IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 11, 2020, accepted July 26, 2020, date of publication July 29, 2020, date of current version August 12, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3012912

Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution

ABDULLAH QAYYUM[1], JAWAD AHMAD[2], (Senior Member, IEEE), WADII BOULILA[3,4], (Senior Member, IEEE), SAEED RUBAIEE[5], ARSHAD[6], FAWAD MASOOD[7], FAWAD KHAN[8], AND WILLIAM J. BUCHANAN[2]

[1]Department of Electrical Engineering, University of Engineering and Technology, Peshawar 25120, Pakistan
[2]School of Computing, Edinburgh Napier University, Edinburgh EH10 5DT, U.K.
[3]RIADI Laboratory, University of Manouba, Manouba 2010, Tunisia
[4]College of Computer Science and Engineering, Taibah University, Medina 42353, Saudi Arabia
[5]Department of Industrial and Systems Engineering, University of Jeddah, Jeddah 21589, Saudi Arabia
[6]Institute for Energy and Environment, University of Strathclyde, Glasgow G1 1XQ, U.K.
[7]Department of Electrical Engineering, Institute of Space Technology, Islamabad 44000, Pakistan
[8]Department of Information Security, National University of Sciences and Technology, Islamabad 44000, Pakistan

Corresponding authors: Wadii Boulila (wadii.boulila@riadi.rnu.tn) and Jawad Ahmad (jawadkhattak@ieee.org)

ABSTRACT The evolution of wireless and mobile communication from 0G to the upcoming 5G gives rise to data sharing through the Internet. This data transfer via open public networks are susceptible to several types of attacks. Encryption is a method that can protect information from hackers and hence confidential data can be secured through a cryptosystem. Due to the increased number of cyber attacks, encryption has become an important component of modern-day communication. In this article, a new image encryption algorithm is presented using chaos theory and dynamic substitution. The proposed scheme is based on two-dimensional Henon, Ikeda chaotic maps, and substitution box (S-box) transformation. Through Henon, a random S-Box is selected and the image pixel is substituted randomly. To analyze security and robustness of the proposed algorithm, several security tests such as information entropy, histogram investigation, correlation analysis, energy, homogeneity, and mean square error are performed. The entropy values of the test images are greater than 7.99 and the key space of the proposed algorithm is 2^{798}. Furthermore, the correlation values of the encrypted images using the proposed scheme are close to zero when compared with other conventional schemes. The number of pixel change rate (NPCR) and unified average change intensity (UACI) for the proposed scheme are higher than 99.50% and 33, respectively. The simulation results and comparison with the state-of-the-art algorithms prove the efficiency and security of the proposed scheme.

INDEX TERMS Henon map, Ikeda map, chaos, encryption, substitution box.

I. INTRODUCTION

In the last few decades, advancement in data communication has given rise to the sharing of multimedia data electronically. In multimedia data, digital images that may be of a sensitive nature such as medical and defence related images are transferred through unsecured communication channels. Owing to the public nature of the Internet, protection of these digital files has become a serious challenge. Proper measures should be taken to secure digital information to avoid the breach of sensitive data and one's privacy [1]–[4]. For securing sensitive information from unauthenticated access, cryptography has been introduced. Cryptography is the process of securing information from unauthenticated access [5]. Many algorithms have been proposed for securing sensitive information such as Advanced Encryption Standard (AES), Rivest–Shamir– Adleman (RSA), Data Encryption Standard (DES), and International Data Encryption Algorithm (IDEA) but these methods can not be used to encrypt images, because they are primarily used to encrypt text [6]–[16]. Due to their unique features such as similarity between adjacent pixels and higher redundancy of digital images, these algorithms are not suitable for digital image encryption. Among the various proposed schemes for image encryption, many are based only on the permutation of pixels but such schemes are not immune to various cryptographic attacks [17]–[19].

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

Chaos theory is used in many fields of science because of its special nature. Apart from its applications in cryptography, it has its value in the fields of mathematics, physics, biology, computer, engineering and the arts. In the last few decades, a strong association between chaos and cryptography has been uncovered [20], [21]. Nowadays, in the implementation of secure image communication, chaotic systems are found to be very useful because of their random and unpredictable behaviour. The characteristic properties of chaos theory such as non-periodicity, sensitivity to initial conditions, deterministic pseudo-random behaviour and sensitivity to control parameters are the basis of the chaotic system's security [22]. The implementation of chaotic maps in modern encryption schemes is because of its non-linear dynamic behaviour and larger key space. With the help of chaos theory and cryptography, efficient encryption schemes can be designed [9], [14], [23]–[25]. For an image encryption scheme to be secure, it must have the properties of confusion and diffusion. Confusion means changing the position of pixels and diffusion refers to changing the individual pixel grey values that leads to the reduction of correlation between image pixels [26]. An image encryption algorithm based on chaotic maps may be vulnerable to different attacks due to weak encryption mechanism and lower key space [10]. These days, researchers are using chaotic maps in the design of new image encryption schemes for increased security. There are two categories of chaotic maps: 1-D chaotic maps which include logistic map, tent map and circle chaotic map [27], [28]. However, because of their simplicity, they can be easily compromised. The other category is high dimensional chaotic maps such as Henon and Ikeda maps, with larger key space and good chaotic behaviour. These chaotic maps are also vulnerable to security attacks; therefore, newly proposed algorithms must fulfil the present day demands of image encryption in real-time.

The digital information in an image can be secured either by covering the original image with some secret cover image or by encryption. The concept of an encryption algorithm based on chaos was given by Matthews [29]. Many image encryption schemes have been proposed in the literature. For encryption and permutation, a 2D baker map is applied for M $\times$ M image and the relationship of cryptography and discreet chaos is analyzed [30]. An image encryption scheme that utilizes orthogonal matrices and chaotic maps has also been proposed which is robust enough to channel noise and image compression [31]. Ahmad *et al.* [32] have presented an image encryption scheme that utilizes Henon and skew tent maps for confusion and diffusion and an S-box for dynamic substitution. Ahmad *et al.* [33] have utilized orthogonal matrices, skew tent map and XOR operation to design an efficient encryption algorithm for images. A light weight image encryption scheme has also been proposed using Chebyshev and Intertwining maps encrypting a small portion of the transformed image for the applications where time is a constraint [34]. An efficient cryptosystem is proposed by Masood *et al.* in [25] employing fractal keys and a Lorenz chaotic map. Fibonacci series and a Kaplan–Yorke chaotic map are utilized for the design of a novel encryption scheme in [35]. In [4], using multiple discreet dynamic maps such as Henon and duffing chaotic maps, a chaos based image encryption scheme is proposed. To overcome the disadvantages of traditional encryption schemes, a new light-weight encryption scheme is proposed [36]. For the security of medical images, a novel encryption schemes is proposed in [37] using logistic, tent and sine chaotic maps. Another encryption scheme for medical images encryption is introduced in [38] which is based on chaotic attractors on frequency domain by integer wavelet transform (IWT) and fused with deoxyribonucleic acid (DNA) sequence on the spatial domain. A new cryptosystem is introduced based on the combination of Mersenne Twister (MT), Deoxyribonucleic Acid (DNA), and Chaotic Dynamical Rossler System (MT-DNA-Chaos) methods [39]. Masood *et al.* [39] proposed robust cryptosystem to secure aerial images information using Mersenne twister method, DNA encoding rule and chaos sequencing, To overcome the disadvantages of logistic mapping, image encryption schemes based on spatiotemporal chaotic maps are proposed but these concepts are also applicable to other schemes for the purpose of security enhancement [40]–[42]. Anees *et al.* [43] identified a flaw in the S-box transformation that is its poor performance for highly correlated data and proposed a new technique based on chaotic substitution to address the issue. The scheme proposed in [43] does not perform well when it comes to the encryption of images with lower gray values. This problem was identified and solved by Ahmad and Hwang *et al.* [19] by the introduction of a chaos-based diffusion scheme.

Since the last decade, many chaos-based image encryption scheme has been proposed, however, many of them have been proved insecure due to lower keyspace and infeasible due to computational complexity [4], [19], [22], [31], [32], [44]. According to previous literature [4], [19], [22], [31], [32], a secure cryptosystem should contain both permutation and diffusion. But in literate, many schemes does not fulfil the aforementioned [4], [19], [22], [31], [32]. In this article, rows and columns of the plaintext image are first permuted using Ikeda map which results in a better permutation. To achieve the diffusion property, the permuted image is XORed bit-wise with the set of values generated through the Henon map. After the XOR operation, the values of the individual pixels are substituted with one of the S-box depending on the condition specified in the algorithm. Due to an additional step of the substitution process, the proposed scheme is more secure than the existing scheme. Our claim of robust security is proved in experimental results and security analysis section using a number of images such as Lena, Baboon, Cameraman, and Barbara. In previous studies [19], [22], [31], the security of these images were lower due to lower keyspace and insecure maps.

It is evident from previous studies [19], [22], [31] that there is a strong relationship between chaos and cryptography. Chaos is the study of dynamic systems behaviour and is

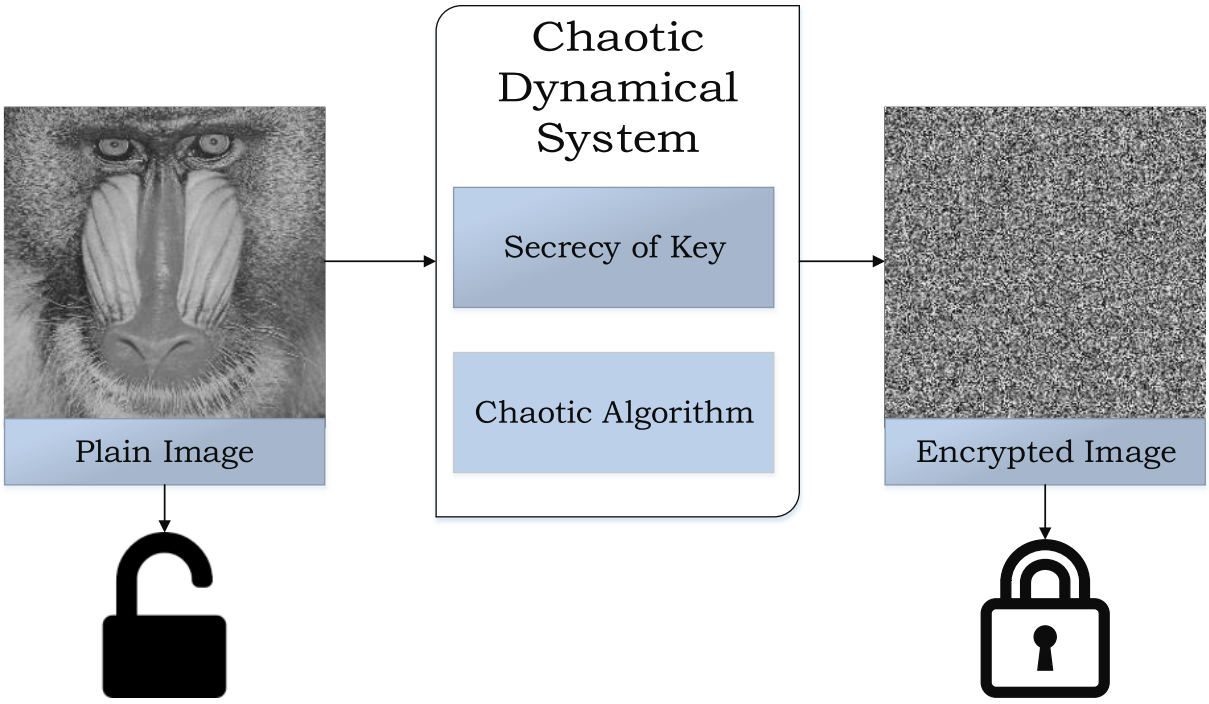


FIGURE 1. Fundamental flow schematic for the chaotic encryption.

a branch of mathematics. Chaotic systems show sensitivity towards the initial conditions and certain other factors. Some important properties that chaotic systems exhibits are topology mixing, strange attractor, ergodicity, randomness and reliance on their initial conditions [23], [29], [45], [46]. These are the properties which give importance to the encryption algorithms based on chaos. The output of chaotic systems can not be determined without a prior knowledge of its initial parameters. Therefore, efficient cryptographic encryption algorithms can be designed using chaos theory. The initial conditions of a map must be known for a good chaotic output. The map becomes deterministic when the initial conditions are known. These chaotic features are used for different cryptosystems. The significant sensitive property of the initial condition defines the ease of realization of the cryptosystem and provide a barrier for the hackers. Fundamental flow schematic of the chaotic encryption is illustrated in Fig. 1.

The use of chaos theory is not limited to computer science and cryptography but also has its applications in other fields such as biology, engineering, mathematics, economics and physics. The theory of chaos deals with processes which demonstrate a particular form of dynamic behaviour in time. Chaos typically arises in complex, nonlinear deterministic systems (NLDS). Chaos happens when the mathematical parameters are constantly and persistently modified. There is a collection of chaotic systems characteristics that have been identified by the experts. The most important ones are as follows [47]:

A. DYNAMIC INSTABILITY

This parameter is often referred as the *butterfly effect*. It is the sensitivity function of initial conditions. A small change in initial conditions results in substantially divergent and contrasting trajectories.

B. TOPOLOGICAL MIXING

This is defined as the mixing of colour dyes. This means that the system can adjust over time to overlap or merge any known region with some other known area.

C. NON-PERIODICITY

The chaotic system never replicates itself with the passage of time and is of a non-periodic nature.

D. PERIODIC ORBITS DENSITY

A chaotic system having dense periodic orbits implies that periodic orbits approach every point in space arbitrarily closely.

E. ERGODICITY

The dynamics exhibit the same properties of statistics when measured immediately over space and time.

F. SELF-SIMILARITY

The system progression show similarity at dissimilar measurement in space or time. Due to this property, the system is unique and seems like an auto-repetitive system at different measurement.

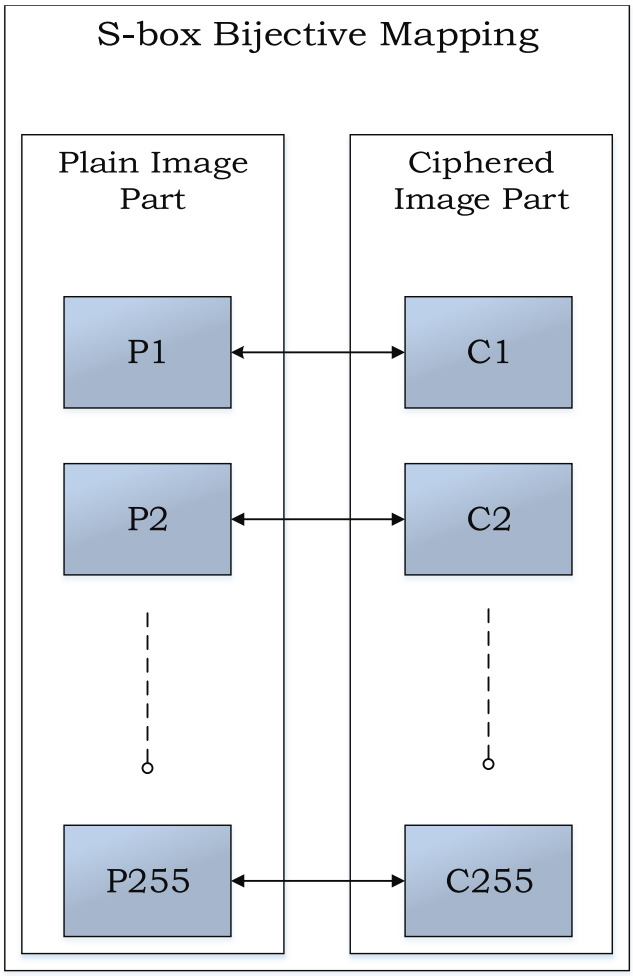


FIGURE 2. Substitution box bijective mapping.

1) PROBLEM STATEMENT

The S-box mapping relation is a one-to-one relationship also known as bijective mapping which means that a message symbol will be replaced with a unique S-box element. This mapping relationship is shown in Fig. 2. The S-box can be represented as a bijective function g(a), hence:

$$\begin{aligned} &S : P \rightarrow C \\ &\text{if } \ a_1 = a_2 \\ &\text{then } \ g\,(a_1) = g\,(a_2) \end{aligned} \tag{1}$$

In Fig. 2, P is the plaintext image pixel and C is the transformed image pixel. If a digital image contains pixels having the same values, they are all encrypted into one specific S-Box symbol. This means that the histogram peaks remain the same after the application of S-box transformation on data that is highly autocorrelated. This effect can be seen in the Lena image shown in Fig. 3. Therefore, it is easy for a fraudulent person to access and extract the information from the encrypted image.

2) PAPER CONTRIBUTION

To fully exploit the advantages of the S-box transformation and avoid its deficiencies, a different approach has been utilized in this article. Instead of using the S-box transformation directly, we have first permuted the image with the help of Ikeda map to achieve confusion property and then the Henon map is used for diffusion. After that, the S-box transformation is applied to the distorted image for the enhancement of the security and to obtain a highly secure encrypted image that hides all the information of the plaintext image.

II. PROPOSED SCHEME

This section will discuss the steps involved in the proposed encryption scheme. To achieve the properties of confusion and diffusion, two different two-dimensional iterative chaotic maps are employed. For further enhancement of the security of the ciphertext images, an S-box is selected from three Sboxes defined in the algorithm for the substitution of pixel values.

A. CHAOTIC MAPS EMPLOYED IN THE PROPOSED ENCRYPTION SCHEME

In this section, the chaotic maps that are employed in the proposed algorithm for confusion and diffusion are discussed.

1) HENON CHAOTIC MAP

The Henon chaotic map proposed by Hénon [48] is a two-dimensional non-linear discreet chaotic map that gives as an output two sets of random values. It takes two inputs (x_n, y_n) to give a random output. Mathematically, the Henon map can be written as follows:

$$\begin{aligned} x_{n+1} &= 1 - ax_n + y_n, \\ y_{n+1} &= bx_n \end{aligned} \tag{2}$$

where x_0 and y_0 are the initial conditions of the map and $a \in (0, 1.4], b \in (0.2, 0.314]$ are the control parameters of the map. The map shows good chaotic behaviour when $x_0 = 0.4009, y_0 = 0.408, a = 1.4089, b = 0.3$. Fig. 4 shows 6000 successive points obtained by the iteration of the map.

2) IKEDA MAP

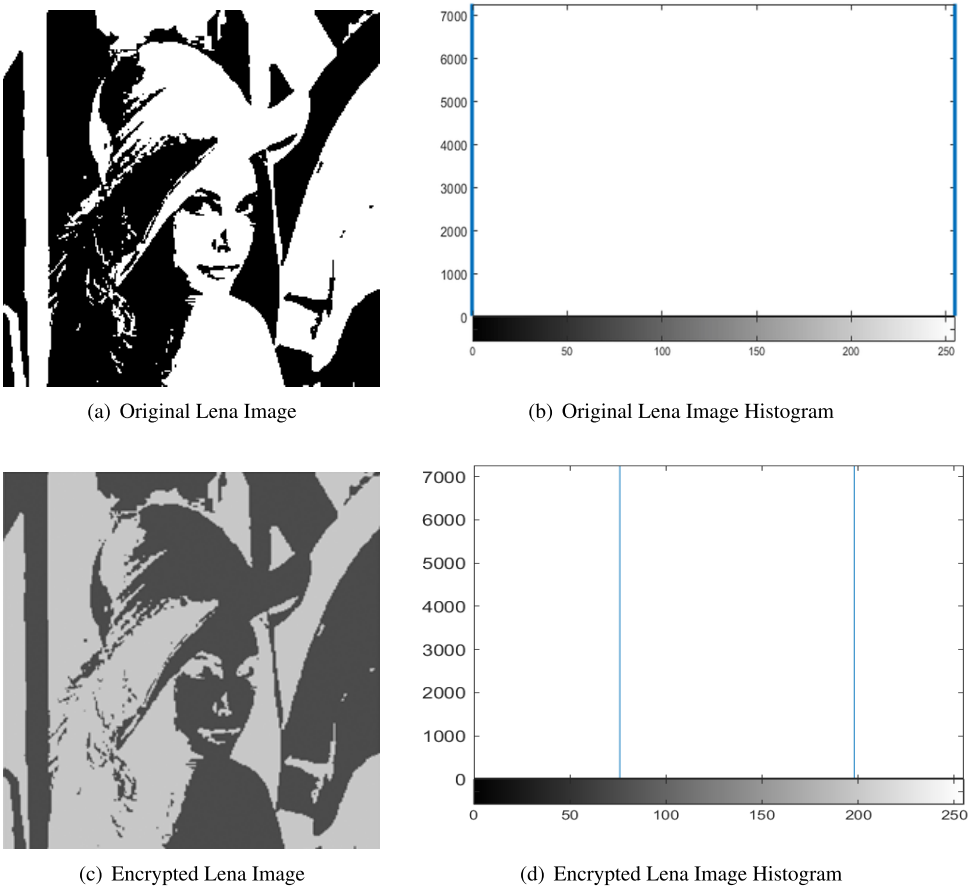
The Ikeda map is a two-dimensional discreet-time complex map with good chaotic behaviour [49]. It takes (x_n, y_n) as input and generates output. It is usually used in its modified form to take into account the saturation factor of a nonlinear dielectric medium. In its real form it can be written as follows:

$$\begin{aligned} x_{n+1} &= 1 + u(x_n cost_n - y_n sint_n), \\ y_{n+1} &= u(x_n sint_n + y_n cost_n), \\ t_n &= 0.4 - \frac{6}{1 + x_n^2 + y_n^2} \end{aligned} \tag{3}$$

The chaotic behaviour is shown when $x_0 = 0.1, y_0 = 0.1, c = 0.39, u = 0.9$ [50].

B. SUBSTITUTION BOXES USED IN THE PROPOSED SCHEME

As discussed earlier, the image obtained after the bit-wise XOR operation has to go through the substitution box



(a) Original Lena Image (b) Original Lena Image Histogram

(c) Encrypted Lena Image (d) Encrypted Lena Image Histogram

FIGURE 3. S-box transformation.

transformation to increase the security of the encrypted image. In this article, three different S-boxes are used which are discussed in detail in the following section.

1) FADIA's S-BOX 1

In [51], a novel 16 × 16 S-box is proposed which is based on the Lorentz equation, shown in Table 1. The security analysis of this S-box also is presented in [51] and it was found out that the proposed S-box is useful in the achievement of confusion property in image encryption. From the simulation results, it is evident that using this S-box improves the efficiency of an encryption algorithm. The ciphertext images generated as a result of the application of the chaotic S-box are invulnerable to different attacks.

2) FADIA's S-BOX 2

In [52], Fadia *et al.* have proposed an S-box shown in Table 2. Due to its ease of implementation and better security, while taking into account several other parameters such as contrast analysis, homogeneity, entropy and energy analysis, the proposed S-Box has been proven to be able to provide better confusion for image encryption. The S-box has been analyzed and declared secure for the encryption of digital images.

3) HUSSAIN's S-BOX

A new S-box is presented in [53] which is based on projective linear group and is applied to the Galois field of order 256. The security and properties of the S-box can be evaluated using a number of parameters [54]–[59]. The efficiency of Hussain's S-box is evaluated using several tests such as the criterion of bit independence, the non-linearity test, the criterion of majority logic and the test of non-linearity. Hussain's S-box is highly secure which has been proven via the aforementioned parameters. The values of the S-box are shown in Table 3.

C. ENCRYPTION PROCEDURE

Let P be the greyscale input image having dimensions of $A \times B$ pixels where A represents the number of rows and B number of columns, both A and B are equal in our case. Input image P has pixels values between 0 and 255. The major steps of the encryption scheme are displayed in Fig. 5. For the sake of understanding, the proposed algorithm is applied on a 4 × 4 sample data as shown in Fig. 6. Below is the description of the steps involved:

1) Two sets of chaotic values having size of A or B have been generated i.e. $LA = (x_1, x_2, x_3 \ldots, x_A)$,

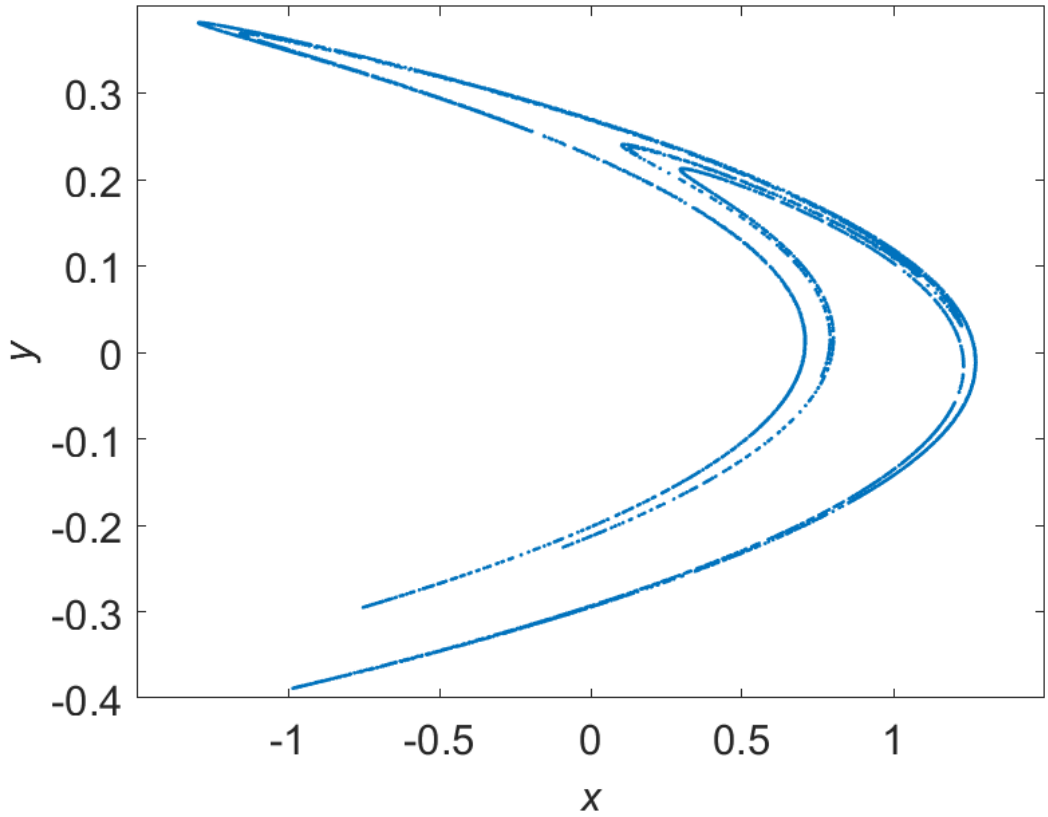


FIGURE 4. Phase diagram of Henon map ($x_0 = 0.4009, y_0 = 0.408, a = 1.4089, b = 0.3$).

TABLE 1. Fadia's S-box 1 [51].

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

$LB = (y_1, y_2, y_3 \ldots, y_B)$ with the help of Ikeda map by setting the values of the parameters $x_0 = 0.1$, $y_0 = 0.1$ and $c = 0.39$, $u = 0.9$.

2) The values of LA and LB are sorted and the indexes of sorted values in the original matrices are retrieved and contained in SA and SB, where both SA and SB are row matrices.

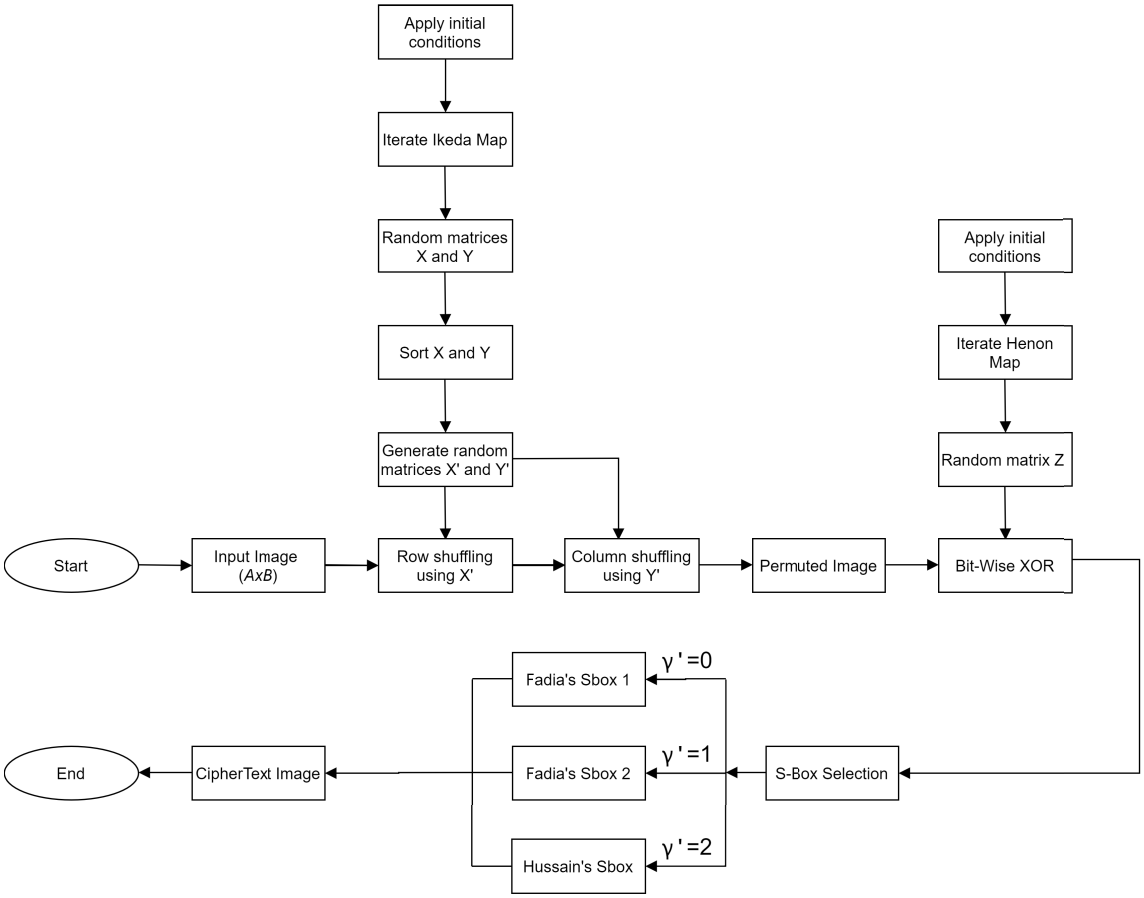


FIGURE 5. Flow chart of proposed scheme.

TABLE 2. Fadia's S-box 2 [52].

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

3) According to the sequence *SA*, the positions of all rows are permuted from the first column until the last column and using the same method and sequence *SB*, all columns are permuted from the first row until the

TABLE 3. Hussain's S-box [53].

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

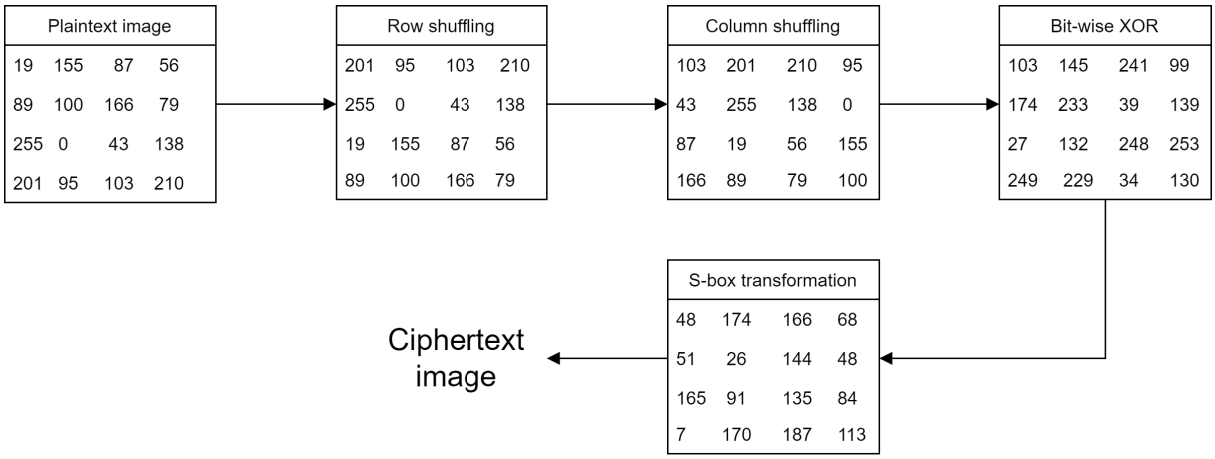


FIGURE 6. Algorithm applied on a 4 x 4 sample data.

last row. The resulting shuffled image is represented as α.

4) The Henon map is iterated $A \times B$ times and the result is placed in β and γ as it is a two-dimensional chaotic map, where $\beta = \beta_1, \beta_2, \ldots \beta_{A\times B}$ and $\gamma = \gamma_1, \gamma_2, \ldots \gamma_{A\times B}$ are sets of random chaotic values.
5) The matrix β is reshaped into $A \times B$ matrix. The reshaped β matrix in then multiplied with a factor of 10^{14} to make the values of reshaped β large enough so that after the application of modulus 256 and floor operation the set of values must not have maximum repetition of a same number, modulus 256 and floor function is applied to obtain matrix β' having integer values only. Mathematically, this operation can be expressed as:

$$\beta' = floor(Mod(10^{14} \times reshape(\beta, A, B)), 256) \quad (4)$$

6) The shuffled image α is XORed bit-wise with the matrix β' to get matrix ω.
7) The second element of matrix γ is selected, multiplied with a factor 10^2 to prepare it for modulus 3 operation, then rounded and modulus 3 function is applied to obtain a value of 0, 1 or 2. This whole operation can

be represented mathematically as:

$$\gamma' = Mod(round(10^2 \times \gamma(:, 2)), 3) \tag{5}$$

8) If the value in γ' is 0, Fadia's S-box 1 will be selected. For $\gamma' = 1$, Fadia's S-box 2 will be selected. For $\gamma' = 2$, Hussain's S-box will be utilized for the substitution of pixels of matrix ω to obtain the final encrypted image C.
The decryption can be done by repeating the steps from step 8 to step 1.

III. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

For the performance analysis of an image encryption scheme, a variety of tests are proposed in [1]. For this specific algorithm, these security tests are conducted using MATLAB 2018a with 4GB memory, 1GHz CPU and Microsoft Windows 10 operating system. Four test images of the Baboon, Cameraman, Lena and Barbara are chosen as shown in Fig. 7 (a, c, e, g). Among these test images, the Lena image is composed of binary values only. The encrypted versions of these test images are shown in Fig. 8 (a, c, e, g). The simulation results are contrasted with the algorithms presented in [19], [43] and [34] to prove the efficiency of the scheme proposed in this article.

For demonstration purposes, the image after every stage is shown for the Baboon image only in Fig. 9.

A. HISTOGRAM AND CHI-SQUARE INVESTIGATION

A histogram tells us about the graphical pixel values replicated in an image. For an encrypted image to be immune to different attacks, its histogram must be uniform. The plaintext image histograms of the four test images are shown in Fig. 7 (b, d, f, h) and Fig. 8 (b, d, f, h) shows the histograms of encrypted images. From Fig. 7 (b, d, f, h), it can be clearly seen that the plaintext histograms have sharp peaks but for the ciphertext images, the histograms are almost uniform as shown in Fig. 8 (b, d, f, h). To prove the uniformity of encrypted images histograms mathematically, chi-square ($\chi 2$) test is used. Mathematical expression for chi-square is:

$$\chi 2 = \sum_{\mathrm{L}=0}^{255} \frac{(\text{observed value-expected value})^{\,2}}{\text{expected value}} \tag{6}$$

where L is the intensity level. Lower values of $\chi 2$ shows that the pixel distribution is uniform. The chi-square values for the encrypted images are tabulated in Table 4 and are also compared with the schemes proposed in [19], [43] and [34]. It is clear from Table 4 that the encrypted images obtained through the proposed algorithms have uniform pixel distribution and have successfully covered all the data from the hackers.

B. INFORMATION ENTROPY

Entropy has a significant role in the measurement of unpredictability and the randomness of information [55]. Entropy illustrates the degree of uncertainty in a communication system in the information theory. It was Claude Elwood Shannon who in 1949 gave this notion of information entropy [60]. Mathematically, the entropy $H(m)$ can be expressed as:

$$H(m) = \sum_{i=0}^{2^N-1} p\,(m_i) \times \log_2 \frac{1}{p\,(m_i)} \tag{7}$$

In the above equation, $p(m_i)$ is the occurrence probability of the symbol m_i. For a random source which generates 2^Z symbols, the entropy $H(m)$ is Z. However, if the encryption process is carried out with a source that emits 2^8 symbols and all of them can occur with equal probability, the ideal entropy value will be 8 but practically it is a value close to 8. The entropy $H(m)$ values of the test images for both plaintext and ciphertext images and that of [19], [43] and [34] are tabulated in Table 5. It can be seen from Table 5 that the values of entropy for the ciphertext images of all four test images are very close to 8 for the proposed algorithm and are greater than the algorithms proposed in [19], [43] and [34]. Furthermore, the local entropy defined in [61] is calculated for all encrypted images. We have selected 30 random non-overlapping blocks and calculated mean of all entropy values. The local entropy for all encrypted images are greater than 7.90 and hence the proposed scheme is secure against entropy attack.

TABLE 4. Histogram uniformity analysis on the basis on chi-square test.

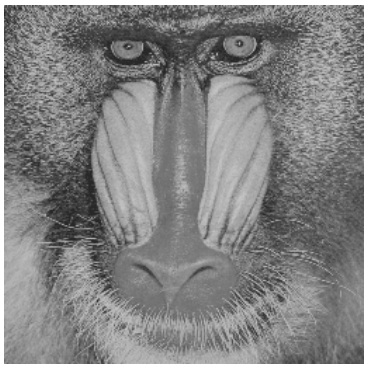
Image	Proposed	[43]	[19]	[34]
Baboon	245.8906	20602	277.0234	246.9063
Cameraman	240.8906	38323	244.2813	293.3438
Lena	246.7578	3499100	3227.3	215.0703
Barbara	221.0859	225120	3227.3	284.4609

C. CORRELATION ANALYSIS OF PLAINTEXT IMAGE AND CIPHERTEXT IMAGE

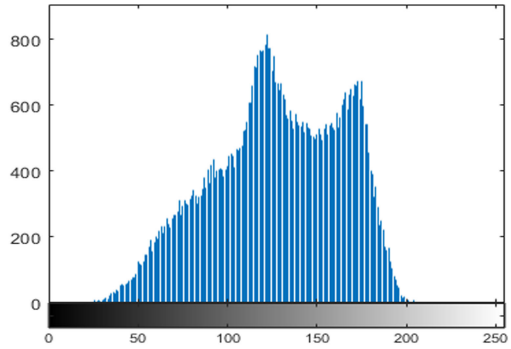
Correlation shows the relationship of two variables. It is useful for checking the quality of encryption of a cryptosystem [62]. For completely different plaintext and ciphertext images, value of the correlation coefficient must be very small and close to zero. The correlation between plaintext and ciphertext images is realized by calculating two-dimension correlation. Mathematically, it is given as:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_{ij}-\bar{I}\right)\left(C_{ij}-\bar{C}\right)}{\sqrt{\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_{ij}-\bar{I}_{ij}\right)^2\right)\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\left(C_{ij}-\bar{C}_{ij}\right)^2\right)}} \tag{8}$$

where $\bar{I}$ is the mean value of the plaintext image and $\bar{C}$ is the mean value of the ciphertext image. The correlation for test images between plaintext and ciphertext is analyzed and compared with [19], [43] and [34], and the results are illustrated in Table 6.

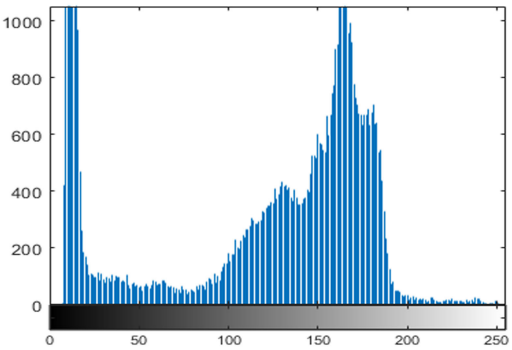


(a) Baboon



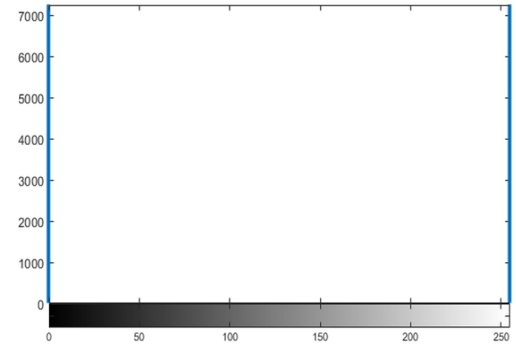
(b) Plaintext Baboon Histogram

(c) Cameraman



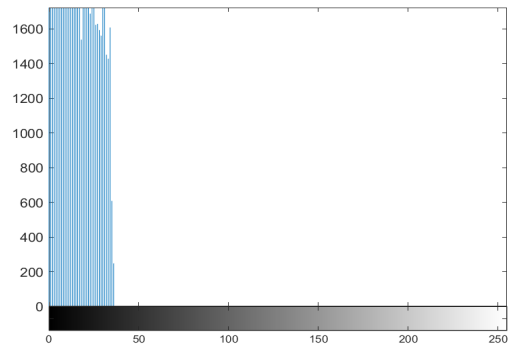
(d) Plaintext Cameraman Histogram

(e) Lena



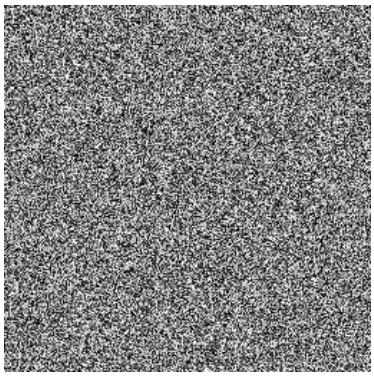
(f) Plaintext Lena Histogram

(g) Barbara

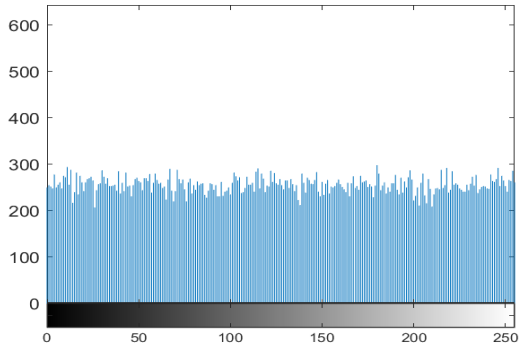


(h) Plaintext Barbara Histogram

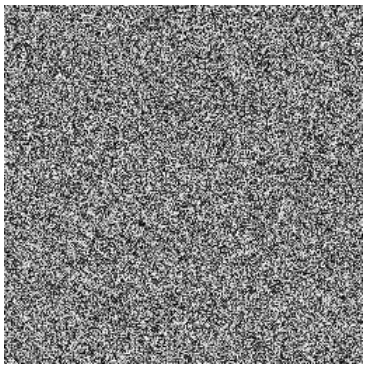
FIGURE 7. **Original test images with histograms.**



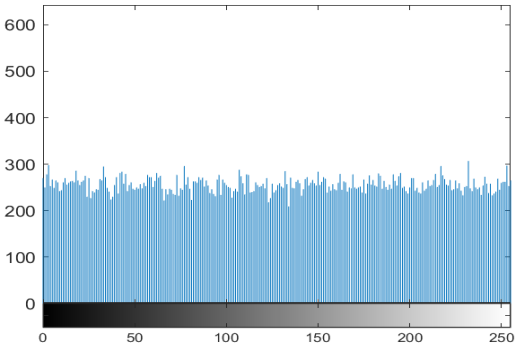
(a) Baboon



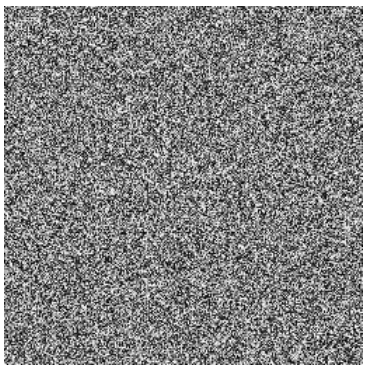
(b) Encrypted Baboon Histogram



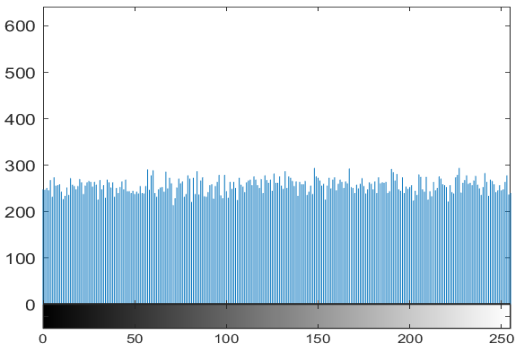
(c) Cameraman



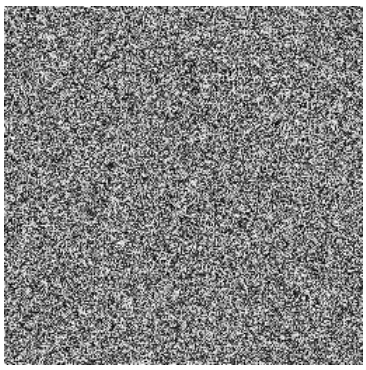
(d) Encrypted Cameraman Histogram



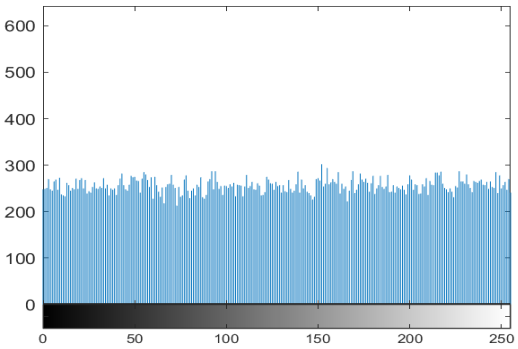
(e) Lena



(f) Encrypted Lena Histogram

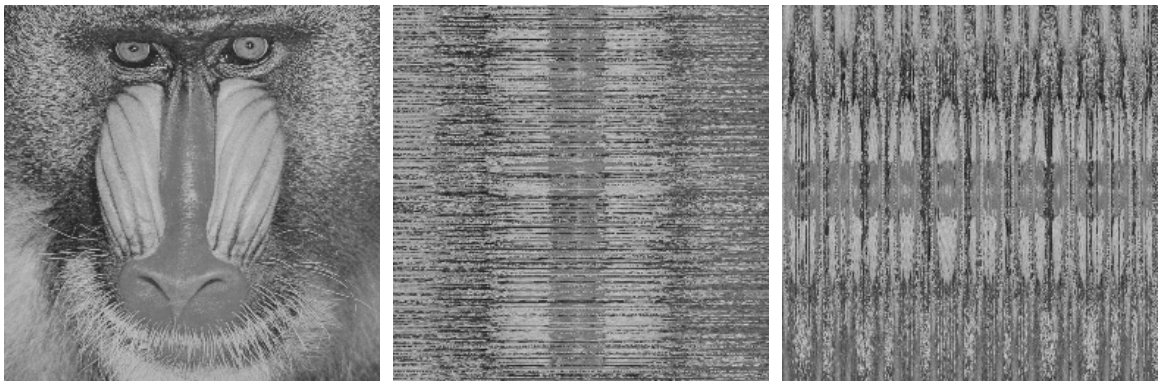


(g) Barbara

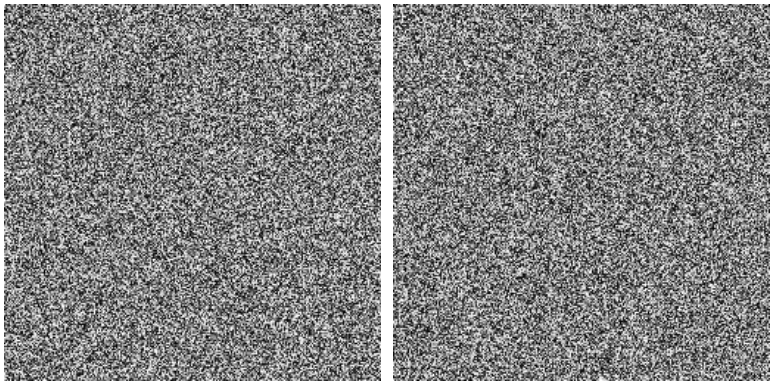


(h) Encrypted Barbara Histogram

FIGURE 8. Encrypted images and their histograms.



(a) Plain text Baboon. (b) Permuted row-wise. (c) Permuted column-wise.



(d) Diffusion through XOR operation. (e) After S-Box transformation

FIGURE 9. Baboon image at different stages of encryption.

TABLE 5. Information entropy.

Image	Plaintext Image	Proposed	[43]	[19]	[34]
Baboon	7.1273	7.9969	7.7394	7.9960	7.9973
Cameraman	7.0097	7.9974	7.6536	7.9973	7.9968
Lena	0.9997	7.9973	2.2785	7.9638	7.9976
Barbara	7.0420	7.9976	5.9745	7.9971	7.9969

TABLE 6. Values of correlation coefficient.

Image	Plaintext image	Proposed	[43]	[19]	[34]
Baboon	0.6860	0.0006	0.0011	0.00097	0.0025
Cameraman	0.9227	-0.0043	0.0447	0.0027	-0.0077
Lena	0.8874	-0.0068	0.1936	-0.0015	0.0010
Barbara	0.9300	-0.0058	0.0563	0.0018	-0.0097

D. CONTRAST INVESTIGATION

Contrast investigation is typically the calculation of the local intensity variance existing in an image. Contrast is the luminous or colour difference due to which the objects in an image can be distinguished and because of which viewers are able to identify different objects. Higher values of contrast demonstrate that the image has considerably different gray levels while constant gray levels are indicated by lower values. For image encryption, higher contrast values are desirable. Mathematically, it is defined as:

$$C = \sum_{i,j} |i-j|^2 \times p(i,j) \tag{9}$$

where $p(i, j)$ indicates the number of gray-level co-occurrence matrices (GLCM). The values of the contrast for plaintext images and ciphertext images are listed in Table 7 which shows that the contrast values are greater than those presented in [19], [43] and [34].

TABLE 7. Values of contrast.

Image	Plaintext image	Proposed	[43]	[19]	[34]
Baboon	0.8582	10.5375	10.2866	10.4733	10.5023
Cameraman	0.5872	10.5872	9.6160	10.5188	10.4816
Lena	2.7570	10.5325	7.4163	10.4968	10.5324
Barbara	0.3276	10.5872	8.1621	10.4989	10.5194

TABLE 8. Energy.

Image	Plaintext image	Proposed	[43]	[19]	[34]
Baboon	0.0898	0.0156	0.0160	0.0156	0.0156
Cameraman	0.1805	0.0156	0.0166	0.0156	0.0156
Lena	0.4471	0.0156	0.0992	0.0156	0.0156
Barbara	0.1889	0.0156	0.0258	0.0156	0.0156

TABLE 9. Homogeneity.

Image	Plaintext image	Proposed	[43]	[19]	[34]
Baboon	0.7502	0.3889	0.3968	0.3904	0.3892
Cameraman	0.8953	0.3876	0.4258	0.3891	0.3901
Lena	0.9508	0.3887	0.5830	0.3896	0.3901
Barbara	0.8891	0.3894	0.4677	0.3903	0.3901

E. ENERGY

The energy calculation results in the addition of squared elements in the GLCM. The value of energy is low when the entries of GLCM are nearly equal and has a high value when some of the entries have higher magnitudes. For an encrypted image, the energy must be low. Mathematically, image energy is calculated as:

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

where $p(i,j)$ is the number of gray-level co-occurrence matrices. The energy values of the plaintext images and ciphertext images and that for [19], [43] and [34] are listed in Table 8.

F. HOMOGENEITY

The homogeneity quantifies how close the elements distribution is in the GLCM. The GLCM illustrates the statistical combination of pixel luminosity or grey levels in the form of table. From the GLCM table, the occurrence of gray scale patterns can be visualized. Lower values of homogeneity are desirable for an efficient encryption scheme. These patterns are read from the GLCM table. Mathematically, it is expressed as:

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

where $p(i,j)$ represents the gray-level co-occurrence matrices in GLCM. The values of the homogeneity for the plaintext images, images encrypted by the proposed algorithm, [19], [43] and [34] are shown in Table 9.

G. MEAN SQUARE ERROR

Mean square error (MSE) is used to analyze the Avalanche effect. The Avalanche effect states that changing the plaintext image or key causes a tremendous change in the corresponding encrypted image. MSE is calculated for two digital images and is the cumulative squared error between them. Mathematically, it can be calculated as:

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [P(i,j) - C(i,j)]^2 \tag{12}$$

where M is the width and N is the height of the image. $P_1(i,j)$ and $C(i,j)$ illustrates the pixel position at ith row and jth column for the plaintext image and ciphertext image respectively. The value of MSE is evaluated for the plaintext image and ciphertext image of all the four test images and tabulated in Table 10. The values for the images encrypted using Amir *et al.* [43] algorithm, [19] and [34] are also mentioned in Table 10. The MSE value should be large for the the purpose of security and robustness against different statistical attacks.

TABLE 10. Mean square error.

Image	Image Size	Proposed	[43]	[19]	[34]
Baboon	256 × 256	6819	6642.7	6772.5	6819.9
Cameraman	256 × 256	9489.7	9330.3	9447.7	9325.6
Lena	256 × 256	21694	26107	21570	21652
Barbara	256 × 256	17997	21073	7767.4	17876

TABLE 11. Encryption time (sec).

Image	Proposed	[43]	[19]	[34]
Baboon	0.736	5.376	5.380	0.093
Cameraman	0.775	5.513	5.106	0.100
Lena	0.719	5.131	5.323	0.101
Barbara	0.798	5.174	5.318	0.087

TABLE 12. Peak signal to noise ratio.

Image	Proposed	[43]	[19]	[34]
Baboon	9.7936	9.9074	9.8233	9.7940
Cameraman	8.3583	8.4318	8.3776	8.4155
Lena	4.7674	3.9633	4.7922	4.7758
Barbara	5.5789	4.8935	9.2281	5.6082

H. TIMING ANALYSIS

An encryption algorithm is efficient when it uses fewer resources and has minimal computation time. For checking the computational complexity, the encryption time of the proposed algorithm is outlined and compared with [19], [43] and [34] in Table 11, which shows the time taken by the proposed algorithm to encrypt each plaintext image. It is obvious from Table 11 that the proposed scheme computational complexity is very low as compared to the schemes proposed in [43] and [19]. Encryption time of [34] is less than the proposed algorithm because it encrypt only one fourth part of the image. This analysis has been done using MATLAB 2018a with 4GB memory, 1GHz GPU and Microsoft Windows 10 operating system.

I. PEAK SIGNAL TO NOISE RATIO

This ratio is used for the analysis of the encryption algorithm. It measures pixel value changes between the plaintext image and the ciphertext image [63]. The mathematical expression for the calculation of PSNR is given in Eq. 13 [63]:

$$PSNR = 10 \times \log_2 \left[\frac{I_{max}^2}{MSE} \right] \tag{13}$$

where I_{max} represents the maximum value of image. For a good encryption algorithm, the PSNR values should be low. For the PSNR values of the test images, see Table 12 which shows PSNR values for the proposed, Ahmad and Hwang *et al.* [19], [43] and [34] algorithms.

J. STRUCTURAL CONTENT

This a test to measure the resemblance between the plaintext and ciphertext images. It shows the similarity between the original and ciphertext image. Mathematically, it is calculated as:

$$SC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(O_{(i,j)}\right)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} \left(E_{(i,j)}\right)^2} \tag{14}$$

where $O_{(i,j)}$ is the original image and $E_{(i,j)}$ is the encrypted image. The desirable values are near to zero that means least similarity between the two images which indicates that the scheme is secured for digital images while values near to 1 means that the two images are identical which indicates an inefficiency of the proposed scheme for digital image encryption. For the proposed scheme, the SC values for Baboon, Cameraman, Lena and Barbara are shown in Table 13 and also compared with the schemes proposed in [19], [43] and [34]. A comparison of the proposed scheme with S-Boxes and without S-Boxes is provided in Table 14. It is clear from Table 14, that with S-Boxes transformation the encryption scheme is more secure.

K. KEY SPACE ANALYSIS

Key space refers to the number of keys that can be used in the process of encryption or decryption. The strength of an encryption algorithm can be evaluated on the basis of its available key space. For an algorithm to be resistant to brute force attacks the key space should be greater that 2^{100} [45].

TABLE 13. Structural content.

Image	Proposed	[43]	[19]	[34]
Baboon	0.0076	0.0119	0.0100	0.0086
Cameraman	0.0092	0.0080	0.0090	0.0095
Lena	0.0043	-0.0512	0.0074	0.0058
Barbara	0.0028	0.0026	0.0101	0.0029

TABLE 14. The proposed scheme with and without dynamic S-Boxes.

	Baboon		Cameraman		Lena		Barbara	
Parameter	without S-box	After S-box	without S-box	After S-box	without S-box	After S-box	without S-box	After S-box
Information entropy	7.9960	7.9969	7.9973	7.9974	7.9966	7.9973	7.9972	7.9976
Correlation Coefficient	0.0103	0.0006	-0.0054	-0.0043	0.0030	-0.0068	0.0009	-0.0058
Contrast	10.4400	10.5375	10.5105	10.5872	10.4555	10.5325	10.4813	10.5872
Energy	0.0156	0.0156	0.0156	0.0156	0.0156	0.0156	0.0156	0.0156
Homogeneity	0.3899	0.3889	0.3892	0.3876	0.3897	0.3887	0.3897	0.3894
Mean square error	6803.7	6819	9453.4	9489.7	21651	21694	17831	17997
Peak signal to noise ratio	9.8034	9.7936	8.3749	8.3583	4.7760	4.7674	5.6190	5.5789
Structural content	0.0085	0.0076	0.0099	0.0092	0.0034	0.0043	0.0034	0.0028

As per the IEEE standard, computational precision is about 10^{-15}, and the total number of keys for an algorithm can be calculated as:

$$\begin{aligned} \text{KS} &= \left(\left(10^{15} \times 10^{15}\right)^{\alpha} \times \left(10^{15} \times 10^{15} \times 10^{15} \times 10^{15}\right)\right)^{\beta} \\ &= \left(\left(10^{30}\right)^{\alpha} \times 10^{60}\right)^{\beta} \end{aligned} \tag{15}$$

From (14), it is evident that even for a single cycle of permutation and diffusion ($\alpha = 1, \beta = 1$) the key space is about $10^{90} \approx 2^{299}$. This key space is large enough to withstand any type of brute force attack. This key space can be further increased by choosing larger values of α and β. For $\alpha = \beta = 2$, the key space is $10^{240} \approx 2^{798}$ that is large enough to resist every kind of brute force attack with available computer and software technologies.

L. KEY SENSITIVITY ANALYSIS

Key sensitivity analysis is another parameter to analyze the strength of an encryption algorithm. A key sensitive algorithm will give a total different output when there is a slight change in the key. Suppose S_1 and S_2 are the two keys that are slightly different 10^{-15} from each other which gives encrypted outputs of E_1 and E_2 respectively. The condition for key sensitivity is met, if the The E_1 and E_2 percentage difference is greater than 99% [22]. For key sensitivity analysis of the proposed algorithm, the key seed parameters are x_0, y_0, a and b of the Henon map. The Baboon image is encrypted with key coefficients ($x_0 = 0.4009$, $y_0 = 0.408$, $a = 1.4089$, $b = 0.3$.) to obtain encrypted image E_1. Another encrypted image E_2 is generated with a slight change of 10^{-15} in only x_0 ($x_0 = 0.4009 + 10^{-15}$, $y_0 = 0.408$, $a = 1.4089$, $b = 0.3$.). The encrypted images E_1, E_2 and their difference is shown in Fig. 10. It is evident from Fig. 10(c) that a slight change in x_0 only results in a considerable change in the resulting encrypted image. The numerical results in terms of percentage difference of all the test images for the proposed, [19], [43] and [34] are tabulated in Table 15. For the proposed algorithm, the value of percentage difference is between $|E_1$ - $E_2|$ is greater that 99.6% for all the test images with a small change in x_0. A minor change in other key seed parameters also led to significant changes. From Table 15, it can be seen that the percentage differences of [19], [43] and [34] are less than the proposed scheme.

M. RESISTANCE AGAINST DIFFERENTIAL ATTACKS

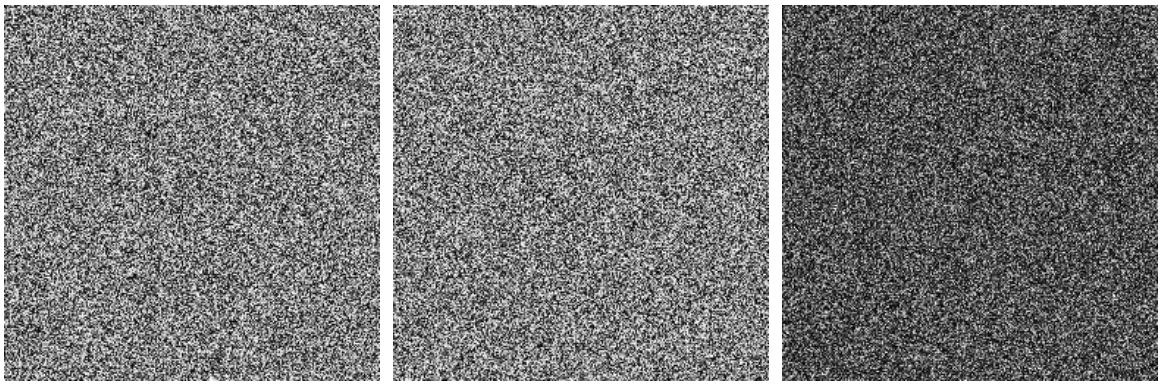
In a secure image encryption algorithm, a single pixel change in the plaintext image should result in a significant change in the corresponding encrypted image. When an encrypted image is significantly changed, it shows that the proposed scheme is resistant to differential attack. To investigate the effect of change of one pixel on a ciphertext image, the commonly used parameters are: (i) Number of Pixel Change Rate (NPCR) and (ii) Unified Average Change Intensity (UACI) [64], [65]. Mathematical expression for NCPR is:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{16}$$

and the Mathematical expression for UACI is:

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{255}\right] \times 100\%, \tag{17}$$

where E_1 is the encrypted image of the original plaintext image and E_2 is the encrypted image obtained as a result of a single pixel value change in the plaintext image. For $E_1 = E_2$, $D_{i,j} = 0$; else $D_{i,j} = 1$. The numerical values of *NCPR* and *UACI* are shown in Table 16 and Table 17. It is evident



(a) Encrypted Image E_1 ($x_0 = 0.4009, y_0 = 0.408, a = 1.4089, b = 0.3$). (b) Encrypted Image E_2 ($x_0 = 0.4009 + 10^{-15}, y_0 = 0.408, a = 1.4089, b = 0.3$). (c) Difference of E_1 and E_2.

FIGURE 10. Key sensitivity analysis.

TABLE 15. Percentage difference between E_1 and E_2.

Image	Proposed	[43]	[19]	[34]
Baboon	99.61	65.90	64.84	0.2
Cameraman	99.61	65.90	64.84	0.2
Lena	99.61	57.68	64.84	0.2
Barbara	99.61	64.86	64.84	0.3

TABLE 16. NCPR values.

Image	Proposed	[43]	[19]	[34]
Baboon	99.61	0	0.39	0.25
Cameraman	99.61	0	0.39	0.23
Lena	99.61	0	0.39	0.22
Barbara	99.61	0	0.39	0.37

TABLE 17. UACI values.

Image	Proposed	[43]	[19]	[34]
Baboon	33.52	0	0.20	0.01
Cameraman	33.49	0	0.10	0.01
Lena	33.49	0	0.10	0.01
Barbara	33.43	0	0.10	0.04

from Table 16 and Table 17, that the proposed algorithm *NCPR* and *UACI* values are better that the schemes proposed in [43] and [19] and [34] which proves high resistance against differential attacks.

N. NIST ANALYSIS

National Institute of Standards and Technology (NIST) is a US (United States) based company that provides guidelines for the protection of data. To make sure that data is protected from attackers/eavesdroppers, security measurements should be taken. Confidential data should be cyber secure and it must follow the guidelines provided by US government or agencies. NIST has outlined 15 significant statistical tests for cryptographic applications which are used to determine the strength of any cryptographic algorithm and estimate the actual randomness produced by the system. The test is applied on encrypted images and results are shown in Tables 18 and 19, respectively. From tables, it is evident that all tests passed the randomness test and hence the proposed scheme is secured.

TABLE 18. NIST test results for encrypted grey images.

Test	P-values for grey encryptions of four encrypted images				Results
		Baboon	Cameraman	Barbara	Lena	
Frequency		0.75183	0.0.50664	0.87437	N/A	Pass
Block Frequency		0.09938	0.80005	0.65797	N/A	Pass
Rank		0.29191	0.50105	0.29191	N/A	Pass
Runs (M = 10,000)		0.094039	0.15267	0.94926	N/A	Pass
Long runs of ones		0.035752	0.0	0.035752	N/A	Pass
Overlapping templates		0.85988	0.85988	0.85988	N/A	Pass
No overlapping templates		1	1	0.99981	N/A	Pass
Spectral DFT		0.46816	1.4679	0.66336	N/A	Pass
Approximate entropy		0.87789	0.86163	0.23975	N/A	Pass
Universal		0.99857	0.3167	0.98494	N/A	Pass
Serial	p values 1	0.0048128	0.39454	0.073956	N/A	Pass
Serial	p values 2	0.020832	0.9044	0.0066613	N/A	Pass
Cumulative sums forward		0.24246	0.23676	0.2459	N/A	Pass
Cumulative sums reverse		1.0587	0.8099	1.0672	N/A	Pass

TABLE 19. NIST random excursions and variants.

Test	P-values for grey encryption of four encrypted images					Results
		Baboon	Cameraman	Barbara	Lena	
Random excursions	X = -4	$4.3758 \times 10^{-}5$	0.022891	0.78498	0.32258	successful outcome
	X = -3	0.0061611	0.29411	0.74809	0.043768	Pass
	X = -2	0.00018035	0.50105	0.35459	0.50522	Pass
	X = -1	0.78078	0.68402	0.3627	0.94668	Pass
	X = 1	0.85748	0.68402	0.78289	0.68335	Pass
	X = 2	0.14271	0.68926	0.90375	0.59013	Pass
	X = 3	0.0033871	0.059012	0.58772	0.66737	Pass
	X = 4	0.005959	0.077712	0.75647	0.55524	Pass
Random excursions variants	X = -5	0.076544	0.26023	0.86102	0.78419	Pass
	X = -4	0.12961	0.3167	0.96042	0.97248	Pass
	X = -3	0.20134	0.51467	0.68103	0.87028	Pass
	X = -2	0.33957	0.37917	0.82009	0.79215	Pass
	X = -1	0.61619	0.35384	0.69364	0.78419	Pass
	X = 1	0.6519	0.35384	0.69364	0.64808	Pass
	X = 2	0.58242	0.20703	0.93957	0.59816	Pass
	X = 3	0.4327	0.49574	0.51832	0.7133	Pass
	X = 4	0.25565	0.98003	0.39884	0.46872	Pass
	X = 5	0.1655	0.87719	0.38137	0.19072	Pass

IV. CONCLUSION

A new image encryption scheme using chaos theory and dynamic substitution is presented in this article. The confusion property is achieved by using a two-dimensional Ikeda map and diffusion through the Henon map, respectively. In the last stage of encryption, the pixel values are

substituted using S-box. However, S-box is selected randomly which enhances the security of the encrypted images. The security of the proposed scheme is analyzed via several security tests. From information entropy, histogram analysis, correlation coefficient, energy, homogeneity and mean square error it is evident that the proposed scheme is highly secure compared to traditional schemes. Furthermore, its use of less computational resources shows that the proposed scheme is feasible for real-time encryption applications. The proposed scheme can be used for the encryption of other digital media such as audio and video with slight modification. In future, we aim to test the proposed scheme on video and audio data. Moreover, proposing an encryption system to secure remote sensing big data will be investigated in future works [66]–[69].

REFERENCES

[1] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Comput.*, vol. 23, no. 4, p. 25, 2010.

[2] M. B. Younas and J. Ahmad, "Comparative analysis of chaotic and non-chaotic image encryption schemes," in *Proc. Int. Conf. Emerg. Technol. (ICET)*, Dec. 2014, pp. 81–86.

[3] I. Bashir, F. Ahmed, J. Ahmad, W. Boulila, and N. Alharbi, "A secure and robust image hashing scheme using Gaussian pyramids," *Entropy*, vol. 21, no. 11, p. 1132, Nov. 2019.

[4] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, Sep. 2019.

[5] O. Abikoye, K. Adewole, and A. Oladipupo, "Efficient data hiding system using cryptography and steganography," Univ. Ilorin, Ilorin, Nigeria, Dec. 2012, vol. 4, no. 11.

[6] R. Sivaraman, R. Sundararaman, J. B. B. Rayappan, and R. Amirtharajan, "Ring oscillator as confusion–diffusion agent: A complete TRNG drove image security," *IET Image Process.*, 2020.

[7] N. Chidambaram, P. Raj, T. Karruppuswamy, and R. Amirtharajan, "An advanced framework for highly secure and cloud-based storage of colour images," *IET Image Process.*, 2020.

[8] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons Fractals*, vol. 35, no. 2, pp. 408–419, Jan. 2008.

[9] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[10] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons Fractals*, vol. 26, no. 1, pp. 117–129, Oct. 2005.

[11] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcation Chaos*, vol. 14, no. 10, pp. 3613–3624, Oct. 2004.

[12] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons Fractals*, vol. 42, no. 3, pp. 1745–1754, Nov. 2009.

[13] F. Sun, S. Liu, Z. Li, and Z. Lü, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons Fractals*, vol. 38, no. 3, pp. 631–640, Nov. 2008.

[14] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, Jan. 2011.

[15] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Phys. Lett. A*, vol. 372, no. 15, pp. 2645–2652, Apr. 2008.

[16] C. Zhu, "A novel image encryption scheme based on improved hyper-chaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, Jan. 2012.

[17] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Phys. Lett. A*, vol. 346, nos. 1–3, pp. 153–157, 2005.

[18] T. Gao and Z. Chen, "Image encryption based on a new total shuffling algorithm," *Chaos, Solitons Fractals*, vol. 38, no. 1, pp. 213–220, Oct. 2008.

[19] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1839–1850, Dec. 2015.

[20] M. Andrecut, "Logistic map as a random number generator," *Int. J. Modern Phys. B*, vol. 12, no. 9, pp. 921–930, Apr. 1998.

[21] L. Kocarev, "Chaos-based cryptography: A brief overview," *IEEE Circuits Syst. Mag.*, vol. 1, no. 3, pp. 6–21, 3rd Quart., 2001.

[22] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools Appl.*, vol. 75, no. 21, pp. 13951–13976, Nov. 2016.

[23] M. Baptista, "Chaos in cryptography," *Phys. Lett. A*, vol. 240, nos. 1–2, pp. 50–54, 1998.

[24] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method," in *Proc. IEEE Int. Symp. Circuits Syst.*, May 2002, p. 2.

[25] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel hybrid secure image encryption based on julia set of fractals and 3D lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, Feb. 2020.

[26] J. Ahmad, S. O. Hwang, and A. Ali, "An experimental comparison of chaotic and non-chaotic image encryption schemes," *Wireless Pers. Commun.*, vol. 84, no. 2, pp. 901–918, Sep. 2015.

[27] R. C. Hilborn *Chaos and Nonlinear Dynamics: An Introduction for Scientists and Engineers*. London, U.K.: Oxford Univ. Press, 2000.

[28] A. G. Radwan and S. K. Abd-El-Hafiz, "Image encryption using generalized tent map," in *Proc. IEEE 20th Int. Conf. Electron., Circuits, Syst. (ICECS)*, Dec. 2013, pp. 653–656.

[29] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989.

[30] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, Jun. 1998.

[31] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, "A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices," *Neural Comput. Appl.*, vol. 28, no. S1, pp. 953–967, Dec. 2017.

[32] 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.

[33] J. Ahmad, M. A. Khan, F. Ahmed, and J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation," *Neural Comput. Appl.*, vol. 30, no. 12, pp. 3847–3857, Dec. 2018.

[34] J. Ahmad, A. Tahir, J. S. Khan, M. A. Khan, F. A. Khan, Arshad, and Z. Habib, "A partial ligt-weight image encryption scheme," in *Proc. UK/China Emerg. Technol. (UCET)*, Aug. 2019, pp. 1–3.

[35] M. Khan, F. Masood, and A. Alghafis, "Secure image encryption scheme based on fractals key with fibonacci series and discrete dynamical system," *Neural Comput. Appl.*, vol. 32, pp. 11837–11857, 2020.

[36] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.

[37] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Comput. Biol. Med.*, vol. 72, pp. 170–184, May 2016.

[38] A. S. Banu and R. Amirtharajan, "A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach," *Med. Biol. Eng. Comput.*, pp. 1–14, 2020.

[39] F. Masood, W. Boulila, J. Ahmad, Arshad, S. Sankar, S. Rubaiee, and W. J. Buchanan, "A novel privacy approach of digital aerial images based on mersenne twister method with DNA genetic encoding and chaos," *Remote Sens.*, vol. 12, no. 11, p. 1893, Jun. 2020.

[40] Y.-Q. Zhang and X.-Y. Wang, "Spatiotemporal chaos in mixed linear–nonlinear coupled logistic map lattice," *Phys. A, Stat. Mech. Appl.*, vol. 402, pp. 104–118, May 2014.

[41] Y.-Q. Zhang, X.-Y. Wang, J. Liu, and Z.-L. Chi, "An image encryption scheme based on the MLNCML system using DNA sequences," *Opt. Lasers Eng.*, vol. 82, pp. 95–103, Jul. 2016.

[42] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.

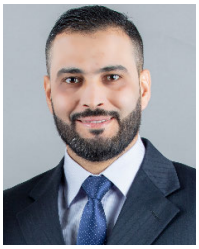
[43] A. Anees, A. M. Siddiqui, and F. Ahmed, "Chaotic substitution for highly autocorrelated data in encryption algorithm," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 9, pp. 3106–3118, Sep. 2014.

[44] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 850–858, Dec. 2017.

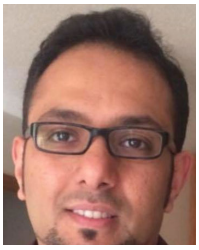
[45] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.
[46] J. M. Amigó, L. Kocarev, and J. Szczepanski, "Theory and practice of chaotic cryptography," *Phys. Lett. A*, vol. 366, no. 3, pp. 211–216, Jun. 2007.
[47] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with gingerbreadman chaotic map and s8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.
[48] M. Hénon, "A two-dimensional mapping with a strange attractor," in *The Theory Chaotic Attractors*. New York, NY, USA: Springer, 1976, pp. 94–102.
[49] K. Ikeda, "Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system," *Opt. Commun.*, vol. 30, no. 2, pp. 257–261, Aug. 1979.
[50] Y. Cao, "A new hybrid chaotic map and its application on image encryption and hiding," *Math. Problems Eng.*, vol. 2013, pp. 1–13, Jan. 2013.
[51] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel substitution box for encryption based on lorenz equations," in *Proc. Int. Conf. Circuits, Syst. Simulation (ICCSS)*, Jul. 2017, pp. 32–36.
[52] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, M. A. Khan, and S. O. Hwang, "A new technique for designing 8 × 8 substitution box for image encryption applications," in *Proc. 9th Comput. Sci. Electron. Eng. (CEEC)*, Sep. 2017, pp. 7–12.
[53] 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.
[54] I. Hussain, T. Shah, H. Mahmood, and M. Afzal, "Comparative analysis of s-boxes based on graphical sac," *Int. J. Comput. Appl.*, vol. 2, no. 5, pp. 1–7, 2010.
[55] J.-X. Chen, Z.-L. Zhu, C. Fu, L.-B. Zhang, and Y. Zhang, "An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 23, nos. 1–3, pp. 294–310, Jun. 2015.
[56] I. Hussain and Z. Mahmood, "Graphical strict avalanche criterion for kasumi s-box," *Can. J. Comput. Math. Nat. Sci. Eng. Med.*, vol. 1, no. 5, pp. 132–136, 2010.
[57] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Statistical analysis of s-box in image encryption applications based on majority logic criterion," *Int. J. Phys. Sci*, vol. 6, no. 16, pp. 4110–4127, 2011.
[58] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, "Some analysis of S-box based on residue of prime number," *Proc. Pak Acad. Sci.*, vol. 48, no. 2, pp. 111–115, 2011.
[59] M. T. Tran, D. K. Bui, and A. D. Duong, "Gray s-box for advanced encryption standard," in *Proc. Int. Conf. Comput. Intell. Secur.*, vol. 1, Dec. 2008, pp. 253–258.
[60] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[61] 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.
[62] O. S. F. Allah, "Homomorphic image encryption," *J. Electron. Imag.*, vol. 18, no. 3, Jul. 2009, Art. no. 033002.
[63] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.
[64] 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.
[65] J. S. Teh, M. Alawida, and Y. C. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102421.
[66] I. Chebbi, W. Boulila, and I. R. Farah, "Big data: Concepts, challenges and applications," in *Computational Collective Intelligence*. New York, NY, USA: Springer, 2015, pp. 638–647.
[67] I. Chebbi, W. Boulila, and I. R. Farah, "Improvement of satellite image classification: Approach based on Hadoop/MapReduce," in *Proc. 2nd Int. Conf. Adv. Technol. Signal Image Process. (ATSIP)*, Mar. 2016, pp. 31–34.
[68] W. Boulila, I. R. Farah, and A. Hussain, "A novel decision support system for the interpretation of remote sensing big data," *Earth Sci. Informat.*, vol. 11, no. 1, pp. 31–45, Mar. 2018.
[69] W. Boulila, "A top-down approach for semantic segmentation of big remote sensing images," *Earth Sci. Informat.*, vol. 12, no. 3, pp. 295–306, Sep. 2019.

ABDULLAH QAYYUM was born in Mardan, Khyber Pakhtunkhwa, Pakistan, in August 1996. He received the B.S. degree in electrical engineering (major in communication) from the University of Engineering and Technology (UET) Peshawar, Pakistan, in 2019. His research interests include wireless communication, 5G, antennas, cybersecurity, and image encryption.

JAWAD AHMAD (Senior Member, IEEE) is currently an Experienced Researcher with more than ten years of Cutting-Edge Research and a Teaching Experience in prestigious institutes, including Edinburgh Napier University, U.K., Glasgow Caledonian University, U.K., Hongik University, South Korea, and HITEC University Taxila, Pakistan. He has coauthored more than 50 research articles, in international journals, and peer-reviewed international conference proceedings. He has taught various courses both at undergraduate (UG) and post-graduate (PG) levels during his career. He regularly organizes timely special sessions and workshops for several flagship IEEE conferences. He is an invited reviewer of numerous world-leading high-impact journals (reviewed 50+ journal articles to date). His research areas are cybersecurity, multimedia encryption, machine learning, and application of chaos theory in cybersecurity.



WADII BOULILA (Senior Member, IEEE) received the Eng. degree in computer science from the Aviation School of Borj El Amri, in 2005, the M.Sc. degree from the National School of Computer Science (ENSI), University of Manouba, Tunisia, in 2007, and the Ph.D. degree conjointly from ENSI and Telecom-Bretagne, University of Rennes 1, France, in 2012. He is currently an Associate Professor of computer science with the IS Department, College of Computer Science and Engineering, Taibah University, Medina, Saudi Arabia. He is also a Senior Researcher with the RIADI Laboratory, University of Manouba, and an Associate Researcher with the ITI Department, University of Rennes 1, France. His primary research interests include big data analytics, deep learning, cybersecurity, data mining, artificial intelligence, uncertainty modeling, and remote sensing images. He has served as the chair, a reviewer, and a TPC member for many leading international conferences and journals.



SAEED RUBAIEE received the B.S. degree in chemical engineering from Tennessee Tech University, Cookeville, TN, USA, in 2009, the M.Sc. degree in industrial engineering/management from the University of South Florida, Tampa, FL, USA, in 2010, and the Ph.D. degree in industrial engineering from the Department of Industrial Systems and Manufacturing, Wichita State University, Wichita, KS, USA, in 2015.

He is currently an Associate Professor with the Department of the Industrial and Systems Engineering, University of Jeddah, Jeddah, Saudi Arabia. His research interests include engineering systems, sustainability and green manufacturing, production equipment operation, renewable energy, energy-efficient production planning, manufacturing engineering, materials engineering, advanced materials, mathematical/statistical optimization, and applied optimization.

ARSHAD received the M.Sc. degree in electrical engineering from the University of Strathclyde and the Ph.D. degree from Glasgow Caledonian University, with special focus on electricity markets, demand side response, electricity aggregation, power quality, ancillary services, and power system design and operation. He is currently a Research Associate at the Institute of Energy and Environment, University of Strathclyde, where he is working on an EPSRC Project titled ''HVDC power networks, power quality and plant reliability.'' His main responsibilities include development of novel and fast data acquisition system for capturing different types of signals, such as partial discharges, transients, and harmonics at various locations along HVDC networks. Before joining the University of Strathclyde, he worked as a Research Engineer at Whittaker Engineering Ltd. He worked on designing an innovative heat pump/engine technology for the provision of ancillary services (frequency support, reactive power support, and fast reserve) to the GB electricity grid. He has diverse work experience as a research assistant, lab demonstrator, and lecturer in the higher education sectors of Pakistan and U.K. He received grants from the National ICT R&D Pakistan, Quebec Research Council Canada, Santander Universities Europe, and the IEEE USA. He has many achievements to his name, including being a Founding Member and the Chair of the IEEE Student Branch, and a Founding Member of the IEEE IAS and PELS Student Chapter in GCU.

FAWAD MASOOD was born in Peshawar, Khyber Pakhtunkhwa, Pakistan, in December 1992. He received the B.S. degree in electrical engineering (major in wireless communication) from CECOS University, Peshawar, Pakistan, in July 2015, and the M.S. degree from the Institute of Space Technology (IST), Islamabad, Pakistan, in February 2019. Previously, he completed his certification in IT (CIT), in 2017. His active research areas include cybersecurity, information security, coding and cryptography, chaos theory and its application, fractals-based image encryption, non-linear dynamical systems, and data communication.

FAWAD KHAN received the B.S. degree in electrical engineering from UET Peshawar and the M.S. degree in electrical engineering CECOS University, in 2010 and 2014, respectively, and the Ph.D. degree from the School of Cyber Engineering, Xidian University, in 2018. He is currently working with the National University of Sciences and Technology, Pakistan. His research interests include cryptography and information security. His professional services include Technical Program Committee Member and a Reviewer of several international journals and conferences, including IEEE Access, the IEEE Transactions on Industrial Informatics, *EURASIP Journal on Information Security* (Springer), and *Neural Computing and Applications* (Springer).

WILLIAM J. BUCHANAN is currently a Professor with the School of Computing, Edinburgh Napier University. He was awarded an OBE in the Queen's Birthday awards, in June 2017. He also leads the Centre for Distributed Computing, Networks, and Security and The Cyber Academy, and works in the areas of security, cloud security, Web-based infrastructures, e-crime, cryptography, triage, intrusion detection systems, digital forensics, mobile computing, agent-based systems, and security risk. He has one of the most extensive academic sites in the World and is involved in many areas of novel research and teaching in computing. He has published more than 27 academic books, and more than 250 academic research articles, along with several awards for excellence in knowledge transfer, and for teaching. He was named as one of the Top 100 people for Technology in Scotland from 2012 to 2017. Recently, he was included in the FutureScot Top 50 Scottish Tech People Who Are Changing The World. He is a Fellow of the BCS and the IET.