Wiley
Computational and Mathematical Methods
Volume 2026, Article ID 1171404, 12 pages
https://doi.org/10.1155/cmm4/1171404

WILEY

Research Article

Safe and Quickest Medical Image Encryption Using Logistic Map Derived S-Boxes and Galois Field

Mahwish Bano,[1] **Umair Habib**,[1] **Jawaid Iqbal**,[2] **Hassan Malik**,[3] **and Insaf Ullah**[4]

[1]*Department of Mathematics, Air University, Islamabad, Pakistan*
[2]*Faculty of Computing, Riphah International University, Islamabad, Pakistan*
[3]*Department of Computing Science, University of East Anglia Research Park, Norwich, UK*
[4]*Institute for Analytics and Data Science, University of Essex, Colchester, UK*

Correspondence should be addressed to Insaf Ullah; insaf.ullah@essex.ac.uk

Received 10 July 2025; Revised 27 October 2025; Accepted 23 December 2025

Academic Editor: Shibiao Wan

The pseudorandomness, simplicity of use, and extreme sensitivity to even the slightest change in the initial value and handling parameters make chaotic maps attractive. The use of medical imaging to diagnose illnesses has grown in significance. These photographs need strong security measures because they are exchanged over public networks. Several techniques have been proposed to decode medical images, but they are not widely used due to their speed and complexity. Given these problems, we suggest a new method for quickly and efficiently encrypting medical images to safeguard private medical information from adversary assaults while it is being sent. This method uses the logistic map (LM), which is the main source of inspiration for this work. A simple polynomial that is not reducible to linear components is used to construct the substitution box (S-Box). When the LM is put into practice, many point pairs are produced. One of the coordinate values is selected from each point. The Galois field (GF) is then added to that value. The finite field inverse is applied if the value is not zero; otherwise, nothing is altered. Choose any value below 256 at random. Make an S-Box using these randomly selected values. Lastly, the Exclusive-NOR (XNOR) operation between the S-Box and picture matrices was used to encrypt the medical image. High-security tests are performed to verify the reliability of the proposed technique. According to performance studies, the medical picture encryption approach based on LM and S-Boxes offers extremely secure encryption in a short period.

Keywords: Exclusive-NOR; Galois field; image encryption; irreducible polynomial; logistic map; S-Box

1. Introduction

Concerns about media transfer security have been raised by the rapid growth of online execution, social media, and communication structure in our day-to-day routine, all of which require a significant amount of data transfer over the Internet. Smartphones, for instance, are one of the sources that can simultaneously transfer and share multimedia across the Internet while taking computerized photos and videos. Scientists and users alike are concerned about the data's safe transmission [1]. Scrambling advanced pictures is a significant safety effort that can assist with safeguarding the privacy and integrity of sensitive data. When computerized pictures are sent through the Internet or kept in a device, they can be intercepted and accessed without permission [2]. By rendering the information unreadable without having an appropriate decryption key, encryption can assist in preventing unauthorized access to these images [3]. Computerized color picture enciphering is the procedure of utilizing mathematical codes to transform a color picture into an unreadable format so that its privacy can be maintained during transferring and in a repository. Utilizing a confidential key that is recognized by the shipper and recipient, the picture is transformed into an unintelligible cipher during the enciphering process. The same key is utilized in reverse for deciphering and reassembling the original picture from the cipher [4–6]. The significance of color picture enciphering becomes abundantly clear when a person thinks about

the delicate nature of numerous kinds of visual data, like medical pictures, investment deeds, and legal documents. Without encryption, those parties that are not allowed could stop or approach these pictures, which could result in the stealing of identity, investment deceit, or other malicious activity. As a result, computerized picture enciphering is a crucial tool for keeping trust in online transmissions and transactions and for safeguarding the privacy and safety of computerized assets [7, 8]. In image refining and investigation, usual metrics include the MSE, PSNR, and CC. Image encryption techniques' quality and accuracy can be evaluated using these metrics [9, 10]. MSE, PSNR, and CC can be utilized in image encryption to assess the quality and efficacy of various encryption methods. A good encryption method, for instance, ought to have a small value of MSE, a large value of PSNR, and a large value of CC. These metrics can be utilized to improve the enciphering limitations and assess how well different encryption algorithms work [11]. By and large, encrypting computerized pictures is an urgent security safety measure that can help with defending sensitive data and forestalling unapproved admittance to information [12, 13]. Several methods, including image forgery detection, watermarking, encryption, and steganography, can be used to protect image content [14]. Watermarking and steganography [15] are aimed at concealing a secret signal, image, or message in a carrier picture to convey important information or protect the owner's copyright.

The following goals are the focus of the recommended approach to digital image encryption that makes use of chaotic LM and S-Box. To develop a digital image encryption method that is simple, effective, and secure while also working with images of any size and to devise an encryption technique that is delicate to beginning circumstances and vigorous against different assaults, and direct a broad examination of the proposed strategy as far as security, quality, responsiveness, and speed.

1.1. Preliminaries. This section describes some of the fundamental security cryptosystems.

- LM

Equation (1) shows the LM.

$$Z_{k+1} = \beta \times Z_k \times (1 - Z_k), \tag{1}$$

$\beta \in [0, 4]$. $Z_{k+1} \in [0, 1]$, Z_k are the beginning values.

- GF

In mathematics, a field with a finite number of elements is called a *GF*. Likewise, with any field, a limited field is a set in which the tasks of duplication, expansion, deduction, and division are characterized and fulfill specific fundamental guidelines. The most well-known instances of finite fields are given by the numbers mod p when p is an indivisible number.

- Irreducible Polynomial

A polynomial that cannot be obtained by multiplying two polynomials is recognized as an irreducible polynomial. For example, $x^3 - 3$ is irreducible if it is regarded as a polynomial with integer coefficients.

➢ XNOR

The XNOR operator evaluates each bit of its fist operand against the bit of its second operand that corresponds to that bit. In case when both the operand bits are 0 or 1, then the corresponding bit is 1. Otherwise, the outcome is 0.

1.2. Contributions. The main contributions of this article are as follows:

- Our proposed scheme uses cutting-edge encryption techniques to improve the security of communications and medical images sent over public networks.
- Our method ensures that sensitive data is protected from these dangers since public networks are susceptible to eavesdropping, data interception, and illegal access.
- We apply image encryption by the implementation of S-Box using the LM to protect sensitive information/images from adversaries' attacks.
- The final encoding of the picture involves applying an XNOR operation between the S-Box and picture matrices.

1.3. Organizations. The remaining parts of the article are arranged as follows: The related literature is explained in Section 2. The algorithm for the development of the S-Box is explained in Section 3. The recommended method for enciphering pictures is described in Section 4. Section 5 portrays the outcomes. Section 6 contains the conclusions.

Table 1 lists the terms and their descriptions that are frequently used in the manuscript.

2. Related Works

A lot of studies have been done recently to develop a trustworthy and safe smart metering communication architecture. For instance, in [16], the authors presented the idea of image encryption by the application of a TCM along with an S-Box. In the proposed scheme, the S-Box is developed by the TCM under GF. DES, 3DES, AES, and BF are just a few of the cryptographic algorithms that have been developed [17]. An encryption strategy for a color (RGB) picture, including Markov lattices and a tumultuous guide, is introduced in [18]. The picture is passed through a chaotic guide, which is utilized as a key to shuffle the pixels of another picture. Ye et al. [19] have proposed a brand-new hyperchaotic chaotic system. Compressive sensing is used to compress the images first, and a public key elliptic curve enciphering code is utilized to encipher the compressed picture. Encryption times for multiple images can be cut down thanks to the proposed algorithm's ability to encrypt two images simultaneously.

TABLE 1: Notation guide.

Notation	Description
MSE	Mean square error
PSNR	Peak signal-to-noise ratio
CC	Correlation coefficient
XNOR	Exclusive-NOR
S-Box/s	substitution box
GF	Galois field
TCM	Trigonometric chaotic map
DES	Data encryption standard
3DES	Triple data encryption standard
AES	Advanced encryption standard
BF	Blow fish
ODE	Ordinary differential equation
TM	Tent map
LM	Logistic map
LSM	Logistic–Sine map
LCM	Logistic–Chebyshev map
HSM	Henon–Sine map
DNA	Deoxyribonucleic acid
n	Highest power of irreducible polynomial
β	Control parameters of the logistic map
z	x-coordinate of pair (z, b)
f	Frequency
R	Rank

Chaos-based encryption codes are frequently used because it is required to handle large sets of information and safeguard them. They offer good security, great throughput, an enormous key space, irregularity, and resistance to beginning constraints, making them an excellent option for encryption calculations [8]. A new approach for enciphering three-dimensional point and mesh information in edge computing with tumultuous guides was suggested in [20]. By utilizing the chaotic dynamics of a chaotic map, the suggested approach generates a string of pseudorandom numerals that serve as the enciphering key. The encryption standard, time complexity, and resistance to attacks of the method were evaluated on the three-dimensional point and mesh data [21]. A cryptosystem dependent on TCM and XOR of an image is proposed in [22]. The authors of [7] suggested a color picture encrypting code that is completely safe and quick. Hyperchaotic maps and S-Box are utilized by the algorithm to give rise to the enciphering key and carry out the enciphering operation. Hyperchaotic maps are implemented to generate the string of pseudorandom integers that will act as the enciphering code, and an S-Box is implemented to replace the pixel values in the initial picture.

The authors in [23] propose the use of the Markov matrix to conceal textual or visual information in the solution of nonlinear ODEs like Rossler and Lorenz. The authors of [24] suggested a medical image encryption scheme based on the chaotic tent map along with the blockchain technology (BCTMES). They have utilized the properties of blockchain to secure image data from adversary attacks. In [25], the authors presented a procedure for scrambling pictures that uses tumultuous and LM in three aspects. They suggested combining an LM and a three-dimensional tumultuous map to create two chaotic strings that join and extend across the picture. An algorithm for using a chaotic system based on the cosine transform to encrypt a picture was presented in [26]. The LM is utilized to develop an arbitrary string, and a 4D chaotic guide is utilized to develop a confidential key in the suggested strategy. A cosine transform is utilized to combine the picture with the chaotic map. In [27], the authors presented a new encryption method for medical photos that combines DNA coding with integer wavelet transform (IWT). The plan seeks to maximize cloud storage and transmission speed while maintaining the privacy of medical images.

Alanezi et al.'s proposed algorithm [28] uses two turbulent guides: The original picture is permuted with a Logistic–Sine map (LSM), and the resulting permuted picture is replaced with a Logistic–Chebyshev map (LCM). The cipher picture is then produced by the algorithm by performing an XOR function on the substituted picture and cascading the two. Ghazvini et al. [29] have suggested a genetic algorithm-based hybrid mechanism for the encryption of pictures. Chen's chaos map was utilized in the confusion process, whereas the LSM was utilized in the diffusion phase. A genetic algorithm is utilized to improve the encrypted picture after that. A picture encryption strategy has altered the value of the pixels by utilizing a chaotic LM and a genetic algorithm to reduce the correlation between neighboring pixels [30]. Alghafis et al. [31] developed a picture-enciphering scheme that depends on DNA and chaotic sequencing. By the utilization of logistics, Henon and Lorenz's chaotic systems, irregular strings are made. The chaotic systems are then combined with DNA computations to produce confusion and diffusion in the pixels.

By using a memristor, the authors of [32] present a new 4D memristive hyperchaotic map (4D-MHM), which increases the original map's complexity. The 4D-MHM can produce extremely unpredictable chaotic sequences appropriate for encryption schemes since it has complicated dynamical behavior and a broad range of chaotic parameters, according to dynamical analysis and randomness tests. The authors of [33] argue that the chosen plaintext attack that was launched over the scheme in [32] cracked it, making it less secure than claimed. The authors of [34] offer a three-tiered encryption technique that combines a chaotic fractal picture encryption scheme with innovative blockchain technology. For increased unpredictability and security, the encryption process uses a diffusion step based on a Chebyshev map, fractal-based key generation using a logistic map-driven Sierpinski triangle, and an S-Box created from the May map for pixel substitution.

3. Recommended S-Box Algorithm

In this segment, we explained the method of development of the S-Box over GF. We developed several 8×8 S-Boxes utilizing the LM over GF(2^8).

TABLE 2: S-Box developed by Logistic Map over GF(2^8).

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

Input: Irreducible polynomial of highest power 8 with $c \in GF(2^8) - \{0\}$.
Output: S-Box.
1. $C = \{\}$
2. *for* each $x \in S$ do.
3. *for* each $y \in S$ do
4. $w_k = z$
5. $w_{k+1} = b$
6. if $Z_{k+1} = \beta \times z_k \times (1 - z_k)$ then
7. $x = w_k$
8. $y = w_{k+1}$
9. $C = C \cup \{x, y\}$.
10. *end*
11. *end*
12. *end*
13. D ⟵1st value of pairs from C.
14. m⟵1 : 256.
15. *if* $D(m) \longleftarrow 0$ *then*
16. unchanged
17. *else* find inverse under $GF(2^8)$
18. *end*

Algorithm 1: Development of S-Box by LM over GF($2^{8\cdot}$).

3.1. Development of S-Box by Implementing LM Over GF(2^8) . The $GF(2^8)$ of order 256 is implemented in this research to organize a more extensive and productive strategy for the development of an enormous amount of unique 8×8 S-Boxes.

3.1.1. Development of S-Box Utilizing LM Over GF(2^8). Select a simple multinomial:

$$f(y) = y^8 + y^4 + y^3 + y^2 + 1. \tag{2}$$

Any multinomial of the highest power 8 with coefficients from the binary field could be selected over the binary field. Select the LM given by Equation (1).

$$Z_{k+1} = \beta \times Z_k \times (1 - Z_k). \tag{3}$$

Whenever we pick LM over GF (2^8), the number of parts in light of it is $2^8 + 1$, along with the point toward the end. In addition, we observe that when this guide is selected over GF (2^8), reiteration is gathered in b-values, and there is no obvious reiteration in the x-values. The fact that this guide has 256 distinct sets of components (x and y), except the point at which it reaches a vastness greater than GF (2^8), is its power. Our necessity of creating an 8×8 S-Box with 256 particular values is satisfied by considering the x-directions of each arranged set of focuses because there is no

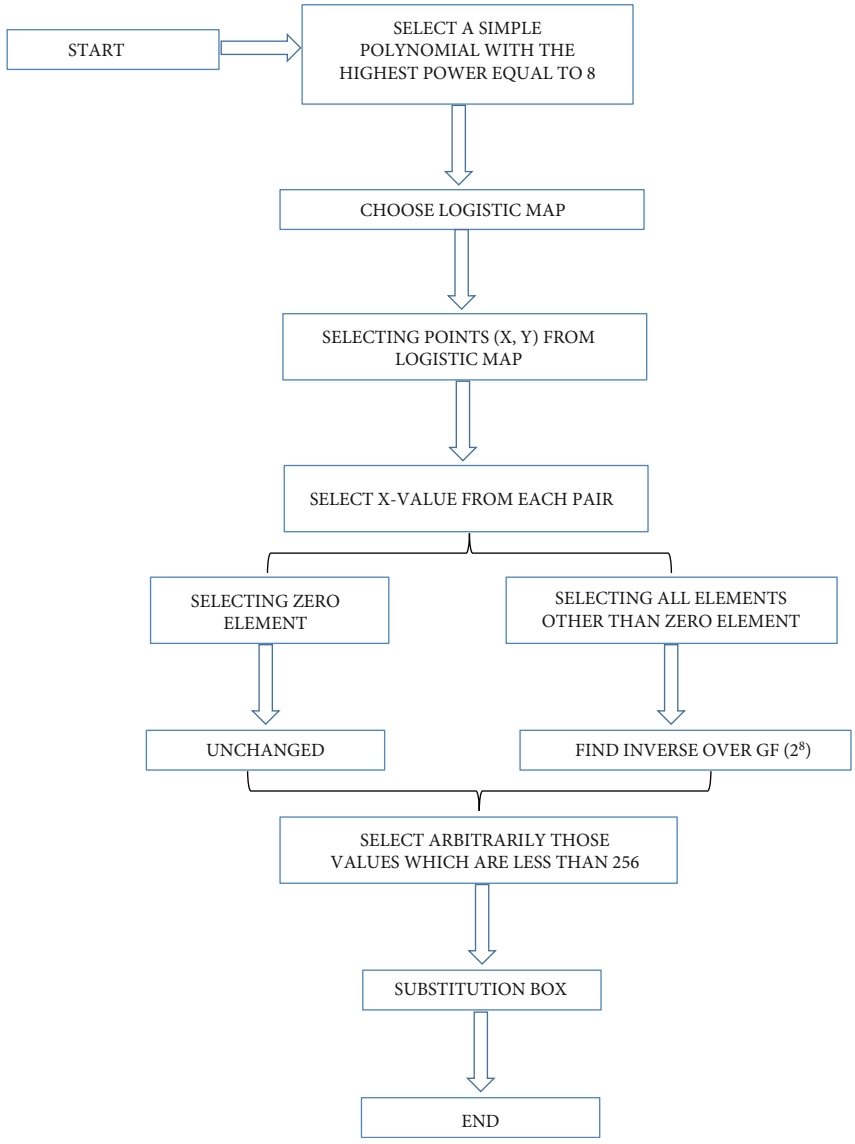

Figure 1: Recommended S-Box scheme based on Logistic Map over GF(2^8).

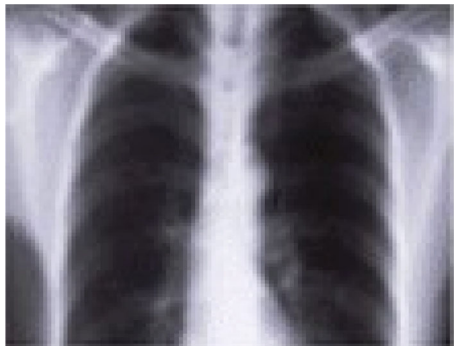

Figure 2: Chest X-ray image.

reiteration in the x-organizes component, providing us with perfect 256 components. Implement inverse function under GF(2^8) on each element of x-coordinate other than zero elements with a simple polynomial as stated in Equation (2). In the end, we created an S-Box possessing a nonlinearity of 112, which is provided in Table 2.

The following Algorithm 1 describes the steps for developing the S-Box using the LM.

4. Proposed Image Encryption Strategy

The recommended picture encryption procedure's steps are summarized below. The actual picture's dimensions are thought to be X by Y.

- As a starting step, reduce the original image's size to 128 by 128 pixels.
- A random picture of the initial picture dimension can be utilized for dispersion operations.

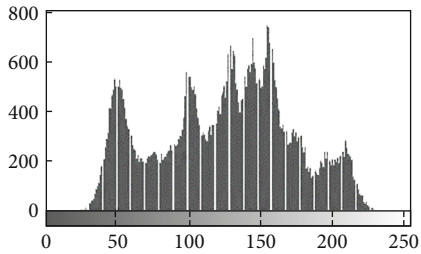

Figure 3: Histogram of original chest X-ray image.

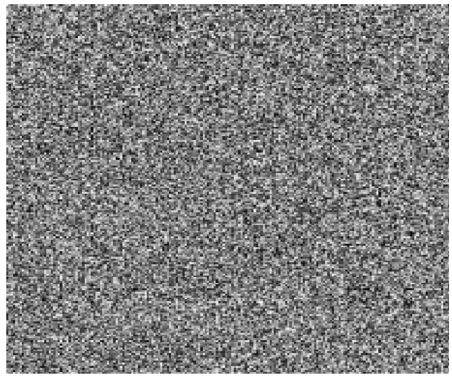

Figure 4: Enciphered chest X-ray image.

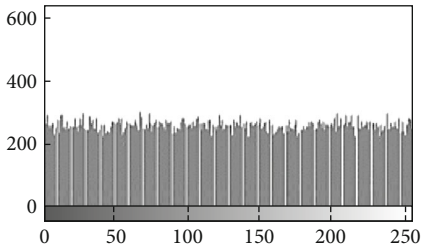

Figure 5: Histogram of enciphered chest X-ray image.

Figure 6: Hand X-ray image.

- Next, the original and random pictures are partitioned into blocks where all the blocks' dimensions are set as $K \times K$ pixels.

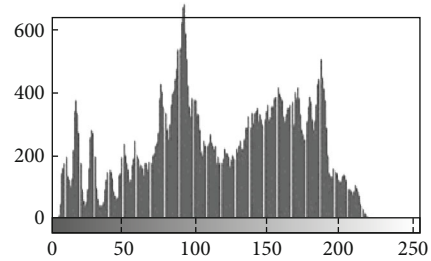

Figure 7: Histogram of original hand X-ray image.

- The formula shown in Equation (4) can be used to calculate "K":
  -

$$K = \frac{\sqrt{X \times Y}}{c^2}. \tag{4}$$

- Every block of real and arbitrary pictures goes through the steps listed below.
  a. A line vector is created by altering the blocks of the real and random pictures. Implement XNOR on a line vector of the real and arbitrary picture to acquire a new line vector.
  b. A line vector having measurement $(1, K \times K)$ is acquired by utilizing the LM to generate pseudorandom numbers. To reorganize the row vector's pixel areas, the generated values are used as pixel location files.
  c. Equation (5) alters the pixel intensity approximation of the disorganized line vector derived from the final step.

$$A = \text{Sin}\,(A + c) + A, \tag{5}$$

where "A" is a key stream that was created with the help of the LM and c is the acquired line vector that was created by using the XNOR operation on the real and arbitrary line vectors from the previous step.

  d. To form the enciphered picture, the final row vector is transformed into a block having dimension $K \times K$ pixels and saved. Finally, the XNOR operation between picture matrices and the S-Box is used for encryption.

The use of XNOR instead of XOR in the diffusion stage introduces a complementary and nonlinear transformation that strengthens the cipher's confusion and diffusion properties. Because XNOR is the bitwise complement of XOR $(A \odot B = \overline{A \oplus B})$, it disrupts the linearity of conventional XOR-based diffusion, enhancing resistance against linear and differential attacks. Additionally, XNOR contributes to balanced bit flipping, improving statistical uniformity and

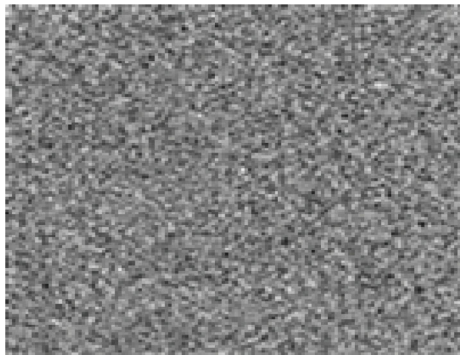

Figure 8: Enciphered hand X-ray image.

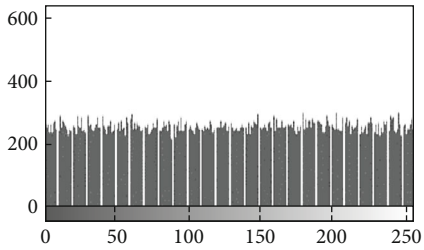

Figure 9: Histogram of enciphered hand X-ray image.

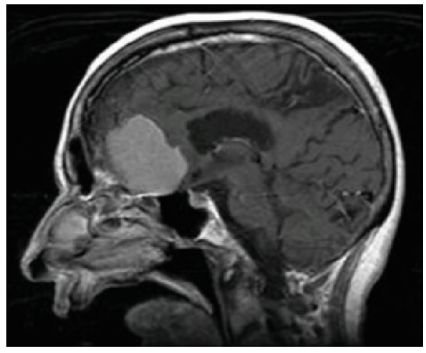

Figure 10: MRI image.

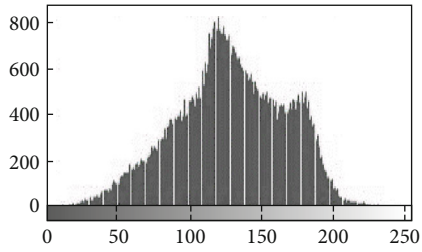

Figure 11: Histogram of the original MRI image.

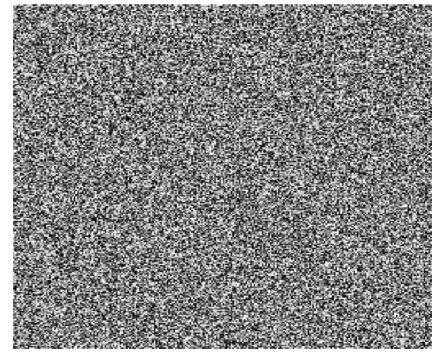

Figure 12: Enciphered MRI image.

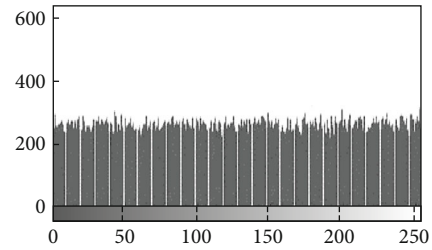

Figure 13: Histogram of enciphered MRI image.

TABLE 3: NIST statistical experimental outcomes for 100 key streams.

Statistical test	p	Proportion
f	0.509020	0.99
Block frequency	0.192501	0.93
Cumulative sums (forward)	0.799453	0.98
Cumulative sums (reverse)	0.305109	0.99
Runs	0.00001	0.78
Longest runs of one	0.000895	0.96
R	0.967835	0.97
Non-periodic-templates	0.898139	0.99
Overlapping-templates	0.395326	0.97
Approximate entropy	0.026989	0.98
Random-excursions	0.544631	0.99
Random-excursions-variant	0.213991	0.99
Linear-complexity	0.494729	0.97
Serial 1	0.699195	0.99
Serial 2	0.499550	0.98

diffusion performance (e.g., net pixel conversion rate [NPCR] and average changing intensity [UACI]).

Figure 1 represents a flowchart of the recommended scheme for the development of the S-Box by LM.

The proposed S-Box construction, based on the Logistic Map over GF(2^8), differs significantly from existing chaotic S-Box generation methods reported in [7, 16, 28]. In prior works, the Logistic Map is typically employed as a source of pseudorandom sequences or control parameters without directly influencing the finite-field substitution process. In contrast, the present design integrates the Logistic Map sequence directly into the S-Box generation over GF(2^8), thereby embedding the nonlinear and ergodic dynamics of chaos within the substitution structure itself. This approach enhances nonlinearity, diffusion, and key-dependency, resulting in an S-Box with superior cryptographic metrics. Furthermore, by varying the control parameter (β) and initial condition (Z_k), multiple key-dependent S-Boxes can be

TABLE 4: Enciphering–deciphering time and total time needed for implementation of the technique on different images of size 128×128 and 512×512.

Picture	Enciphering time (s)		Deciphering time (s)		Total time (s)		Scheme [35]
Dimension	128×128	512×512	128×128	512×512	128×128	512×512	512×512
Chest X-ray	1.22	2.24	1.06	1.92	2.28	4.16	4.5477
Hand X-ray	1.34	2.3	1.18	2.16	2.52	4.46	4.5204
MRI	1.27	2.34	1.10	2.01	2.37	4.35	—

TABLE 5: Outcomes of the correlation coefficient values.

Image	Components	Horizontal	Vertical	Diagonal
Chest X-ray	Original (grayscale)	0.9482	0.9687	0.9166
	Encrypted	−0.0009	0.0059	−0.0028
Hand X-Ray	Original (grayscale)	0.9405	0.9535	0.9003
	Encrypted	0.0001	0.0179	0.0063
MRI	Original (grayscale)	0.8965	0.8995	0.8145
	Encrypted	0.0079	0.0303	0.0022

TABLE 6: Comparison of the correlation coefficient values with existing schemes.

	Proposed scheme	Scheme [36]	Scheme [37]	Scheme [38]	Scheme [39]	Scheme [40]
Horizontal Correlation	−0.0009	−0.0012	0.0027	0.0023	0.0944	0.0098
Vertical correlation	0.0059	0.0099	0.0015	−0.0010	0.0057	−0.0078
Diagonal correlation	−0.0028	−0.0032	0.0019	0.0009	0.0067	0.0181

TABLE 7: Enciphered picture entropy value.

	Original image	Encrypted image
Chest X-ray	7.0097	7.9927
Hand X-Ray	7.1025	7.9972
MRI	7.2685	7.9973

generated, significantly increasing unpredictability and resilience against linear, differential, and algebraic cryptanalysis.

5. Results and Discussion

This portion summarizes several security analysis findings. The output of the algorithm after the application of the encoding and decoding steps is shown. The system specifications that are used for simulation purposes are as follows: The hardware consists of an Intel Core i3-1005G1 CPU with a processor speed of 1.2 GHz with 6 GB of RAM and MATLAB 2019a version. The grayscale image of the chest X-ray and hand X-ray is used to test whether the suggested method for encryption of the medical image works. MATLAB is used to put the proposed encryption method into action. As shown in Figure 2, the image of a chest X-ray is utilized for testing. Figure 3 depicts the chest X-ray nonuniform histogram.

To determine "K" in Equation (4), the parameter "c" is set to four, resulting in a 16×16 block. The enciphered picture of the chest X-ray that was acquired following the execution of the recommended picture-enciphering procedure is depicted in Figure 4. Figure 5 displays the enciphered chest X-ray image's histogram.

The original image of the hand X-ray is shown in Figure 6, and its histogram is shown in Figure 7. Figure 8 shows the enciphered image of the hand X-ray, and Figure 9 displays the histogram of the enciphered image of the hand X-ray.

The original MRI image is shown in Figure 10, and its histogram is shown in Figure 11.

Figure 12 shows the enciphered MRI image and Figure 13 displays the histogram of the enciphered MRI image.

Table 3 displays the NIST statistical experimental outcomes for 100 key streams of dimension 200,000 pieces developed by LM, each developed by LM for control parameter $\beta = 3.97$ and an arbitrarily selected beginning value.

MATLAB programs are repeatedly applied to various images. The recommended technique's time to encipher and decipher pictures of various dimensions has been determined. Table 4 displays the results. Additional experiments were carried out on numerous medical images of different dimensions to guarantee the suggested encryption algorithm's generalizability. The algorithm's robustness was confirmed by the statistical analysis of major performance metrics (entropy, correlation coefficient, NPCR, and UACI), which produced consistent results across datasets.

This demonstrates the enciphering technique's resistance to histogram attacks. The immunity of encryption against

TABLE 8: Comparison of the entropy values with existing schemes.

	Proposed scheme	Scheme [36]	Scheme [37]	Scheme [38]	Scheme [39]	Scheme [40]
Entropy	7.9927	7.9090	7.9926	7.9900	4.7450	7.9993

TABLE 9: Enciphered picture's NPCR and UACI values.

Proposed algorithm	NPCR	UACI
Chest X-ray	99.6033	33.460
Hand X-Ray	99.6094	33.312
MRI	99.6140	33.487

TABLE 10: Comparison of the enciphered picture's NPCR and UACI values.

	Proposed scheme	Scheme [36]	Scheme [37]	Scheme [38]	Scheme [39]	Scheme [40]
NPCR	99.6033	99.610	99.532	99.51	99.79	99.6067
UACI	33.4600	33.261	33.450	33.39	33.16	33.4954

brute force attacks is also the subject of investigation. According to the literature [36], an encryption algorithm should have a complexity of $O(2^{128})$ to be sufficiently secure against brute force attacks. The trial results demonstrate that the suggested enciphering strategy is complex in order $O(2^{130})$. The high correlation between neighboring picture pixels is studied in terms of encryption immunity. Consequently, Equation (6) below can work out the flat, vertical, and corner relationships between any adjacent pixels.

$$r = \frac{2\sum_{i=1}^{2}(x_i, y_i) - \sum_{i=1}^{2} x_i \sum_{i=1}^{2} y_i}{\sqrt{\left(2\sum_{i=1}^{2} x_i^2 - \left(\sum_{i=1}^{2} x_i\right)^2\right)\left(2\sum_{i=1}^{2} y_i^2 - \left(\sum_{i=1}^{2} y_i\right)^2\right)}}, \quad (6)$$

where the "correlation coefficient" is denoted by "r". One thousand one next to the other pixels chosen aimlessly to work out the flat, vertical, and corner-to-corner connection. Table 5 displays the correlation coefficient values of the original and encrypted images using the proposed image encryption technique. The closer two neighboring pixels' correlations are to 0, the smaller their correlations. Based on simulation studies, the correlation in all three directions is practically nil as Table 5 illustrates, demonstrating that the cryptographic method described in this study has almost no correlation. Additionally, the results show that the scrambled image's pixel-to-pixel relationship is extremely poor. Table 6 presents a comparison of the correlation coefficient values of our proposed scheme with existing schemes.

Also, entropy is used to figure out how much randomness is in a picture. The outcomes presented in Table 7 endorse that the original picture's entropy value is quite small, whereas the scrambled image yields high entropy values. Entropy's ideal value is 8. The recommended image encryption method's robustness against entropy attacks is demonstrated by the fact that its entropy value is close to the ideal value, which is 8. The entropy is calculated by using the formula mentioned in Equation (7).

$$H(\mathrm{y}) = -\sum_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{g}(\mathrm{y}) \times \log_2 \mathrm{g}(\mathrm{y_i}). \quad (7)$$

The gained semi-unvaried histogram, statistical correlation, and entropy values demonstrate the recommended method's greater permutation and replacement properties. Table 8 presents a comparison of the entropy values of our proposed scheme with existing schemes.

The distinctive analysis is another name for plaintext susceptibility analysis in cryptography. To test the effectiveness of performing single pixel conversion in both plain and encrypted images, we use the Net Pixel Conversion Rate (NPCP) and dissimilarity in the middle of plain and encrypted images with Unified Average Changing Intensity (UACI). The mathematical expressions shown in (8) and (9) can be used to express both indices.

$$NPCR = \frac{\sum_{i,j} K(i,j)}{w \times h} \times 100, \quad (8)$$

$$UACI = \frac{1}{w \times h}\left[\sum_{i,j} \frac{\left|X(i,j) - X'(i,j)\right|}{255}\right] \times 100, \quad (9)$$

where "h" and "w" in the presented mathematical expression indicate the height and width of the ciphered image, respectively. X' represents a single pixel change in the plain image, where X ciphered image. If $X \neq X'$, $K(i,j) = 1$; else $K(i,j) = 0$. The accurate values of UACI and NPCR must be reached to make them impervious to differential attacks. Table 9 compares the results of the ciphered picture of the chest X-ray from the NPCR and UACI. It indicates that the current cryptosystem performs well for both values. The current cryptosystem offers a stronger defense against "Known Plain-text Attack" and "Chosen Plain-text Attack" in this instance. The findings, therefore, demonstrate that the plaintext sensitivity of our suggested technique is good.

Table 10 presents a comparison of the NPCR and UACI values of our proposed scheme with existing schemes.

6. Conclusion

In this work, we laid out a safer picture cryptosystem depending on the LM and XNOR of an irregular picture with S-Boxes (created by LM). We used a basic turbulent guide to make the encryption safer and more resistant and to develop a line vector of the real and arbitrary picture. The disarray and dispersion are obtained in a succession-wise methodology like XNOR fosters a line vector, which furthermore carries out the LM, bringing about the state of the encoded picture, which is moreover encoded by taking XNOR with S-Boxes. The technique's security is tested frequently, and the results have been achieved and demonstrated. Although chaotic systems such as the Logistic map exhibit idealized randomness in theory, their behavior degrades under finite-precision arithmetic due to quantization effects. In the proposed scheme, this issue is mitigated by using double-precision computation and $GF(2^8)$-based mapping, which together preserve long periodicity and maintain the unpredictability required for secure S-Box generation.

The NIST measurable test suite tentatively approves that the produced keystreams hold arbitrary conduct, making the recommended method reasonable for cryptographic applications. The findings of the experiments indicate resistance to entropy and brute force attacks. The results also show that the recommended picture encryption method has better substitution and permutation properties.

In addition to evaluating the security performance, it is also essential to consider the applicability of the proposed approach in clinical environments. The suggested encryption technique has been developed as a modular and format-independent framework that can be added to medical image standards like DICOM in the future, even though it is not yet directly integrated with them. To further its usefulness in clinical and bioinformatics settings, future research will concentrate on incorporating this encryption module into picture archiving and communication systems (PACS) and DICOM-based medical imaging workflows.

Data Availability Statement

Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Conflicts of Interest

The authors declare no conflicts of interest.

Author Contributions

Mahwish Bano: formal analysis, supervision. Umair Habib: writing review and original draft, code preparation, result analysis. Jawaid Iqbal: results verification. Hassan Malik: results verification and writing review draft Insaf Ullah: results analysis.

Funding

No funding was received for this manuscript.

Acknowledgements

No AI-based software is used for the preparation of the manuscript. No third-party services were involved in the research or manuscript preparation.

References

[1] B. Rezaei, H. Ghanbari, and R. Enayatifar, "An Image Encryption Approach Using Tuned Henon Chaotic Map and Evolutionary Algorithm," *Nonlinear Dynamics* 111 (2023): 9629–9647, https://doi.org/10.1007/s11071-023-08331-y.

[2] K. Sirikantisophon, M. Bano, and T. Panityakul, "Image Encryption Using Quantum Spinning and Trigonometric Chaotic Map," *Songklanakarin Journal of Science & Technology* 44, no. 4 (2022): 1000–1007.

[3] H. Arora, G. K. Soni, R. K. Kushwaha, and P. Prasoon, "Digital Image Security Based on the Hybrid Model of Image Hiding and Encryption," in *2021 6th International Conference on Communication and Electronics Systems (ICCES)* (IEEE, 2021), 1153–1157, https://doi.org/10.1109/ICCES51350.2021.9488973.

[4] M. Abu-Faraj, A. Al-Hyari, I. Altaharwa, Z. Alqadi, and B. J. A. Ali, "Increasing the Security of Transmitted Text Messages Using Chaotic Key and Image Key Cryptography," *International Journal of Data and Network Science* 7 (2023): 809–820, https://doi.org/10.5267/j.ijdns.2023.1.008.

[5] M. Abu-Faraj, A. Al-Hyari, B. Al-Ahmad, Z. Alqadi, and A. Alhaj, "Building a Secure Image Cryptography System Using Parallel Processing and Complicated Dynamic Length Private Key," *Applied Mathematics & Information Sciences (AMIS)* 16, no. 6 (2022): 1017–1026, https://doi.org/10.18576/amis/160619.

[6] A. Khan, A. Chefranov, and H. Demirel, "Image-Level Structure Recognition Using Image Features, Templates, and Ensemble of Classifiers," *Symmetry* 12 (2020): https://doi.org/10.3390/sym12071072.

[7] Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, et al., "Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map," *IEEE Access* 10 (2022): 26257–26270, https://doi.org/10.1109/ACCESS.2022.3151174.

[8] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach," *Journal of Imaging* 8, no. 6 (2022): https://doi.org/10.3390/jimaging8060167.

[9] M. Abu-Faraj, A. Al-Hyari, and Z. Alqadi, "A Complex Matrix Private Key to Enhance the Security Level of Image Cryptography," *Symmetry* 14, no. 4 (2022): 664–677, https://doi.org/10.3390/sym14040664.

[10] M. Abu-Faraj, K. Aldebei, and Z. Alqadi, "Simple, Efficient, Highly Secure, and Multiple Purposed Method on Data Cryptography," *Traitement du Signal* 39, no. 1 (2022): 173–178, https://doi.org/10.18280/ts.390117.

[11] M. Abu-Faraj, A. Al-Hyari, I. Al-Taharwa, B. Al-Ahmad, and Z. Alqadi, "CASDC: A Cryptographically Secure Data System Based on Two Private Key Images," *IEEE Access* 10 (2022): 126304–126314, https://doi.org/10.1109/ACCESS.2022.3226319.

[12] D. Ibrahim, K. Ahmed, M. Abdallah, and A. A. Ali, "A New Chaotic-Based RGB Image Encryption Technique Using a Nonlinear Rotational 16×16 DNA Play Fair Matrix," *Cryptography* 6 (2022): https://doi.org/10.3390/cryptography6020028.

[13] R. J. Rasras, M. Abuzalata, Z. Alqadi, J. Al-Azzeh, and Q. Jaber, "Comparative Analysis of Color Image Encryption-Decryption Methods Based on Matrix Manipulation," *International Journal of Computer Science and Mobile Computing* 8 (2019): 14–26.

[14] A. A. Khan, M. Qiyas, S. Abdullah, J. Luo, and M. Bano, "Analysis of Robot Selection Based on 2-Tuple Picture Fuzzy Linguistic Aggregation Operators," *Mathematics* 7 (2019): https://doi.org/10.3390/math7101000.

[15] N. Soliman, M. Khalil, A. Algarni, S. Ismail, and R. Marzouk, "Efficient HEVC Steganography Approach Based on Audio Compression and Encryption in QFFT Domain for Secure Multimedia Communication," *Multimedia Tools and Applications* 80, no. 3 (2021): 4789–4823, https://doi.org/10.1007/s11042-020-09881-8.

[16] R. Chinram, M. Bano, U. Habib, and P. Singavananda, "Highly Secured and Quickest Image Encryption Algorithm Based on Trigonometric Chaotic Map and S-Box," *Soft Computing* 27, no. 16 (2023): 11111–11123, https://doi.org/10.1007/s00500-023-08493-2.

[17] A. Labao and H. Adorna, "A CCA-PKE Secure-Cryptosystem Resilient to Randomness Reset and Secret-Key Leakage," *Cryptography* 6, no. 1 (2022): https://doi.org/10.3390/cryptography6010002.

[18] T. Panityakul, M. Bano, T. M. Shah, and D. Prangchumpol, "An RGB Color Image Double Encryption Scheme," *International Journal of Mathematics and Computer Science* 17, no. 1 (2022): 183–194.

[19] G. Ye, M. Liu, and M. Wu, "Double Image Encryption Algorithm Based on Compressive Sensing and Elliptic Curve," *Alexandria Engineering Journal* 61, no. 9 (2022): 6785–6795, https://doi.org/10.1016/j.aej.2021.12.023.

[20] K. R. Raghunandan, R. Dodmane, K. Bhavaya, N. S. K. Rao, and A. K. Sahu, "Chaotic-Map Based Encryption for 3D Point and 3D Mesh Fog Data in Edge Computing," *IEEE Access* 11 (2023): 3545–3554, https://doi.org/10.1109/ACCESS.2022.3232461.

[21] H. Jin, S. Ashraf, S. Abdullah, M. Qiyas, M. Bano, and S. Zheng, "Linguistic Spherical Fuzzy Aggregation Operators and Their Applications in Multi-Attribute Decision Making Problems," *Mathematics* 7, no. 5 (2019): https://doi.org/10.3390/math7050413.

[22] O. Thinnukool, T. Panityakul, and M. Bano, "Double Encryption Using Trigonometric Chaotic Map and XOR of an Image," *Computers, Materials & Continua* 69, no. 3 (2021): 3033–3046, https://doi.org/10.32604/cmc.2021.019153.

[23] M. Bano, S. Abdullah, T. M. Shah, T. Panityakul, and R. Chinram, "An Extended Image Encryption With MARKOV Processes in Solutions Images Dynamical System of Non-Linear Differential Equations," *Journal of Mathematical and Computational Science* 10, no. 6 (2020): 2191–2207, https://doi.org/10.28919/jmcs/4833.

[24] U. Shahid, S. Kanwal, M. Bano, S. Inam, M. E. M. Abdalla, and Z. A. Shaikh, "Blockchain Driven Medical Image Encryption Employing Chaotic Tent Map in Cloud Computing," *Scientific Reports* 15, no. 1 (2025): 1–23, https://doi.org/10.1038/s41598-025-90502-5.

[25] P. He, K. Sun, and C. Zhu, "A Novel Image Encryption Algorithm Based on the Delayed Maps and Permutation-Confusion-Diffusion Architecture," *Security and Communication Networks* 2021 (2021): 6679288, https://doi.org/10.1155/2021/6679288.

[26] L. M. H. Yepdia, A. Tiedeu, and G. Kom, "A Robust and Fast Image Encryption Scheme Based on a Mixing Technique," *Security and Communication Networks* 2021 (2021): 6615708, https://doi.org/10.1155/2021/6615708.

[27] Q. Lai and H. Hua, "Secure Medical Image Encryption Scheme for Healthcare IoT Using Novel Hyperchaotic Map and DNA Cubes," *Expert Systems with Applications* 264 (2025): https://doi.org/10.1016/j.eswa.2024.125854.

[28] A. Alanezi, B. Abd-El-Atty, H. Kolivand, et al., "Securing Digital Images Through Simple Permutation-Substitution Mechanism in Cloud-Based Smart City Environment," *Security and Communication Networks* 2021 (2021): 6615512, https://doi.org/10.1155/2021/6615512.

[29] M. Ghazvini, M. Mirzadi, and N. Parvar, "A Modified Method for Image Encryption Based on Chaotic Map and Genetic Algorithm," *Multimedia Tools and Applications* 79, no. 37 (2020): 26927–26950, https://doi.org/10.1007/s11042-020-09058-3.

[30] S. Noshadian, A. Ebrahimzade, and S. J. Kazimitabar, "Breaking a Chaotic Image Encryption Algorithm," *Multimedia Tools and Applications* 79, no. 35 (2020): 25635–25655, https://doi.org/10.1007/s11042-020-09233-6.

[31] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool, and M. Amin, "An Efficient Image Encryption Scheme Based on Chaotic and Deoxyribonucleic Acid Sequencing," *Mathematics and Computers in Simulation* 177 (2020): 441–466, https://doi.org/10.1016/j.matcom.2020.05.016.

[32] Q. Lai, H. Wang, X.-W. Zhao, and M. Ahmed, "Shuffle Medical Image Encryption Scheme Based on 4D Memristive Hyperchaotic Map," *Nonlinear Dynamics* 113 (2025): 12289–12307, https://doi.org/10.1007/s11071-024-10692-x.

[33] J. Chen, L. Chen, and Y. Zhou, "Cryptanalysis of a DNA-Based Image Encryption Scheme," *Information Sciences* 520 (2020): 130–141, https://doi.org/10.1016/j.ins.2020.02.024.

[34] S. Inam, S. Kanwal, M. Batool, S. Al-Otaibi, and M. M. Jamjoom, "A Blockchain-Integrated Chaotic Fractal Encryption Scheme for Secure Medical Imaging in Industrial IoT Settings," *Scientific Reports* 15, no. 1 (2025): https://doi.org/10.1038/s41598-025-89604-x.

[35] J. Chandrasekaran and S. J. Thiruvengadam, "A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images," *Security and Communication Networks* 2017 (2017): 6729896, https://doi.org/10.1155/2017/6729896.

[36] C. Paar, *Understanding Cryptography: A Textbook for Students and Practitioners* (Springer, 2014).

[37] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A Novel Image Encryption Scheme Based on DNA Sequence Operations and Chaotic Systems," *Neural Computing and Applications* 31, no. 1 (2019): 219–237, https://doi.org/10.1007/s00521-017-2993-9.

[38] X. Wang and C. Liu, "A Novel and Effective Image Encryption Algorithm Based on Chaos and DNA Encoding," *Multimedia Tools and Applications* 76, no. 5 (2017): 6229–6245.

[39] S. Kumar, B. Panna, and R. Kumar, "Medical Image Encryption Using Fractional Discrete Cosine Transform With Chaotic Function," *Medical & Biological Engineering &*

Computing 57, no. 11 (2019): 2517–2533, https://doi.org/10.1007/s11517-019-02037-3.

[40] M. Chen, G. Ma, C. Tang, and Z. Lei, "Generalized Optical Encryption Framework Based on Shearlets for Medical Image," *Optics and Lasers in Engineering* 128 (2020): https://doi.org/10.1016/j.optlaseng.2020.106026.