Est. 1841 | YORK ST JOHN UNIVERSITY

Rehman, Mujeeb Ur, Shafique, Arslan, Khalid, Sohail and Hussain, Iqtadar (2021) Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps. IEEE Access, 9. pp. 52277-52291.

Downloaded from: https://ray.yorksj.ac.uk/id/eprint/8167/

The version presented here may differ from the published version or version of record. If you intend to cite from the work you are advised to consult the publisher's version: http://dx.doi.org/10.1109/ACCESS.2021.3069591

Research at York St John (RaY) is an institutional repository. It supports the principles of open access by making the research outputs of the University available in digital form. Copyright of the items stored in RaY reside with the authors and/or other copyright owners. Users may access full text items free of charge, and may download a copy for private study or non-commercial research. For further reuse terms, see licence terms governing individual outputs. Institutional Repositories Policy Statement

RaY

Research at the University of York St John

For more information please contact RaY at ray@yorksj.ac.uk

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 4, 2021, accepted March 24, 2021, date of publication March 29, 2021, date of current version April 9, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3069591

Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps

MUJEEB UR REHMAN[1], ARSLAN SHAFIQUE[1], SOHAIL KHALID[1], (Member, IEEE), AND IQTADAR HUSSAIN[2]

[1]Department of Electrical Engineering, Riphah International University, Islamabad 46000, Pakistan
[2]Department of Mathematics, Statistics and Physics, Qatar University, Doha 2713, Qatar

Corresponding author: Mujeeb Ur Rehman (mujeeb.rehman@riphah.edu.pk)

This work was supported by Riphah International University, Islamabad.

ABSTRACT The advancement in wireless communication has encouraged the process of data transferring through the Internet. The process of data sharing via the Internet is prone to several attacks. The sensitive information can be protected from hackers with the help of a process called Encryption. Owing to the increase in cyber-attacks, encryption has become a vital component of modern-day communication. In this article, an image encryption algorithm is suggested using dynamic substitution and chaotic systems. The suggested scheme is based upon the chaotic logistic map, chaotic sine maps and the dynamical substitution boxes (S-boxes). In the proposed scheme, the S-box selection is according to the generated sequence by deploying the chaotic sine map. To evaluate the robustness and security of the proposed encryption scheme, different security analysis like correlation analysis, information entropy, energy, histogram investigation, and mean square error are performed. The keyspace and entropy values of the enciphered images generated through the proposed encryption scheme are over 2^{278} and 7.99 respectively. Moreover, the correlation values are closer to zero after comparison with the other existing schemes. The unified average change intensity (UACI) and the number of pixel change rate (NPCR) for the suggested scheme are greater than 33, 99.50% respectively. The simulation outcomes and the balancing with state-of-the-art algorithms justify the security and efficiency of the suggested scheme.

INDEX TERMS Encryption, chaotic map, confusion, diffusion, dynamic substitution.

I. INTRODUCTION

Over the last decades, evolution in communication systems has encouraged the sending of multimedia data with electronic assistance. Among the multimedia data, the digital images that contain sensitive data such as the medical and defense connected images are sent through an insecure channel that includes the Internet. Due to the ease in Internet availability, the security of important data has become a serious ultimatum. There should be proper precautions that could help secure the important data so the breach could be avoided and one's privacy could be maintained [1]–[6]. To secure the information from any doubtful access, cryptographic security protocols have been proposed over the last decade [7]–[12]. The process of securing important information from unknown resources is known as cryptography [13]. Several algorithms are suggested to secure the important information, including the Data Encryption Standard (DES), Advanced Encryption Standard (AES). Rivest–Shamir– Adleman (RSA), and the International Data Encryption Algorithm (IDEA). These schemes are not suitable for image encryption because their primary function is to encrypt the textual data [14]–[17]. Having unique features like the similarity between the pixels and the high redundancy of the digital images, these algorithms cannot encrypt the image properly. Out of the several suggested image encryptions schemes, many are based only on the pixel scrambling, but these schemes are not resistant to cryptographic attacks. [18]–[20]. Chaotic maps serve many purposes in the field of science due to their special nature. Besides its implementations in cryptography, it plays a major role in different fields such as biology, computer mathematics, physics, engineering, and the arts. Over the past decades, a strong connection between cryptography and chaos has been exposed [21]–[24]. These days, chaotic systems are

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

This work is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 License.
For more information, see https://creativecommons.org/licenses/by-nc-nd/4.0/

considered very helpful when it comes to applying secure image communication due to their casual and random behavior. The distinctive properties of chaotic maps like deterministic pseudo-random actions,non-periodicity and sensitivity to the initial conditions are the foundation of the chaotic system's security [25], [26]. The applications of chaotic maps in the latest encryption schemes is due to their non-linear dynamic action and greater keyspace. Chaos theory and cryptography can be used for better encryption schemes designed [27]–[30]. Any encryption scheme must contain the properties of diffusion and confusion so that it can be considered secure. Confusion means a change in the pixel's position and diffusion refers to the change in individual pixel gray values that cause a reduction of correlation between the image pixels [31], [32]. The image encryption scheme based on chaotic maps might be unprotected against different attacks due to the lower keyspace and overall weak encryption mechanism [33]–[35]. Researchers use chaotic maps such as chaotic logistic and sine maps to introduce new encryption algorithms for strong security. The newly suggested encryption schemes based on multiple chaotic maps must accomplish the modern-day requirements of image encryption in real-time applications. The information present in the image can be protected through some noisy images or by means of encryption algorithms. The chaos-based encryption system was first introduced by Matthews [36]. Several image encryption algorithms have been suggested in the literature.

In [37], discrete chaos has been examined and to encrypt the plaintext image of size M $\times$ N, a 2D chaotic Baker's map is implemented. The encryption algorithm that uses the chaotic maps and orthogonal matrices has also been suggested that is robust to image compression and noise [38]. In [39], Ahmad *et al.* have proposed an encryption algorithm in which diffusion and confusion are incorporated using skew tent maps and Henon map, respectively. Also, to make the proposed system more robust, S-box is applied to the processed image. In [40], the authors have used XOR operation, skew tent map, and orthogonal matrices to design a well-organized encryption algorithm to secure the digital images. A lightweight algorithm scheme has also been suggested utilizing Intertwining maps and Chebyshev that encrypts a portion of the transformed image. The reason behind encrypting a certain portion of the image is to required less encryption computational time so that it can be useful for real-time applications [41]. A very well-organized cryptosystem is suggested in [28] that utilizes a Lorenz chaotic map and fractal keys. In [5], utilizing discrete maps like duffing and Henon chaotic maps, an image encryption algorithm is suggested. To overcome traditional encryption algorithms' drawbacks, a new lightweight encryption algorithm is presented in [42]. While in [43], a chaotic logistic map is used to secure the medical images that contain sensitive information. Another encryption algorithm was proposed in [38] for the encryption of medical images in which the chaotic attractors and integer wavelet transform (IWT) is applied in the frequency domain while the deoxyribonucleic acid (DNA) sequence is applied in the spatial domain. In [28], a robust cryptosystem for aerial image information security is suggested, which utilizes three different systems such as DNA, Mersenne Twister (MT) and chaotic Dynamical Rossler system.

In [44], the authors presented the chaos and multiple s-box based image encryption algorithm to secure the digital images. The main idea was to provide the solution corresponding to the drawbacks of using a single S-box in the encryption schemes. As the images contain highly correlated data, a single s-box cannot be the right option to break the image pixels' correlation. The authors in [44] have used three different S-boxes in which the selection of S-box was performed by generating the random sequence using the chaotic map. Although the proposed scheme works well for those images containing a greater number of gray levels, it completely fails to encrypt the images containing less gray levels i.e., binary or single gray-level images. This issue was raised by Ahmed *et al.* in [20] and provided the solution by combining the confusion-diffusion mechanism with the scheme proposed in [44].

From the last few decades, several chaos-based image encryption schemes have been suggested; however, numerous of them have been proven unsecured because of lower keyspace and computational difficulties [45]. In accordance with the encryption schemes presented in the literature [29], [46]–[48], a secure encryption scheme must hold both diffusion and permutation mechanisms. But unfortunately, several existing schemes do not fulfill the above mentioned [49], [50]. In this article, the columns and rows of the plaintext image are scrambled using the chaotic logistic map that results in a finer transformation. For the diffusion purpose, the scrambled image is XORed with the noisy image generated with the chaotic sine map's help. After applying the XOR operation, a dynamical S-box mechanism is incorporated to substitute the image pixel with the S-box values. The selection of the S-box is depended on the steps specified in the proposed encryption algorithm. Because of the substitution process's additional step, the suggested scheme is secure compared to the existing algorithms. Our robust security declaration is demonstrated in the experimental outcomes and security analysis section utilizing several images like Cameraman, Baboon, Lena, and Barbara. The foundational flow of the proposed encryption system schematic is demonstrated in Figure 1. In the prior studies, [51]–[53], the image security was low owing to the lower keyspace and insecure chaotic maps. It is noticeable from the preceding studies [51]–[53], there is a strong bond between cryptography and chaos. The chaos is the study of dynamic system response and the branch of mathematics. The chaotic system demonstrates sensitivity toward certain factors and conditions. The chaotic systems show some considerable properties such as strange attractors, topology mixing, randomness, ergodicity, and reliance on their seed values [54], [55].

The properties as mentioned earlier, show importance toward the chaos-based encryption algorithms. The output of

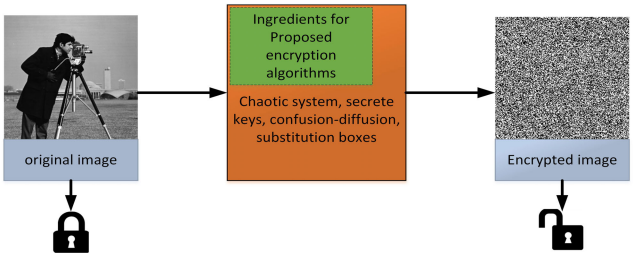


FIGURE 1. Fundamental flow schematic for the proposed encryption scheme.

the chaotic system cannot be determined without the knowledge of its seed values. Therefore, well organized cryptographic encryption algorithms can be presented using the chaos theory. The chaotic features are utilized for several cryptosystems. The most critical, sensitive property of the initial conditions explains the simplicity of awareness of the cryptosystem and contributes to creating difficulties for the hackers. The utilization of the chaos theory is not restricted to cryptography and computer science, but it has implementations in the field of mathematics, economics, biology, engineering, and physics. The chaos theory deals with the operations which illustrate a specific form of dynamic behavior in time. There is a multitude of chaotic systems characteristics that have been examined by a group of researchers. Some of the important ones are as follows [56]:

A. SELF-SIMILARITY

The system progression indicates the resemblance at different measurements in time or space. Because of these characteristics, the chaotic system is distinctive and looks like an auto-repetitive system at several measurements.

B. APERIODICITY

The chaotic dynamical system does not repeat itself with time and this is because of the aperiodic nature.

C. PERIODIC ORBITS DENSITY

The chaotic system containing dense periodic orbits suggests that periodic orbits can reach every point in the space arbitrarily nearly.

D. DYNAMIC INSTABILITY

It is frequently mentioned as the butterfly effect. It is the responsive function of the seed values. A minor change in the seed values is substantially different contrasting trajectories.

In the spatial domain encryption, one can directly manipulate the pixel values by applying some mathematical functions such as substitution and permutation [57]. In [58], it was claimed that the frequency domain pixel manipulation is comparatively faster than the spatial domain pixel manipulation. Therefore, according to [ref], for real-time applications, one can incorporate frequency domain encryption to secure the digital images in a more sophisticated manner. In the proposed work, we have used frequency domain encryption

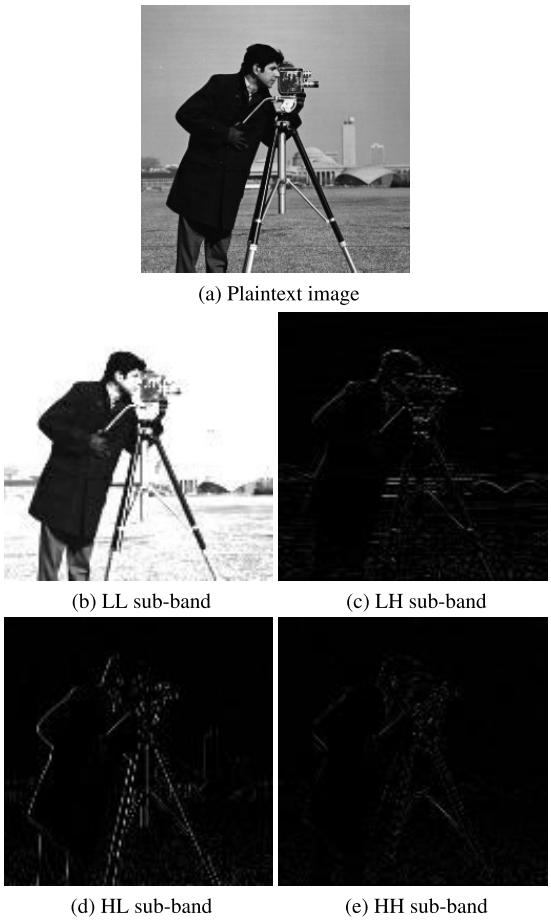


FIGURE 2. Decomposition of plaintext image using discrete wavelet transform.

to secure the digital images. To convert the pixel values of the plaintext image into the frequency domain, we have used discrete wavelet transform. It converts the plaintext image into four sub-bands (LL, LH, HL, and HH), in which the LL sub-band consists of most of the information of the plaintext image as it can be seen n Figure 2. Therefore, it is necessary to encrypt the LL sub-band with strong mathematical transformation rather we use more resources to encrypt other sub-bands (LH, HL, and HH). It will also increase the overall encryption computational time. To overcome the time complexity problem, we have only encrypted the LL sub-band. Moreover, to increase the robustness of the proposed encryption algorithm, we have also used dynamic S-boxes and chaotic maps due to their tremendous properties as we mentioned earlier.

E. PAPER CONTRIBUTION

To overcome the vulnerabilities of the single and multiple S-box encryption schemes, our contributions are following:

- To make use of the S-box effective and get rid of its deficiencies, a unique perspective has been used in this article. Rather than utilizing the S-box transformation directly on the plaintext image pixels, We first convert the plaintext image into four different frequency bands

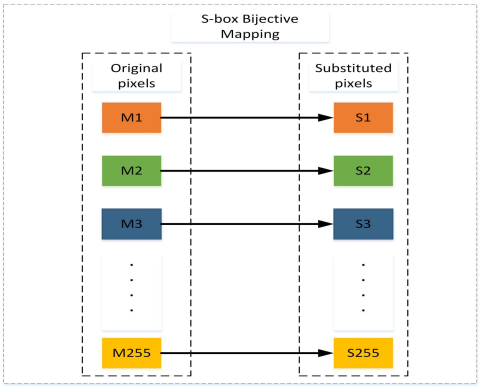


FIGURE 3. Mapping of original pixel using a substitution box.

by using Discrete Wavelet Transform. After converting the original image into its frequency components, we manipulate the rows and columns of only LL-band by incorporating a scrambling process. The reason of considering only LL-band is that most of the information of the original image present in the LL-bad. By the considering only LL-band, it will also help to keep the encryption computational time low.

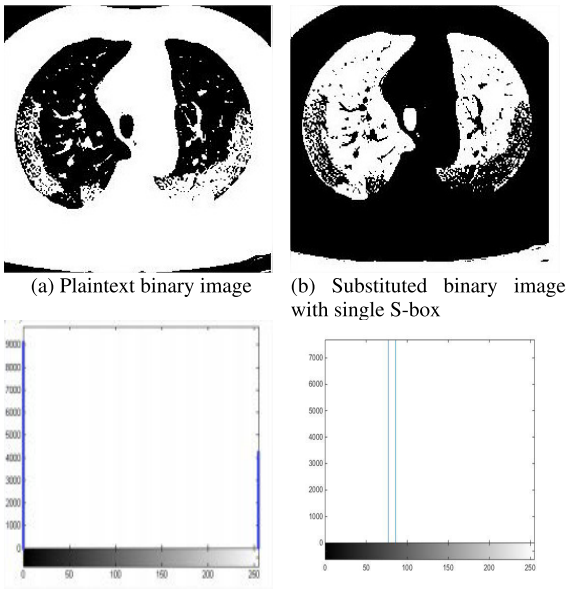
- To achieve the diffusion property, we have created a noisy image using a sine map. The noisy image is then applied to the scrambled image using the bit Xor operation.
- After achieving the confusion-diffusion property, the S-box transformation is implemented to improve the security and achieve extremely secure images that properly conceal the plaintext image.

II. PROBLEM STATEMENT

Image pixels values replace with the S-box values according to a one-to-one relationship called bijective mapping. That means every unique pixel U of the image will replace with the unique value of the S-box. Bijective mapping is shown in Figure 3. When substitution Y is applied on the plaintext image P, the S-box might be represented a bijective function g(v), hence:

$$\begin{aligned} &Y : P \rightarrow C \\ &\text{if } U_1 = U_2 \\ &\text{then } g(a_1) = g(a_2) \end{aligned} \tag{1}$$

In Figure 3, 'M' is the original pixel value and S is the substituted value. If an individual plaintext image contains a portion of the same pixels, all the pixels of that portion will be replaced with a unique value. It means that after applying the S-box on the plaintext image, the peaks in the histogram of the plaintext and substituted images will remain the same. For instance, there are two different peaks in the histogram of the binary image; one for the zero values and the other is for the greatest gray level, which is 256. As the binary images contain only two different pixel values, the histogram of the substituted version of the binary image will also show



(a) Plaintext binary image (b) Substituted binary image with single S-box

(c) Histogram of Plaintext binary image (d) Histogram of Substituted binary image

FIGURE 4. S-box substitution.

two different peaks similar to the original binary image histograms but at different positions. This impact can be seen in the binary Nike image illustrated in Figure 4. Hence, it will not be difficult for the eavesdroppers to access the plaintext information from an enciphered image.

III. PROPOSED SCHEME

This section will highlight the steps involved in the suggested encryption scheme. Two distinct iterative chaotic maps are incorporated to accomplish the properties of substitution-permutation network or diffusion and confusion. To make the enciphered image more secure, distinct S-boxes are employed to substitute the image generated after achieving the confusion diffusion properties. The S-box selection will be based on the random values generated using the sine map as defined in the proposed algorithm.

A. CHAOTIC MAPS USED IN THE PROPOSED WORK

Two different chaotic maps are used in the proposed work for confusion and diffusion purposes, which are discussed in this section.

1) CHAOTIC LOGISTIC MAP

A one-dimensional (1-D) logistic map is capable of generating random values. This 1-D system is susceptible to seed values. This logistic map is derived from the continuous form of the differential equation described as [37]:

$$\frac{dy}{dz} = \alpha * \omega(1 - \omega) \tag{2}$$

The discrete equation for the logistic map is defined as:

$$\omega(n + 1) = \alpha * \omega(n)(1 - \omega(n)) \tag{3}$$

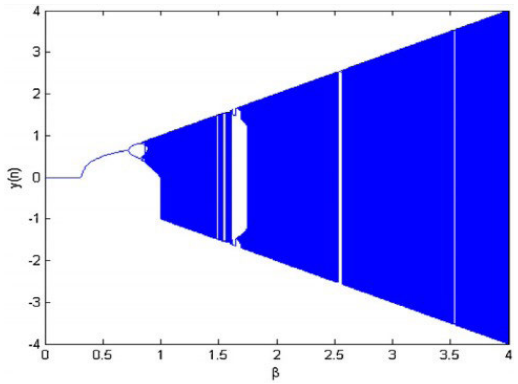


FIGURE 5. Bifurcation of chaotic sine map.

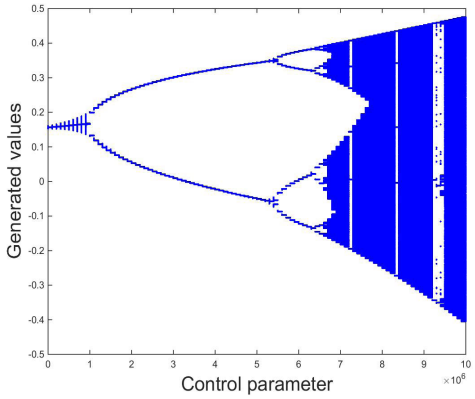


FIGURE 6. Bifurcation diagram for chaotic logistic map.

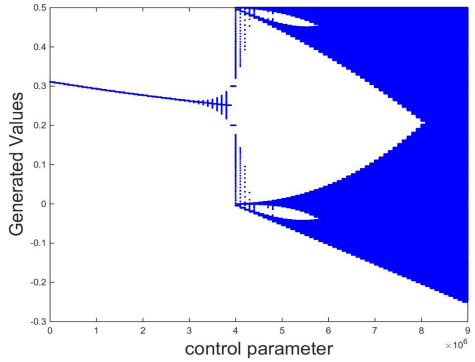


FIGURE 7. Bifurcation diagram for chaotic tent map.

The rang for the initial values are:

$$\alpha \in (0, 4)$$
$$\omega \in (0, 1)$$

2) CHAOTIC SINE MAP

A dynamical chaotic system for sine map system is described as [54]:

$$Z_{n+1} = \beta sin(\pi Z_n) \tag{4}$$

Here the control parameter β must be greater than zero ($\beta > 0$), while $Z_n \in [0\ \ 1]$ and Z_0 is the initial condition which can be choose from the range (0 1]. In [59], researchers proved by different experiments that the Sine map is chaotic. Figure 5 illustrates the bifurcation diagram of the Sine map with $\beta \in (0\ 1]$, it is reported from Figure 5 that the sine map becomes chaotic as β approaches to 1. This chaotic map has been selected due to its simplicity compared to the other chaotic systems with an affirmation of high-level security.

The reason for choosing the logistic map over other 1-D chaotic map is that the time complexity of the chaotic logistic map is less than the other 1-D maps. Moreover, if we use a 1-D chaotic map other than a chaotic logistic map such as a chaotic tent map, the algorithm can be attacked by the attacker using key space analysis. To be more precise, from Figures 6 and 7 which are the bifurcation diagram of the chaotic logistic and tent map respectively, it can be seen that the tent map enters into the chaotic region when we select the control parameter from the range [2.1 2.4]. While for the logistic map, we can select the control parameter from the range [3.4 3.99] to produce more random sequences. This shows that by selecting the chaotic logistic map over other 1-D chaotic maps, the algorithm can have a larger key space which is enough to resist the key space attacks.

IV. SUBSTITUTION BOXES USED IN THE PROPOSED SCHEME

As per the earlier discussion, the image gathered after the bit-wise XOR operation has to pass through the substitution box transformation to enhance the encrypted image's security further. Five different S-boxes are utilized, which are debated in the detailed section.

A. FADIA's S-BOX 1

In [60], a novel 16 × 16 Lorentz system-based S-box is suggested as illustrated in Table 1. To investigate the strength of this S-box, several experiments are presented in [51] and it was found that the suggested S-box plays a vital role in the accomplishment of diffusion property in image encryption. The simulation results showed that it is quite logical that the utilization of S-box enhances an encryption algorithm's efficiency.

B. FADIA's S-BOX 2

In [61], an S-box is proposed by Fadia *et al.*, as illustrated in Table 2. Because of its easy implementation and superior security, while considering several other parameters that include energy analysis, contrast, entropy and homogeneity analysis, the suggested S-Box has proven to be capable of providing better diffusion for image encryption.

C. HUSSAIN's S-BOX

A new S-box is suggested in [62] that is truly based on a projective linear group and is implemented to the Galois field of order 256. Hussain's S-box properties and security can be assessed utilizing different parameters, including the

TABLE 1. Fadia's substitution box 1.

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	294	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	133	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

TABLE 2. Fadia's substitution box 2.

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	41	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

TABLE 3. Hussain's substitution box.

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	31
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

non-linearity and criterion of bit independence. Hussain's S-box is capable of providing high security to digital images. The values of the S-box are illustrated in Table 3.

D. C-LOGO S-BOX

In [17], a logistic map based S-box is designed which has been given the name C-logo S-box. The proposed S-box utilizes the chaotic logistic map with suitable initial conditions. C-logo S-box is tested via different experiments including contrast, correlation, energy, Strict avalanche criterion, Differential approximation probability, Linear approximation probability, Bit independent criterion and non-linearity. It is also compared with the other S-boxes presented in the literature to show the superiority of C-logo S-box over the existing S-boxes. The values for the C-logo S-box are displayed in Table 4

TABLE 4. C-logo S-box.

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

TABLE 5. Chaotic S-box.

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

E. CHAOTIC S-BOX

In 2015, Anees *et al.* proposed an S-box using Van der Pol oscillator and chaotic map. The random values are generated by iterated the chaotic map 256 × 256 times. After that, the values converted into an integer number, also applied modulo function to restrict the value between [0 255]. At last, to choose the first 256 distinct values, a ceiling function is applied. The proposed S-box is tested using contrast, correlation, energy, MSE and PSNR analysis. Table 5 shows the values for the Chaotic S-box.

F. ENCRYPTION PROCEDURE

Let P is a plaintext gray-scale image of size M × N. Here, M and N indicate the number of rows and columns, respectively. Whereas M and N are equals in our scenario. The range of the pixel values in the plaintext between [0 255]. The important steps of the encryption scheme are shown in Figure 8. The encryption steps are given below:

1) Choose a plaintext image of size $M \times N$ and take a Discrete wavelet transform to convert the original image into four frequency bands (LL, LH, HL and HH). In this case, the size of all the frequency bands will be $\frac{M}{2} \times \frac{N}{2}$.
2) A couple of sets of chaotic values i.e. set-1: $\alpha = 3.79$, $\omega = 0.3$ and set-2: $\alpha = 3.59$, $\omega = 0.4$ are selected to create two random sequences having size of $\frac{M}{2}$ or $\frac{N}{2}$ i.e. $SM = (t_1, t_2, t_3 \ldots, x_{M/2})$ and $LN = (v_1, v_2, v_3 \ldots, v_{N/2})$ with the assistance of Logistic map.
3) The positions of all the rows and columns of the LL sub-band are scrambled from the first column to the last column and from the first row to the last row according to the sequence *SM* and *LN* respectively. The processed frequency band is represented as γ.
4) The Sine map is iterated $\frac{M}{2} \times \frac{N}{2}$ times and the result is saved in α as a row matrix.
5) The matrix α is converted into a 2-D array having the size of $\frac{M}{2} \times \frac{N}{2}$. The values of α matrix is then amplified with a large integer number using the multiplication operation. After that floor function and modulus 256 are applied to achieve the integer values in the matrix α. Mathematically this term can be represented as:

$$\alpha' = mod\left[(floor(10^{14} \times (\alpha_{matrix}))), 256\right]$$
$$\alpha^{'} = \text{reshape}(\alpha', 256, 256) \quad (5)$$

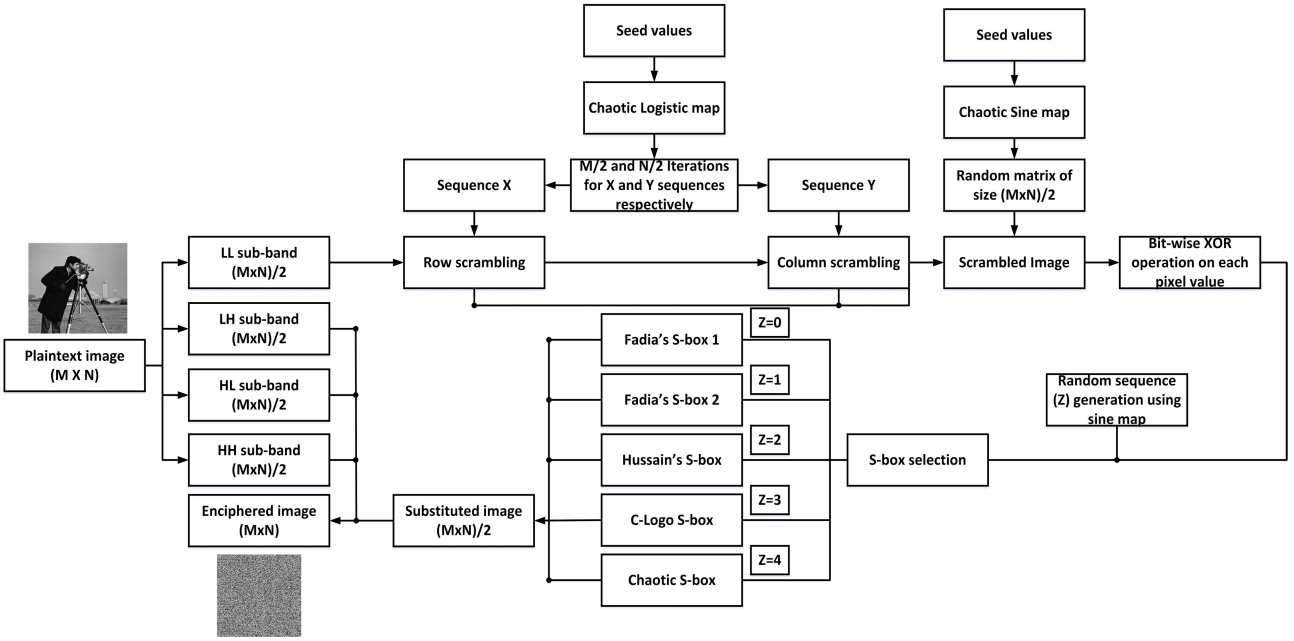


FIGURE 8. Proposed encryption methodology.

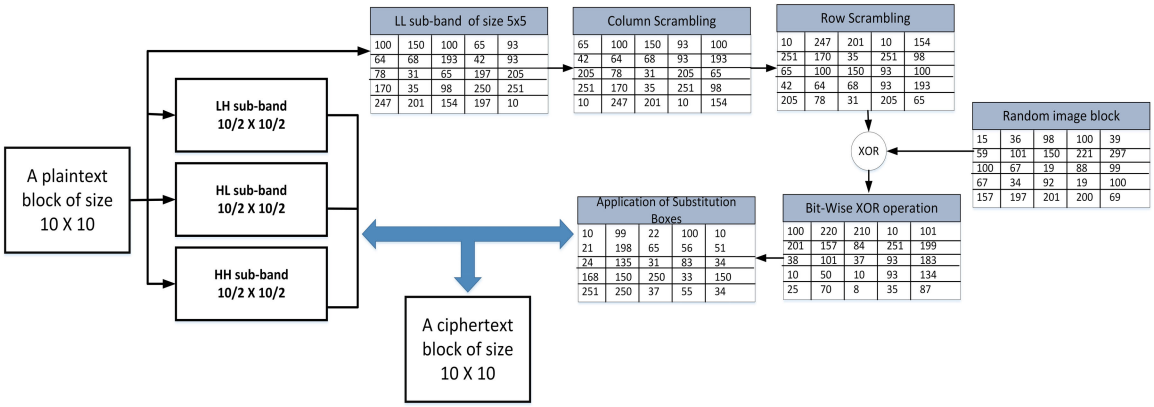


FIGURE 9. Proposed encryption methodology applied on a 10 × 10 image pixels block.

6) The scrambled γ is bit-wise XORed bit- with the matrix α' to get a new matrix ω.
7) The third sequence Z is generated using the sine map with seed values, i.e., (seed values), to select a specific S-box. The values in the sequence Z are then multiplied with an integer number greater than 100 i.e., int > 100, so it could be prepared for modulus 5 operation, then rounded and modulus 5 function is implemented to achieve a value of 0,1,2,3, or 5. Below is the mathematical explanation of the whole operation.

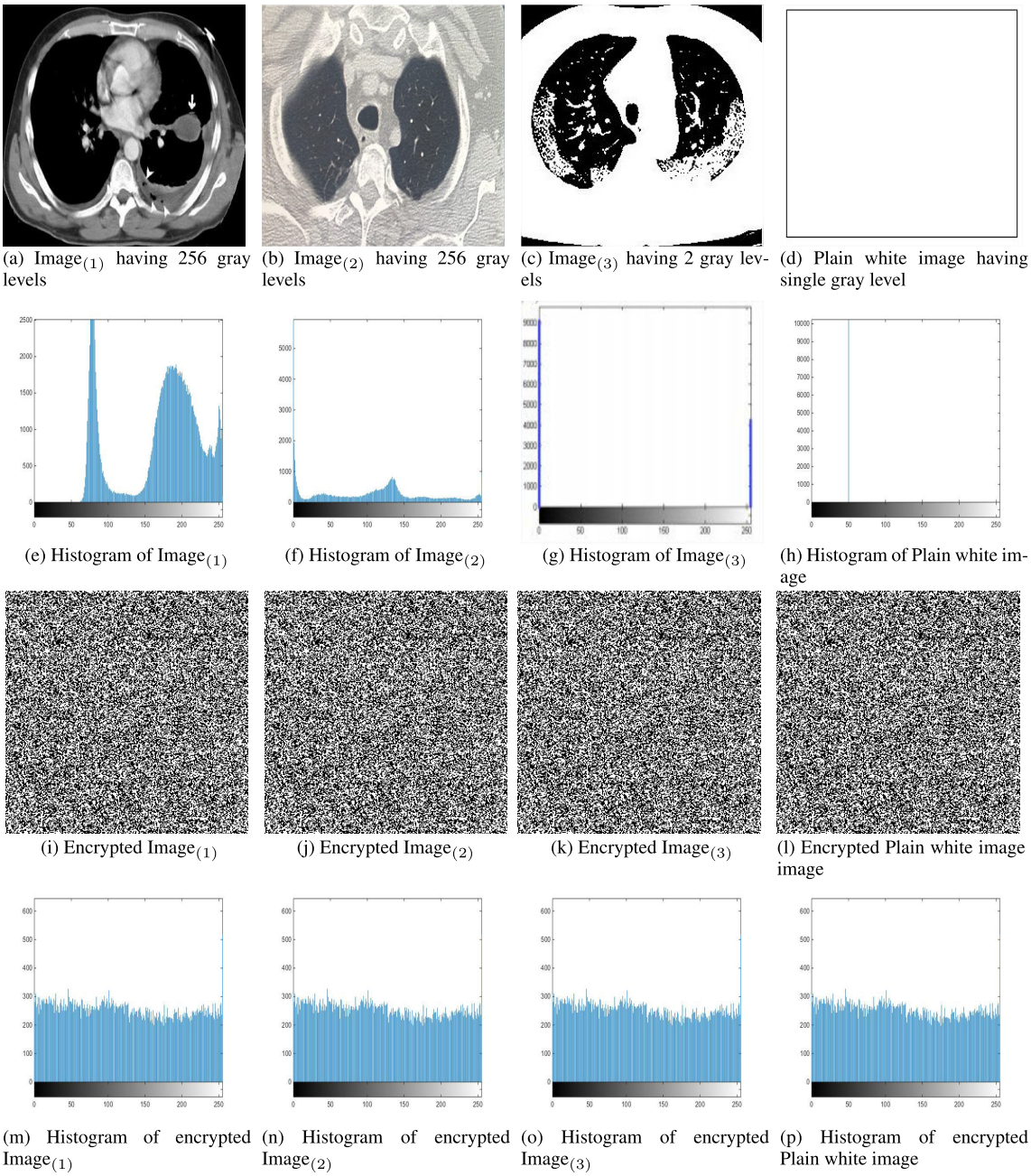
$$Z = mod\left[(floor(10^{15} \times (sequence))), 5\right] \quad (6)$$

8) C-logo S-box will be selected for Z = 0. For Z = 1, Z = 2, Z = 3 and Z = 4, Fadia's S-box 1, Fadia's S-box 2, Hussain's S-box and Gray S-box will be selected respectively for the substitution of the image pixel which is at the position (1,1). Likewise, the substitution process will continue till the last value of the LL sub-band. After processing the LL- sub-band, combine three unchanged frequency bands (LH, HL and HH) and the processed band (LL sub-band) by taking the inverse discrete wavelet transform to obtain the final encrypted image.

The suggested encryption algorithm is implemented on a 10 × 10 sample data chosen randomly from the LL sub-band for better understanding as illustrated in Figure 9. For decryption, entire encryption steps can be performed in a reverse manner.

V. EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

Several tests are proposed in [1] to analyze the performance of an image encryption scheme. For the particular algorithm,



(a) Image$_{(1)}$ having 256 gray levels
(b) Image$_{(2)}$ having 256 gray levels
(c) Image$_{(3)}$ having 2 gray levels
(d) Plain white image having single gray level
(e) Histogram of Image$_{(1)}$
(f) Histogram of Image$_{(2)}$
(g) Histogram of Image$_{(3)}$
(h) Histogram of Plain white image
(i) Encrypted Image$_{(1)}$
(j) Encrypted Image$_{(2)}$
(k) Encrypted Image$_{(3)}$
(l) Encrypted Plain white image image
(m) Histogram of encrypted Image$_{(1)}$
(n) Histogram of encrypted Image$_{(2)}$
(o) Histogram of encrypted Image$_{(3)}$
(p) Histogram of encrypted Plain white image

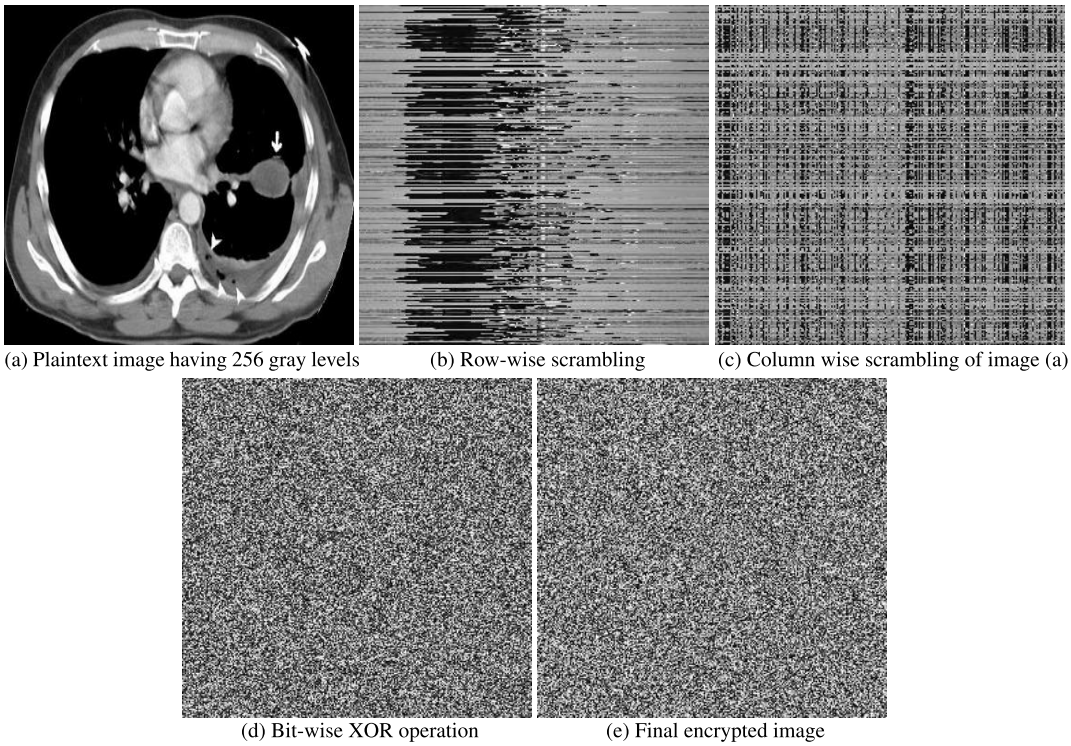
FIGURE 10. **Plain images, encrypted images and their corresponding histograms.**

all the tests are performed using MATLAB 2016a with 1GHz CPU and 4GB memory, Microsoft Windows 08 operating system. The four test images selected, as shown in Figure 10 (a, b, c, d). The image$_{(3)}$ is a binary image between all these test images and contained only two different values 0 or 1. While Figure 10(d) a plain white image containing only a single gray level. The enciphered images corresponding to the test images are illustrated in Figure 10 (i, j, k, l). The statistical results are compared with the encryption schemes are proposed in [39], [63], [64] to justify the effectiveness of the scheme suggested in this paper.

For the sake of confirmation, the processed image after every stage is illustrated for the for the plaintext image as shown in Figure 11.

A. HISTOGRAM AND CHI-SQUARE ANALYSIS

A histogram notifies about the graphical pixel values that are duplicated in an image. The histogram of an encrypted mage that is resistant to the different attacks must be consistent. The histograms of the plaintext and histogram of the corresponding ciphertext images are illustrated in Figure 10 (e, f, g, h) and Figure 10 (m, n, o, p) respectively. Moreover, from the



(a) Plaintext image having 256 gray levels (b) Row-wise scrambling (c) Column wise scrambling of image (a)

(d) Bit-wise XOR operation (e) Final encrypted image

FIGURE 11. Step-wise encrypted images generated through proposed work.

TABLE 6. Chi-square analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	216	240	255	249	255	261	336	237	243
Baboon	389	241	270	257	250	270	297	241	244
Nike	371	242	271	254	264	266	167	298	245
Lena	228	240	268	252	261	260	397	376	242
Brabra	201	243	256	253	253	261	469	401	241

Figure. 10 (b, d, f, h), It can be easily noticed that the plaintext histograms have edged peaks. At the same time, the histograms are steady for the ciphertext images. To demonstrate the consistency of the histograms of the encrypted images mathematically, the chi-square can be expressed as:

$$Z^2 = \sum_{L=1}^{255} \frac{(\text{calculated value - expected value})^2}{\text{expected value}} \tag{7}$$

In this mathematical explanation, L is the gray-level. Lower values of Z^2 defines that pixel distribution is consistent. The chi-square values for the encrypted images are displayed in Table 6 and the comparison of these values with the suggested schemes in [39], [63], [64] is also given. It is proved from Table 6 that encrypted image is achieved through the suggested algorithms have consistent pixel distribution and succeeded in securing the data from the unusual hackers.

B. INFORMATION ENTROPY

Entropy plays a vital role in the quantification of uncertainty and casualness of the information [70]. The entropy shows the degree of unpredictability in a communication system. Claude Shannon presented the idea of information entropy back in 1949 [71]. Below is the mathematical explanation of entropy.

$$Ent(p) = \sum_{a=0}^{2^n-1} m(p_a) log_2 \frac{1}{m(p_a)} \tag{8}$$

In equation 8, p_a is the occurrence probability of the message symbol m. Any random source which generates 2^a message symbols, the maximum entropy cannot be exceeded by a. Whereas, if the encryption process is performed with a source releases 2^8 symbols, the maximum absolute entropy value will be 8. The entropy H(m) values for different plaintext and ciphertext images and their comparison [39], [63], [64] is shown in Table 7. It can be easily observed from table 7 that entropy values of the ciphertext images generated through the proposed encryption scheme are near to 8 as compared to the encryption schemes presented in [39], [63], [64]. Therefore, the suggested scheme is considered secure against entropy attacks.

C. CORRELATION ANALYSIS OF PLAINTEXT IMAGE AND CIPHERTEXT IMAGE

Correlation defines that how much two pixel values are close to each other. More the close relationship between the pixels means there is meaningful information in the image[62]. So, for the secure encryption process, correlation values for the ciphertext images should be minimum. The range of the

TABLE 7. Information entropy analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	7.9865	7.9991	7.9990	7.9975	7.9981	7.9980	7.9913	7.8963	7.9980
Baboon	7.9763	7.9993	7.9995	7.99963	7.9966	7.9961	7.9463	7.8963	7.9979
Nike	7.9913	7.9990	7.9993	7.9943	7.9955	7.9986	7.9536	7.8736	7.9961
Lena	7.9831	7.9992	7.9994	7.9978	7.9970	7.9966	7.9635	7.8836	7.9971
Brabra	7.9896	7.9995	7.9991	7.9952	7.9941	7.9952	7.9563	7.8630	7.9963

TABLE 8. Correlation analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	0.0037	0.0005	0.0008	0.0001	0.0005	0.0002	0.0016	0.0009	0.0002
Baboon	0.0029	0.0001	-0.0031	-0.0026	0.0001	0.0002	0.0017	0.0003	-0.0027
Nike	0.0013	-0.0001	-0.0025	0.0001	-0.0035	-0.0030	0.0031	-0.0014	-0.0021
Lena	0.0017	-0.0015	-0.0033	-0.0013	0.0002	0.0001	0.0025	0.0003	-0.0018
Brabra	0.0011	-0.0098	-0.0063	0.0001	0.0005	-0.0083	0.0020	0.0009	-0.0099

correlation values is $[-1\ +1]$. The correlation between two adjacent pixels can be calculated by equation 9.

$$C_r = \frac{L\sum_{i=1}^{L}(x_i \times y_i) - \sum_{i=1}^{L} x_i \times \sum_{i=1}^{L} y_i}{\sqrt{(L\sum_{i=1}^{L} x_i^2 - (\sum_{i=1}^{L})^2) \times (L\sum_{i=1}^{L} y_i^2 - (\sum_{i=1}^{L} y_i)^2)}} \tag{9}$$

where x and y are the two adjacent pixel values in the image and L is the total number of pixels selected from the image for calculation. The comparison of correlation values for the ciphertext image generated through the encryption scheme proposed in this paper is given in Table 8 which shows that the correlation values for the proposed scheme are significantly lower than the existing schemes that are evidence that the proposed scheme can be performed better than the existing ones in term of correlation.

D. CONTRAST INVESTIGATION

The contrast investigation is a method of calculation of the local variance that exists in the images. Contrast is a property by which anyone can differentiate between the pixels. Higher contrast values indicate that the image has significantly higher gray levels. For robust encryption algorithms, contrast values for the cipher images should be as high as possible. Mathematically it can be calculated as:

$$Con = \sum_{x,y} |x - y|^2 \times p(x, y) \tag{10}$$

where p(x, y) specifies the number of gray-level co-occurrence matrices (GLCM). The comparison of the contrast values for the original and processed image with the existing schemes [39], [63], [64] are given in Table 9. From Table 9, it can be seen that the proposed encryption algorithm can perform better than the existing ones in terms of contract analysis.

E. ENERGY

The energy of the image shows how much meaningful content is present. Higher energy values mean more information present in the image. So, an encrypted image must have lower

TABLE 9. Contrast analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	9.9965	9.9978	9.9861	9.8963	9.4963	9.9936	9.9671	10.0312	10.7843
Baboon	9.9863	9.9987	9.9876	9.97956	9.9896	9.9965	9.9632	10.0341	10.4131
Nike	9.8632	9.9784	9.3671	9.9715	9.941	9.684	10.0031	99.9931	10.7721
Lena	9.9638	9.6781	9.9876	9.9781	9.9631	9.6974	9.9936	9.9364	10.8298
Brabra	9.9341	9.9781	9.9647	9.9984	9.9931	9.7798	10.1031	9.9784	10.9994

TABLE 10. Energy analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	0.0157	0.0159	0.0158	0.0159	0.0161	0.0160	0.0159	0.0159	0.0154
Baboon	0.0163	0.0160	0.0158	0.0162	0.0162	0.0163	0.0162	0.0158	0.0155
Nike	0.0157	0.0158	0.0158	0.0161	0.0160	0.0164	0.0162	0.0162	0.0155
Lena	0.0157	0.0157	0.0159	0.0160	0.0161	0.0163	0.0168	0.0168	0.0154
Brabra	0.0164	0.0161	0.0160	0.0159	0.0161	0.0162	0.0167	0.0160	0.0153

energy values. Mathematically, the energy of the image can be calculated as:

$$En = \sum_{a,b} p(a, b) \tag{11}$$

where p(a, b) represents the gray-level co-occurrence matrices in GLCM, energy values of the plaintext images and their corresponding ciphertext images are listed in Table 8. Moreover, the comparison of the energy values with the proposed encryption scheme is also given in Table 10 in which it can be analyzed that the energy values of the proposed encryption scheme are significantly lower than the plaintext images and algorithms presented in [39], [63], [64].

F. MEAN SQUARE ERROR (MSE) AND PEAK SIGNAL TO NOISE RATIO (PSNR)

MSE is an error between two images. In the case of encryption schemes, researchers frequently quantify the MSE between the plaintext and ciphertext images. The pixel change occurs, meaning a huge difference between the two plaintext and ciphertext images. It means higher values for the MSE is required for effective encryption schemes. In contrast, there is another term called PSNR, which is the inverse of the MSE. Higher values of MSE will result in lower values of PSNR. So, PSNR values should be minimum for the robust encryption schemes. The result of MSE and PSNR for the proposed encryption scheme and the schemes proposed in [39], [63], [64] are reported in Table 11 and 12 Mathematically both the matrices can be calculated as:

$$MSE = \frac{1}{MN} \sum_{a=0}^{M-1} \sum_{b=0}^{M-1} (P(a, b) - C(a, b))^2 \tag{12}$$

$$PSNR = 10 \times log_2 \frac{H_{max}^2}{MSE} \tag{13}$$

G. COMPUTATIONAL TIME ANALYSIS

An encryption scheme is considered efficient when it utilizes fewer resources and consumes minimum time for the computation. To analyze the computational complexity, the computational time of the suggested algorithm is defined and

TABLE 11. MSE analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	35.31	35.91	36.86	35.13	33.18	39.98	31.67	36.64	41.68
Baboon	37.94	33.93	35.68	39.90	34.54	39.78	34.31	39.67	42.97
Nike	36.97	40.54	40.16	39.48	39.66	39.61	32.61	40.10	41.99
Lena	34.38	39.87	39.18	38.99	39.97	38.99	33.37	40.36	42.99
Brabra	37.59	40.38	39.94	41.033	42.08	40.16	34.34	39.32	43.82

TABLE 12. PSNR analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	20.3581	20.9781	18.9831	19.3641	19.6798	21.9987	25.6713	19.378	13.5351
Baboon	21.0146	21.3987	19.0166	20.1982	20.4930	20.1887	26.3014	18.3751	15.2493
Nike	20.8913	23.4680	20.6798	21.6782	20.1889	21.3368	22.3871	20.3781	16.6789
Lena	22.8712	21.0387	21.978	20.7965	21.3687	20.7341	28.3746	20.3781	12.2972
Brabra	21.6715	21.3363	20.6985	22.9981	20.3369	21.7319	22.1472	19.3741	16.7916

TABLE 13. Computational time analysis (sec).

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	2.6813	0.1698	0.1381	0.1649	0.1644	0.1973	0.0690	2.1793	0.0068
Baboon	2.3610	0.6812	0.3871	0.9671	0.3112	0.0971	0.0668	2.1352	0.0048
Nike	3.6710	0.3187	0.0371	0.3741	0.3478	0.1972	0.0541	3.9733	0.0051
Lena	2.3792	0.8912	0.0987	0.3178	0.1349	0.0963	0.0896	2.3970	0.0053
Brabra	2.7913	0.4613	0.3175	0.1360	0.1336	0.1339	0.0799	3.9934	0.0061

compared with [39], [63], [64] in Table 13, which shows the time utilized by the suggested scheme to encrypt the plaintext image. It can be clearly seen in Table 13 that the computational time for the suggested scheme is significantly less in comparison with [39], [64]. However, the computational time for [63] is relatively less than the suggested algorithm. The reason being it encrypts only one-fourth area of the plaintext image.

H. STRUCTURAL CONTENT (SC)

This is a parameter to check the similarity between the original and the cipher image. Below is the mathematical explanation for SC.

$$SC = \frac{\sum_{a=1}^{M}\sum_{b=1}^{N}\left(Pl_{a,b}\right)^2}{\sum_{a=1}^{M}\sum_{b=1}^{N}(En)_{a,b}^2} \tag{14}$$

where Pl(a,b) and C(a,b) is the plaintext and ciphertext images respectively. The SC values lie in the range [0 1]. For the efficient encryption scheme, SC should be near to zero. While the SC value near to 1 shows that the two images are similar and the encryption scheme is inefficient. Table 14 provides the comparison between the SC values for proposed and the encryption schemes suggested in [39], [63], [64]. From Table 14, it can be seen that the proposed encryption scheme can generate a significantly different cipher image in comparison to the other existing scheme, which is evidence that the proposed scheme is efficient than the existing schemes in terms of SC analysis.

I. KEYSPACE ANALYSIS

To resist the brute force attack, an encryption scheme must have a large enough keyspace. In the proposed algorithm, there are eight different keys are used in which each key retain the sensitivity of 10^{-15}. This means that the total key space will be 10^{-15*6} which is approximately equal to 2^{256} which is enough to resist the brute force attack. According to Li and Alvarez's criteria [72], the minimum possibilities for the secrete key is 2^{100}. So, according to this, the proposed algorithm fulfills the key space criteria.

TABLE 14. Structural content analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	0.0498	0.0089	0.0098	0.0079	0.0080	0.0089	0.0189	0.0963	0.0061
Baboon	0.0387	0.0094	0.0090	0.0091	0.0089	0.0088	0.0168	0.0793	0.0075
Nike	0.0681	0.0078	0.0073	0.0077	0.0070	0.0080	0.018	0.0371	0.0052
Lena	0.0361	0.0091	0.0081	0.0075	0.0079	0.0074	0.0987	0.0930	0.0061
Brabra	0.0671	0.0099	0.0096	0.0097	0.0098	0.00097	0.0337	0.0861	0.0082

TABLE 15. Percentage difference between plaintext and ciphertext images when decrypted with tiny modified keys.

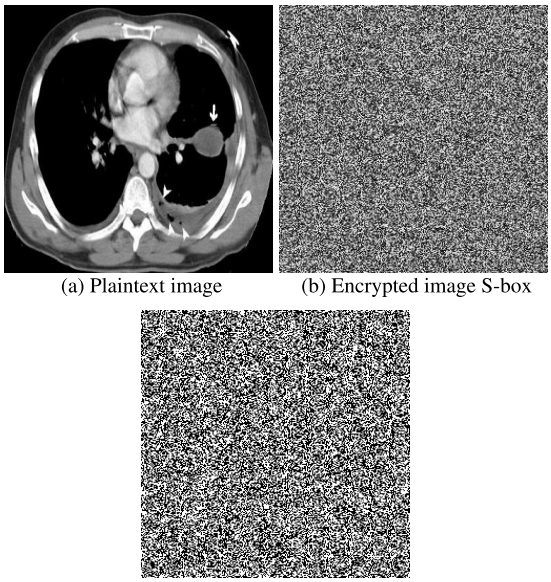
Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	80.65	98.79	97.68	98.78	98.98	99.15	85.31	88.75	99.71
Baboon	78.68	96.56	98.49	97.98	98.98	98.99	86.35	87.64	99.95
Nike	80.93	98.77	97.49	97.63	98.79	99.76	87.10	87.65	99.87
Lena	79.12	98.86	99.46	99.66	98.99	99.81	85.97	86.74	99.86
Brabra	81.96	97.67	98.76	97.99	99.16	99.79	89.83	86.99	99.73

J. KEY SENSITIVITY

To present a secure encryption algorithm, it is important that the keys which are used to secure the digital data must be sensitive. Sensitivity to the secrete keys means that a tiny change in the original keys may change the ciphertext image completely. Another way to explain the sensitivity of the keys is that when anyone makes a tiny change in the key, it would not be able to decrypt the original image from the ciphertext image. In the proposed encryption algorithm, we have encrypt the plaintext image using the original keys which are: $\alpha_0 = 0.31000000000000$, $\omega_0 = 3.470000000000000$, $\alpha_1 = 0.45000000000000$, $\omega_1 = 3.620000000000000$, $\beta_0 = 0.960000000000000$, $\beta_1 = 0.8600000000000000$. For the decryption of the plaintext image from the ciphertext image, we have made a tiny change in each original key i.e $\alpha_0' = 0.31000000000001$, $\omega_0' = 3.470000000000001$, $\alpha_1' = 0.45000000000001$, $\omega_1' = 3.620000000000001$, $\beta_0' = 0.960000000000001$, $\beta_1' = 0.860000 - 0000000001$. After decrypting the plaintext image using the modified keys, the decrypted image is completely different from the plaintext image as it can be seen in Figure 12 in which Figure 12(a) is an original image, Figure 12(b) is an encrypted image with correct or original keys while Figure 12(c) is a decrypted image with incorrect keys. For the statistical analysis of the sensitivity of secrete keys, a percentage difference values between the plaintext and ciphertext images are shown in Table 15. It can be analyzed from Table 15 when we decrypt a plaintext image with tiny modified keys, there is more than 99% change occurs between the plaintext and ciphertext images. While the percentage difference for the schemes proposed in [39], [63], [64] is much less than the proposed encryption scheme.

K. CROPPING AND DATA LOSS ANALYSIS

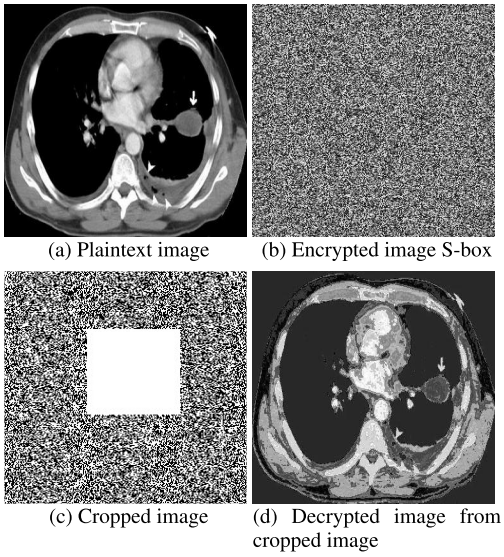
To any encryption scheme, it is necessary to resist the noise attack. The eavesdroppers frequently attempt cropping



(a) Plaintext image (b) Encrypted image S-box

(c) decyrpted image with slight change of 10^{-15}in the original keys

FIGURE 12. Key sensitivity analysis.



(a) Plaintext image (b) Encrypted image S-box

(c) Cropped image (d) Decrypted image from cropped image

FIGURE 13. Cropping analysis.

attacks to destroy the encrypted information in the image. Therefore, the encryption should also be noise resistant, so that, in case the attacker wants to crop the encrypted image to destroy the information, the decryption still be able to decrypt the plain image. It is obvious that after cropping the ciphertext image, all the pixels of the plaintext image will not be recovered properly, but the content of the image must be perceptually identical to the plaintext image.

To perform the cropping and data loss analysis, we have cropped the ciphertext image and then tried to decrypt the plaintext image from the cropped image. It is analyzed that after decryption of the plaintext image from the cropped ciphertext image, the content is visible as it can be seen in Figure 13. Moreover, we have calculated the

TABLE 16. Data loss analysis (percentage of data loss).

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	15.68	13.26	14.52	13.78	16.64	17.98	11.365	12.37	9.38
Baboon	14.24	12.98	14.68	12.99	15.68	17.68	19.67	15.67	9.71
Nike	14.68	12.54	14.99	12.78	14.98	16.98	19.72	14.37	8.46
Lena	14.99	13.10	15.11	11.99	15.64	15.67	18.37	11.37	9.12
Brabra	15.01	12.86	14.23	12.46	14.69	18.93	20.37	12.31	9.81

TABLE 17. NPCR analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	98.99	99.68	98.99	99.76	99.88	98.95	99.67	99.45	99.67
Baboon	98.24	99.89	99.46	99.31	98.97	98.89	98.99	98.69	99.34
Nike	98.64	98.99	99.01	98.98	98.98	99.67	99.64	99.14	99.98
Lena	99.35	98.98	99.67	99.67	99.36	98.99	99.34	99.30	99.37
Brabra	99.30	99.98	99.68	99.42	98.86	98.98	99.47	98.89	99.79

TABLE 18. UACI analysis.

Plaintext images	ref [39]	ref [65]	ref [66]	ref [67]	ref [68]	ref [69]	ref [63]	ref [64]	Proposed
Cameraman	30.69	31.68	33.14	32.99	32.01	33.68	33.41	31.56	33.98
Baboon	31.36	32.68	33.99	32.65	31.54	33.14	30.68	31.98	33.83
Nike	31.68	31.37	32.22	31.98	31.87	33.81	30.13	31.78	33.37
Lena	31.10	31.01	31.65	32.39	32.99	32.57	30.35	32.43	33.97
Brabra	31.98	31.97	32.19	33.89	33.48	31.98	30.19	31.98	33.49

percentage of data loss after decrypting the plaintext image from the cropped image. To compare data loss analysis for the proposed encryption algorithm with the existing schemes, we have cropped those ciphertext images that are generated through the existing encryption algorithms and decrypted them using the corresponding decryption algorithm. The data loss percentage values are displayed in Table 16. From Table 16, it can be seen that the proposed algorithm can perform better than the existing schemes in terms of data loss analysis.

L. RESISTANCE AGAINST DIFFERENTIAL ATTACKS

A change of a single pixel in the plaintext image in any secure image encryption algorithm should significantly change the corresponding ciphertext image. For the investigation of this test, (i) Number of Pixel Change Rate (NPCR) and (ii) Unified Average Change Intensity (UACI) are most frequently used by the security experts [64,65]. NPCR and UACI can be calculated using equation 15 and 16 respectively.

$$NPCR = \frac{\sum_{a,b} D(a,b)}{MN} \times 100\% \tag{15}$$

$$UACI = \frac{1}{MN}\left[\sum_{a,b} \frac{|En_1(a,b) - En_2(a,b)|}{255}\right] \times 100\% \tag{16}$$

where:

$$D(a,b) = \begin{cases} 1, & \text{if } En_1 = En_2 \\ 0, & \text{otherwise} \end{cases}$$

where En_1 and En_2 are ciphertext images generated through the proposed encryption scheme corresponding to the original and one pixel change image respectively. The statistical

values of NCPR and UACI are illustrated in Tables 17 and 18. It is noticeable from Tables 17 and 18 that the suggested encryption scheme is better than existing schemes [39], [63], [64] in term of UACI and NPCR analysis.

VI. CONCLUSION

In this article, a new image encryption scheme utilizes chaos theory, confusion-diffusion property, and dynamic substitution. The confusion property is accomplished by utilizing a chaotic logistic map, whereas for the diffusion purpose, a chaotic sine map is incorporated. In the final stage of the encryption, the pixel values are altered utilizing S-box. However, the S-box is chosen randomly according to the sequence generated through the chaotic sine map. For evaluating the proposed encryption, several security tests are performed and compared to the existing schemes, which reveals that the suggested scheme performs better than the other encryption algorithms. The proposed scheme also takes less time to encrypt the plaintext image, which means it can be used for real-time encryption.

REFERENCES

[1] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Computing*, vol. 23, p. 25, Jun. 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] A. Anees and Z. Ahmed, "A technique for designing substitution box based on van der pol oscillator," *Wireless Pers. Commun.*, vol. 82, no. 3, pp. 1497–1503, Jun. 2015.
[4] 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.
[5] 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.
[6] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of cryptographic S-Boxes based on mobius transformation and chaotic tent-sine system," *IEEE Access*, vol. 7, pp. 173273–173285, 2019.
[7] A. Firdous, A. ur Rehman, and M. M. S. Missen, "A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24809–24835, Sep. 2019.
[8] A. Anees, "An image encryption scheme based on lorenz system for low profile applications," *3D Res.*, vol. 6, no. 3, pp. 1–10, Sep. 2015.
[9] S. Anwar and S. Meghana, "A pixel permutation based image encryption technique using chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 19, pp. 27569–27590, Oct. 2019.
[10] Q. Cai, "A secure image encryption algorithm based on composite chaos theory," *Traitement Signal*, vol. 36, no. 1, pp. 31–36, Apr. 2019.
[11] W. Major, W. J. Buchanan, and J. Ahmad, "An authentication protocol based on chaos and zero knowledge proof," *Nonlinear Dyn.*, vol. 3, pp. 1–23, Jan. 2020.
[12] A. Anees and A. M. Siddiqui, "A technique for digital watermarking in combined spatial and transform domains using chaotic maps," in *Proc. 2nd Nat. Conf. Inf. Assurance (NCIA)*, Dec. 2013, pp. 119–124.
[13] A. OluwakemiC., A. Kayode S., and O. Ayotunde J., "Efficient data hiding system using cryptography and steganography," *Int. J. Appl. Inf. Syst.*, vol. 4, no. 11, pp. 6–11, Dec. 2012.
[14] R. Sivaraman, S. Rajagopalan, J. B. B. Rayappan, and R. Amirtharajan, "Ring oscillator as confusion–diffusion agent: A complete TRNG drove image security," *IET Image Process.*, vol. 14, no. 13, pp. 2987–2997, May 2020.
[15] N. Chidambaram, P. Raj, K. Thenmozhi, and R. Amirtharajan, "Advanced framework for highly secure and cloud-based storage of colour images," *IET Image Process.*, vol. 14, no. 13, pp. 3143–3153, Nov. 2020.
[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] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *Eur. Phys. J. Plus*, vol. 135, no. 2, pp. 1–13, Feb. 2020.
[18] I. Hussain, A. Anees, T. Al-Maadeed, and M. Mustafa, "Construction of S-box based on chaotic map and algebraic structures," *Symmetry*, vol. 11, no. 3, p. 351, Mar. 2019.
[19] A. Shafique and J. Shahid, "Novel image encryption cryptosystem based on binary bit planes extraction and multiple chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 8, p. 331, Aug. 2018.
[20] 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.
[21] M. Andrecut, "Logistic map as a random number generator," *Int. J. Mod. Phys. B*, vol. 12, no. 9, pp. 921–930, Apr. 1998.
[22] A. Shafique and J. Ahmed, "Dynamic substitution based encryption algorithm for highly correlated data," *Multidimensional Syst. Signal Process.*, vol. 32, no. 1, pp. 91–114, Jan. 2021.
[23] F. Ahmed and A. Anees, "Hash-based authentication of digital images in noisy channels," in *Robust Image Authentication in the Presence of Noise*. Cham, Switzerland: Springer, 2015, pp. 1–42.
[24] I. Hussain, A. Anees, and A. Algarni, "A novel algorithm for thermal image encryption," *J. Integrative Neurosci.*, vol. 17, nos. 3–4, pp. 447–461, Sep. 2018.
[25] 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.
[26] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Secur. Commun. Netw.*, vol. 2018, pp. 1–20, Jun. 2018.
[27] I. Hussain, A. Anees, T. Alassiry Al-Maadeed, and M. T. Mustafa, "A novel encryption algorithm using multiple semifield S-boxes based on permutation of symmetric group," 2020, *arXiv:2004.12264*. [Online]. Available: http://arxiv.org/abs/2004.12264
[28] 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, 2020.
[29] I. Hussain, A. Anees, M. Aslam, R. Ahmed, and N. Siddiqui, "A noise resistant symmetric key cryptosystem based on S8 S-boxes and chaotic maps," *Eur. Phys. J. Plus*, vol. 133, no. 4, p. 167, Apr. 2018.
[30] A. Anees and Y.-P.-P. Chen, "Designing secure substitution boxes based on permutation of symmetric group," *Neural Comput. Appl.*, vol. 32, no. 11, pp. 7045–7056, Jun. 2020.
[31] 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.
[32] I. Hussain, F. Ahmed, U. M. Khokhar, and A. Anees, "Applied cryptography and noise resistant data security," *Secur. Commun. Netw.*, vol. 2018, pp. 1–2, Dec. 2018.
[33] 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.
[34] I. Hussain *et al.*, "Image encryption based on Chebyshev chaotic map and S8 S-boxes," *Optica Applicata*, vol. 49, no. 2, 2019.
[35] A. Shafique, J. Ahmed, W. Boulila, H. Ghandorh, J. Ahmad, and M. U. Rehman, "Detecting the security level of various cryptosystems using machine learning models," *IEEE Access*, vol. 9, pp. 9383–9393, 2021.
[36] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, Jan. 1989.
[37] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools Appl.*, vol. 78, no. 15, pp. 22023–22043, Aug. 2019.
[38] L. Gong, K. Qiu, C. Deng, and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Opt. Laser Technol.*, vol. 115, pp. 257–267, Jul. 2019.
[39] 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.
[40] 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.
[41] N. Iqbal, M. Hanif, S. Abbas, M. A. Khan, S. H. Almotiri, and M. A. Al Ghamdi, "DNA strands level scrambling based color image encryption scheme," *IEEE Access*, vol. 8, pp. 178167–178182, 2020.

[42] 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.
[43] D. Ravichandran, V. Balasubramanian, S. Fathima, A. Banu, Anushiadevi, and R. Amirtharajan, "Chaos and IWT blended image encryption for grey scale image security," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Mar. 2019, pp. 1–5.
[44] 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.
[45] 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.
[46] A. Shafique and F. Ahmed, "Image encryption using dynamic S-box substitution in the wavelet domain," *Wireless Pers. Commun.*, vol. 115, no. 3, pp. 2243–2268, Dec. 2020.
[47] A. Anees, A. M. Siddiqui, J. Ahmed, and I. Hussain, "A technique for digital steganography using chaotic maps," *Nonlinear Dyn.*, vol. 75, no. 4, pp. 807–816, Mar. 2014.
[48] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," *Wireless Pers. Commun.*, vol. 77, no. 4, pp. 2771–2791, Aug. 2014.
[49] 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. 1, pp. 953–967, Dec. 2017.
[50] 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.*, pp. 1–21, 2019.
[51] I. Hussain, A. Anees, A. H. AlKhaldi, A. Algarni, and M. Aslam, "Construction of chaotic quantum magnets and matrix lorenz systems S-boxes and their applications," *Chin. J. Phys.*, vol. 56, no. 4, pp. 1609–1621, Aug. 2018.
[52] C. Zou, Q. Zhang, X. Wei, and C. Liu, "Image encryption based on improved lorenz system," *IEEE Access*, vol. 8, pp. 75728–75740, 2020.
[53] A. Anees and I. Hussain, "A novel method to identify initial values of chaotic maps in cybersecurity," *Symmetry*, vol. 11, no. 2, p. 140, Jan. 2019.
[54] 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.
[55] Y. Luo, S. Tang, J. Liu, L. Cao, and S. Qiu, "Image encryption scheme by combining the hyper-chaotic system with quantum coding," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105836.
[56] E. Tanyildizi and F. Ozkaynak, "A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps," *IEEE Access*, vol. 7, pp. 117829–117838, 2019.
[57] Kam and Davida, "Structured design of substitution-permutation encryption networks," *IEEE Trans. Comput.*, vol. C-28, no. 10, pp. 747–753, Oct. 1979.
[58] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," *IET Image Process.*, vol. 13, no. 9, pp. 1535–1539, Jul. 2019.
[59] A. Belazi and A. A. A. El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, Feb. 2017.
[60] 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. Simul. (ICCSS)*, Jul. 2017, pp. 32–36.
[61] 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)*, 2017, pp. 7–12.
[62] 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.
[63] J. Ahmad, A. Tahir, J. S. Khan, and M. A. Khan, "A partial ligt-weight image encryption scheme," in *Proc. UK/China Emerg. Technol. (UCET)*, 2019, pp. 1–3.
[64] 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.*, pp. 1–19, 2019.
[65] 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.
[66] 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.
[67] M. K. Balajee and J. Gnanasekar, "Evaluation of key dependent S-box based data security algorithm using Hamming distance and balanced output," *Tem J.*, vol. 5, no. 1, p. 67, 2016.
[68] S. Katiyar and N. Jeyanthi, "Pure dynamic S-box construction," *Int. J. Comput.*, vol. 1, p. 15, Feb. 2016.
[69] T. Ao, J. Rao, K. Dai, and X. Zou, "Construction of high quality key-dependent S-boxes," *Nonlinearity*, vol. 13, no. 14, p. 15, 2017.
[70] 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.
[71] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[72] 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.

MUJEEB UR REHMAN received the B.E. and M.S. (Hons.) degrees in electrical engineering from Riphah International University (RIU), Islamabad, Pakistan, in 2014 and 2018, respectively, where he is currently pursuing the Ph.D. degree with the Faculty of Engineering and Applied Sciences. He is also a certified Professional Engineer (Pakistan Engineering Council) and serving as a Lecturer with the Faculty of Engineering and Applied Sciences, RIU. His research interests include cryptography, secure communication, and machine learning.

ARSLAN SHAFIQUE received the B.E. degree in mechatronics engineering from Wah Engineering College, Wah Cantt, in 2014, and the M.S. degree in electrical engineering from Heavy Industries Taxila Education City (HITEC) University, Taxila, in 2017. He is currently pursuing the Ph.D. degree with the Faculty of Engineering and Applied Sciences, Riphah International University, Islamabad, Pakistan. He is also serving as a Research Associate with the Faculty of Engineering and Applied Sciences, Riphah International University. He has five journal publications with a cumulative impact factor of 14.54. His research interests include cryptography, secure communication, and machine learning.

SOHAIL KHALID (Member, IEEE) received the B.Eng. degree (Hons.) from CIIT Islamabad, in 2008, the M.Sc. degree in wireless networks from the Queen Mary University of London, in 2009, and the Ph.D. degree from Universiti Teknologi PETRONAS, Malaysia, in 2014. He is currently serving as an Associate Professor and the Head of the Department of Electrical Engineering, Riphah International University, Islamabad, Pakistan, where he is teaching various ungraduated and postgraduate engineering courses. His research interests include synthesis and design of passive microwave devices, and millimeter wave applications for biomedical engineering and biomedical signal processing.

IQTADAR HUSSAIN received the Ph.D. degree in mathematics with a focus on algebraic cryptography, in 2014. He is currently an Assistant Professor with Qatar University. His H-index score is 23 and i-10 index score is 34. His articles have 1320 Google scholar citations. His current research interests include the applications of mathematical concepts in the field of secure communication and cybersecurity, where he has published 63 articles in well-known journals.