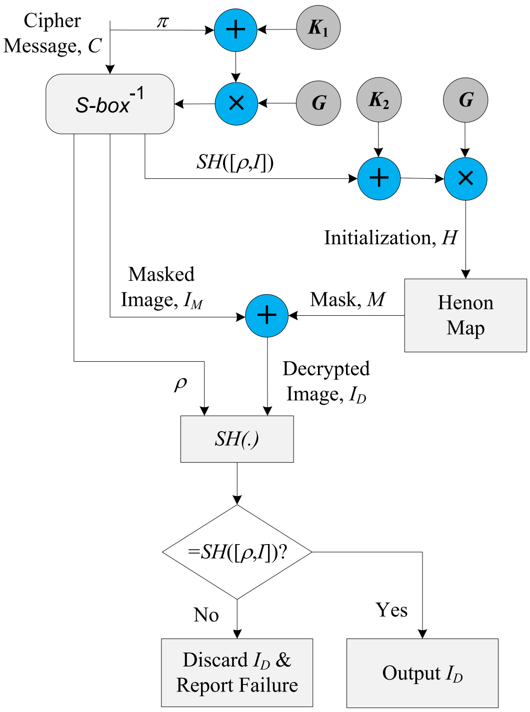


FIGURE 2. Proposed image decryption procedure.

Algorithm 4 Image Decryption

Input: cipher message C, session key (K_1, K_2), number of permutation rounds, ω.
Output: decrypted image, I_D.

1. $[\pi, Q] \leftarrow C$
2. $K_S \leftarrow (\pi + K_1)\, G$
3. $(x_S, y_S) \leftarrow$ precondition (double (K_S))
4. $S \leftarrow \Pi_{(x_S,y_S),\omega}$ using Algorithm 2
5. $[\rho, SH([\rho, I]), I_M] = S^{-1}(Q)$.
6. $K_H \leftarrow (SH([\rho, I]) + K_2)\, G$
7. $(x_H, y_H) \leftarrow$ precondition (double (K_H))
8. $I_D \leftarrow S^{100,\#I}_{(x_0,y_0)} \oplus I_M$
9. If $SH([\rho, I]) = SH([\rho, I_D])$, output I_D. Otherwise, discard I_D and report failure ■

IV. EVALUATION OF S-BOX CONSTRUCTION ALGORITHM

To evaluate the security of the proposed encryption scheme, we first evaluate the cryptographic strength of the constructed S-boxes. Namely, we generate dynamic S-boxes with random initialization (x_S, y_S), then test the strength of each generated S-box by running a set of standard S-box tests, including nonlinearity, linear approximation probability, differential approximation probability, bit-independence criterion, and the strict avalanche criterion [46]–[48]. Table 1 lists the standard criteria used for testing S-boxes and the optimal value corresponding to each test.

Table 2 shows a sample S-box in the standard 16 × 16 format. Table 3 shows the tests results for some of the high-quality S-boxes that are generated using the proposed algorithm. All test results in Table 3 are very close to the optimal values indicated in Table 1. To compare the nonlinearity of the S-boxes generated by the proposed scheme with respect to other dynamic S-box construction methods, we constructed ten thousand S-boxes with random keys using each of the compared methods and reported the resulting statistics in Table 4 . Results indicate that the proposed method generates good nonlinearity with higher probability than other methods.

TABLE 1. Standard tests of S-box cryptographic strength.

Test	Optimal Value
Nonlinearity (NL) Test	120
Linear Approximation Probability (LAP)	0
Differential Approximation Probability (DAP)	0
Strict Avalanche Criterion (SAC)	0.5
Bit Independence Criterion (BIC)	0.5

TABLE 2. S-box corresponding to $(x_S, y_S) = (0.7854811649683301, 0.9868192007103721)$ and $\omega = 1$.

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

TABLE 3. S-box analysis results for a sample of S-boxes generated by the proposed algorithm with $\omega = 1$.

Box	NL	LAP	DAP	SAC		BIC-SAC	
				min.	max	min.	max
S_1 [a]	106	0.1250	0.0391	0.4219	0.5781	0.4668	0.5254
S_2 [b]	106	0.1328	0.0391	0.4062	0.5781	0.4766	0.5254
S_3 [c]	106	0.1328	0.0391	0.4219	0.5781	0.4688	0.5293
S_4 [d]	106	0.1250	0.0391	0.4063	0.5781	0.4844	0.5195

[a] $(x_S, y_S) = (0.7523418512788702, 0.8479819270232232)$
[b] $(x_S, y_S) = (0.015801752485450238, 0.09712270996915162)$
[c] $(x_S, y_S) = (0.0352940019873631, 0.33767566645781344)$
[d] $(x_S, y_S) = (0.1411387127531113, 0.6636150003084085)$

Table 5 compares the results of standard tests of a selected sample of dynamic S-boxes generated by the proposed algorithm and dynamic S-boxes constructed by rival methods. Clearly, the proposed dynamic S-box construction algorithm is able to construct high quality S-boxes, which pass test results very close to the optimal values indicated earlier in Table 1.

The main advantages of using Henon map as a source of entropy for S-box construction are the relative simplicity and computational efficiency of Henon map.

V. PERFORMANCE OF THE PROPOSED IMAGE ENCRYPTION SCHEME

Due to the peculiar nature image data and its related applications, a secure image encryption scheme has other objectives

TABLE 4. Statistical comparison of nonlinearity of a random sample of 100'000 S-boxes by each method.

NL	Ref. [2]	Ref. [49]	Ref. [10]	Proposed
Min.	56	0	82	82
Avg.	92.44	89.67	99.08	99.07
Max.	102	106	106	106

TABLE 5. Test results of high-quality S-boxes generated by the proposed algorithm compared to results of relevant dynamic S-box algorithms.

S-Box	LAP	DAP	SAC Max. offset	BIC Max. offset
S_1	0.1250	0.0391	0.0781	0.0332
S_2	0.1328	0.0391	0.0938	0.0254
S_3	0.1328	0.0391	0.0781	0.0312
S_4	0.1250	0.0391	0.0781	0.0195
Ref. [50], 2020	0.1328	0.0391	0.1094	0.0508
Ref. [51], 2020	0.1328	0.0391	0.1094	0.0313
Ref. [2], 2019	0.1484	0.0391	0.0938	0.0449
Ref. [16], 2019	0.1406	0.054	0.0938	0.0391
Ref. [15], 2018	0.1875	0.0391	0.1094	0.0352
Ref. [13], 2017	0.1328	0.0391	0.1406	0.0254
Ref. [49], 2017	0.1328	0.0391	0.1250	0.0273
Ref. [52], 2017	0.1250	0.0391	0.1094	0.0332
Ref. [10] , 2014	0.0938	0.0313	0.0938	0.0293
Ref. [53], 2012	0.1406	0.0391	0.0781	0.0313

in addition to confusion and diffusion. According to [1], an image encryption scheme should be; 1) secure, 2) computationally efficient, 3) based on standardized algorithms, and 4) flexible, and 5) the scheme should produce a cipher image not larger than the plain image. To evaluate the performance of the proposed scheme, standard tests are performed including statistical analysis, differential analysis, key sensitivity analysis, key space analysis, and encryption speed analysis.

A. STATISTICAL ANALYSIS

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

1) HISTOGRAM TEST

The closer to a uniform (flat) distribution the histogram of the encrypted image, the stronger the scheme's resistance to statistical attacks is. We have performed the histogram test to a set of standard images and two special one-color images. Table 6 shows the histograms of the encrypted images generated by the proposed scheme. Histograms appear uniform indicating that the proposed scheme passes this test. Numerically, histogram uniformity can be estimated using χ^2 null hypothesis testing. The test measures how likely the histogram, f_i, matches the histogram of a truly random image with the same number of pixels, N, using the formula

$$X^2 = \sum_{i=0}^{L-1} \left(f_i - \frac{N}{256}\right)^2 \Big/ \left(\frac{N}{256}\right),$$

The resulting X^2, also known as the p-value, is tested against the $\chi^2(255, \alpha)$ distribution, where α is the desired significance level. If the p-value is greater than α, the histogram passes the randomness test. The p-values corresponding to each of the encrypted image histograms are listed in Table 6 , indicating that encrypted images are indistinguishable from random images at significance level $\alpha = 0.05$.

2) CORRELATION TEST

Another common test measures the disparity between the encrypted image and the plain image. The correlation test is utilized to measure how uncorrelated the two images are. Obviously, the optimal correlation is zero. The correlation test is performed as follows:

$$C_{x,y} = \frac{cov(x, y)}{\sqrt{v\,(x)} \cdot \sqrt{v(y)}} \tag{10}$$

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

$$cov\,(x, y) = \frac{1}{N} \sum\nolimits_{j=1}^{N} \left(x_j - \bar{x}\right)\left(y_j - \bar{y}\right),$$
$$v\,(x) = \frac{1}{N} \sum\nolimits_{1j=1}^{N} (x_j - \bar{x})^2, \quad \text{and}$$
$$\bar{x} = \frac{1}{N} \sum\nolimits_{j=1}^{N} x_j.$$

Table 7 shows that the values of correlation are 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.

Table 8 shows the values of correlation between the neighboring pixels in horizontal, vertical and diagonal directions for the plain and encrypted images. The correlation values for plain images are almost 1, which indicates a high correlation between pixels, while the correlation values for the encrypted images are almost 0, which indicates that the proposed scheme succeeds in bringing the correlation between neighboring pixels down to a satisfactory level.

The spatial correlation distribution is depicted in Figure 3 for the plain and encrypted images, illustrating how the strong spatial correlation in the plain image was removed in the encrypted image.

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:

$$E\,(X) = -\sum\nolimits_{j=0}^{L-1} P_j\, log_2 P_j \tag{11}$$

The local Shannon entropy (LSE) is a more reliable metric of randomness than global entropy, because LSE is the mean entropy of a set of randomly selected blocks. Since a perfect cipher image is indistinguishable from a random image,

TABLE 6. Histogram analysis of the proposed scheme.

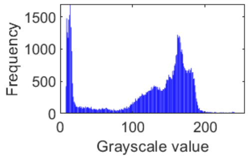
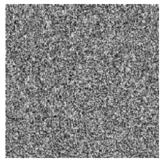
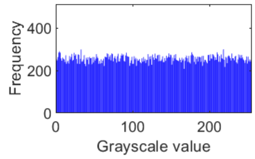
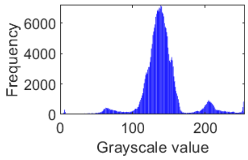
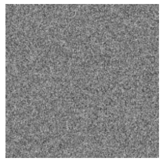
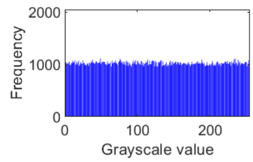
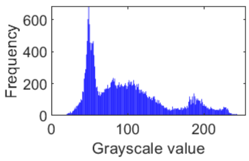
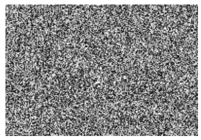
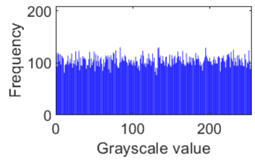
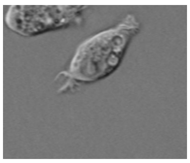
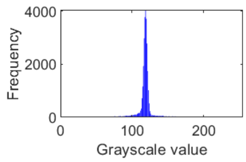
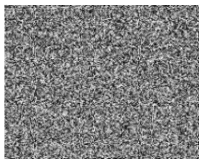
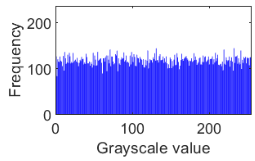
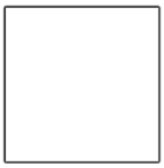
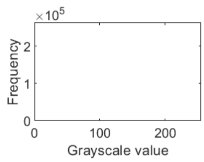
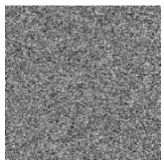
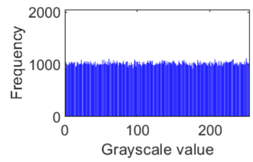
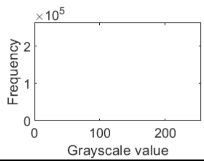
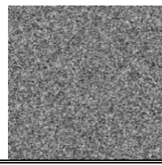
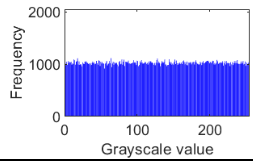
Image	Plain Image	Plain Image Histogram	Cipher Image	Cipher Image Histogram	p-Value
Cameraman					0.4313
Liftingbody					0.3924
Onion					0.7437
Cell					0.9799
White					0.3203
Black					0.5150

TABLE 7. Correlation between original and encrypted images.

Test	Cameraman	Liftingbody	Onion	Cell
Correlation	-0.00308	0.000002	-0.00496	-0.00023

TABLE 8. Correlation for plain and encrypted images in horizontal (H), vertical (V) and diagonal (D) directions.

Image		Cameraman	Liftingbody	White	Black
Plain image	H	0.9335	0.9707	---	---
	V	0.9592	0.9711	---	---
	D	0.9087	0.9530	---	---
Encrypted image	H	-0.0039	0.0015	-0.0160	-0.0071
	V	0.0003	0.0052	-0.0062	0.0026
	D	0.0047	-0.0028	-0.0028	0.0027

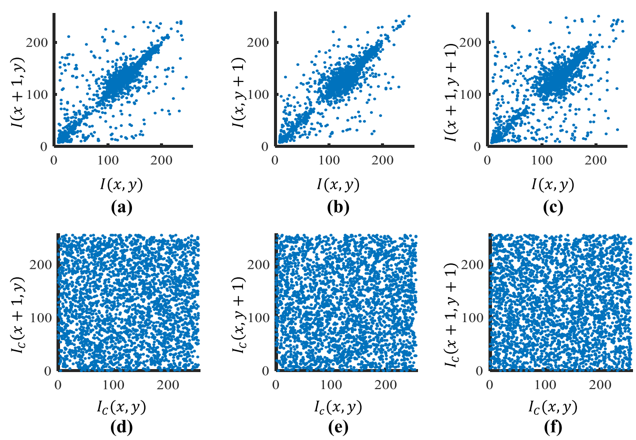


FIGURE 3. Effect of the proposed encryption scheme on spatial correlation. Plain image, I, spatial correlation in (a), (b) and (c). Cipher image, I_C, spatial correlation in (d), (e) and (f).

the cipher image should achieve an acceptable level of LSE metric. LSE is calculated as follows:

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

2- Calculate the entropy $E(B_i), i = 1, 2, \ldots, N_B$ for each block using equation (11).

TABLE 9. Entropy test results.

Test	Image	C-man	L-body	White	Black
Global entropy	Plain	7.0097	6.4903	0	0
	Cipher	7.9973	7.9994	7.9992	7.9992
$LSE^{N_B=30}_{T_B=1936}$	Cipher	7.9023	7.9028	7.9025	7.9027

3- Compute the mean (LSE) as follows:

$$\bar{E}_{N_B,T_B}(B) = \frac{1}{N_B}\sum_{i=1}^{N_B} E(B_i) \quad (12)$$

According to [54], the optimum value of LSE is 7.9024693 when $N_B = 30$ and $T_B = 1963$. The acceptable values of LSE, with confidence level $\alpha = 0.05$, are in the interval (7.901901305, 7.903037329).

Table 9 shows that the global entropy test results for images encrypted with the proposed scheme are near the value 8, which indicates a completely uniform distribution of pixel values. The LSE results shown in Table 9 indicate that images encrypted with the proposed scheme satisfy the randomness hypothesis with confidence level $\alpha = 0.05$.

B. DIFFERENTIAL ANALYSIS (PLAINTEXT SENSITIVITY)

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 small changes in plain images. To test immunity to differential attacks the encryption scheme is applied to two plain images with a slight variation. The encryption scheme should produce a corresponding major variation in the cipher image (diffusion). The test is performed by evaluating the Unified Average Change Intensity (UACI), the Number of Pixels Change Rate (NPCR), the Structural Similarity (SSIM) and correlation.

The test induces a change in one pixel of the original image and measures the changes in the resulting encrypted image. The encryption scheme shows immunity against differential attacks if the UACI value is close to 33.4635% [55], the NPCR value is close to 99.6094% [55], and the SSIM and the correlation are close to 0. Let the plain image I_1 produce a cipher image I_{C1}, and plain image with the only one-pixel value change is I_2 produce a cipher image I_{C2}. The UACI, NPCR and SSIM are computed as follows.

$$UACI = \frac{1}{MN}\sum_{i,j}\frac{|I_{C2}(i,j) - I_{C1}(i,j)|}{255} \times 100\% \quad (13)$$

$$NPCR = \sum_{i,j}\frac{D(i,j)}{MN} \times 100\% \quad (14)$$

$$SSIM(I_{C1}, I_{C2}) = \frac{(2\mu_{c1}\mu_{c2} + \alpha)(2\sigma_{c1c2} + \beta)}{(\mu_{c1}^2 + \mu_{c2}^2 + \alpha)(\sigma_{c1}^2 + \sigma_{c2}^2 + \beta)} \quad (15)$$

TABLE 10. Summary of differential attack test.

Test		Cameraman	Liftingbody	Black
UACI	min	33.1535	33.2798	33.1204
	avg.	33.4409	33.4308	33.4179
	max	33.7453	33.5781	33.7571
NPCR	min	99.4598	99.5445	99.4598
	avg.	99.6086	99.6087	99.6093
	max	99.7436	99.6719	99.7345
SSIM	min	-0.00749	-0.00049	-0.01429
	max	0.01869	0.01289	0.02720
|Correlation|	min	0.000005	0.000001	0.000003
	avg.	0.00350	0.00167	0.00567
	max	0.01477	0.00705	0.02146

TABLE 11. Results of key sensitivity analysis for changes in K_1.

Test	Cameraman	Liftingbody	Black
Correlation	-0.0561	-0.0566	-0.0551
NPCR	100	100	100
UACI	33.9193	33.9863	33.9566

TABLE 12. Results of key sensitivity analysis for changes in K_2.

Test	Cameraman	Liftingbody	Black
Correlation	-0.0060	0.0029	0.0012
NPCR	99.6292	99.6025	99.6025
UACI	33.5387	33.3840	33.4424

where

$$D(i,j) = \begin{cases} 1, & if\ 1_{C1}(i,j) \neq 1_{C2}(i,j) \\ 0, & otherwise, \end{cases}$$

and $\mu_{c1}, \mu_{c2}, \sigma_{c1}, \sigma_{c2}$, and σ_{c1c2} are the local means, standard deviations, and cross-covariance of cipher images I_{C1} and I_{C2}, whereas α and β are arbitrary constants.

The UACI, NPCR, SSIM and correlation tests were carried out 1000 times. For each run, the value of just one randomly chosen bit of the image is flipped. The pixel position and the bit position of the change are randomly chosen. The results shown in Table 10 indicate that the proposed scheme is immune to differential cryptanalysis.

C. KEY SENSITIVITY ANALYSIS

To resist key analysis attacks, the encryption scheme should be sensitive to slight changes in the decryption key. If an attacker attempts to decrypt the image with a wrong key that is relatively close to the correct key, the resulting decrypted image should still be uncorrelated to the plain image. To test the key sensitivity of the proposed scheme, the plain image, I, is encrypted with an encryption key (K_1, K_2) to produce the cipher image I_C. A related key $\left(K_1', K_2\right)$ is generated by inducing a one-bit change to K_1 and used to produce the cipher image I_C'. The difference between I_C and I_C' is tested using correlation, NPCR and UACI tests.

Results presented in Table 11 and Table 12 show the key sensitivity analysis for (K_1', K_2) and (K_1, K_2'), respectively. The correlation coefficient is close to 0, the NPCR is greater than 99.60%, and the UACI is close to 33.46%, which indicates that the scheme is highly sensitive to both encryption keys.

D. KEY SPACE ANALYSIS (BRUTE-FORCE ATTACK)

Based on Kerchoff's principle [56], the security of an encryption scheme depends on the key search space. In our scheme, the behavior of the system is modulated by two keys $K_1, K_2 \in \mathbb{Z}_2^{256}$. When mapped to floating-point numbers using (9), the limited precision of the floating-point number reduces the number of significant key bits to 52 bits for each floating-point number. Therefore, the total number of effective key bits is $4 \times 52 = 208$ bits. Therefore, the size of the key space is $2^{208} \cong 4.11 \times 10^{62}$, which rules out the possibility of a brute-force attacks.

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 plaintexts to reveal some information about the encryption key. Immunity to 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 come information about the encryption key.

A simple chosen-plaintext attack might use an all-white or an all-black image and attempt to detect any non-random patterns in the cipher image. As shown earlier in Table 6, the resulting cipher images have no visible patterns and their histogram is uniform. Moreover, Table 9 , shown earlier, demonstrates that the entropy of the cipher images corresponding to the all-white and all-black images are very close to the ideal of a pseudorandom image.

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

1) RESISTANCE TO KNOWN- AND CHOSEN-PLAINTEXT ATTACKS

According to [57], chaos systems which are defined by polynomial nonlinearities, such as Henon map, are susceptible to known-plaintext cryptanalysis. Namely, if the attacker were able to obtain the chaotic sequence, M, its corresponding Henon map initialization, H, may be recoverable by an algebraic attack. However, as noted in [44], chaotic encryption schemes which include an S-box have more security against cryptanalysis. By applying the S-box, the cipher image, $I_C = S(I \oplus M)$, doesn't provide direct information about the mask M. The adversary in this case must cryptanalyze both the chaotic mask, M, and the S-box function, S, simultaneously.

A trivial attack against the S-box attempts to gain access to its input and corresponding output. The use of the random nonce, ρ, plays an important role in protecting the S-box

TABLE 13. Execution time of the encryption procedure of the proposed algorithm.

Image Size ($pixels$)	Encryption Time (ms)	Encryption Throughput (MB/s)
$256 \times 256 \cong 65K$	16.8	3.9
$512 \times 512 \cong 262K$	19.3	13.6
$1024 \times 1024 \cong 1MB$	29.6	35.4

TABLE 14. Comparison of cipher-image spatial correlation and global entropy with recent image encryption schemes.

Scheme	Correlation			Global entropy	
	H	V	D	Small[a]	Large[b]
Proposed	0.0021	0.0117	0.0125	7.9973	7.9994
Ref. [58] , 2020	0.0026	0.0051	0.0264	7.9970	
Ref. [59] , 2020	0.0016	0.0020	0.0014	7.9987	7.9993
Ref. [60] , 2020	0.0001	0.0015	0.0013	7.9972	
Ref. [2] , 2019	0.0012	0.0003	0.0010		7.9993
Ref. [61] , 2019	0.0058	0.0064	0.0059	7.9988	
Ref. [62] , 2019	0.0004	0.0030	0.0030	-	
Ref. [20] , 2019	0.0002	0.0013	0.0006	-	
Ref. [22] , 2019	0.0084	0.0017	0.0019	7.9975	
Ref. [63] , 2019	0.0032	0.0007	0.0002	-	
Ref. [64] , 2019	0.0022	0.0013	0.0029	7.9975	
Ref. [40] , 2019	0.0019	0.0024	0.0011		7.9993
Ref. [65] , 2019	0.0025	0.0029	0.0027		7.9993
Ref. [66] , 2019	-	-	-	7.9455	
Ref. [14] , 2018	0.0000	0.0000	0.0000	7.9979	
Ref. [24] , 2018	0.0005	0.0030	0.0008	-	
Ref. [42] , 2018	0.0012	0.0044	0.0046	7.9986	
Ref. [67] , 2018	0.0060	0.0134	0.0068	-	
Ref. [6] , 2018	-	-	-	7.9965	
Ref. [68] , 2017	0.0001	0.0089	0.0091	7.9916	
Ref. [43] , 2017	0.0004	0.0018	0.0001	7.9985	
Ref. [19] , 2016	0.0095	0.0170	0.0119	7.9985	
Ref. [69] , 2016	0.0032	0.0004	0.0009	-	
Ref. [70] , 2017	-	-	-	7.9901	

[a]Small image has 256×256 pixels
[b]Large image has 512×512pixels

against such an attack. With a chosen-plaintext attack, the attacker in this case has access to I, $S(\rho)$, $S(SH([\rho, I]))$, and $S(I \oplus M)$. We must prevent the attacker from accessing any of the S-box inputs, i.e., ρ, $SH([\rho, I])$, and $I \oplus M$. We have already shown that M is difficult to obtain. Due to the security of the SHA256 hash function, it is also difficult to guess ρ given I and $S(SH([\rho, I]))$. And it is equally difficult to guess $SH([\rho, I])$ given $S(\rho)$ and I. Thus, the S-box is safe against chosen-plaintext attacks.

2) RESISTANCE TO CHOSEN-CIPHERTEXT ATTACKS

The integrity verification step at the end of the decryption algorithm effectively thwarts all forms of chosen-ciphertext attacks. An attacker attempting to use the decryption oracle to decrypt a chosen cipher image, I_C, must form a consistent cipher message with $S(\rho)$, $S\left(SH\left([\rho, S^{-1}(I_C)]\right)\right)$, and $I_C = S(I \oplus M)$. Upon adjusting I_C, the corresponding adjustment in the hash value $SH\left(\left[\rho, S^{-1}(I_C)\right]\right)$ is intractable due to the properties of secure hash functions. Malformed cipher messages are rejected by the decryption algorithm, as shown in Figure 2, thus thwarting the chosen-ciphertext attack.

TABLE 15. Comparison of local Shannon entropy with recent image encryption schemes. $K = 30$, $T_B = 1936$, $\alpha = 0.05 \vdash$ LSE $\in$ [7.901901305, 7.903037329].

File name	[71] 2013	[72] 2015	[73] 2017	[74] 2018	[22] 2019	[20] 2019	[60] 2020	Proposed
5.2.08	7.902356	7.903327	7.9043155	7.90194564	7.902487	7.89911169	7.902733	7.902776
5.2.09	7.899853	7.901765	7.9036303	7.90229806	7.902681	7.9021513	7.901584	7.902132
5.2.10	7.902654	7.902748	7.9024444	7.90299861	7.902150	7.9009431	7.902983	7.902858
5.3.01	7.902647	7.901772	7.9032011	7.90238296	7.902531	7.9029481	7.901996	7.902628
5.3.02	7.910474	7.903328	7.9029093	7.90194284	7.902483	7.9024863	7.902003	7.902637
7.1.01	7.902634	7.901305	7.9021978	7.90222122	7.902725	7.9027466	7.903056	7.902732
7.1.02	7.901634	7.901578	7.9029369	7.90279019	7.893536	7.8999371	7.903288	7.902297
7.1.03	7.905423	7.903099	7.9022684	7.90198572	7.900743	7.9039913	7.901603	7.901087
7.1.04	7.902125	7.902607	7.9009099	7.90220791	7.902163	7.9017415	7.902366	7.902165
7.1.05	7.883653	7.905305	7.9065666	7.90246781	7.902208	7.9021942	7.902362	7.902634
7.1.06	7.902356	7.902695	7.9043870	7.90229890	7.903055	7.9019996	7.902365	7.901596
7.1.07	7.902364	7.902896	7.9026480	7.90280377	7.902832	7.9021436	7.902942	7.902235
7.1.08	7.904456	7.901632	7.9019985	7.90234949	7.902407	7.9020712	7.901728	7.902929
7.1.09	7.903012	7.903173	7.9006977	7.90299876	7.902674	7.9009463	7.901992	7.902409
7.1.10	7.901598	7.901524	7.9050126	7.90280083	7.902699	7.9033234	7.902994	7.902524
7.2.01	7.901989	7.902454	7.9042864	7.90290947	7.901923	7.9021532	7.901713	7.902332
boat.512	7.901879	7.903088	7.9035797	7.90242160	7.902488	7.9023686	7.902938	7.902466
ruler.512	7.903001	7.903052	7.9040475	7.90291543	7.898703	7.9029163	7.903170	7.902432
gray21.512	7.905107	7.902688	7.9028993	7.90281517	7.887108	7.8989296	7.903376	7.901355
Pass	10/19	6/19	8/19	19/19	14/19	11/19	11/19	16/19

TABLE 16. Comparison of differential attack metrics with recent image encryption schemes.

Scheme	Differential Analysis	
	UACI	NPCR
Proposed	33.4409	99.6086
Ref. [58], 2020	33.4590	99.6100
Ref. [59], 2020	33.4509	99.6110
Ref. [60], 2020	24.2534	76.1681
Ref. [2], 2019	33.50	99.60
Ref. [40] , 2019	33.4682	99.6113
Ref. [62] , 2019	33.3797	99.6495
Ref. [20] , 2019	33.5253	99.6094
Ref. [61] , 2019	33.6259	99.6118
Ref. [65] , 2019	33.4756	99.6173
Ref. [14], 2018	33.6046	99.6369
Ref. [42] , 2018	33.11	99.95
Ref. [24] , 2018	33.4928	99.6087
Ref. [6] , 2018	34.1474	99.6446
Ref. [75] , 2018	33.6435	99.6094
Ref. [67] , 2018	33.5226	99.5986
Ref. [74] , 2018	33.6413	99.6231
Ref. [43], 2017	33.48	99.60
Ref. [68], 2017	33.47	100.0
Ref. [76] , 2017	33.41	99.59
Ref. [77] , 2017	33.32	99.61
Ref. [78] , 2016	33.4018	99.4644
Ref. [19] , 2016	33.7786	99.6205
Ref. [79] , 2016	33.3830	99.5574

3) THE ROLE OF ELLIPTIC CURVE CRYPTOGRAPHY

By using elliptic curve cryptography, we add a last line of defense to the proposed scheme against cryptanalysis. Namely, if the attacker somehow manages to gain access to the Henon map initialization H for a set of encryption instances, calculating the key K_2 incurs solving $(SH([\rho, I]) + K_2)\,G = H$, which requires solving the ECDLP. Similarly, if we assume the attacker were able to recover the S-box, S, for some specific encryption instances, and guesses the initialization of the S-box construction, K_S. To recover the encryption key K_1, the attacker must solve $(\pi + K_1)\,G = K_S$, which again requires solving the ECDLP.

TABLE 17. Comparison of encryption throughput with related image encryption schemes.

Scheme	Implementation	Throughput
Proposed	Java / Core i7 @ 1.8 GHz	55.7 MB/s
Ref. [80]	Mathematica / Xeon @ 3.6 GHz	2.5 MB/s
Ref. [37]	— / Atom @ 1.6 GHz	0.01 MB/s
Ref. [63]	— / Core i7 @ 3.6 GHz	0.64 MB/s
Ref. [20]	— / —	0.06 MB/s
Ref. [61]	Mathematica ./ Xeon @ 3.7 GHz	0.14 MB/s
Ref. [43]	C# / Core i7	1.77 MB/s
Ref. [42]	— / —	0.01 MB/s
Ref. [24]	MATLAB / Core i7 @ 2.9GHz	1.35 MB/s
Ref. [67]	MATLAB / AMD 1.9 GHz	0.77 MB/s
Ref. [74]	MATLAB / Core i5 @ 2.3 GHz	0.051MB
Ref. [78]	MATLAB / AMD A4 @ 1.9 GHz	2.27 MB/s
Ref. [81]	— / Core i5 @ 2.6 GHz	9.6 MB/s
Ref. [82]	Mathematica / Core i7 @2.2 GHz	2.8 MB/s
Ref. [40]	MATLAB / Core 3.9GHz	0.05 MB/s
Ref. [41]	— / —	0.05 MB/s
Ref. [83]	MATLAB / Core i5 @ 3.4 GHz	0.1 MB/s
Ref. [35]	C++ / Core i5 @ 3.1 GHz	55.2 MB/s

F. SPEED ANALYSIS

One of the most important features of the proposed scheme is its encryption speed. This is in particular because of the use of very efficient encryption constructs, namely the S-box and Henon map. To assess the efficiency of the proposed scheme, we performed the speed analysis with MATLAB on a PC with a Core-i7-8565U with a base frequency of 1.8 GHz and 12GB of RAM. Table 13 shows the average execution time of the proposed encryption algorithm for images of different sizes. Experimental results in Table 13 indicate the linear complexity of the proposed encryption algorithm.

VI. COMPARISON AND DISCUSSION

The proposed scheme exhibits a near optimal and competitive performance compared to recent image encryption schemes. Table 14 compares the spatial correlation in horizontal, vertical and diagonal directions with recent schemes. The table also compares the global entropy of encrypted images. The comparison is split into two columns depending on the size of the image being encrypted. Small images have 256×256 pixels, whereas large images have 512×512 pixels. The results indicate that the proposed scheme achieves a correlation value and global entropy that is very close to the ideal value and in harmony with the results of the other schemes.

Table 15 shows the LSE test results for the USC-SIPI "Miscellaneous" image dataset in comparison with recent schemes. The proposed scheme achieves one of the highest passing rates among its peers.

Regarding plain image sensitivity, Table 16 shows that the proposed scheme achieves some of the best values of UACI and NPCR among recent schemes. These results indicate that the proposed scheme offers competitive immunity against differential attacks.

It's worth noting that the use of a cryptographic secure hash function to calculate the initialization of a chaotic system makes it sensitive to any change in pixel values. In contrast, the summation method proposed by [2], for instance, does not recognize pixel value changes when the summation is not affected by the change, i.e. when changes cancel each other. The sensitivity of the hash function makes it extremely difficult for an attacker to launch a differential cryptanalysis attack, as shown earlier by the optimal values for NPCR and UACI criteria in Table 10.

As shown in Table 17, the encryption throughput of the proposed scheme is very competitive.

VII. CONCLUSION AND FUTURE WORK

In this paper, we presented an image encryption scheme based on a dynamic S-box and a chaotic additive mask. The proposed scheme is shown to resist chosen-plaintext and chosen-ciphertext attacks by utilizing two techniques: 1) the use of random nonce and secure hash algorithm in calculating per-image Henon map initialization, and 2) the use of elliptic curve encryption in protecting the secret key. The proposed algorithm has high computational efficiency achieving encryption speeds close to 60 MB/s. Although this scheme is designed to encrypt gray scale uncompressed images, it can easily be extended to uncompressed color images. Joint image compression and encryption is an interesting challenge that may be the subject of future research.

REFERENCES

[1] I. F. Elashry, O. S. F. Allah, A. M. Abbas, S. El-Rabaie, and F. E. A. El-Samie, "Homomorphic image encryption," *J. Electron. Imag.*, vol. 18, no. 3, 2009, Art. no. 033002.

[2] 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, doi: 10.1016/j.sigpro.2018.10.011.

[3] M. Hénon, "A two-dimensional mapping with a strange attractor," *Commun. Math. Phys.*, vol. 50, no. 1, pp. 69–77, Feb. 1976.

[4] J. Khan, J. Ahmad, and S. O. Hwang, "An efficient image encryption scheme based on: Henon map, skew tent map and S-Box," in *Proc. 6th Int. Conf. Modeling, Simulation, Appl. Optim. (ICMSAO)*, May 2015, pp. 1–6, doi: 10.1109/ICMSAO.2015.7152261.

[5] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Process., Image Commun.*, vol. 41, pp. 144–157, Feb. 2016, doi: 10.1016/j.image.2015.10.004.

[6] S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, "Optimizing chaos based image encryption," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25569–25590, Oct. 2018, doi: 10.1007/s11042-018-5807-x.

[7] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Comput. Appl.*, vol. 22, no. 6, pp. 1085–1093, May 2013, doi: 10.1007/s00521-012-0870-0.

[8] D. Souravlias, K. E. Parsopoulos, and G. C. Meletiou, "Designing bijective S-boxes using algorithm portfolios with limited time budgets," *Appl. Soft Comput.*, vol. 59, pp. 475–486, Oct. 2017, doi: 10.1016/j.asoc.2017.05.052.

[9] P. Junod, "Statistical cryptanalysis of BLOCK CIPHers," M.S. thesis, Dept. Commun. Syst., EPFL, Lausanne, Switzerland, 2005. [Online]. Available: http://infoscience.epfl.ch/record/33648/files/EPFL_TH3179.pdf

[10] 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, doi: 10.1016/j.chaos.2013.11.001.

[11] 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, doi: 10.1007/s11042-018-6250-8.

[12] M. F. Khan, A. Ahmed, and K. Saleem, "A novel cryptographic substitution box design using Gaussian distribution," *IEEE Access*, vol. 7, pp. 15999–16007, 2019, doi: 10.1109/ACCESS.2019.2893176.

[13] 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, doi: 10.1007/s11071-016-3295-y.

[14] 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, doi: 10.1007/s11071-017-3874-6.

[15] N. A. Azam, U. Hayat, and I. Ullah, "An injective S-Box design scheme over an ordered isomorphic elliptic curve and its characterization," *Secur. Commun. Netw.*, vol. 2018, pp. 1–9, Dec. 2018, doi: 10.1155/2018/3421725.

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

[17] J. Daemen and V. Rijmen, *The Design of Rijndael*. Berlin, Germany: Springer-Verlag, 2002, p. 255, doi: 10.1007/978-3-662-04722-4.

[18] N. A. Azam, U. Hayat, and I. Ullah, "Efficient construction of a substitution box based on a mordell elliptic curve over a finite field," *Frontiers Inf. Technol. Electron. Eng.*, vol. 20, no. 10, pp. 1378–1389, Oct. 2019, doi: 10.1631/FITEE.1800434.

[19] 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, doi: 10.1016/j.sigpro.2016.03.021.

[20] 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, doi: 10.1109/ACCESS.2019.2893538.

[21] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Trans. Syst., Man, Cybern. Syst.*, early access, Aug. 28, 2019, doi: 10.1109/TSMC.2019.2932616.

[22] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Process.*, vol. 160, pp. 45–58, Jul. 2019, doi: 10.1016/j.sigpro.2019.02.016.

[23] B. Song and Q. Ding, "Comparisons of typical discrete logistic map and henon map," in *Intelligent Data analysis and its Applications*, vol. 1, J.-S. Pan, V. Snasel, E. S. Corchado, A. Abraham, and S.-L. Wang, Eds. Cham, Switzerland: Springer, 2014, pp. 267–275.

[24] P. Ping, F. Xu, Y. Mao, and Z. Wang, "Designing permutation–substitution image encryption networks with henon map," *Neurocomputing*, vol. 283, pp. 53–63, Mar. 2018, doi: 10.1016/j.neucom.2017.12.048.

[25] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, p. 203, Jan. 1987, doi: 10.1090/s0025-5718-1987-0866109-5.

[26] V. S. Miller, "Use of elliptic curves in cryptography," in *Advances in Cryptology—CRYPTO*, H. C. Williams, Ed. Berlin, Germany: Springer, 1986, pp. 417–426.

[27] A. J. Menezes, T. Okamoto, and S. A. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1639–1646, Sep. 1993, doi: 10.1109/18.259647.

[28] 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. ISRC*, 2017, pp. 1–7.

[29] X. Wang, Ü. Çavuşoğlu, 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, doi: 10.3390/app9040781.

[30] 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, doi: 10.1109/access.2020.2970806.

[31] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, "A new image encryption scheme based on dynamic S-boxes and chaotic maps," *3D Res.*, vol. 7, no. 1, p. 7, Mar. 2016, doi: 10.1007/s13319-016-0084-9.

[32] P. Devaraj and C. Kavitha, "An image encryption scheme using dynamic S-boxes," *Nonlinear Dyn.*, vol. 86, no. 2, pp. 927–940, Oct. 2016, doi: 10.1007/s11071-016-2934-7.

[33] 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, doi: 10.1007/s11042-019-08342-1.

[34] A. Belazi, A. A. Abd 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, doi: 10.1016/j.optlaseng.2016.07.010.

[35] 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, doi: 10.1007/s11071-014-1445-7.

[36] X.-P. Zhang, R. Guo, H.-W. Chen, Z.-M. Zhao, and J.-Y. Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *Chin. Phys. B*, vol. 27, no. 8, Aug. 2018, Art. no. 080701, doi: 10.1088/1674-1056/27/8/080701.

[37] R. Anandkumar and R. Kalpana, "Designing a fast image encryption scheme using fractal function and 3D henon map," *J. Inf. Secur. Appl.*, vol. 49, Dec. 2019, Art. no. 102390, doi: 10.1016/j.jisa.2019.102390.

[38] S. J. Sheela, K. V. Suresh, and D. Tandur, "Image encryption based on modified henon map using hybrid chaotic shift transform," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 25223–25251, Oct. 2018, doi: 10.1007/s11042-018-5782-2.

[39] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-sine map and DNA approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018, doi: 10.1016/j.sigpro.2018.06.008.

[40] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[41] Z. E. Dawahdeh, S. N. Yaakob, and R. R. bin Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *J. King Saud Univ. Comput. Inf. Sci.*, vol. 30, no. 3, pp. 349–355, Jul. 2018, doi: 10.1016/j.jksuci.2017.06.004.

[42] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018, doi: 10.1109/ACCESS.2018.2879844.

[43] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Process.*, vol. 141, pp. 217–227, Dec. 2017, doi: 10.1016/j.sigpro.2017.06.010.

[44] 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, doi: 10.1016/j.jisa.2019.102361.

[45] A. Langley and M. H. Turner. (2016). *Elliptic Curves for Security*. Internet Research Task Force (IRTF). [Online]. Available: https://tools.ietf.org/html/rfc7748#section-4.1

[46] A. F. Webster and S. E. Tavares, "On the design of S-boxes," in *Advances in Cryptology—CRYPTO*, H. C. Williams, Ed. Berlin, Germany: Springer, 1986, pp. 523–534.

[47] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Advances in Cryptology—EUROCRYPT*, vol. 93. Berlin, Germany: Springer, 1994, pp. 386–397.

[48] T. W. Cusick and P. Stănică, *Cryptographic Boolean Functions and Applications*. London, U.K.: Academic, 2017.

[49] 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, doi: 10.1007/s11071-016-3199-x.

[50] 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.

[51] B. B. Cassal-Quiroga and E. Campos-Cantón, "Generation of dynamical S-boxes for block ciphers via extended logistic map," *Math. Problems Eng.*, vol. 2020, pp. 1–12, Mar. 2020, doi: 10.1155/2020/2702653.

[52] F. Özkaynak, "Construction of robust substitution boxes based on chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, Aug. 2019, doi: 10.1007/s00521-017-3287-y.

[53] Y. Wang, K.-W. Wong, C. Li, and Y. Li, "A novel method to design S-box based on chaotic map and genetic algorithm," *Phys. Lett. A*, vol. 376, nos. 6–7, pp. 827–833, Jan. 2012, doi: 10.1016/j.physleta.2012.01.009.

[54] 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, doi: 10.1016/j.ins.2012.07.049.

[55] 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, doi: 10.1109/TIP.2003.819861.

[56] F. A. P. Petitcolas, "Kerckhoffs' principle," in *Encyclopedia of Cryptography and Security*, H. C. A. van Tilborg and S. Jajodia Eds. Boston, MA, USA: Springer, 2011, p. 675.

[57] F. Anstett, G. Millerioux, and G. Bloch, "Chaotic cryptosystems: Cryptanalysis and identifiability," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 12, pp. 2673–2680, Dec. 2006, doi: 10.1109/TCSI.2006.885979.

[58] 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.

[59] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Sci. Rep.*, vol. 10, no. 1, p. 9784, Jun. 2020, doi: 10.1038/s41598-020-66486-9.

[60] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ElYazeed, "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," *Signal Process.*, vol. 167, Feb. 2020, Art. no. 107280, doi: 10.1016/j.sigpro.2019.107280.

[61] 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, doi: 10.1016/j.image.2019.08.014.

[62] Z. Hua, B. Xu, F. Jin, and H. Huang, "Image encryption using Josephus problem and filtering diffusion," *IEEE Access*, vol. 7, pp. 8660–8674, 2019, doi: 10.1109/ACCESS.2018.2890116.

[63] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019, doi: 10.1016/j.ins.2018.12.048.

[64] M. Asgari-Chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Process.*, vol. 157, pp. 1–13, Apr. 2019, doi: 10.1016/j.sigpro.2018.11.010.

[65] 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.

[66] B. Mondal, S. Singh, and P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *J. Inf. Secur. Appl.*, vol. 45, pp. 117–130, Apr. 2019, doi: 10.1016/j.jisa.2019.01.010.

[67] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018, doi: 10.1016/j.sigpro.2017.08.020.

[68] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017, doi: 10.1016/j.sigpro.2017.04.006.

[69] Z. Fawaz, H. Noura, and A. Mostefaoui, "An efficient and secure cipher scheme for images confidentiality preservation," *Signal Process., Image Commun.*, vol. 42, pp. 90–108, Mar. 2016, doi: 10.1016/j.image.2016.01.009.

[70] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 127–133, Jan. 2017, doi: 10.1007/s11071-016-3030-8.

[71] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Process.*, vol. 93, no. 11, pp. 3039–3052, Nov. 2013, doi: 10.1016/j.sigpro.2013.04.021.
[72] 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, doi: 10.1016/j.ins.2014.11.018.
[73] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dyn.*, vol. 89, no. 1, pp. 61–79, Jul. 2017, doi: 10.1007/s11071-017-3436-y.
[74] X. Wang, X. Zhu, and Y. Zhang, "An image encryption algorithm based on josephus traversing and mixed chaotic map," *IEEE Access*, vol. 6, pp. 23733–23746, 2018, doi: 10.1109/ACCESS.2018.2805847.
[75] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-Box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018, doi: 10.1016/j.ins.2018.03.055.
[76] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017, doi: 10.1016/j.optlaseng.2016.08.009.
[77] S. Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," *Opt. Eng.*, vol. 56, no. 11, p. 1, Nov. 2017.
[78] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016, doi: 10.1016/j.optlaseng.2016.03.019.
[79] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016, doi: 10.1016/j.optlaseng.2015.09.007.
[80] 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.
[81] 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.
[82] 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.
[83] 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, doi: 10.1016/j.optlaseng.2015.12.004.

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.

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

AYMAN 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, USA, in 2012 and 2015, respectively.

Since 2010, he has been a member with the UConn's Underwater Sensor Networks Laboratory. He was a Chairman of the Computer Engineering Department. He is currently an Assistant Professor with Umm Al-Qura University. He also works as a Vice-Principle of the Department of Investment, Umm Al-Qura University.