Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A Grayscale image encryption using cubic fractional transformation and logistic map

Abdul Qadeer

abdulqadeer00478@gmail.com

Capital University of Science and Technology

Rashid Ali

Capital University of Science and Technology

Tahir Sajjad Ali

National University of Modern Languages

Research Article

Keywords: Image encryption, Logistic map, S-box, CFT, Random sequences

Posted Date: July 22nd, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10125592/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A grayscale image encryption scheme using cubic fractional transformation and logistic map

Abdul Qadeer[a,*], Rashid Ali[b] [†] and Tahir Sajjad Ali[c] [‡]

[a] *National Testing Service - Pakistan (NTS)*

[b] *Department of Mathematics,Capital University of Science and Technology, Islamabad, Pakistan*

[c] *Department of Mathematics National University of Modern Languages, Islamabad, Pakistan*

Abstract

The study of image encryption has grown popularity and interest in the modern technological era. Image encryption techniques ensures the secure transmission of images by converting recognizable form into unrecognizable ones. A new grayscale image encryption method based on Substitution-box (S-box) and Logistic map is proposed. First of all, an S-box is generated with the help of the cubic fractional transformation (CFT). Then, two random sequences produced by CFT are used to further diffuse these modified values. Finally, the pre-encrypted image components are subjected to the scrambling process using the `XOR` Boolean operation and random sequences created by the logistic map to produce the encrypted image. The S-box and Logistic map based scheme is particularly well-suited for key space analysis, key sensitivity analysis, NPCR, UACI, correlation coefficients, entropy analysis and histogram in image encryption.

Keywords: Image encryption, Logistic map, S-box, CFT, Random sequences.

1 Introduction

In the modern era, the rapid evolution of information technology, necessitate methods for the protection of data especially containing images. A reliable and secure data storage system is required to ensure that sensitive information remains private and confidential. Image encryption is a technique for protecting private image-based information from unauthorized sources. The digital image is changed in such a way that it cannot be directly viewed and has completely differed from the original image. If the image is desired to viewed, it must be changed back to its original form with the help of decryption algorithm.In cryptography, the methods for protecting information generally include an algorithm and a key. There are two primary categories of image encryption techniques: symmetric key encryption and asymmetric key encryption [30]. The data is encrypted and decrypted using the same key in symmetric key encryption. To overcome the risk involved during in sharing the key in symmetric key encryption. Diffie and Hellman in 1976 introduced the asymmetric key encryption [14]. They show that it is possible to create a mathematical function that can easy to compute in one direction, but extremely difficult to compute in other direction, unless you had a special piece of information called the "trapdoor". They used this function to generate a pair of keys. For the encryption and decryption of the data in asymmetric key encryption, pairs of keys are used. One key is called a public key that is shared publicly, and the other is

[*] *Corresponding author: abdulqadeer00478@gmail.com*

[†] *E-mail address: rashid.ali@cust.edu.pk*

[‡] *E-mail address: tahir.ali@numl.edu.pk*

known as a private or secret key that is kept secret and known only to the person who generated both keys. The person who knows the public key does not necessarily know the private key.
There are several image encryption techniques available, each varying in terms of their intricacy, level of security, and appropriateness for different applications. Some commonly used techniques are Block Cipher Encryption, Chaotic Encryption, Substitution Techniques, Permutation Techniques and Confusion and Diffusion.
In block cipher, S-box is an important component. S-boxes are frequently chosen with care to avoid cryptanalysis. An S-box is a non-linear component in symmetric block ciphers that uses look-up tables to give the confusion property in the cryptosystem. As a result, in cryptographic methods, constructing an S-box with strong cryptographic characteristics is crucial. The substitution process converts the input bits to the output bits after several layers of substitutions, thereby producing the ciphertext.In order to determine the strength and confusion-inducing capacity of an S-box, it is necessary to examine the bit change patterns at the output, which are based on one or more bit changes at the input.
S-boxes are look-up tables that represent vectorial Boolean functions. An S-box takes a tiny block of bits and replaces it with another block of bits To make decryption effective, this substitution should be one-to-one. S-box converts n input bits into m output bits. The use of an S-box as a look-up table will give 2^n words, each with m bits. As employed in the Data Encryption Standard (DES) [6], a 4-bit S-box is a box of $2^4 = 16$ components with hexadecimal values ranging from 0 to F that is randomly organized. Similarly, the number of elements in an 8-bit S-box is $2^8 = 256$, with values ranging from 0 to 255, is used in the Advance Encryption Standard (AES) [8]. The output length can either be the same as the input length, as in AES [8], or different, as in DES [6, 7].
The communication of data and information has grown to be a crucial component of modern technology and is now regarded as one of an individual or an organization's most valuable assets. In the present sciences, information security has become a crucial aspect. Due to rapid changes in image transmission, researchers are working on creating efficient and secure image encryption algorithms. Researchers analyse, identify, and solve problems in the real world using image-based data. Ullah et al. [32] suggest a novel scheme for encrypting the images using an S-box and chaotic systems. Fridrich [12] suggested a chaotic map based image encryption scheme. Wang et al. [34] suggest a novel hybrid chaotic map-based and dynamic random growth image encryption technique. The author confused the original image by using the Arnold cat map and dynamic random growth method. In 2010 Patidar et al. [26] suggested a "substitution-diffusion based image encryption scheme" utilising chaotic logistic and standard maps. The proposed scheme was strong because it had the properties of confusion and diffusion. In 2012, Francois et al. [11] was proposed a new image encryption method that depended on `XOR` operator and coupling of chaotic function. The major factors of his encryption algorithm were its capacity for producing a large key space, its ability to produce images of any entropy structure, and its diffusion and confusion properties.
Khan et al. [21] proposed an algorithm for constructing the non-linear S-box used in image encryption algorithm. For image encryption, the Boolean bit function is used to construct non-linear substitution components. Farwa et al. [9] in 2017 suggested a new and reliable image encryption scheme that use then Arnold transform and algebraic S-box for scrambling. The suggested image encryption method is very easy to use and very efficient. In 2020 Lidong et al. [22] proposes a novel triple-image encryption method based on image compression, S-box and chaotic system. The security analysis shows that the algorithm can effectively resist common cryptographic attack. Ali and Ali [2] suggested a new algorithm based on chaotic maps for image encryption using substitution, Boolean operation and permutation. In 2022, another scheme was proposed by Ali and Ali [3] for image encryption that uses a dynamic chaotic map and S-box.
This paper proposed a novel approach to image encryption that combines an S-box and Logistic

map as secret keys is proposed. The S-box that is utilized for encryption purposes is constructed using a cubic fractional transformation (CFT). This is the first method to use the CFT to construct an S-box. Zahid et al. in 2019, [37] proposed a novel technique to construct an efficient S-box using the cubic fractional transform (CFT). This S-box is used for the purpose of substituting the image pixel values. After the substitution the CFT is used to generate two sequences that are used for permutation. After the permutation layer, a logistic map is utilized to construct the final encrypted picture, coupled with the Boolean operation `XOR`. The experimental results demonstrate that performance and security of the proposed approach is comparable to existing image encryption methods.
Following is a summary of the remaining paper: Section 2 introduces the chaotic map and logistic map. Section 3 provides a brief overview of the S-box construction process. The proposed image encryption algorithm's concept is presented in Section 4, and the decryption algorithm is presented in Section 5. The security analyses presented in Section 6 include NPCR, UACI, entropy analysis, key sensitivity analysis, correlation analysis, and histogram analysis. The conclusion of the suggested algorithm is given in Section 7.

2 Chaotic Map

The chaotic map is a mathematical structure that shows some kind of chaotic behavior. A random sequences are constructed by using a chaotic map. The sequence is unpredictable and appears random, making it difficult for attakers to decipher the encrypted message involving random sequence. Two types of parameters, discrete-time and continuous-time, are utilized to parameterize the maps. Discrete maps are typically iterated functions. The output of such maps is very dependent on the control parameters and initial conditions. Chaos-based cryptography can utilize these parameters as covert keys. Many chaotic maps exhibit chaotic behavior on a specific control parameter region. Chaotic cryptology is divided into two branches: chaotic cryptography and chaotic cryptanalysis. Chaotic cryptography encrypts information, while chaotic cryptanalysis decrypts the encrypted messages. Chaos-based cryptography has gained so much attention that it now has a vast range of uses in different of fields, including telecommunications, medical imaging, video, image, DNA cryptography, and others.

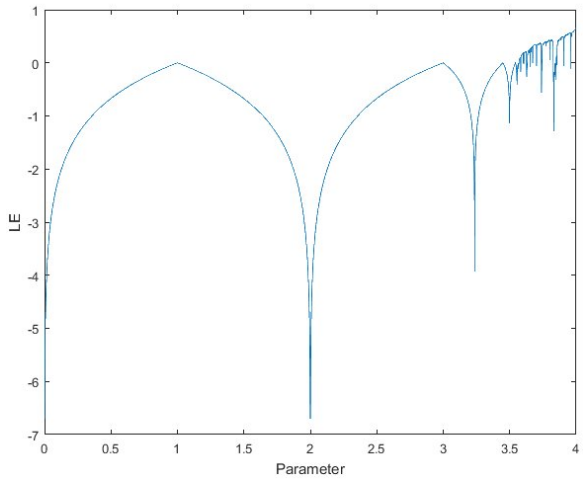


Figure 1: Lyapunove exponent of Logistic map

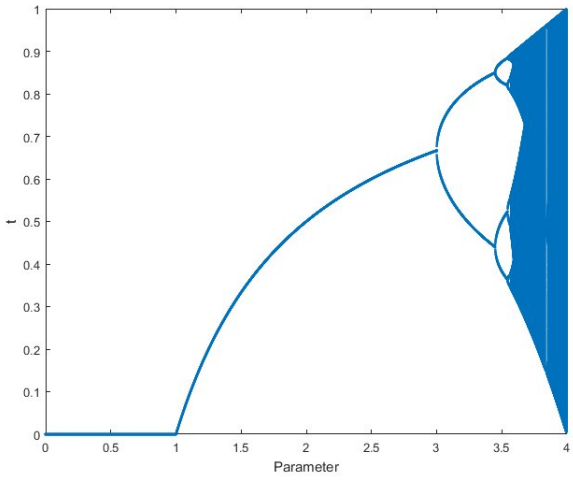


Figure 2: Bifurcation diagram for the Logistic map with iterations = 65536

2.1 Logistic Map

The logistic map is a mathematical function that exhibits chaotic behavior for a specific region. The logistic map was originally introduced by Pierre Francois Verhulst, a Belgian mathematician, in 1845 [31]. It is a function of second degree [17]. Although a simple one dimensional mathematical structure [25], but its chaotic behaviour is complex. Logistic map is a non-linear, discrete-time with quadratic non-linearity. It is defined by the equation below:

$$t_{n+1} = \gamma \times t_n \left(1 - t_n\right) \tag{1}$$

where $\gamma \in [0, 4]$ and $t_n \in (0, 1)$. The value of γ is the most essential part of the logistic map expression because it determines the chaotic behaviour:
Figure 1 shows the logistic map's Lyapunove exponent. Figure 2 shows the logistic map's bifurcation diagram.

3 S-box

The currently available literature makes it clear that S-boxes generated using random approaches like chaos or another pseudo-random source do not have strong cryptographic properties compared to S-boxes generated using algebraic methods [19]. Linear fractional transformation (LFT) is another field that aids in the creation of new S-boxes. In [10, 18, 4, 28, 19] authors propose effective algorithms to construct better S-boxes based on LFT. A LFT can be defined as:

$$L(w) = \frac{v_1 w + v_2}{v_3 w + v_4}, \qquad w \in Z_n \tag{2}$$

where, the four values v_1, v_2, v_3, and v_4 are taken from a finite field $GF(2^8)$. Linear fraction transformation is also called Möbius transformation.
In 2019 Zahid et al. [37] proposed an extended form of the linear fractional transformation for S-box construction, known as the cubic fractional transformation. In this study, the S-box is generated by following the CFT-based construction reported in [37]. The transformation is defined as

$$F(x) = \frac{1}{ax^3 + b} \mod (2^n + 1) \tag{3}$$

where $a, b, x \in Z_n$ and $Z_n = \{0, 1, 2, \cdots, 2^n - 1\}$,. Following [37], the parameters are selected as $a = 95$ and $b = 15$. Equation (3) produces the invalid output $256 \notin Z_n$ when $x = 176$, and for $x = 184$ the denominator of Equation (3) becomes 0 which contradicts the condition $ax^3 + b \neq 0$. Hence the modified CFT becomes as following:

$$F(x) = \begin{cases} \dfrac{1}{ax^3 + b} \mod 257 & \text{if } x \in Z_n - \{176, 184\} \\ 0 & \text{if } x = 176 \\ 106 & \text{if } x = 184 \end{cases} \tag{4}$$

Table 1: S-Box

78	FA	C1	B4	58	DF	B9	70	D2	F2	E9	F1	5B	5F	35	AE
84	73	7D	DC	4A	87	BE	50	48	68	2B	08	EF	26	C2	BA
B7	99	1F	A0	74	9D	72	A5	30	0D	34	DD	F4	3F	18	77
2E	AB	A9	9E	09	B1	2A	7B	8C	7A	6F	D8	F5	62	46	C5
CB	EB	A8	BB	0E	1A	89	8A	65	3C	E1	64	71	1C	C3	92
1D	C7	BD	56	D6	66	C8	27	B2	BF	E3	2C	1B	0F	F6	8D
90	86	FF	13	16	CC	12	8B	52	23	9C	39	D1	B5	4F	5D
BC	E7	CE	61	4D	80	8F	9B	A7	3B	D0	AF	FD	03	49	DA
3E	3D	2F	9F	4E	44	88	7E	3A	24	98	FC	F9	2D	43	E5
36	38	63	06	5E	C6	91	E2	AD	F7	22	0B	55	57	F8	76
C0	D5	85	D4	ED	15	5C	14	D7	79	DB	31	6D	32	EE	40
00	B0	42	01	4C	FE	96	DE	6A	81	CD	28	C4	7F	E6	B3
9A	45	1E	A3	21	0A	04	37	02	69	07	75	47	41	51	FB
94	AA	B6	D9	E8	EC	97	7C	E0	11	83	29	A6	A1	60	B8
6B	53	A2	25	82	AC	E4	4B	19	67	F0	93	6C	CF	D3	EA
20	6E	33	17	10	C9	CA	A4	0C	54	95	F3	8E	05	5A	59

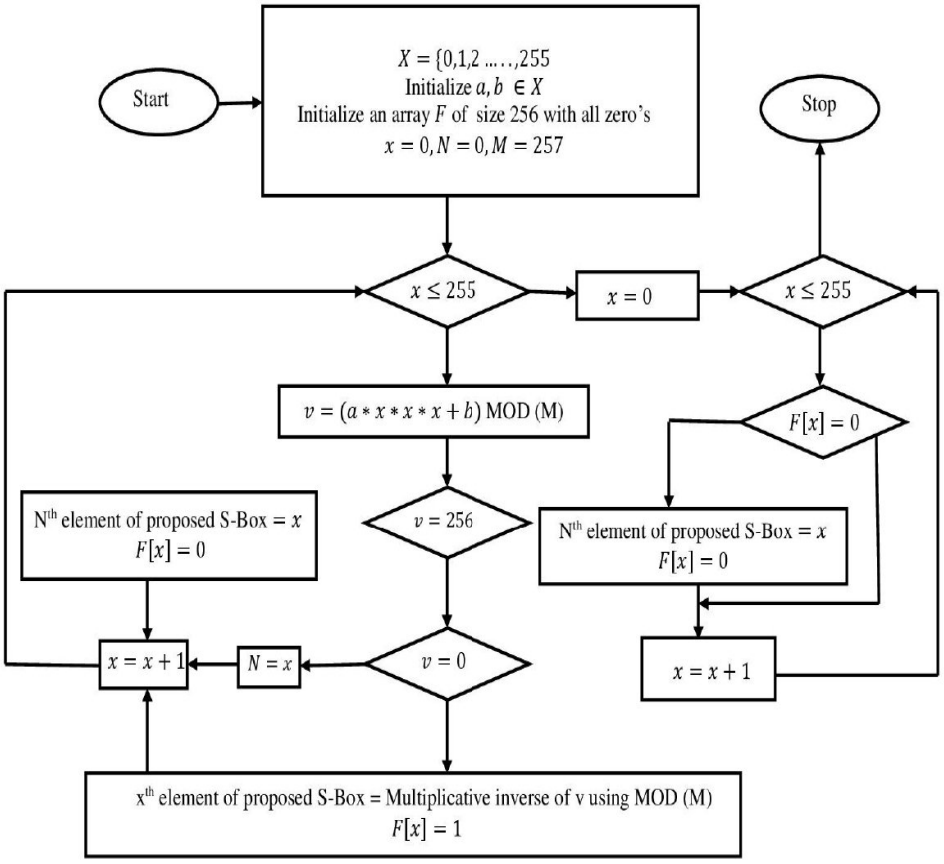


Figure 3: Flow Chat of S-box

4 Description of Proposed Image Encryption Algorithm

In this section, S-box and Logistic map based encryption algorithm is proposed for image encryption. The gray-scale image of size $(n \times m)$ is used, where n and m represent the number of rows and columns of a gray-scale image. The size of the gray-scale image that is used for encryption is 256×256. First, the image is converted into its pixel matrix. Then, for substitution purposes, the proposed S-box elements are utilized. After that, a row and column circular permutation is applied. At the end, the scrambling process is applied by taking bit-wise `XOR` with the chaotic sequence that is constructed by using the secret key and logistic map.

Table 2: Inverse S-Box

B0	B3	C8	7D	C6	FD	93	CA	1B	34	C5	9B	F8	29	44	5D
F4	D9	66	63	A7	A5	64	F3	2E	E8	45	5C	4D	50	C2	22
F0	C4	9A	69	89	E3	1D	57	BB	DB	36	1A	5B	8D	30	82
28	AB	AD	F2	2A	0E	90	C7	91	6B	88	79	49	81	80	2D
AF	CD	B2	8E	85	C1	3E	CC	18	7E	14	E7	B4	74	84	6E
17	CE	68	E1	F9	9C	53	9D	04	FF	FE	0C	A6	6F	94	0D
DE	73	3D	92	4B	48	55	E9	19	C9	B8	E0	EC	AC	F1	3A
07	4C	26	11	24	CB	9F	2F	00	A9	39	37	D7	12	87	BD
75	B9	E4	DA	10	A2	61	15	86	46	47	67	38	5F	FC	76
60	96	4F	EB	D0	FA	B6	D6	8A	21	C0	77	6A	25	33	83
23	DD	E2	C3	F7	27	DC	78	42	32	D1	31	E5	98	0F	7B
B1	35	58	BF	03	6D	D2	20	DF	06	1F	43	70	52	16	59
A0	02	1E	4E	BC	3F	95	51	56	F5	F6	40	65	BA	72	ED
7A	6C	08	EE	A3	A1	54	A8	3B	D3	7F	AA	13	2B	B7	05
D8	4A	97	5A	E6	8F	BE	71	D4	0A	EF	41	D5	A4	AE	1C
EA	0B	09	FB	2C	3C	5E	99	9E	8C	01	CF	8B	7C	B5	62

For the encryption purposes, a gray-scale image I of size $(n \times m)$ of clock is used, where m and n represent the number of columns and the number of rows of I respectively. The size of the gray-scale image that used for encryption is 256×256. The encryption process is described below:

Algorithm 4.1. (Substitution algorithm)
Input: Image (I), Secret key $k_0 = (u_0, v_0)$, Equation (4), S-box.
Output: Substituted Image S'.

1. Read the gray-scale secret image I.
2. Create a digital form of the gray-scale image I with a size of $M = n \times m$, where $n \times m$ is the size of image matrix with integer entries lies in the range of $[0, 255]$ and n, m are the rows and columns in M respectively.
3. Using the secret key $k_0 = (u_0, v_0) = (95, 15)$ for Equation (4) to generate an S-box take only those values that lies in [0, 255].
4. Replace each entry of pixel value matrix m_i of the image $M = \{m_1, m_2, m_3, \ldots, m_i\}$ by $S(m_i)$ where $i \in \{1, 2, 3, \ldots, n \times m\}$. After substitution of the pixel value matrix with S-box, the resultant array is denoted by S' which is $\{s_1, s_2, s_3, \ldots, s_{n \times m}\}$.

Permutation Algorithm: A suitable permutation is used to change the pixel positions of the substituted image S'. The Cubic Fractional Transformation (CFT) is used to generate the permutation array.

$$F(w) = \begin{cases} \dfrac{1}{uw^3 + v} \mod (257) & \text{if } w \in Z_n - \{43, 135\} \\ 0 & \text{if } w = 43 \\ 11 & \text{if } w = 135 \end{cases} \tag{5}$$

Here $u = 90$ and $v = 20$. The Equation (5) gives the value of $Z_n - \{0, 11\}$ when $w \in Z_n - \{43, 135\}$.

$$F(w) = \begin{cases} \dfrac{1}{uw^3 + v} \mod (257) & \text{if } w \in Z_n - \{176, 62\} \\ 0 & \text{if } w = 142 \\ 40 & \text{if } w = 62 \end{cases} \tag{6}$$

Here $u = 115$ and $v = 45$. The Equation (6) gives the value of $Z_n - \{0, 40\}$ when $w \in Z_n - \{142, 62\}$.

Algorithm 4.2. (Permutation algorithm)
Input: S', Secret key $k_1 = (u_1, v_1)$ and $k_2 = (u_2, v_2)$.
Output: Pre-encrypted Image P.

1. Utilize the same algorithm as used in [37] to construct the elements of the sequences $S1 = \{s_{11}, s_{12}, s_{13}, \ldots, s_{1m}\}$ and $S2 = \{s_{21}, s_{22}, s_{23}, \ldots, s_{2n}\}$ by using Equations (5) and (6) and secret keys $k_1 = (u_1, v_1)$ and $k_2 = (u_2, v_2)$.

2. Apply a column-wise circular shift on substitution image S'. Use the value of S1 to permute the value of substitution image S'. The resulting matrix is stored in P'.

3. After applying a column-wise circular shift on image S', another row-wise circular shift is applied on image P' with the help of S2. The resulting matrix is saved in P.

The logistic map (1), along with the `XOR` Boolean operation, is utilized to obtain the final encrypted image after the permutation layer.

Algorithm 4.3. (Scrambling Process)
Input: Pre-encrypted image P', Logistic map (1) and Secret key $k_3(\gamma, t)$
Output: Final Encrypted image C.

1. Iterate the logistic map (1) using initial state t_0 and control parameter γ as secret key k_3 for W times to create a chaotic sequence of length W.

2. Apply the following relation to convert the obtained sequence it into 8-bit integer values.

$$X = \mod (\text{floor}(x \times 10^{14}), 256)$$

3. To eliminate the transient impact, dispose off the first $(L - (n \times m))$ numbers of the chaotic sequence, then generate a new chaotic sequence of length 65536, denoted by SK.

4. Rewrite matrix P as one dimensional array $P'' = \{p''_1, p''_2, p''_3, \ldots, p''_{n \times m}\}$.

5. Then the scrambling process is performed as following:

$$\begin{aligned}
&\text{for } i = 1 \;\; and \;\; j = 1 : n \times m \\
&\quad \text{if } \; j = 1, \text{then} \\
&\qquad C(i,j) \leftarrow P''(i,j) \oplus Sk(i,j); \\
&\quad \text{else} \\
&\qquad C(i,j) \leftarrow C(i,j-1) \oplus P''(i,j) \oplus Sk(i,j); \\
&\quad end \\
&\quad end
\end{aligned}$$

6. Convert the array into $n \times m$ matrix obtained from scrambling.

7. In the end, a cipherimage C is created by converting the resulting matrix of pixel values into an image format.

5 Decryption Algorithm

The decryption algorithm removes all traces of encryption from the original image. The plainimage I is extracted from the cipherimage C using the procedures listed below:

Algorithm 5.1. (Decryption Algorithm)
Input: Encrypted image C, S-box, Secret key $k_0(u_0, v_0)$ $k_1(u_1, v_1)$, $k_2(u_2, v_2)$ and $k_3(\gamma, t)$
Output: Original Image I.

1. Converts the cipherimage into digital form N, where N is the pixel value matrix of $n \times m$ size with entries from 0 to 255.

2. Convert the matrix into one dimensional array of length $n \times m$.

3. Perform the unscrambling process as described below:

$$\begin{aligned}
&\text{for } i = 1 \;\; \text{and} \;\; j = 1 : m \times n \\
&\quad \text{if } \; j = 1, \text{then} \\
&\qquad P''(i,j) \leftarrow C(i,j) \oplus SK(i,j); \\
&\quad \text{else} \\
&\qquad P''(i,j) \leftarrow C(i,j-1) \oplus C(i,j) \oplus SK(i,j); \\
&\quad end \\
&\quad end
\end{aligned}$$

4. Rewrite P'' into 2-dimension matrix P.

5. Apply a reverse row-wise circular shift on P by using the element of $S2$. Then resulting matrix is stored in P'.

6. Another reverse column-wise circular shift is applied with the help of the array $S1$. Hence generated resulting matrix is stored in S'.

7. Generate an S-box 'S' by using Equation (4).

8. Construct the inverse S-box of S that is S^{-1}.

9. Replace each pixel value s'_i of the matrix S' by using inverse S-box generated in step 8, as $S^{-1}(s'_i)$ where $i \in \{1, 2, 3..., n \times m\}$. After replacing the pixel values of S' with the inverse S-box, the resultant pixel matrix is I.

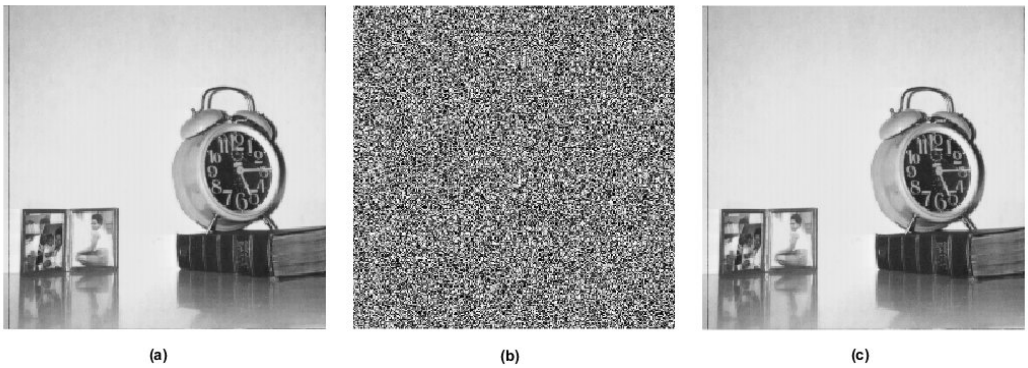


Figure 4: Results of Clock image encryption and decryption algorithm: (a) Plainimage, (b) Cipherimage, (c) Decrypted image.

6 Results and Discussions

The tests are performed to illustrate the efficiency and validity of the suggested algorithm. The algorithms (4.1), (4.2) and (4.3) have been applied on different images such as Clock, Lena, Girl, Baboon and Pepper using MATLAB R2017a. These images are taken from the http://sipi.usc.edu/database/, known as the USC-SIPI open image repository.
The standard gray image of Clock (256×256) is used in first example shown in Figure 4(a). After applying the encryption algorithm the cipherimage is depicted in Figure 4(b). The decryption algorithm (5.1) is then used for decoding the cipherimage, as shown in Figure 4(c). The decryption outcome shows that the suggested algorithm is effective in recovering the original image.
A Lena image with a size of (256×256) is chosen for the next example. The plainimage is shown in Figure 5(a), the cipherimage result is shown in 5(b). The decryption algorithm is then used to perform the decoding the cipherimage, the decrypted image shown in Figure 5(c). The results of the decryption demonstrate that the proposed algorithm is effective in recovering the plainimage.

Table 3: Key space comparison

Algorithm	Key Space
Ye et al. [36]	2^{128}
Chen et al. [5]	2^{199}
Xian et al. [35]	2^{154}
Mondal et al. [24]	2^{256}
Mondal et al. [23]	2^{213}
Proposed	2^{147}

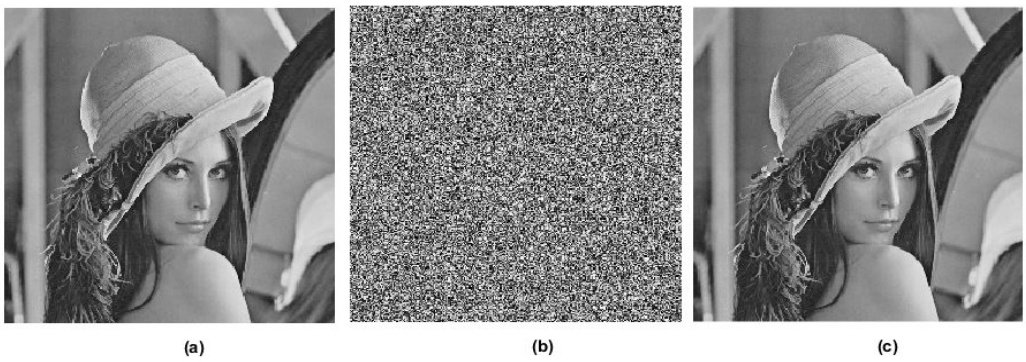


Figure 5: Results of Lena image encryption and decryption algorithm: (a) Plainimage, (b) Cipherimage, (c) Decrypted image.

6.1 Security Analysis

Security evaluations that examine the effectiveness of encryption may consider key space, differential analysis, key sensitivity analysis, correlation coefficients, entropy (values of information), and histogram analysis, among other factors.

6.1.1 Key Space

In the encryption algorithm, a Cubic Fractional Transformation (CFT) and Logistic map are used. The CFT involve u and v as parameter and Logistic map involves γ as control parameters and t as a variable. The key is a comprising of 4 secret keys $k = (k_0, k_1, k_2, k_3)$. The number of possible key combinations is 2^{147}. The resulting key space exceeds the minimum key size requirement.

6.1.2 Key Sensitivity Analysis

The secret key must be incorporated into the image encryption scheme, and any modification to one bit of the key should lead to a completely different encrypted output. An effective image encryption scheme must be key sensitive in order to prevent unauthorized preliminary attacks. The cipherimage shouldn't be accurately decrypted even if the encryption key changes slightly. For example, if 0.000000000000005 is added to the γ secret key's parameter of the encryption algorithm, the new value of the parameter will be 3.995000000000005. The original image will not be obtained by using this to decrypt.
The plainimage of Lena is represented in Figure 6(a), the encrypted image depicted in Figure 6(b), and the decryption results are achieved with a slightly different key in Figure 6(c). This shows that the algorithm is extremely sensitive to key.

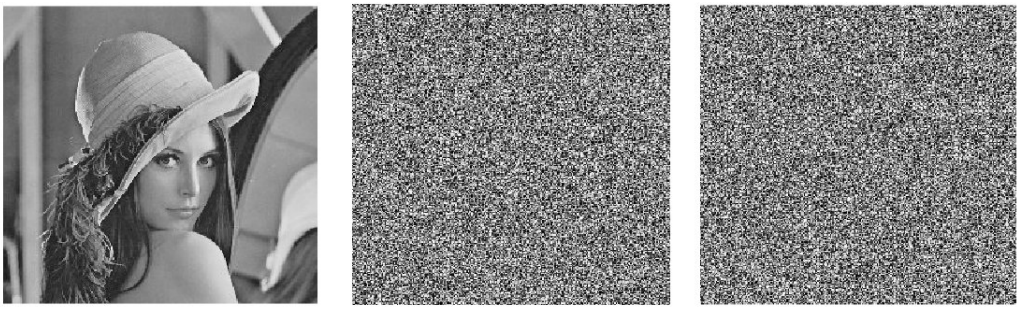


Figure 6: Key sensitivity test for Lena: (a) Plainimage (b) Cipherimage (c) Decrypted image by slightly changed key

6.1.3 Differential Analysis

Images encrypted with a high-performance image encryption method should appear completely different from plainimages; this is one of its key characteristics. To compare a cipherimage to the original image and the cipherimage after changing one pixel in the original image, the number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used. The NPCR and UACI values can be calculated as;

$$\text{NPCR} = \frac{\sum_{i,j} M(i,j)}{w \times h} \times 100 \tag{7}$$

$$\text{UACI} = \frac{1}{w \times h} \left[\sum_{i,j} \frac{|Y(i,j) - Y'(i,j)|}{255} \right] \times 100 \tag{8}$$

Here w and h represent the encrypted image's width and height, respectively. Y and Y' are cipher-images generated from plainimages and by planeimages with a difference of one pixel, respectively. If $Y = Y'$ then $M(i,j) = 0$ otherwise 1. To withstand differential attacks, NPCR and UACI values need to be high and close to ideal. Table 4 shows the NPCR and UACI values performance for the proposed schemes is perfect. As a result, it will provide great resistance to "known plaintext attacks" and "chosen plaintext attacks".

Table 4: Comparison of NPCR and UACI of the images.

Algorithm	Image	NPCR	UACI
Hanif et al. [16]	Lena	99.5743	33.0509
Khalil et al. [20]		99.62	33.56
Abdullah et al. [1]		99.69	30.65
Proposed		99.5910	33.3255
Mondal et al. [23]	Baboon	99.2252	32.8760
Gao et al. [13]		99.636	33.429
Hanif et al. [16]		99.6521	33.1627
Zareai et al. [38]		99.6311	33.4761
Proposed		99.6047	33.3913
Zareai et al. [38]	Peppers	99.6315	33.4706
Abdullah et al. [1]		99.56	28.99
Wang et al. [33]		99.6002	33.4531
Mondal et al. [23]		99.2130	32.6708
Gao et al. [13]		99.623	33.529
Proposed		99.6032	33.4638

Table 5: Two adjacent pixels' correlation coefficient in a plain and cipher image.

image	Clock		Lena		Female	
Direction	Original	Cipher	Original	Cipher	Original	Cipher
Horizontal	0.9740	-0.0057	0.9451	-0.0049	0.9656	0.0053
Vertical	0.9564	0.0036	0.9052	0.0006	0.9740	-0.0057
Diagonal	0.9389	-0.0005	0.8843	0.0015	0.9515	-0.0018

6.1.4 Correlation Coefficients Analysis (CCA)

Correlation coefficients is a powerful tool for determining the rate of success of an attack on an encrypted image. Correlation is used to connect adjacent pixels that have correlation coefficients. A good encryption algorithm minimizes the correlation coefficient between pairs of encrypted neighboring pixels in the vertical, horizontal, and diagonal directions. The Correlation Coefficients (CC) is calculated as following:

$$C_{a,b} = \frac{cov(a,b)}{\sqrt{D(a)} \times \sqrt{D(b)}} \tag{9}$$

where a and b are the values of two pixels from the input grayscale image. $D(a)$ and $D(b)$ are the variances of a and b, respectively. $cov(a,b)$ represents the a and b covariance. The following

equations are used to calculate the correlation coefficients:

$$cov(a,b) = \frac{1}{K}\sum_{j=1}^{K}(a_j - X(a))(b_j - X(b))$$

$$X(a) = \frac{1}{K}\sum_{j=1}^{K} a_j$$

$$D(a) = \frac{1}{K}\sum_{j=1}^{K}(a_j - X(a))^2$$

Table 5 shows that the cipherimage correlation coefficient is closer to zero.

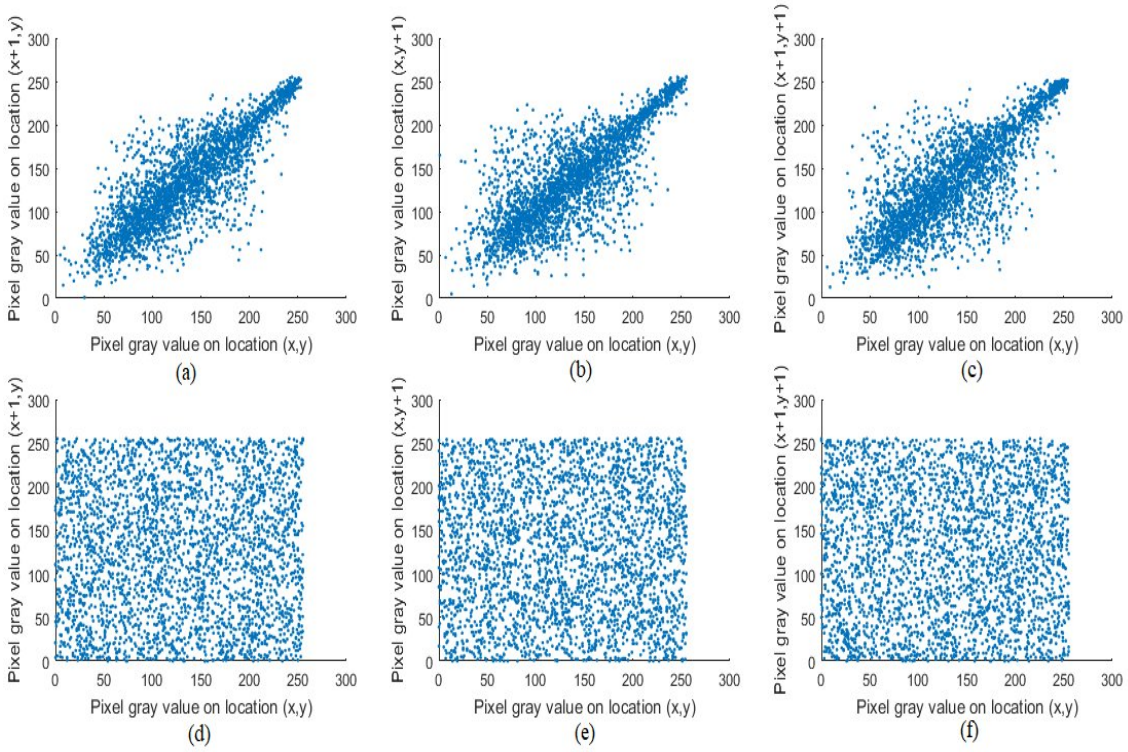


Figure 7: Correlation coefficients of Baboon; (a) horizontal correlation of plainimage of baboon, (b) vertical correlation of plainimage, (c) diagonal correlation of plainimage, (d) horizontal correlation of cipherimage, (e) vertical correlation of cipherimage, and (f) diagonal correlation of cipherimage.

6.1.5 Entropy Analysis

Information entropy was first presented by Shannon in 1948 [29]. In cryptography, the term "entropy" refers to the randomness that a system accumulates for use in techniques that uses random data. Lack of entropy can make a cryptosystem susceptible and prevent it from securely encrypting data.

This component of examination estimates the randomness in a cipherimage. It additionally lets us know the typical measure of data conveyed by the coded image. If β is an encrypted image, then

the entropy of β can be determined by the following equation:

$$E(\beta) = \sum_{j=0}^{2^N-1} P(\beta_j) \log_2 \frac{1}{P(\beta_j)} \tag{10}$$

Where $P(\beta_j)$ in Equation (10) represents the probability of symbol β_j appearing in cipherimage β. For a (256×256) grayscale image, the ideal value of the entropy is 8. The entropy values of various images that were encrypted using the proposed schemes are displayed in Table 7. The result shows that the generated entropy of the proposed encryption algorithm approaches the ideal entropy in a very close range.

Table 6: Comparison of the correlation coefficients of the images.

Image	Direction	Plainimage	Cipherimage			
			Proposed	Ping et al. [27]	Mondal et al. [23]	Zareai et al. [38]
Lena	Horizontal	0.9451	-0.0049	-0.0008	0.0008	-0.0012
	Vertical	0.9052	0.0006	-0.0025	0.0004	-0.0006
	Diagonal	0.8843	0.0015	0.0010	0.0020	-0.0009
Baboon	Horizontal	0.8141	-0.0009		0.0047	-0.0031
	Vertical	0.8573	0.0021	-	- 0.0001	0.0006
	Diagonal	0.8046	-0.0020	-	- 0.0011	-0.0008
Peppers	Horizontal	0.9481	0.0080	-	0.0046	-0.0013
	Vertical	0.9477	-0.0046	-	0.0039	0.0006
	Diagonal	0.9035	-0.0038	-	- 0.0018	0.0002
Clock	Horizontal	0.9740	-0.0057	0.0033	-	-
	Vertical	0.9564	0.0036	-0.0020	-	-
	Diagonal	0.9389	-0.0005	-0.0011	-	-

Table 7: Entropy analyses

Images	Clock	Lena	Female	Baboon	Pepper
Plainimage	6.7056	7.4749	7.7066	7.5641	7.3102
Cipherimage	7.9973	7.9973	7.9971	7.9972	7.9975

Table 8: Comparison of the information entropies of the images.

Image	Plainimage	Cipherimage			
		Proposed	Mondal et al. [23]	Hanif et al. [16]	Girdhar et al. [15]
Lena	7.4749	7.9973	7.9995	7.9957	-
Baboon	7.7066	7.9971	7.9974	7.9952	7.998
Pepper	7.5641	7.9972	7.9889	-	7.997
Clock	6.7056	7.9973	-	7.9955	-

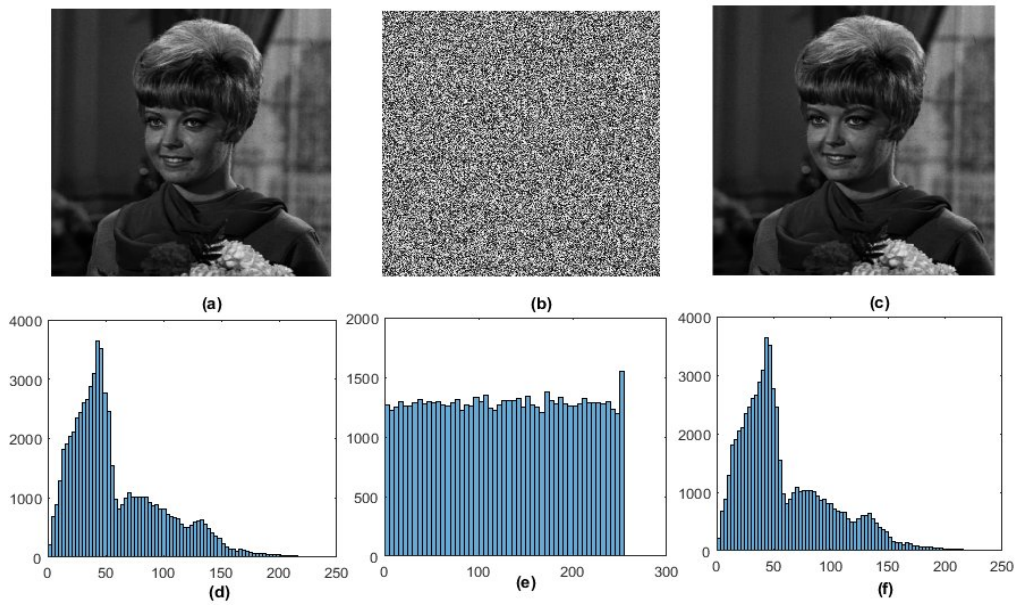


Figure 8: Result for the histigram grayscale image of female: (a) Plainimage (b) Cipherimage (c) Decrypted image (d) Histogram of plainimage (e) Histogram of cipherimage (f) Histogram of decrypted image.

6.1.6 Histogram Analysis

A histogram of pixel intensity values is typically referred to as an image histogram. The image's histogram is a graph that displays the pixel value at each of the various intensities present in the image. A grayscale image with 8 bits can have 256 different intensities, so the histogram will graphically display 256 numbers showing the distribution of pixels among those grayscale values. The encrypted image needs a histogram with a uniform distribution in order to be compatible with high-security image encryption algorithms. Figure 8 shows the plain and cipherimage histograms for the image clock. It is clear that, there is no hint of a statistical attack on the cipherimage.

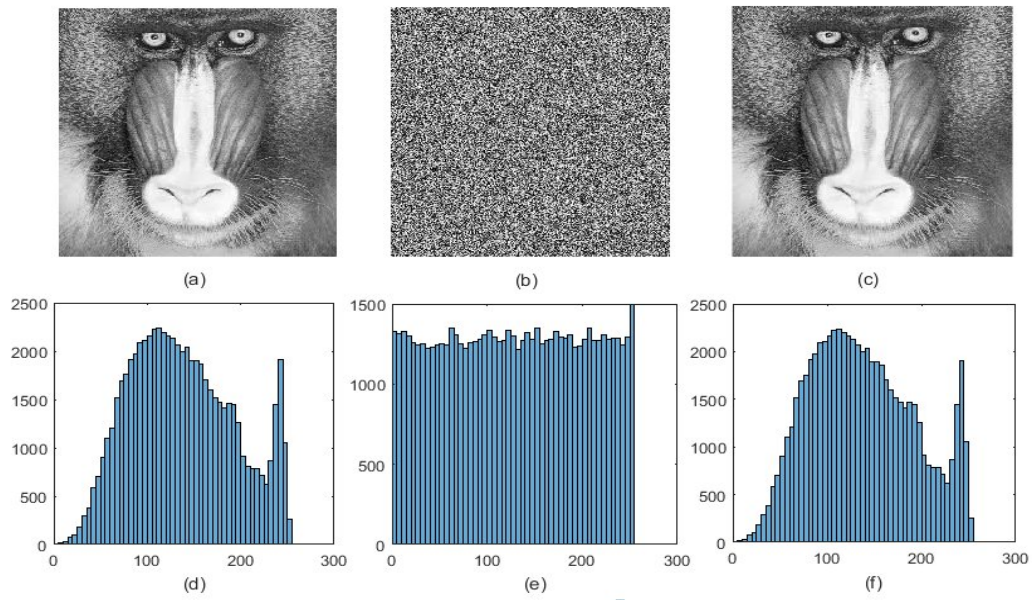


Figure 9: Image encryption and decryption result for baboon: (a) Plainimage, (b) Ciphermage, (c) Decrypted image (d) Histogram of plainimage (e) Histogram of cihperimage (f) Histogram of decrypted image

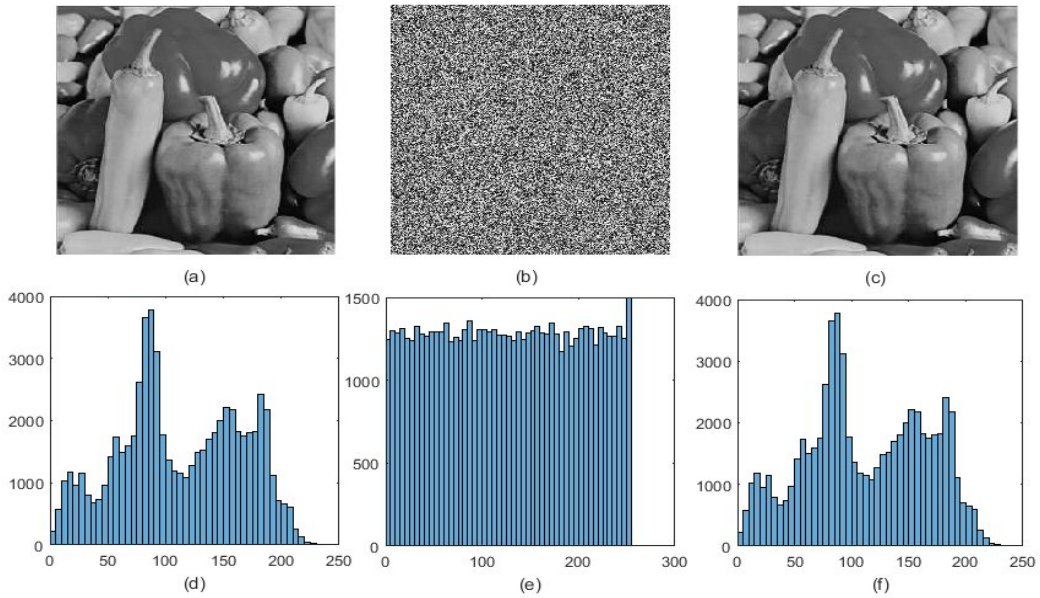


Figure 10: Image encryption and decryption result for pepper: (a) Plainimage, (b) Encrypted Image, (c) Decrypted Image (d) Histogram of plainimage (e) Histogram of Cipherimage (f) Histogram of decrypted image

7 Conclusion

The S-box that is used for encryption is highly non-linear and has low linear probability (LP) and differential probability (DP), so the proposed S-box resists differential and linear cryptanalysis attacks. The S-box has 106.75 average non-linearity, 0.1484 value of LP and 0.0391 DP. The S-box is used in the image encryption algorithm for substitution purpose. After this, different circular shifts are performed to create more confusion. Finally, a Logistic map is used to generate a random sequence that is then used to scramble the pixels of the image by applying the `XOR` operation. Entropy analysis, key sensitivity analysis, key space analysis, statistical analysis, and differential analysis are all tools used in security analysis. Security analysis shows that it is not possible to obtain the original image through cryptographic attacks. Which tells that this encryption algorithm is a secure algorithm and can be used for image encryption algorithm. This algorithm can also be used for encrypting images of different types and size.

Declarations

Ethical approval

Not applicable.

Consent to participate

Not applicable.

Consent to publish

Not applicable.

References

[1] Hikmat N. Abdullah and Hamsa A. Abdullah. Image encryption using hybrid chaotic map. In *2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT)*, pages 121–125, 2017.

[2] Tahir Sajjad Ali and Rashid Ali. A new chaos based color image encryption algorithm using permutation substitution and boolean operation. *Multimedia Tools and Applications*, 79(27):19853–19873, 2020.

[3] Tahir Sajjad Ali and Rashid Ali. A novel color image encryption scheme based on a new dynamic compound chaotic map and s-box. *Multimedia Tools and Applications*, pages 1–25, 2022.

[4] Anas Altaleb, Muhammad Sarwar Saeed, Iqtadar Hussain, and Muhammad Aslam. An algorithm for the construction of substitution box for block ciphers based on projective general linear group. *AIP Advances*, 7(3):035116, 2017.

[5] Junxin Chen, Zhi-liang Zhu, Li-bo Zhang, Yushu Zhang, and Ben-qiang Yang. Exploiting self-adaptive permutation–diffusion and dna random encoding for secure and efficient image encryption. *Signal Processing*, 142:340–353, 2018.

[6] Yvo Desmedt and Jean-Jacques Quisquater. Public-key systems based on the difficulty of tampering (is there a difference between des and rsa?). In *Conference on the Theory and Application of Cryptographic Techniques*, pages 111–117. Springer, 1986.

[7] Whitfield Diffie and Martin E Hellman. Special feature exhaustive cryptanalysis of the nbs data encryption standard. *Computer*, 10(6):74–84, 1977.

[8] Ghada F Elkabbany, Heba K Aslan, and Mohamed N Rasslan. A design of a fast parallel-pipelined implementation of aes: Advanced encryption standard. *arXiv preprint arXiv:1501.01427*, 2015.

[9] Shabieh Farwa, Nazeer Muhammad, Tariq Shah, and Sohail Ahmad. A novel image encryption based on algebraic s-box and arnold transform. *3D Research*, 8(3):1–14, 2017.

[10] Shabieh Farwa, Tariq Shah, and Lubna Idrees. A highly nonlinear s-box based on a fractional linear transformation. *SpringerPlus*, 5(1):1–12, 2016.

[11] Michael François, Thomas Grosges, Dominique Barchiesi, and Robert Erra. A new image encryption scheme based on a chaotic function. *Signal Processing: Image Communication*, 27(3):249–259, 2012.

[12] Jiri Fridrich. Image encryption based on chaotic maps. In *1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation*, volume 2, pages 1105–1110. IEEE, 1997.

[13] Wenjian Gao, Jie Sun, Wei Qiao, and Xu Zhang. Digital image encryption scheme based on generalized mandelbrot-julia set. *Optik*, 185:917–929, 2019.

[14] Simson L Garfinkel. Public key cryptography. *Computer*, 29(6):101–104, 1996.

[15] Ashish Girdhar, Himani Kapur, and Vijay Kumar. A novel grayscale image encryption approach based on chaotic maps and image blocks. *Applied Physics B*, 127:1–12, 2021.

[16] Muhammad Hanif, Nadeem Iqbal, Fida Ur Rahman, Muhammad Adnan Khan, Taher M Ghazal, Sagheer Abbas, Munir Ahmad, Hussam Al Hamadi, and Chan Yeob Yeun. A novel grayscale image encryption scheme based on the block-level swapping of pixels and the chaotic system. *Sensors*, 22(16):6243, 2022.

[17] Khalid M Hosny. *Multimedia security using chaotic maps: principles and methodologies*, volume 884. Springer, 2020.

[18] Iqtadar Hussain, Tariq Shah, Muhammad Asif Gondal, Majid Khan, and Waqar Ahmad Khan. Construction of new s-box using a linear fractional transformation. *World Appl. Sci. J*, 14(12):1779–1785, 2011.

[19] Sajjad Shaukat Jamal, Tariq Shah, Ali H AlKhaldi, Mohammad Nazim Tufail, et al. Construction of new substitution boxes using linear fractional transformation and enhanced chaos. *Chinese Journal of Physics*, 60:564–572, 2019.

[20] Noura Khalil, Amany Sarhan, and Mahmoud AM Alshewimy. An efficient color/grayscale image encryption scheme based on hybrid chaotic maps. *Optics & Laser Technology*, 143:107326, 2021.

[21] Majid Khan, Tariq Shah, and Syeda Iram Batool. Construction of s-box based on chaotic boolean functions and its application in image encryption. *Neural Computing and Applications*, 27(3):677–685, 2016.

[22] Liu Lidong, Donghua Jiang, Xingyuan Wang, Linlin Zhang, and Xianwei Rong. A dynamic triple-image encryption scheme based on chaos, s-box and image compressing. *IEEE Access*, 8:210382–210399, 2020.

[23] Bhaskar Mondal, Pratap Kumar Behera, and Sugata Gangopadhyay. A secure image encryption scheme based on a novel 2d sine–cosine cross-chaotic (sc3) map. *Journal of Real-Time Image Processing*, 18(1):1–18, 2021.

[24] Bhaskar Mondal, Shrey Singh, and Prabhakar Kumar. A secure image encryption scheme based on cellular automata and chaotic skew tent map. *Journal of information security and applications*, 45:117–130, 2019.

[25] MA Murillo-Escobar, C Cruz-Hernández, L Cardoza-Avendaño, and R Méndez-Ramírez. A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dynamics*, 87(1):407–425, 2017.

[26] Vinod Patidar, NK Pareek, G Purohit, and KK Sud. Modified substitution–diffusion image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation*, 15(10):2755–2765, 2010.

[27] Ping Ping, Jinyang Fan, Yingchi Mao, Feng Xu, and Jerry Gao. A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access*, 6:67581–67593, 2018.

[28] M Sarfraz, Iqtadar Hussain, and Fateh Ali. Construction of s-box based on mobius transformation and increasing its confusion creating ability through invertible function. *International Journal of Computer Science and Information Security*, 14(2):187, 2016.

[29] CE Shannon. Une théorie mathématique des télécommunications. *Bell. Syst. Techn. J.*, 27(3):379–423, 1948.

[30] William Stallings. *Cryptography and network security, 4/E*. Pearson Education India, 2006.

[31] Richard Taylor. *LOGISTIC MAPS AND SYNCHRONIZATION*. PhD thesis, Brigham Young University, 2007.

[32] Atta Ullah, Sajjad Shaukat Jamal, and Tariq Shah. A novel scheme for image encryption using substitution box and chaotic system. *Nonlinear Dynamics*, 91(1):359–370, 2018.

[33] Xingyuan Wang and Suo Gao. Image encryption algorithm for synchronously updating boolean networks based on matrix semi-tensor product theory. *Information sciences*, 507:16–36, 2020.

[34] Xingyuan Wang, Lintao Liu, and Yingqian Zhang. A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering*, 66:10–18, 2015.

[35] Yongjin Xian and Xingyuan Wang. Fractal sorting matrix and its application on chaotic image encryption. *Information Sciences*, 547:1154–1169, 2021.

[36] Guodong Ye, Kaixin Jiao, Xiaoling Huang, Bok-Min Goi, and Wun-She Yap. An image encryption scheme based on public key cryptosystem and quantum logistic map. *Scientific Reports*, 10(1):21044, 2020.

[37] Amjad Hussain Zahid, Muhammad Junaid Arshad, and Musheer Ahmad. A novel construction of efficient substitution-boxes using cubic fractional transformation. *Entropy*, 21(3):245, 2019.

[38] Delavar Zareai, Mohammadali Balafar, and Mohammad Reza Feizi Derakhshi. A new grayscale image encryption algorithm composed of logistic mapping, arnold cat, and image blocking. *Multimedia Tools and Applications*, 80:18317–18344, 2021.