Computer Systems
Science and Engineering

Tech Science Press

DOI: 10.32604/csse.2023.038439
Article

Securing Healthcare Data in IoMT Network Using Enhanced Chaos Based Substitution and Diffusion

Musheer Ahmad[1], Reem Ibrahim Alkanhel[2,*], Naglaa F. Soliman[2], Abeer D. Algarni[2], Fathi E. Abd El-Samie[3] and Walid El-Shafai[3,4]

[1]Department of Computer Engineering, Jamia Millia Islamia, New Delhi, 110025, India
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P.O. Box 84428, Riyadh, 11671, Saudi Arabia
[3]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf, 32952, Egypt
[4]Security Engineering Laboratory, Department of Computer Science, Prince Sultan University, Riyadh, 11586, Saudi Arabia
*Corresponding Author: Reem Ibrahim Alkanhel. Email: rialkanhal@pnu.edu.sa
Received: 13 December 2022; Accepted: 24 February 2023; Published: 28 July 2023

Abstract: Patient privacy and data protection have been crucial concerns in E-healthcare systems for many years. In modern-day applications, patient data usually holds clinical imagery, records, and other medical details. Lately, the Internet of Medical Things (IoMT), equipped with cloud computing, has come out to be a beneficial paradigm in the healthcare field. However, the openness of networks and systems leads to security threats and illegal access. Therefore, reliable, fast, and robust security methods need to be developed to ensure the safe exchange of healthcare data generated from various image sensing and other IoMT-driven devices in the IoMT network. This paper presents an image protection scheme for healthcare applications to protect patients' medical image data exchanged in IoMT networks. The proposed security scheme depends on an enhanced 2D discrete chaotic map and allows dynamic substitution based on an optimized highly-nonlinear S-box and diffusion to gain an excellent security performance. The optimized S-box has an excellent nonlinearity score of 112. The new image protection scheme is efficient enough to exhibit correlation values less than 0.0022, entropy values higher than 7.999, and NPCR values around 99.6%. To reveal the efficacy of the scheme, several comparison studies are presented. These comparison studies reveal that the novel protection scheme is robust, efficient, and capable of securing healthcare imagery in IoMT systems.

Keywords: Secure communication; healthcare data encryption; Internet of Medical Things (IoMT); discrete chaotic map; substitution box (S-box)

1 Introduction

Privacy and security have always been important issues and requirements for any healthcare organization. Any intrusion should be scrutinized to check the authenticity of the attempt to access the service [1–6]. Patient privacy is violated when sensitive data is shared on the Internet of Medical Things (IoMT) networks. As a result, there is a serious risk to the security of medical data carried across the IoMT network as part of an e-healthcare service [7]. Additionally, for intelligent monitoring, diagnosis, and decision-making processes, many smart devices contribute real-time sensitive healthcare data to IoMT networks [8]. However, a public communication channel is used to exchange the generated healthcare data, creating questions regarding diagnosis security and privacy. Therefore, cryptographic solutions that can be used to securely transmit the image data are tough security requirements for IoMT applications [9]. This is because healthcare data generated by various image-intensive and other IoMT devices must be protected against unauthorized access and alterations. An enormous amount of images is currently exchanged across open channels because of the rapid advancement of technologies like the Internet of Things (IoT), cloud computing, and fifth-generation (5G) communications. Private information about specific individuals is frequently included in the images sent. They may contain a person's social security number, health information, and, occasionally, secret defense information about a country [10]. Since only approved and intended recipients may access the images, they must be processed before being delivered.

1.1 Related Works

Image encryption is one of the potential techniques to enable the safe transmission of data across networks. This approach conceals real message data by transforming images into meaningless, noise-like data. Images are frequently sent across the network extensively and frequently have significant pixel correlation and redundancy. Additionally, images are frequently multi-dimensional image data. Therefore, considerations like security, speed, computational complexity, and transmission cost must be thought of when building a digital image encryption algorithm [11,12]. Images can be securely communicated over the network and transmitted effectively by taking these parameters into account in the algorithm. Numerous image encryption algorithms have been proposed in the literature, employing various techniques. For instance, techniques based on DNA computing [13], compressive sensing [14,15], cellular automata [16], and chaotic systems [13–17] have been utilized to create cipher images. Due to the unique characteristics of chaotic maps, chaos-based encryption is regarded as an effective solution for image encryption [18]. There are a lot of chaos-based image cryptosystems that depend on confusion and diffusion features to work properly. The confusion property is related to moving pixel positions in an image. The diffusion property is related to altering image pixel values. Both confusion and diffusion can be implemented at either the pixel level [19] or the bit level [20]. Pixel-level operation modifies the location pixels while preserving the image histograms. On the other hand, the operation at the bit level modifies the pixel values. To achieve a high level of encryption efficiency, a good level of confusion needs to be achieved. Many of the existing image ciphering algorithms are depend on the heavy usage of chaotic mechanisms, like multiple chaotic maps and/or high-dimensional chaotic systems. Others rely on computationally intensive approaches to realize good encryption quality. However, these schemes suffer from low throughput and long encryption times, making them unsuitable for real-time applications.

The properties of chaotic dynamical systems include high sensitivity to initial conditions and system parameters, excellent auto-correlation properties, pseudo-random behaviour of produced sequences, large entropy, and mixing, which have made them appropriate for potential applications in cryptography [21]. Therefore, these systems are conducive to developing effective and robust

cryptographic algorithms. Chaotic systems have been used to develop cryptographic algorithms for multimedia encryption, S-boxes, information hiding, and hash functions for the past few decades [22]. However, the security of such algorithms largely depends on the dynamics of chaotic maps. Nonetheless, one should be cautious because not all chaotic maps are suitable for obtaining robust chaos-based cryptosystems. One should avoid using a chaotic system with frail performance and considerable non-chaotic regions [23]. For example, many research findings have established that some existing discrete chaotic maps, such as Logistic, Sine, Cubic, and other chaotic maps, provide weak performance [24]. Therefore, there is a need to design chaotic systems with rich dynamical characteristics to qualify for robust cryptographic applications.

1.2 Motivation and Research Contributions

Based on the literature analysis, it is found that there exist limitations in image encryption methods including:

– The conventional discrete chaotic maps have a low Lyapunov exponent, revealing a low degree of chaoticity and sensitivity of the map, low entropy, high computations, and non-uniform coverage of space through phase attractors. The robustness and security of the encryption scheme heavily rely on the features of utilized chaotic maps.
– Numerous computationally-intensive meta-heuristics-based S-box generation algorithms are available in the literature, but very few achieve a nonlinearity of up to 112 for 8×8 S-box design. A simple and effective dynamic S-box generation method is desirable to produce highly nonlinear S-boxes. Furthermore, a single S-box usage for image encryption typically reveals some patterns of the plain image. These patterns may be used by attackers to gain some knowledge about the plain image information.
– Almost multimedia ciphering techniques heavy floating-point computations, which cause low throughput and long encryption times and making them unsuitable for real-time applications.

The above limitations and challenges motivate the need to develop cryptographically strong S-boxes, chaotic maps with frail-free performance, and efficient image encryption algorithms that are fast and robust. This paper tackles all these issues and provides three contributions. We present a proposed security scheme to investigate and meet the security need of protecting medical image data exchanged in IoMT networks that are responsible for intelligent, smart operations and decisions. The proposed security framework explores the features of an enhanced model of discrete chaos and adopts dynamic substitution to achieve excellent performance. To validate the efficacy and prestige of the framework, several comparison studies will be examined and analyzed to justify that the novel data transmission framework is robust, efficient, and capable of securing the imagery data. To achieve this goal, this paper is committed to designing an enhanced 2-D discrete chaotic map. The proposed map is applied to generate cryptographic, highly nonlinear S-boxes meant for the dynamical substitution of image pixels. The novel map is also responsible for carrying out required pixel diffusion operations, resulting in a strong image cryptosystem and encryption quality.

The main contributions suggested in this paper are the following:

- A novel and a dynamically rich 2-D discrete chaotic map are designed, which guarantees frail-free performance.
- A strong and highly nonlinear cryptographic S-boxes method is analyzed and investigated.
- A fast and efficient image encryption scheme is proposed to secure healthcare data generated and exchanged in an IoMT environment.

- Analyses have been performed to evaluate the performance of the proposed enhanced chaotic map, generated S-box, and image protection scheme.

1.3 Paper Organisation

The flow of the rest of this work is as follows: The proposed 2D discrete chaotic map is discussed in Section 2, and its dynamical features are analyzed in Section 3. The cryptographic S-box generation procedure using the enhanced 2D chaos map is discussed in Section 4. Next, Section 5 describes a method for securing digital image data generated in IoMT networks. The security evaluation of the proposed image data secure transmission scheme is done, and the comparison of the suggested secure ciphering approach is achieved in Section 6. Lastly, the summary of this work is concluded in Section 7.

2 Proposed Discrete Chaotic Map

The security and robustness of cryptographic schemes are heavily reliant on the dynamic properties of the chaotic maps used. The frail performance of chaotic maps may result in a weak security impact provided by cryptographic systems [24]. However, many of the existing chaotic maps were shown to have one or more drawbacks that limited their use in developing a strong cryptographic scheme. Chaos systems with poor dynamics are week for ciphering process and render them vulnerable to assaults. Such chaotic maps have issues like restricted chaotic range and behavior, and no uniform reportage of chaos attractors [25]. This encourages the development of chaotic maps with richer and better dynamical properties than typical chaotic maps [26]. As a result, an enhanced 2D chaotic map is created, which has many superior properties compared to 2D chaotic maps. The dynamics of the novel 2-D discrete chaotic map have the mathematical form given in Eq. (1).

$$\begin{aligned} x_{i+1} &= (a.\cos(y_i) + b.x_i) \bmod (1) \\ y_{i+1} &= (b.\sin(x_i) + y_i) \bmod (1) \end{aligned} \tag{1}$$

where, x_i, y_i are state variables that take bounded values in (0, 1), a and b are control parameters of the chaotic map. Dynamical characteristics of the suggested chaotic map are demonstrated in the below subsections, and the features of the new map are compared with the conventional 2-D Henon chaotic map [27] and the 2-D SLMM chaotic map investigated in [28].

3 Analysis of Proposed Chaotic Map

This section offers the performance and dynamical features analysis of the novel enhanced 2-D discrete chaotic map and its comparison study with the well-known chaotic maps, i.e., the 2-D Henon map and 2-D SLMM map. The simulations are done for the initial conditions for $x_0 = 0.726$ and $y_0 = 0.238$.

3.1 Lyapunov Exponents Analysis

The Lyapunov exponent (LE) is an indicator of the chaotic degree of dynamical maps. Dynamical maps having positive LE specify the existence of chaotic phenomena underlying the map [25]. The higher value of LE specifies the accelerated divergence pace of its trajectory and corresponds to the high degree of chaos exhibited by the map [24]. The behaviour of the LE for the proposed 2-D discrete map is shown in Eq. (1) is studied for different values of control parameters a and b. The new map's LEs are displayed in Figs. 1c–1f. The exponents for different values of parameter a from 0 to 20 are shown in Fig. 1c when $b = 3$. The exponents' behaviour for varying values of b from 0 to 20 is presented in Fig. 1d when $a = 7$. This range of parameters a and b are only used for experimentation.

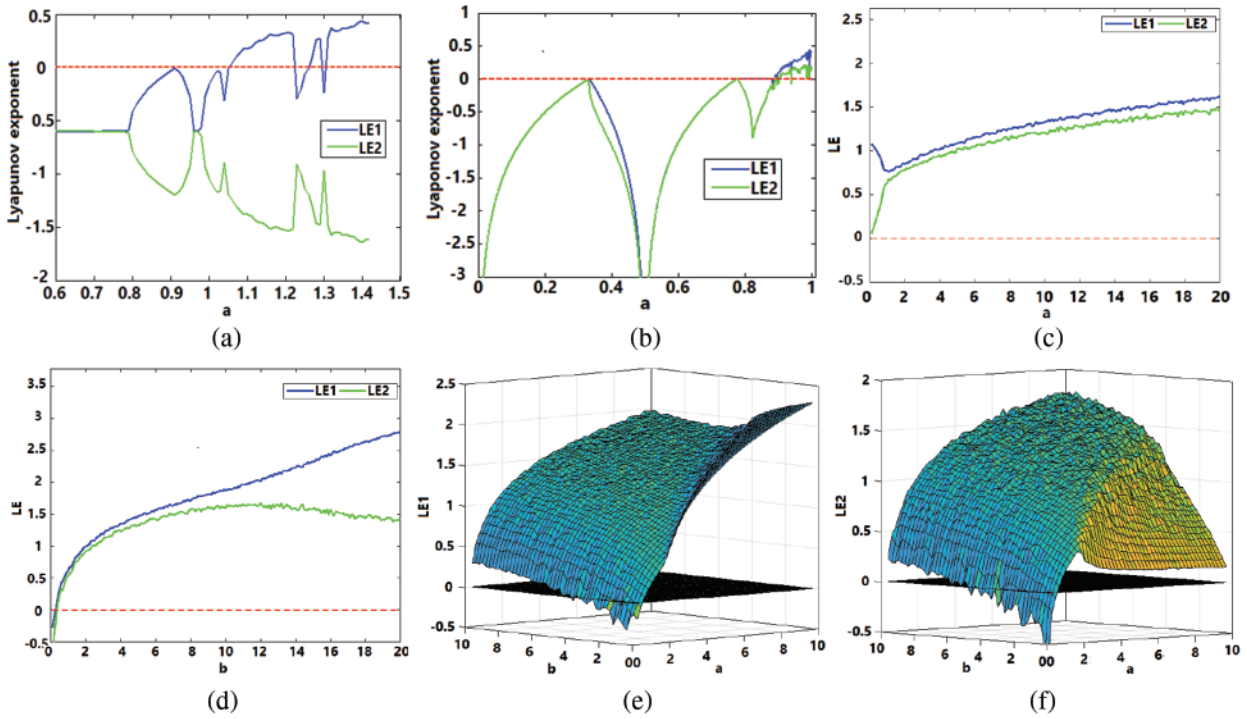

Figure 1: Lyapunov exponents analysis for $x_0 = 0.726$, $y_0 = 0.238$: (a) Henon map, (b) SLMM map, and (c) proposed map: LE *vs.* a when $b = 3$, (d) proposed map: LE *vs.* b when $a = 7$, (e) proposed map: LE1 *vs.* a and b, and (f) proposed map: LE2 *vs.* a and b

The simulation is performed to study the behaviour of both LE for simultaneous variations in parameters a and b, and the obtained behaviours of Lyapunov exponent-1 (LE1) and Lyapunov exponent-2 (LE2) are shown in Figs. 1e and 1f, respectively. According to Fig. 1c, both exponents increase as the parameter increases, reflecting the greater divergence of trajectories and arduous chaotic behaviour in the proposed discrete map. Fig. 1e also demonstrates that the magnitude of LE1 rises with an increase in the values of parameters a and b as well. For higher values of parameters, both LEs come out to be sufficiently greater than zero, which confirms the hyperchaotic nature of the proposed 2-D discrete map. Consequently, the KY dimension of the proposed discrete map comes out to be 2 since both exponents are positive. The LE feature of the novel map is compared with the 2-D Henon map and 2-D SLMM maps. Their LE spectrums are shown in Figs. 1a and 1b, respectively. The LE plots of the maps make it evident that the suggested chaotic map shows better exponent behaviour, i.e., larger LE values and greater chaoticity for a wider range of control parameters compared to the two well-known existing chaotic maps.

3.2 Bifurcation Analysis

The bifurcation diagram assists in gaining knowledge of the long-term state of dynamical maps, which may include stable, unstable, periodic, and chaotic states. The state behaviour of a dynamical map is analyzed for varying values of control parameters, usually referred to as bifurcation parameters [23]. Since the proposed 2-D discrete chaotic map has two parameters, the bifurcation diagrams for one control parameter are simulated, as shown in Fig. 2c (for $b = 3$). The proposed chaotic map also exhibits similar bifurcation behaviour for parameter b as well. Whereas the bifurcation behaviour of

the 2-D Henon chaotic map and the 2-D SLMM chaotic map is simulated, as shown in Figs. 2a and 2b. The bifurcation diagrams show that there exist no periodic or non-chaotic windows in Fig. 2c, unlike in Figs. 2a and 2b. As a result, the proposed chaotic map demonstrates that it has superior bifurcation conduct than the Henon and SLMM maps because it covers the entire control parameter region.

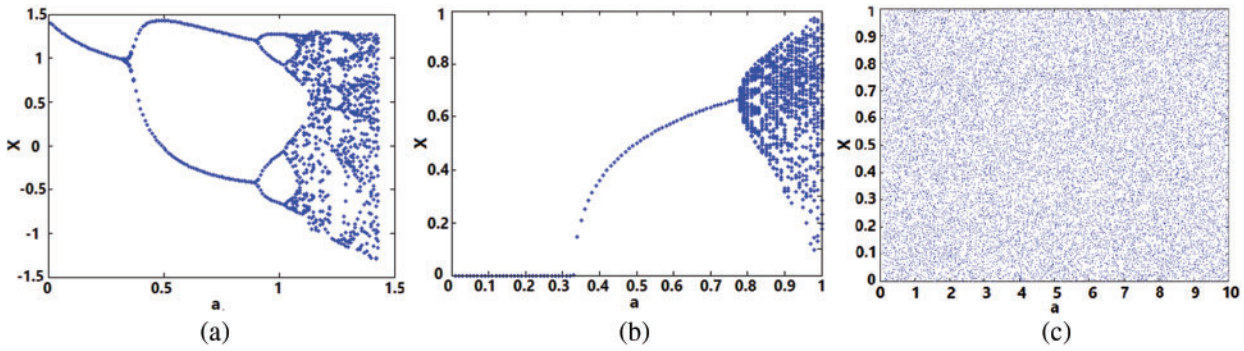

Figure 2: Bifurcation behavior of 2D chaotic maps (a) Henon, (b) SLMM, and (c) proposed

3.3 Approximate Entropy Analysis

The approximate entropy measure is aimed at assessing the complexity contained in dynamical systems and maps. It quantifies the extent of unpredictability and irregularities within the time series generated by the system. ApEn with a higher magnitude is expected for systems containing greater complexity and randomness [29]. The ApEn measure is computed for the three 2-D chaotic maps with similar initial values. The ApEn for different permissible values of their bifurcation parameter is stored, and the behaviour is shown in Fig. 3. The mean and maximum statistics from the ApEn plots for the three chaotic maps are determined and listed in Table 1. The maximum and mean ApEn scores for the proposed chaotic are 1.3276 and 1.2924, respectively. The comparison in Fig. 3 and Table 1 demonstrates that the proposed chaotic map attains higher values than the 2-D chaotic Henon and SLMM maps, which clearly indicates that our map has higher complexity, unpredictability, or randomness. This analysis demonstrates that the proposed chaotic map is well-suited for cryptographic applications and security primitive designs.

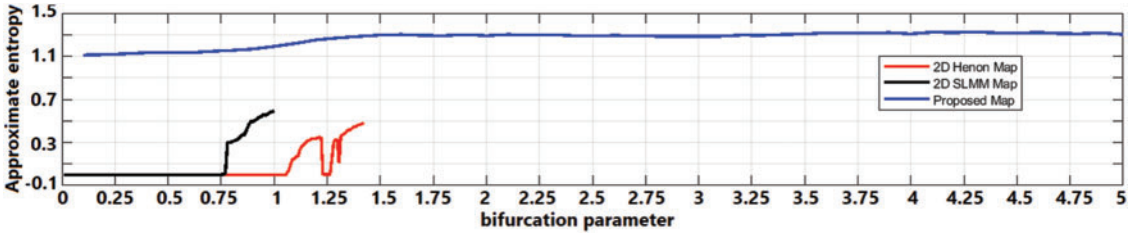

Figure 3: Approximation entropy complexity of 2D chaotic maps: Henon, SLMM, and proposed

Table 1: Comparison of approximate entropies for 2-D chaotic maps

2D Chaotic map	Max	Mean
Henon	0.4765	0.1212
SLMM	0.5950	0.1038
Proposed	1.3276	1.2924

3.4 Phase Attractors Analysis

A chaotic sequence showing rich randomness performance should be able to cover the entire phase space uniformly and randomly. Hence, the phase coverage of the trajectories of chaotic maps is analyzed, as shown in Fig. 4. A suitable cryptographic chaotic map should have an attractor with a specific shape. It can be seen from Fig. 4 that there is an uneven distribution of chaotic sequences generated from 2-D chaotic Henon and SLMM maps. Moreover, the entire phase space is not covered by the chaotic variables. The chaotic variables never visit many areas of the phase space. In comparison, the proposed chaotic map has a uniform distribution of its generated sequences and covers the entire phase space randomly and uniformly.

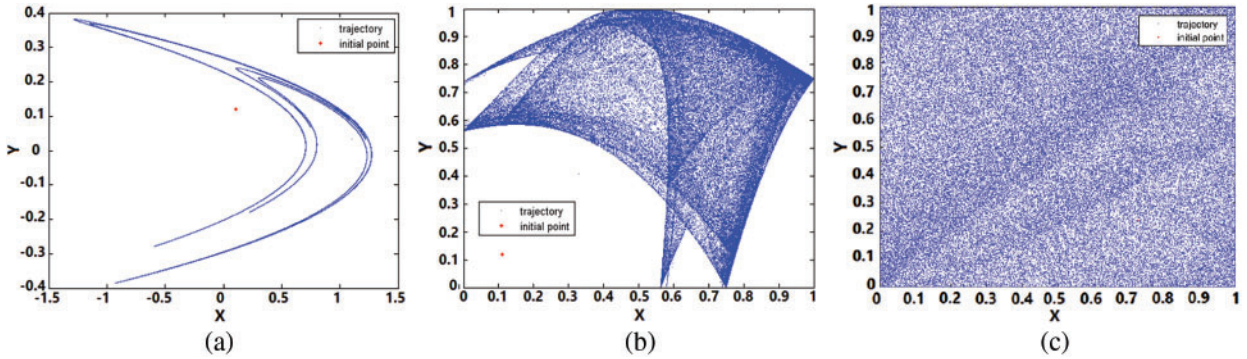

Figure 4: Phase diagrams depicting attractors of 2D chaos maps (a) Henon, (b) SLMM, and (c) proposed

4 Dynamic S-box Generation

In the proposed security scheme, strong S-boxes are needed during the image encryption phase to perform the dynamic substitution. Highly nonlinear and robust S-boxes are needed, which can bring a strong nonlinear transformation of plain data to make the encryption algorithm resistant to possible attempts. The anticipated S-box generation is based on the effective hill-climbing approach by swapping operations [30]. The S-box procedure explores the dynamics of the proposed chaotic map for preliminary S-box design and the random coordinates needed for swapping the elements of the current S-box. The S-box procedure depicted in Algorithm 1 aims to achieve high nonlinearity. The chaotic map, as shown in Algorithm 2, is used to generate an initial 8×8 S-box. Then, two random coordinates in the range of [0,255] are derived from the chaotic map as $coord_1 \leftarrow (floor(xi \times 10^{14}))\%(2^8)$, and $coord_2 \leftarrow (floor(yi \times 10^{14}))\%(2^8)$. The two elements in the current S-box are swapped. The change in the S-box is retained if the new S-box has better or equal nonlinearity. Repeating the operation of swapping for a specified number of counts produces S-boxes with pretty decent nonlinearity. The S-box procedure

is executed for $x_0 = 0.726$, $y_0 = 0.238$, $a = 7$, $b = 3$, and $max\_itr = 250000$ or until the nonlinearity of 112 is reached. For the mentioned setting, an S-box shown in Table 2 is obtained. However, with a slight variation in the initial conditions x_0 and y_0, entirely different configurations of S-boxes with a nonlinearity score of 112 can be obtained.

Algorithm–1: ConstructSbox((*xi, yi, a, b, max_itr*)

Input: *xi, yi, a, b, max_itr*

Output: 8×8 S-box with high nonlinearity

```
g_sbox ← ChaoticInitialisedSbox(xi, yi, a, b)
g_fit ← ComputeNL(g_sbox)
for k ← 1 to max_itr do:
        Get coord1, coord2 from 2D chaotic map
        t_sbox ← g_sbox
        Swap(t_sbox[coord1], t_sbox[coord2])
        t_fit ← ComputeNL(t_sbox)
        if (t_fit ≥ g_fit) then:
                g_sbox ← t_sbox
                if (t_fit > g_fit) then:    // good hit
                        g_fit ← t_fit
                end if
        end if
end for
return g_sbox
```

Algorithm–2: ChaoticInitialisedSbox(*xi, yi, a, b*)

Input: *xi, yi, a, b*

Output: Initial 8×8 S-box

```
for k ← 0 to (2^8 - 1) do:
        [xi, yi] ← Chaso_2d(xi, yi, a, b)
        chaos_array[i] ← xi + yi
end for
s_array ← Sort(chaos_array,'ascend')
for k ← 0 to (2^8 - 1) do:
q ← s_array[k]
for j ← 0 to (2^8 - 1) do:
      if (q = = chaos_array[j]) then:
            sbox[k] ← j - 1
          break
      end if
end for
end for
return sbox
```

Table 2: Suggested optimized S-box

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

Some well-known standard parameters are used to assess the performance of S-boxes, such as nonlinearity, SAC, BIC, differential uniformity, LAP, etc., [31]. A higher nonlinearity score is responsible for making the transformation of plaintext data into ciphertext data more complex. It mitigates any linear attacks. SAC stands for strict avalanche criterion, which entails that there should be around a 50% change in output if any of the input bits are flipped, thereby indicating the uniform change in the output vectors so as to avoid leaking any information to the attackers. The bits independence criterion states that the possible input vectors are mutually exclusive from each other and that each of the vectors should have high nonlinearity performance. Low differential uniformity values are essential to nullify any possibility of leakage of information to the attackers. This parameter is responsible for offering resistance to differential cryptanalysis. Linear approximation probability is equally significant in mitigating linear cryptanalysis [32]. The good tradeoff of these parameters makes a strong S-box that can do effective substitution while encrypting the plaintext data into ciphertext data. For a detailed description of these S-box parameters, readers are referred to the author's previous S-box in [24]. Here, the strength of the S-box is improvised with respect to nonlinearity, and we quantified the performance of our S-box. The performance scores are shown in Table 3. It also reports the performance indices of some recently investigated S-box studies. From Table 3, it is apparent that the proposed S-boxes have quite decent and better cryptographic strength compared to some recent S-boxes investigated in [33–40].

Algorithm–3: Encrypting medical image data

```
IMG=reshape(P,1,M*N)
//generating 256-bit hash code
img_data=dec2hex(IMG)
img_data=reshape(img_data,1, M*N*2);
H=sha256_hash(img_data) //hex-codes
L=length(H)
for k=1:1:len
  hash(k)=hex2dec(H(k))
end
t=1;
//obtaining 8-bit encoded values
for k=1:2:len
  H(t)=16*hash(k)+hash(k+1)
  t=t+1
end
C0=H(1)
x0=mod(x0+sum(H)/(255*32), 1);
y0=mod(y0+sum(H)/(255*32), 1);
//image pixels shuffling
for k=1:2:M
  [x1, y1]=chaos_2d(x0, y0)
  x0=x1; y0=y1
  arr(k)=x1
  arr(k+1)=y1
end
R=zeros(M, N)
parr=pindex(arr, M)
for t=1:1:M
  R(t, parr(t))=1
end
S=transpose(P×R)×R //shuffled image
S=reshape(S,1,M*N)
// substitution and diffusion
for k=1:1:M*N
  [x1, y1]=chaos_2d(x0, y0)
  x0=x1; y0=y1
  x2=floor(x1*10^10)
  y2=floor(y1*10^10)
  r=mod(x2,16)+1
  c=mod(y2,16)+1
  K1=SB(r, c)
  x2=floor(x1*10^14)
  y2=floor(y1*10^14)
  K2=mod(x2,256)
  K3=mod(y2,256)
  A=mod(SP(k)+K2+K3,256)
  B=bitxor(K1,bitxor(A,C0))
  q=mod(K1+K2+K3,32)+1
  C(k)=bitxor(B,H(q))
  C0=C(k)
end
encrypted image C
```

Table 3: Cryptographic performance comparison of S-boxes

S-box	NL_{min}	NL_{max}	NL_{avg}	SAC	BIC	DU	LAP
Proposed	112	112	112	0.4993	103.36	10	0.1250
S-box [33]	104	110	107	0.4993	103.29	10	0.1328
S-box [34]	102	108	105.75	0.4062	102.36	10	0.1406
S-box [35]	105	110	107	0.5197	102.75	10	0.1328
S-box [36]	106	110	108.5	0.4995	103.85	10	0.1328
S-box [37]	108	112	110	0.4995	103.14	10	0.1328
S-box [38]	108	112	109.75	0.5068	104.35	10	0.1250
S-box [39]	108	110	108.75	0.4946	102.79	10	0.1328
S-box [40]	102	108	105	0.5029	102.9	12	0.1484

5 Secure Image Data Transmission Scheme

In the Internet of Medical Things networks, real-time sensitive healthcare data has been generated by various smart sensing devices for intelligent monitoring, decision-making, and smart diagnosis operations. However, the generated clinical imagery data is exchanged over a public channel, which raises concerns about the security and privacy of patients' data. Therefore, to protect sensitive medical data from various image sensing and other IoMT devices against illegal access by an adversary, a cryptographic solution that can preserve image data privacy is one of the challenging security needs for secure and trustworthy healthcare systems. It is worth noting that traditional data privacy schemes designed for either text or image data have been found to be inadequate for meeting the real-time and fast processing of transmitted multimedia data in IoMT networks. The existing encryption schemes involve high computation, long encryption and decryption times, low robustness to pertinent attacks, etc. Hence, such shortcomings and challenges motivate the need for low-cost, robust, and fast data privacy schemes through which real-time, secure data transmission for IoMT and healthcare systems becomes practical.

The security strength of an S-box-based cryptosystem heavily influences its security. Therefore, strong S-boxes are essential to building secure cryptosystems. We proposed an optimization process to evolve the nonlinear features of the initial S-box and generate highly nonlinear S-boxes for use in robust and fast image data protection. This phase is about the scheme for protecting the image data for the IoMT system. The proposed security scheme involves the encrypting of image data using the action of a strong S-box and enhanced chaotic map. The encryption scheme is simple to have low computation time but with high robustness and security features. The proposed image encryption scheme is presented in Algorithm 3. Take the initial values of $x0$, $y0$, a, and b and retrieve the optimized 8×8 S-box SB (as demonstrated in Table 1) using the suggested chaotic map through the procedure described in the previous section. Let $\boldsymbol{P}$ be the pending plain image, the SB be the generated optimized S-box (shown in Table 1), M and N be the size of the image P, and $0 \leq C0 \leq 255$. The presented encryption algorithm is to be followed reversely to perform the decryption of the encrypted image at the receiver side to maintain the integrity of the sensitive image data.

6 Performance Analysis of Encryption Scheme

To implement our encryption scheme, the experimental environment involves Windows 10 Pro with an Intel CoreTM i3 processor running at 3.4 GHz and 8 GB of RAM. The proposed security scheme for image-data protection consists of many prominent performance results. The key features of the performance outcomes include: (a) the proposed encryption scheme is suitable for lightweight applications like IoMTs due to its simplicity, low computation, and lower encryption time, resulting in high throughputs of more than 1450 Kbps; (b) the proposed security scheme has a sufficiently large key space $\geq 2^{251}$ and is highly sensitive to slight variations in the pending image, (c) the inclusion of an enhanced chaotic map assisting in the generation of highly nonlinear and dynamic S-boxes in the scheme makes it extremely robust against adversarial cryptanalysis attempts. The recital evaluation of the suggested encryption scheme is presented, and various security analyses have been studied along with the results, which are also compared with a few recent encryption schemes.

6.1 Distribution Analysis

To avoid cryptanalysis via the pixels distribution pattern by an attacker in a cipher-only attack, a histogram of a ciphered image must depict a flat or shape of pixel intensities. The first row in Fig. 5 illustrates plain images as our benchmark images considered for analysis. Their corresponding

encrypted images using our proposed encryption scheme are shown in the fourth row of Fig. 5. On visually inspecting the figure, it is clear that the encrypted images show no traces or patterns of original data, therefore exhibiting effective encryption. The second and fifth rows of Fig. 5 depict histograms of plain and encrypted images, respectively. The encrypted image's histogram has a uniform and flat pixel distribution, whereas the plain image's histogram illustrates peaks, indicating a non-uniform distribution of pixel intensities. Henceforth, the image information will be difficult to discern because the histogram of an encrypted image depicts an undeviating pixel distribution all throughout the plot. The chi-square χ^2 can be used to determine how pixels are distributed in an image.

$$\chi^2 = \sum_i \frac{[P_i - E_i]}{E_i} \tag{2}$$

where P_i represents the actual occurrence, and E_i denotes the expected pixel frequency of the i-th pixel value. If the chi-square test value of an image is less than 293.2478 (a standard value at a significance level of 0.05 [41]), then the image is likely to have a uniform pixel spread. Table 4 lists the calculated chi-square values of different plain images that mostly have associated pixels and encrypted images that have randomly distributed pixels. The average of the chi-square test value over the plain images is 918258.7. This high score indicates the pixels in the images are highly dispersed in a non-uniform fashion, which can provide some clue about the information content of the attacker. Where the average chi-square test value computed over the listed encrypted images is 249.5. The score of 249.5 is near the expected value presented in [41] and very far from the average obtained for the plain images. The obtained score for the proposed encryption method is found to be comparable to the chi-square reported in [40]. It is inferred from the chi-square test results that the encrypted image pixel intensities are uniformly distributed. This analysis verifies that the proposed encryption method can substantially withstand statistical attacks.

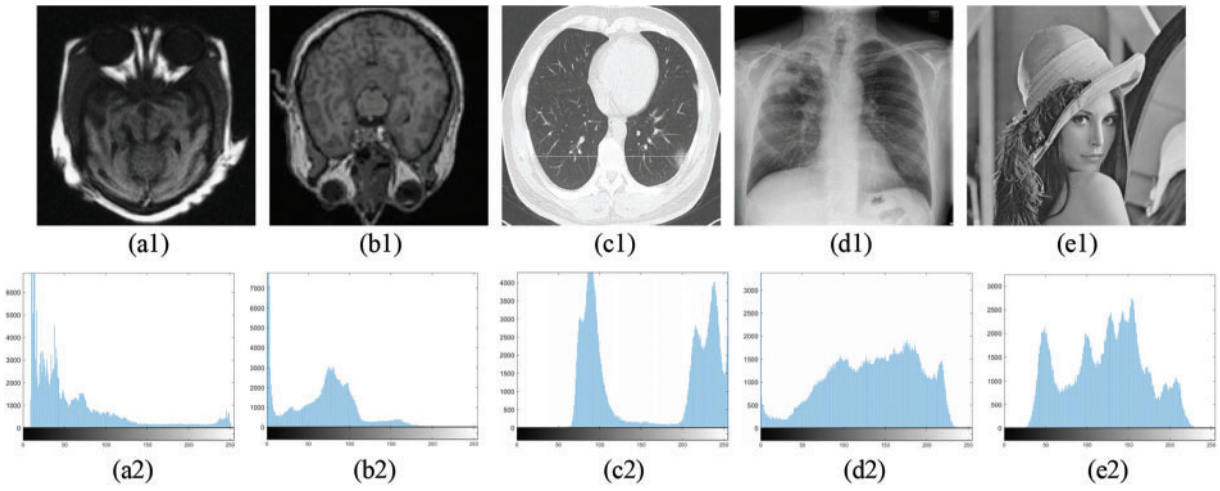

Figure 5: (Continued)

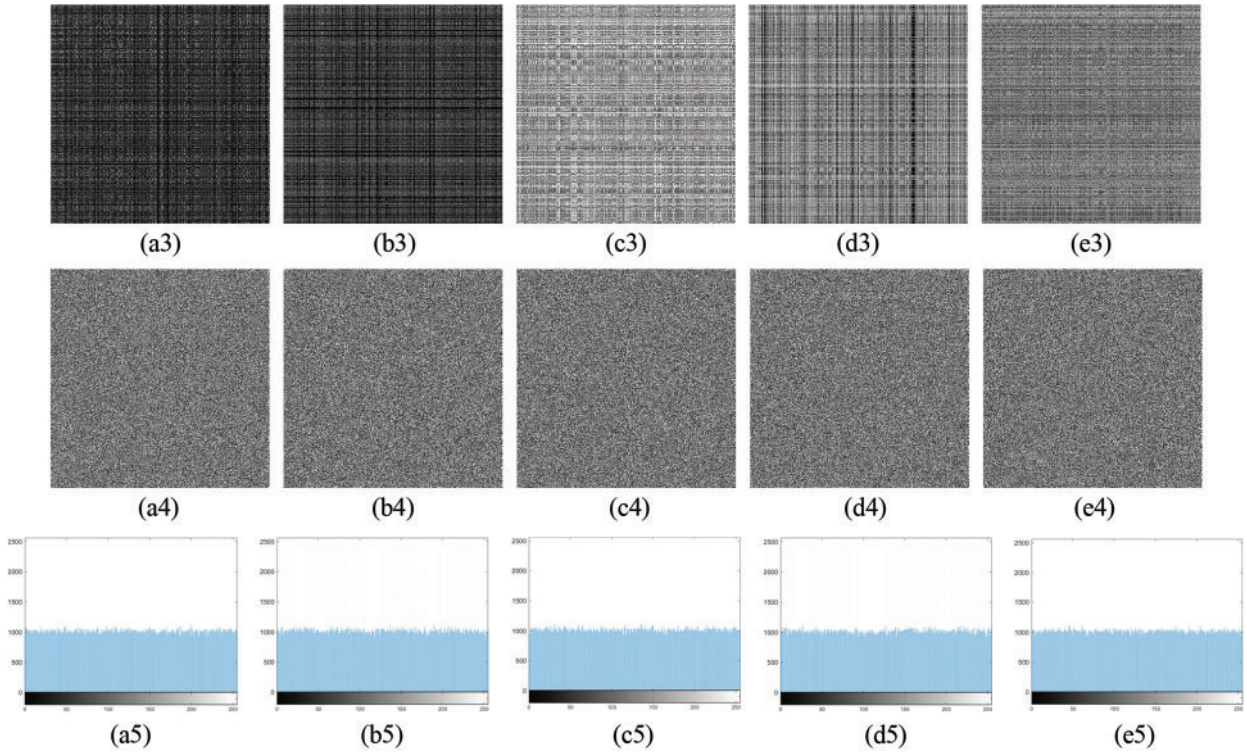

Figure 5: Simulation of proposed encryption scheme: (a1–a5) plain-images *P*, (b1–b5) histograms of *P*, (c1–c5) shuffled images *S*, (d1–d5) encrypted images C, and (e1–e5) histograms of *C*

Table 4: Chi-square results on different standard images

Image	Plain	Encrypted
Fig. 5a	1619631.48	227.71
Fig. 5b	2152134.83	277.13
Fig. 5c	468928.04	240.76
Fig. 5d	192933.63	293.02
Fig. 5e	157665.73	208.9
Ref. [40]	–	238.4

6.2 Correlation Analysis

The image pixels usually retain high correspondence with their adjoining pixels. This interdependence of pixels expedites cryptanalysis. Therefore, a good cipher is required to reduce or even remove the correlation between pixels in order to prevent any statistical analysis. The dissimilarity or likeness of image pixels with their adjacent pixels is computed using a correlation coefficient [42]. Very low values

of the correlation coefficient (near zero) for an image suggest the least similarity among its pixels. Therefore, the image is considered robust for transmission over an unreliable channel. The correlation coefficient γ is defined as:

$$\gamma = \sum \frac{(i - \mu i)\,(j - \mu j)}{\sigma_i \sigma_j} \tag{3}$$

where i and j signify the position of row and column values in an image under observation. The factors μ and σ denote the variance and the standard deviation, respectively. The correlation is computed using Eq. (3) and presented in Table 5. The correlation scores clearly illustrate that the correlation are fairly near 1.0, implying a strong correlation between their neighbouring pixels. However, the ciphertext images exhibit weak correlation, as the correlation coefficients are near zero. The visual analyses of the correlation among adjacent pixels of images have been performed, and the results obtained are shown in Fig. 6. The figure signifies the correlation of pixels in plain images and encrypted images. We can observe that the pixels in plain-images are closely correlated to their neighbouring pixels because the adjacent pixel is confined close to its neighbouring pixels. But, there is no such correlation or confinement visible in the second row of the figure, which is for encrypted images. In encrypted images, the pixel values are uniformly distributed and cover the whole available space. Table 5 shows that the adjacent pixels in encrypted images obtained from the proposed method are more uncorrelated compared to the scores reported in [40,43–48]. It can be inferred that the low correlation of pixels in encrypted images will prevent attackers from obtaining meaningful information via any statistical attacks. So, we can say that the proposed encryption algorithm protects strongly against any statistical analysis.

Table 5: Correlation coefficients and entropies of plain-images and encrypted images

Image	Correlation coefficients		Information entropy	
	Plain	Encrypted	Plain	Encrypted
Fig. 5a	0.98687	0.000938	6.53647	7.99937
Fig. 5b	0.97374	0.000212	6.3684	7.99924
Fig. 5c	0.98182	0.002080	6.7900	7.99934
Fig. 5d	0.98825	0.002155	7.58308	7.99919
Fig. 5e	0.95022	0.001607	7.4473	7.99942
Ref. [40]	–	−0.0045	–	7.9992
Ref. [43]	–	−0.0011	–	7.9634
Ref. [44]	–	−0.0005	–	7.9992
Ref. [45]	–	0.0023	–	7.9894
Ref. [46]	–	−0.0029	–	7.9986
Ref. [47]	–	0.0137	–	7.99928
Ref. [48]	–	0.00229	–	7.9993

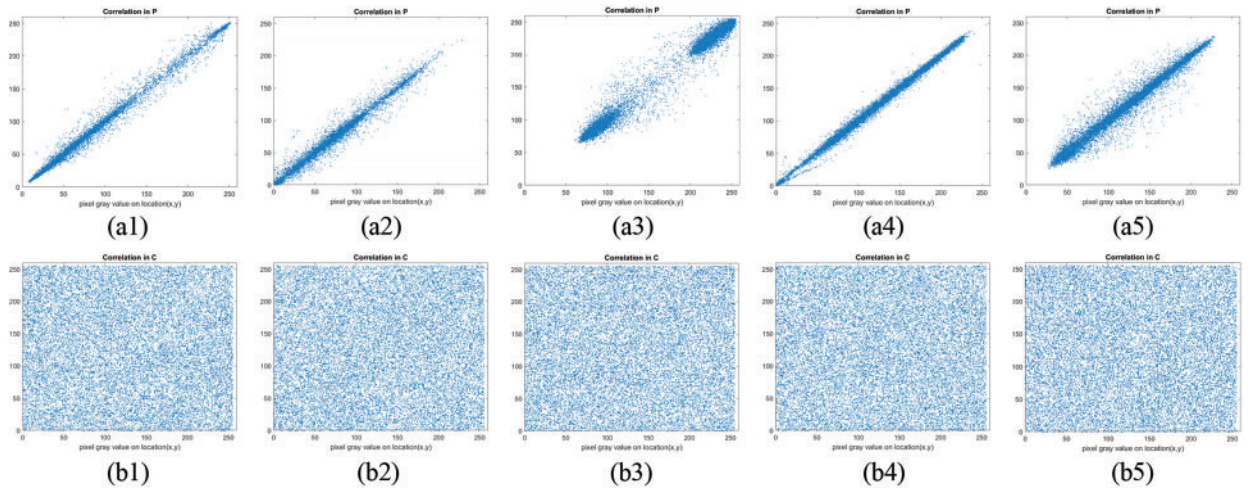

Figure 6: Simulation of correlation among adjacent pixels of (a1–a5) plain-images P, and (b1–b5) encrypted images C

6.3 Entropy Analysis

In information theory, the entropy of a variable is the quantity of uncertainty of information [47]. It typically reflects the randomness and unpredictability of test information. It is normally measured in bits and mathematically defined as:

$$H(x) = \sum_i p(x_i) \log_2 \left(\frac{1}{p(x_i)} \right) \tag{4}$$

where $p(x_i)$ is the probability of the message source x_i. If the information entropy value for an encrypted image is high, then it suggests a uniform spread of pixels' intensities, thereby strengthening image security. In contemporary, if it is lower than 8, then there is a high chance of envisaging the image, hence intimidating the image's security. The information entropy scores for the selected test images are determined, and the results are offered in Table 5. The entropies of plain images are considerably away from their ideal value. However, the encrypted images have entropy values greater than 7.999. This entails that each pixel's intensity is equally probable in the encrypted content. Moreover, the obtained entropy score for the proposed scheme is better than a few of the encryption schemes investigated in [43,45,46] and comparable to other schemes mentioned in Table 5. So, the proposed image protection scheme is strong enough to add enough information and randomness to the encrypted content so that it can withstand attempts made to steal sensitive plain-image information that is based on entropy.

6.4 Differential Attack Analysis

The primary goal of the cryptanalyst is to gain partial or full access to the contents of the secret data, which the sender legitimately encrypts for its intended recipient before its transmission over the network [44]. During normal practice, the attacker tries to obtain information about the original unencrypted (plain-image) data by making changes to plain images, encrypting them, and comparing the output with a list of encrypted images. This approach of attackers can be avoided by employing a strategy in which the encryption process is entirely dependent on plain images. This method will ensure that exclusively different encrypted data will be obtained from the encryption process even when a plain image is minutely changed. We have offered an image encryption method that incorporates the method

of having high sensitivity to change in plain images so as to thwart differential cryptanalysis attempts. In order to assess these, we selected two performance metrics, namely the number of pixels change rate (NPCR) and the unified average changing intensity (UACI). The NPCR metric quantifies the pace of altered pixels in the encrypted data that get changed when a minor alteration is made in the plain-text data. While the UACI metric measures the average of the difference in intensities between plain-text and encrypted images. The two metrics are computed by following a process. First, we selected two plain images, P1 and P2, which are only different by one pixel. Second, the encrypted images for these images are computed and named C_1 and C_2. The metrics are then mathematically defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100 \tag{5}$$

$$UACI = \frac{1}{M \times N}\left[\sum \frac{|C_1(i,j) - C_2(i,j)|}{2^8 - 1}\right] \times 100 \tag{6}$$

where $D(i,j)$ is 1 if C1$(i,j) \neq$ C2(i,j) else it is 0, and M $\times$ N is the size of the plain-image. The experimental results of this differential attack analysis through the computation of NPCR and UACI parameters for the selected five plain-images are presented in Table 6. It is evident that the minute change in the plain-image has an extreme effect on the encrypted content. The scores of NPCR and UACI provided in Table 6 are about 99.6 and 33.33, respectively. Differential analysis is one of the crucial tests to assess the robustness against differential attacks by attackers. The obtained scores demonstrate that the projected image protection approach is robust enough to resist differential attacks and offers great sensitivity to even small changes in the plain-image data.

Table 6: Differential attacks analysis

Image	NPCR	UACI
Fig. 5a	99.594	33.372
Fig. 5b	99.59	33.38
Fig. 5c	99.59	33.46
Fig. 5d	99.60	33.44
Fig. 5e	99.60	33.44
Ref. [40]	99.55	33.4
Ref. [44]	99.61	33.44
Ref. [46]	99.62	33.47
Ref. [48]	99.61	33.46

6.5 Encryption Speed Analysis

To fulfill standards with today's high-speed communication technologies, an encryption algorithm should spawn encrypted data at a swift pace. Therefore, an efficient image encryption algorithm is considered effective for real-world applications. In the proposed image encryption scheme, we have

taken into account the time complexity of the encryption process. The encryption time taken by our scheme is around 1.402 s for encrypting a 512 × 512 image, which offers a throughput of 1495 Kbps. The short encryption time and high throughput indicate that the proposed encryption scheme is suitable for real-time applications to realize security. We make a comparative study by listing the encryption time incurred by some existing encryption schemes in Table 7. The comparison made in Table 7 shows that our encryption has a fairly shorter time, hence faster and greater throughput, compared to some existing encryption schemes investigated in Refs. [47–51] except Ref. [52], wherein selective encryption of only the facial portion within the image is performed.

Table 7: Encryption time comparison (time in secs)

Scheme	Configuration	Time
Proposed	CPU Core i3, 3.4 GHz, 8 GB RAM on Windows 10	1.402
Ref. [47]	CPU 2.5 GHz, 4 GB RAM on Windows 7	15.14
Ref. [48]	CPU 2.5 GHz, 4 GB RAM on Windows 7	5.69
Ref. [49]	CPU Core i3, 4 GB RAM on Windows 7	22.43
Ref. [50]	CPU 3.3 GHz, 4 GB RAM on Windows 7	1.489
Ref. [51]	CPU Core i5 3.1 GHz, 8 GB RAM on Windows 7	4.749
Ref. [52]	CPU Core i5 on Windows 10	0.165198

In contrast, our proposed method performs full encryption of the images. Hence, the proposed encryption scheme can encrypt the images quickly with better throughput compared to many recently investigated schemes.

7 Conclusions and Future Work

This paper described a security scheme for the protection and secure transmission of healthcare image data originating in the Internet of Medical Things network. The proposed encryption scheme is simple, effective, robust, and faster, which makes it suitable for securing healthcare data in IoMT environments. The proposed scheme explores the features of the newly developed 2D discrete chaotic map, which has better dynamics than existing 2D Henon and SLMM maps and optimizes highly nonlinear S-boxes that are spawned with the new chaotic map. The optimized S-box also has greater and stronger security strength compared to many recently investigated S-boxes. Several experimental and standard simulation analyses have been conducted to assess the recital of the suggested image protection scheme. The performance and comparative results validate the consistency and better performance of the new encryption scheme. The proposed scheme has been found suitable for encrypting the healthcare imagery generated in IoMT networks. For future work, we intend to use multiple stages for securing medical data in healthcare applications. Also, artificial intelligence tools may be incorporated to secure medical information in big data medical applications.

Acknowledgement: The authors would like to acknowledge the support received from the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University, through the Research Funding Program, Grant No. (FRP-1443-11).

Funding Statement: This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University, through the Research Funding Program, Grant No. (FRP-1443-11).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] A. Wani and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," *CAAI Transactions on Intelligence Technology*, vol. 6, no. 3, pp. 281–290, 2021.

[2] S. Das and S. Namasudra, "MACPABE: Multi-authority-based CP-ABE with efficient attribute revocation for IoT-enabled healthcare infrastructure," *International Journal of Network Management*, vol. 2, no. 1, pp. 1–15, 2022.

[3] A. Gutub, "Boosting image watermarking authenticity spreading secrecy from counting-based secret-sharing," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 1–13, 2022.

[4] Z. Chen, "Research on internet security situation awareness prediction technology based on improved RBF neural network algorithm," *Journal of Computational and Cognitive Engineering*, vol. 3, no. 2, pp. 1–16, 2022.

[5] R. Verma, A. Kumari, A. Anand and V. S. S. Yadavalli, "Revisiting shift cipher technique for amplified data security," *Journal of Computational and Cognitive Engineering*, 2022. https://doi.org/10.47852/bonviewJCCE2202261

[6] S. Das and S. Namasudra, "Multi-authority CP-ABE-based access control model for IoT-enabled healthcare infrastructure," *IEEE Transactions on Industrial Informatics*, 2022. https://doi.org/10.1109/TII.2022.3167842

[7] A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon *et al.,* "A novel hybrid cryptosystem for secure streaming of high efficiency H.265 compressed videos in IoT multimedia applications," *IEEE Access*, vol. 8, pp. 128548–128573, 2020.

[8] W. El-Shafai, M. Aly, A. Algarni, F. Abd El-Samie and N. Soliman, "Secure and robust optical multi-stage medical image cryptosystem," *Computers, Materials & Continua*, vol. 70, no. 1, pp. 895–913, 2022.

[9] R. Hamza, Z. Yan, K. Muhammad, P. Bellavista and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Information Sciences*, vol. 52, no. 7, pp. 493–510, 2020.

[10] J. Sheikh, S. Akhter, S. Parah and G. Bhat, "Blind digital speech watermarking using filter bank multicarrier modulation for 5G and IoT driven networks," *International Journal of Speech Technology*, vol. 21, no. 3, pp. 715–722, 2018.

[11] W. Feng, Y. He, H. Li and C. Li, "A plain-image-related chaotic image encryption algorithm based on DNA sequence operation and discrete logarithm," *IEEE Access*, vol. 7, pp. 181589–181609, 2019.

[12] A. Toktas, U. Erkan, F. Toktas and Z. Yetgin, "Chaotic map optimization for image encryption using triple objective differential evolution algorithm," *IEEE Access*, vol. 9, pp. 127814–127832, 2021.

[13] X. Wu, H. Kan and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Applied Soft Computing*, vol. 3, no. 7, pp. 24–39, 2015.

[14] F. Musanna and S. Kumar, "A novel image encryption algorithm using chaotic compressive sensing and nonlinear exponential function," *Journal of Information Security and Applications*, vol. 5, no. 4, pp. 102–125, 2020.

[15] L. Zhu, D. Jiang, J. Ni, X. Wang, X. Rong *et al.,* "A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing," *Signal Processing*, vol. 19, no. 5, pp. 108–119, 2022.

[16] P. Naskar, S. Bhattacharyya, D. Nandy and A. Chaudhuri, "A robust image encryption scheme using chaotic tent map and cellular automata," *Nonlinear Dynamics*, vol. 100, no. 3, pp. 2877–2898, 2020.

[17] J. Zheng, Z. Luo and Q. Zeng, "An efficient image encryption algorithm based on multi chaotic system and random DAN coding," *Multimedia Tools and Applications*, vol. 79, no. 39, pp. 29901–29921, 2020.

[18] D. Trujillo-Toledo, O. López-Bonilla, E. García-Guerrero and E. Inzunza-González, "Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps," *Chaos, Solitons & Fractals*, vol. 15, no. 3, pp. 111–119, 2021.

[19] C. Pak, K. An, P. Jang, J. Kim and S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools and Applications*, vol. 7, no. 8, pp. 12027–12042, 2019.

[20] H. Li, Y. Wang and Z. Zuo, "Chaos-based image encryption algorithm with orbit perturbation and dynamic state variable selection mechanisms," *Optical Lasers and Engineering*, vol. 11, no. 5, pp. 197–207, 2019.

[21] J. Teh, M. Alawida and Y. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *Journal of Information Security and Applications*, vol. 50, no. 9, pp. 102–124, 2020.

[22] L. Kocarev and S. Lian, "Chaos-based cryptography: Theory, algorithms and applications," *Science & Business Media*, vol. 35, no. 6, pp. 102–117, 2011.

[23] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Transactions on Systems*, vol. 51, no. 6, pp. 3713–3724, 2021.

[24] M. Ahmad, E. Al-Solami, A. Alghamdi and M. Yousaf, "Bijective S-boxes method using improved chaotic map-based heuristic search and algebraic group structures," *IEEE Access*, vol. 8, pp. 110397–110411, 2020.

[25] Z. Hua, B. Zhou and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1273–1284, 2018.

[26] M. Alawida, A. Samsudin, J. S. Teh and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, no. 3, pp. 45–58, 2019.

[27] J. Gallas, "Structure of the parameter space of the Hénon map," *Physical Review Letters*, vol. 70, no. 3, pp. 2714–2717, 1993.

[28] Z. Hua, Y. Zhou, C. Pun and C. Chen, "2D sine logistic modulation map for image encryption," *Information Sciences*, vol. 29, no. 7, pp. 80–94, 2015.

[29] S. Pincus, "Approximate entropy as a measure of system complexity," *Sciences of the United States of America*, vol. 8, no. 18, pp. 2297–2301, 1991.

[30] Y. Wang, P. Lei and K. Wong, "A method for constructing bijective S-box with high nonlinearity based on chaos and optimization," *International Journal of Bifurcation and Chaos*, vol. 25, no. 10, pp. 155–169, 2015.

[31] M. Ahmad, H. Haleem and P. Khan, "A new chaotic substitution box design for block ciphers," in *Proc. of IEEE Int. Conf. on Signal Processing and Integrated Networks (SPIN)*, Noida, India, pp. 255–258, 2014.

[32] M. Ahmad and M. Malik, "Design of chaotic neural network based method for cryptographic substitution box," in *Proc. of IEEE Int. Conf. on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, Chennai, India, pp. 864–868, 2016.

[33] P. Zhou, J. Du, K. Zhou and S. Wei, "2D mixed pseudo-random coupling PS map lattice and its application in S-box generation," *Nonlinear Dynamics*, vol. 103, no. 10, pp. 1151–1166, 2021.

[34] M. Açikkapi and F. Özkaynak, "A method to determine the most suitable initial conditions of chaotic map in statistical randomness applications," *IEEE Access*, vol. 9, pp. 1482–1494, 2020.

[35] U. Çavuşoğlu and A. Kökçam, "A new approach to design S-box generation algorithm based on genetic algorithm," *International Journal of Bio-Inspired Computation*, vol. 17, no. 1, pp. 52–62, 2021.

[36] H. Alhadawi, M. Majid, D. Lambić and M. Ahmad, "A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm," *Multimedia Tools and Applications*, vol. 80, no. 5, pp. 7333–7350, 2021.

[37] F. Artuğer and F. Özkaynak, "An effective method to improve nonlinearity value of substitution boxes based on random selection," *Information Sciences*, vol. 57, no. 6, pp. 577–588, 2021.

[38] K. Zamli, "Optimizing S-box generation based on the adaptive agent heroes and cowards algorithm," *Expert Systems with Applications*, vol. 18, no. 2, pp. 115–209, 2021.

[39] T. Zhang, C. Chen, L. Chen, X. Xu and B. Hu, "Design of highly nonlinear substitution boxes based on I-Ching operators," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3349–3358, 2018.

[40] Y. Zhang, J. Hao and X. Wang, "An efficient image encryption scheme based on S-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.

[41] X. Wang, P. Li, Y. Zhang, L. Liu and X. Wang, "A novel color image encryption scheme using DNA permutation based on the Lorenz system," *Multimedia Tools and Applications*, vol. 77, no. 5, pp. 6243–6265, 2018.

[42] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li *et al.,* "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Processing*, vol. 202, no. 1, pp. 728–745, 2023.

[43] L. Liu, S. Miao, H. Hu and M. Cheng, "N-phase logistic chaotic sequence and its application for image encryption," *IET Signal Processing*, vol. 10, no. 3, pp. 1096–1104, 2016.

[44] M. Wang, X. Wang, T. Zhao, C. Zhang and N. Yao, "Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme," *Information Sciences*, vol. 5, no. 4, pp. 1–24, 2020.

[45] X. Li, D. Xiao, H. Mou, D. Lu and M. Peng, "Compressive sensing based image encryption and compression algorithm with identity authentication and blind signcryption," *IEEE Access*, vol. 8, pp. 211676–211690, 2020.

[46] Z. Gan, X. Chai, J. Zhang, Y. Zhang and Y. Chen, "An effective image compression-encryption scheme based on compressive sensing (CS) and game of life (GOL)," *Neural Computing and Applications*, vol. 32, no. 17, pp. 14113–14141, 2020.

[47] X. Wang and D. Xu, "A novel image encryption scheme based on Brownian motion and PWLCM chaotic system," *Nonlinear Dynamics*, vol. 75, no. 1, pp. 345–353, 2021.

[48] X. Chai, Z. Gan, K. Yuan, Y. Lu and Y. Chen, "An image encryption scheme based on three-dimensional Brownian motion and chaotic system," *China Physics B*, vol. 26, no. 2, pp. 99–113, 2017.

[49] M. Samiullah, W. Aslam, H. Nazir, M. Lali and H. Afzal, "An image encryption scheme based on DNA computing and multiple chaotic systems," *IEEE Access*, vol. 8, pp. 25650–25663, 2020.

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

[51] X. Zhang, R. Guo, H. Chen, Z. Zhao and J. Wang, "Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes," *China Physics B*, vol. 27, no. 8, pp. 111–119, 2018.

[52] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li *et al.,* "EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory," *Information Sciences*, vol. 621, no. 1, pp. 766–781, 2023.