A novel symmetric image cryptosystem resistant to noise perturbation based on S_8 elliptic curve S-boxes and chaotic maps

Haris Aziz[1, 2], Syed Mushhad Mustuzhar Gilani[1, a], Iqtadar Hussain[3], Muhammad Azeem Abbas[1]

[1]*University Institute of Information Technology, Pir Mehr Ali Shah Arid Agriculture University, Rawalpindi, Pakistan*

[2]*U.S-Pakistan Center for Advanced Studies in Energy (USPCAS-E), National University of Sciences and Technology (NUST), H-12, Islamabad 44000, Pakistan*

[3]*Department of Mathematics, Statistics and Physics, Qatar University, Doha 2713, Qatar*

Abstract

The recent decade has seen a tremendous escalation of multimedia and its applications. These modern applications demand diverse security requirements and innovative security platforms. In this manuscript, we proposed an algorithm for image encryption applications. The core structure of this algorithm relies on confusion and diffusion operations. The confusion is mainly done through the application of the elliptic curve and S_8 symmetric group. The proposed work incorporates three distinct chaotic maps. A detailed investigation is presented to analyze the behavior of chaos for secure communication. The chaotic sequences are then accordingly applied to the proposed algorithm. The modular approach followed in the design framework and integration of chaotic maps into the system makes the algorithm viable for a variety of image encryption applications. The resiliency of the algorithm can further be enhanced by increasing the number of rounds and S-boxes deployed. The statistical findings and simulation results imply that the algorithm is resistant to various attacks. Moreover, the algorithm satisfies all major performance and quality metrics. The encryption scheme can also resist channel noise as well as noise-induced by a malicious user. The decryption is successfully done for noisy data with minor distortions. The overall results determine that the proposed algorithm contains good cryptographic properties and low computational complexity makes it viable to low profile applications.

[a] Email: mushhad@uaar.edu.pk (*corresponding author*)

1 Introduction

The precipitous progression of information technology has contributed to an immense rise in digital systems. This perceives information security as a vital component of any digital system. Therefore, research and development in information security gather remarkable attention. Researchers around the globe have introduced substantial approaches along with new and novel assaults to secure digital systems. Recently data concealment techniques to encode and decode the data with the intention to stop any unauthorized access becomes front runner in information security [1], [2]. Cryptography relies on three core principals of authentication, integrity, and privacy. Moreover, it has been further segregated into symmetric and asymmetric ciphers. Symmetric algorithms have been evolved via algebraic constructs and extensively deployed in a wide range of applications. Symmetric algorithms are classified as block ciphers or stream ciphers depending on their implementations [3]. Shannon [4] introduced a novel concept of Substitution Permutation Network (SPN) for block ciphers. This principle of elementary confusion and diffusion becomes the building block of modern block ciphers. Daemen and Rijmen [5] present Rijndael cipher based on SPN and this has been adopted as Advanced Encryption Standard (AES) by the National Institute of Standards and Technology (NIST). AES is extensively deployed in numerous business applications for example [6]–[8]. AES algorithm is composed of four steps but the most prominent is byte substitution attained by Substitution box (S-box). The S-box is the lone nonlinear fragment of any block cipher and signifies a confused association among input and output bits. S-boxes are vector Boolean functions and conveniently deployed in programming instructions. S-box is a nucleus for block ciphers and the endurance of any block cipher relies on the resiliency of their S-box. It is beyond the scope of this work to discuss extensive literature available on the algebraic properties of S-box and their implementations. The readers are recommended to study [9]–[11] and reference therein for understanding.

To develop and design robust S-boxes multiple frameworks are rendered such as algebraic structures, pseudo-random generation, analytical approaches, automata theory, control mapping, etc. to design nonlinear components of the block cipher. Cui and Cao [12] designed S-box using Affine-Power-Affine structure to enhance algebraic complexity. Tran et al. [13] fabricated algebraically strong Gray S-boxes by the application of the Gray augmentation scheme as a pre-processing step. Abuelyman and Alsehibani [14] presented optimized S-boxes by employing residue of prime numbers. Ahmad et al. [15] synthesized cryptographically potent S-boxes based

on the traveling salesman problem. Kazlauskas et al. [16] generated key-dependent S-boxes for block cipher cryptosystems. In [17] heuristic approach involving genetic programming is used to construct a nonlinear component. Ruisanchez et al. [18] constructed S-boxes with high diffusion characteristics through a novel algorithm. Bikov et al. [19] fabricated bijective S-boxes of varying sizes through the application of binary quasi-cyclic codes with good cryptographic properties. There were many other approaches such as cellular automata [20], disjoint linear codes [21], binomial power functions [22], Matrix Power function [23] used to map new S-boxes.

Miller and Koblitz [24], [25] introduced the concept of elliptic curves (ECs) to evolve immensely secure cryptosystems. Miller [26] demonstrated that cryptosystems powered via ECs are highly robust and exceptionally secure as compared with RSA. Recently researchers successfully constructed cryptographically strong S-boxes by applications of ECs. Hayat et al. in a series of papers [26], [27] devised a novel strategy that utilizes ECs across the prime field to generate 8x8 S-boxes. Sapna and Parsad [28] recently generated an optimized and efficient S-box for AES through elliptic curve cryptography (ECC). Azam et al. [29] presented an efficient S-box construction technique over a finite field through the application of the Mordell elliptic curve (MEE). This work will reinforce MEE S-boxes through the application of symmetric group S_8 and synthesize a collection of new S-boxes with identical algebraic properties [30].

Chaotic maps come with several unique peculiarities such as hypersensitive dependence, ergodicity, pseudo-randomness, and unpredictability[31]–[33]. Those parameters established vast applications of chaos in constructing secure cryptosystems. The researchers exploit random conduct by chaotic frameworks to construct S-boxes and encryption applications, especially where nonlinear transformations are needed [34]–[38]. The predominant applications of chaotic systems are in multimedia encryption applications [39]–[47]. These applications require nonlinearity, randomness, accuracy, and amalgamation accomplished via chaotic frameworks.

1.1 Related work

In the modern era of digital technology new applications are emerging that come up with diverse security requirements. Researchers are keenly looking to design and develop next-generation encryption algorithms. Despite its cryptographic forte, the AES algorithm is not feasible to use with certain applications for two reasons. AES algorithm possesses high computational complexity and does not synchronize with modern low processing platforms. On the other hand, the algorithm

does not condone any channel noise. To overcome computational complexity, numerous lightweight cryptographic algorithms have been proposed for constricted environments [48]–[54]. These algorithms reduce intricacy and hold resistance against linear and differential attacks. The researchers have also introduced noise-tolerant ciphers capable of resisting disruptive effects, both intended and unintended [55]–[58]. Lightweight ciphers have a drawback that they can't tolerate noise caused by the channels. On the contrary, the noise-tolerant ciphers possess enough computational complexity and not ideal with applications limited to constrained computing capability.

Now a day's chaos-based encryption algorithms are gaining attention because of their excellent cryptographic attributes. Through the application of a 1-D piecewise linear chaotic map an efficient image encryption scheme was proposed by kumar and Acharya [59]. Similarly, another image encryption approach using new and improved 1-D Logistic and Sine chaotic maps were synthesized via output sequences of the existing chaotic maps with the better performance was reported by Li et al. [60]. They identified security flaws and able to cryptanalysis above schemes by the application of chosen plain text attacks. Chaotic image cryptosystems based on bit-level permutations change both pixel and bit position and yield promising outcomes as compared to pixel-level permutation algorithms. Therefore, chaotic image encryption algorithms grounded on bit-level permutation were introduced by Li et al. [61] and Zhang et al. [62]. So far the permutation operation is carried out at a bit level but diffusion is still done at the pixel level. To overcome deficiencies Cao et al. [63] presented an image encryption scheme employing two-dimensional logistic cascade modulation couple hyperchaotic map (2D-LICM) was offered using both bit-level permutation and diffusion concurrently. However, a thorough security review is lacking and it is challenging to determine the resilience of algorithms against attacks. Feng et al. [64] has oversight of some rationality issues and presents an attack to decrypt the scheme. In another image encryption approach, the optical grayscale image is encrypted by the application of QR codes but the results were not verified through cryptographic investigation (see details in Jiao et al. [65]). Following previous studies, Chai et al. [66] documented an efficient chaotic image encryption scheme by the application of elementary cellular automata and compressive sensing. However, the findings of the security analysis demonstrated that the scheme is not appropriate for practical applications. Later on, Chai et al. [67] proposed an image encryption approach by embedding both compressive sensing and the least significant bit. The outcomes are promising but the scheme

required a pre-encryption step and thus enhances the computational complexity. Chaotic image cryptosystems still possess several vulnerabilities and can be cryptanalysis in a shorter span.

Recently, Qayyum et al. [68] proposed an image encryption scheme by the application of two-dimensional chaotic maps. S-boxes are chosen dynamically to execute substitution operation. The scheme is efficient and can deal with modern real-time applications. In Cheng et al. [69], authors developed a hyper-chaotic image encryption algorithm based on quantum genetic algorithm (QGA) and compressive sensing. The output cipher images are optimized through QGA whereas compressive sensing is further adopted to speed up the algorithm. Xian et al. [70] proposed a chaotic image encryption scheme based on pixel scrambling and chaotic digit selection diffusion. The scheme employed two chaotic sequences to improve the diffusion effect and efficiency. Image encryption algorithms aiming at medical and forensic domains were also proposed in [71] and [72]. They utilized a multilayered hybrid cryptosystem through the application of hyperchaotic and hyperelliptic curves and the chaotic Lorenz system and primitive irreducible polynomial S-boxes respectively. Liu and Zhang [73] carried an important analysis of a multidimensional chaotic image encryption scheme to achieve a balance between security and computational complexity. Their proposed scheme only encrypts region of interest calculated through histogram of oriented gradients and support vector machines. Though the algorithm still lacks compression and performance metrics and it’s hard to comment on the application of the proposed scheme. Ahmad et al. [74] reported the chaotic image encryption scheme based on the properties of the orthogonal matrices. This scheme has the capability of tolerating channel noise and JPEG compression, whereas to achieve faster processing, the proposed algorithm encrypts only a small portion of DCT coefficients in the frequency domain. Elashry et al. [75] proposed a new design for the baker chaotic map to encrypt images by utilizing three modes of operation. The proposed scheme intends to elevate security with noise resistance. Patro et al. [76] in another approach introduced a lossless noise-resistant image encryption algorithm using hyperchaos and DNA shuffling operation. Niyat and Moattar [77] employed a DNA sequence with a hybrid Chen chaotic system to encrypt color images. The main idea is to use Chen's chaotic system to produce and deploy three chaotic sequences simultaneously to reduce computational time. Noshadian et al. [78] used a genetic algorithm to optimize the chaotic image encryption scheme. The security simulations reveal vulnerability and further harness the Knuth shuffle technique to overcome

security flaws. In this approach substitution permutation network is employed with multiple chaotic maps to enhance resiliency and overcome security vulnerabilities.

1.2 Motivations

In the aforementioned studies and the survey of current literature, limited research was carried out to study noise resistance via chaotic algorithms for modern low profile applications. The literature shows development surrounding hyperchaos does not guarantee the required security for digital systems, especially to multimedia applications. This is due to inadequate and unreliable implementations of chaos. The available literature on chaos-based multimedia encryption algorithms predominantly lacks cryptanalysis. Moreover, limited security evaluations were carried out to check the resiliency of cryptosystems against attacks.

Modern multimedia encryption algorithms are desired to remain stable against noise added intentionally or unintentionally and have low computational complexity. In this paper, we have proposed a novel, secure and noise-tolerant symmetric image cryptosystem to deal with the modern low profile applications. The present algorithm is based on the S_8 elliptic curve S-boxes with three distinct chaotic maps. The algorithm is developed to be noise resilient with reduced computational requirements.

1.3 Contributions of this work

In this article, three distinct chaotic maps are engaged to develop a paradigm for image encryption. Comprehensive evaluations of the framework show endurance and efficiency of the proposed scheme. The major offerings through this research are outlined below:

1) Chaotic maps are already introduced in detail but the chaotic ranges are re-examined to adequately utilize in the application of the proposed image cryptosystem.

2) Collection of S_8 elliptic curve S-boxes are constructed through the application of symmetric group S_8 and elliptic curves. The permutation operation is utilized in the construction mechanism of new S-boxes and therefore all of them hold identical cryptographic forte. The image encryption framework is presented by employing S_8 elliptic curve S-boxes, cyclic shift with three separate chaotic maps and permutation operation to encrypt digital content. The cryptographic resilience of the proposed scheme is heightened in two ways one is confusion capability and the other is the use of chaotic maps to generate a secure pseudo-random sequence.

3) To evaluate the practicability of the proposed scheme noise resistance of cryptosystem was investigated. The noise was induced in digital information either by channel disturbance or induced deliberately. The cryptosystem shows satisfactory resistance and successfully decipher the corrupted image with minor variations.

4) Series of analyses are then executed on the proposed scheme to establish cryptographic strength. The outcomes of these analyses are further equated with modern renowned encryption schemes. The findings depict eminent performance by the proposed scheme.

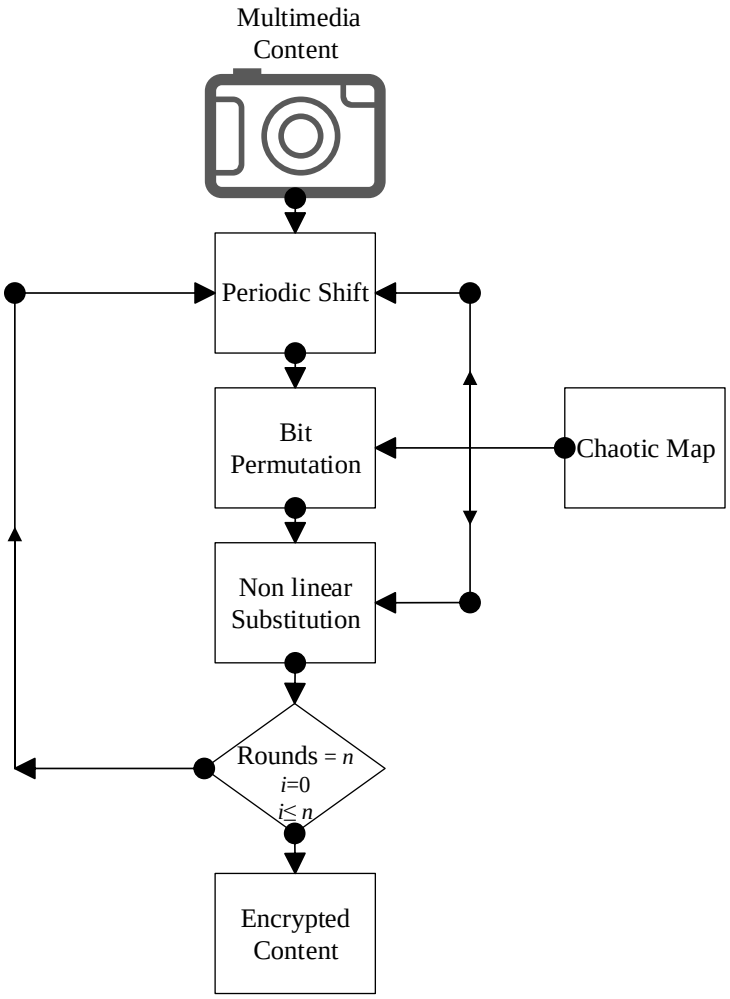


Fig. 1. Overview of the proposed encryption scheme

2 Preliminaries

This segment presents concise details about the building blocks of the proposed scheme. First, the basic details about 3 chaotic maps i.e. Piecewise Linear Chaotic map, Tangent Delay Ellipse

Reflecting Cavity Map System (TD-ERCS) map and Chaotic Logistic map are explained. Second, we will introduce S_8 Elliptic Curve Boxes and finally in the last section introduces our target problem.

2.1 Significance of chaotic maps

The chaotic structures are predominantly employed in secure communication and multimedia security. This section highlights a brief introduction and security of the chaotic maps deployed in the algorithm. The piecewise linear chaotic map or skew tent map is represented as [79]

$$q_n = \begin{cases} \frac{q}{I} & if\ q\ \in [0, I], \\ \frac{(1-q)}{(1-q)} & if\ q\ \in [I, 1], \end{cases} \tag{1}$$

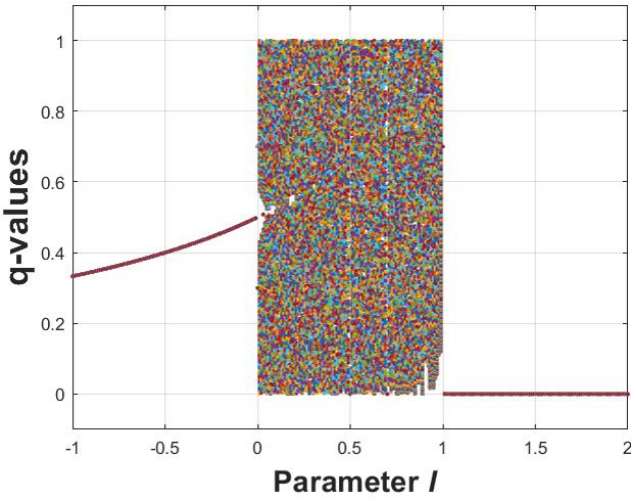


Fig. 2. Bifurcation diagram of the piecewise linear chaotic map. Iteration sequence of q after 700 iterations. Rehashed for every last estimation of I with duration 0.01 and beginning from − 1 to 1

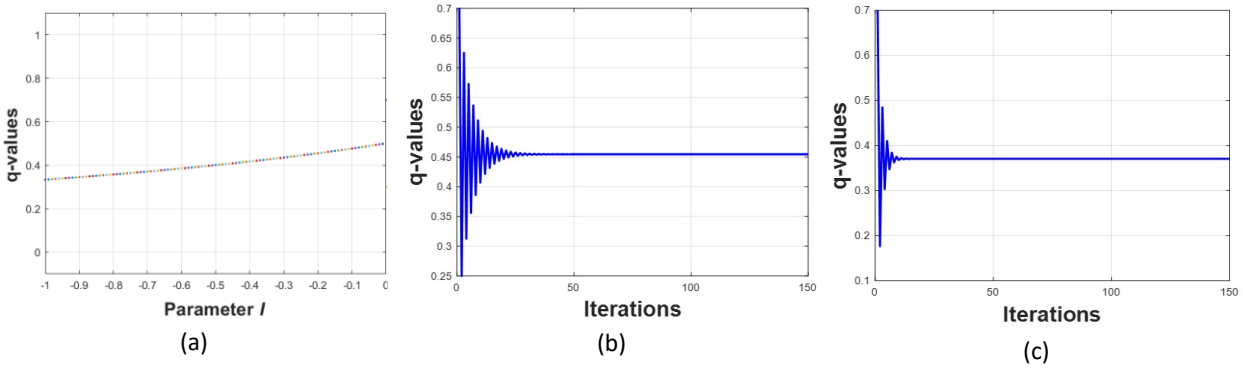


Fig. 3. Plot of skew tent map for period I = -1 to q = 0 and with initial conditions q_0 = 0.7 and I = -0.2, q_0 = 0.7 and I = 0.7 in bifurcation diagram

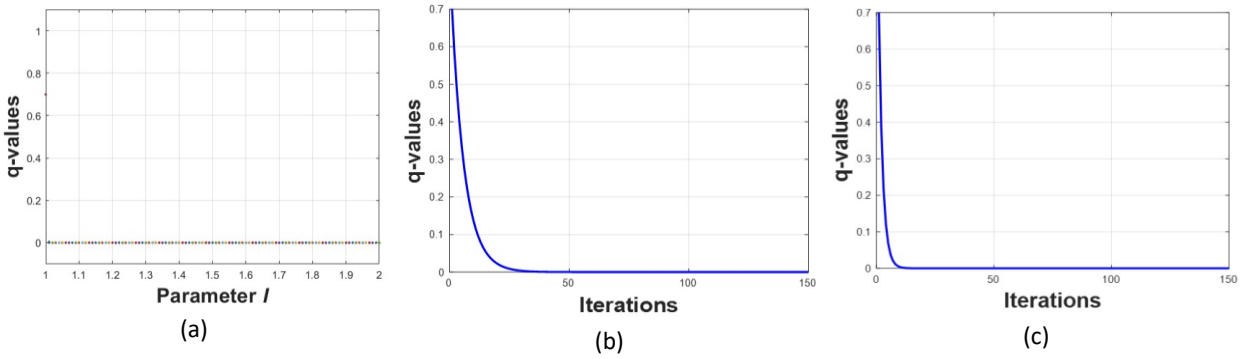


Fig. 4. Plot of of skew tent map for period I = 1 to q = 2 and with initial conditions q_0 = 0.7 and I = 1.2, q_0 = 0.7 and I = 1.8 in bifurcation diagram

The parameter I is the focal parameter and q_0 is the first condition of q having period (0, 1). In fig. 2 bifurcation diagram of the chaotic map is plotted to evaluate performance. The iterations graph is plotted for chaotic sequence after 700 iterations for first value to I to all initial conditions of q and then repeated against each value to I in period -1 to 1 with duration 0.01. Considering I values the graph can be segmented into three regions. The iteration sequence of q_n shows stable behavior after few iterations when I is in the interval $(-\infty, 0]$ and $[1, \infty)$. Fig. 3 and 4 show plot of a skew tent map for I with the interval [-1 0] and [1 2]. The graphs of iterations are plotted for interval [-1 0] with conditions q_0= 0.7, I = -0.2 & q_0=0.7, I= -0.7 shown in fig. 3(b) & 3(c). Similarly, fig. 4(a) & 4(b) shows graphs for interval [1 2] with conditions q_0 = 0.7, I =1.2 and q_0 =0.7, I =1.8. It is noticed that iteration sequences show steady behavior after few iterations and therefore can't be employed in security applications.

In the third segment values of I in the range [0 1] chaotic map has positive Lyapunov exponent [80]. The positive Lyapunov exponent specifies the chaotic behavior of the skew tent map and can be observed through the iteration sequence of q_n. It is observed the whole range does not exhibit chaotic behavior and can be excluded. Fig 5(b) and (c) show that cyclic grouping exhibit steady behavior when plotted with initial conditions q_0 = 0.7, I =0.5 and q_0 =0.7, I =0.7 and hence excluded for secure communication. Nevertheless, the majority of I in the interval [0 1] have chaotic properties and suitable for security applications as seen in fig 5 (d)-(f). Their cyclic behavior is totally random when plotted using initial conditions q_0 = 0.7, I =0.3, q_0 =0.7, I =0.4 and q_0 = 0.7, I =0.8.

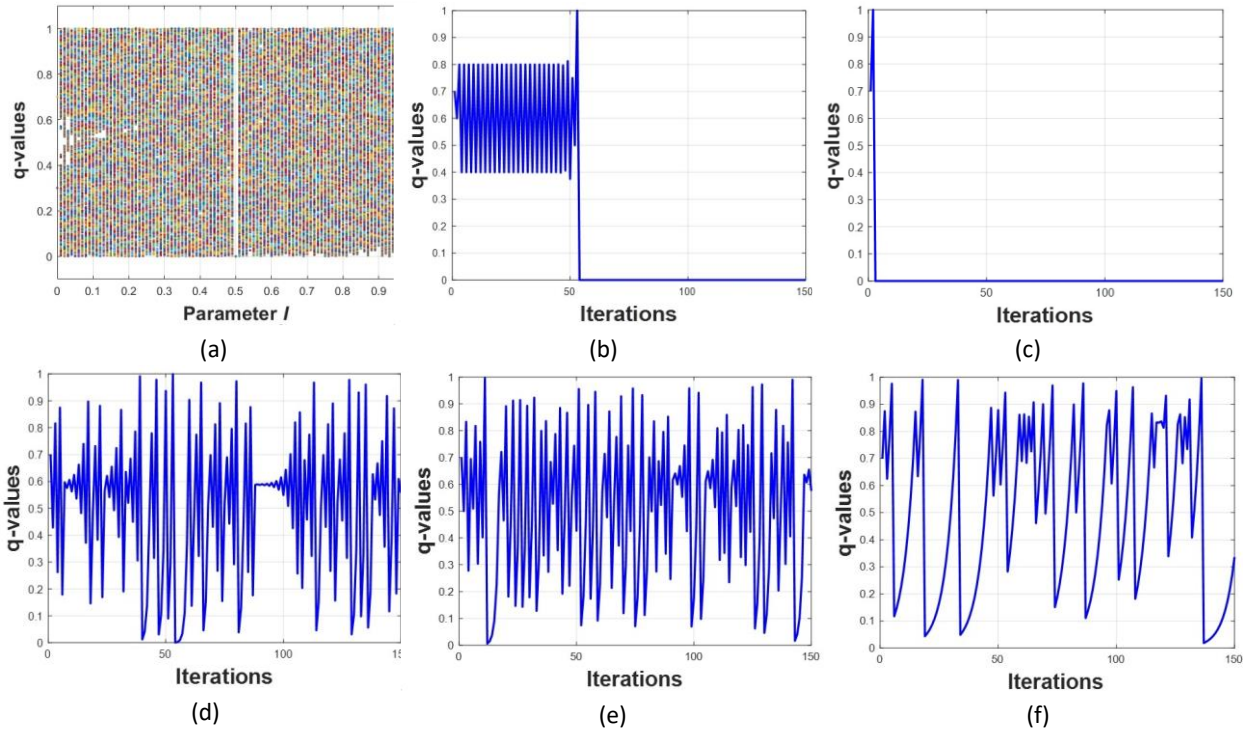


Fig. 5. Bifurcation diagram of skew tent map in interval [0 1] and with initial conditions $q_0 = 0.7$ and $I = 0.5$, $q_0 = 0.7$ and $I = 0.7$, $q_0 = 0.7$ and $I = 0.3$, $q_0 = 0.7$ and $I = 0.4$, $q_0 = 0.7$ and $I = 0.8$

Test Name	**Result**
Approximate Entropy Test	Success
Frequency Test with block (3,4,5,6,7,8)	Success
Frequency Test (Mono bit)	Success
Cumulative (forward/reverse) Sum Test	Success
Discrete Fourier Transform Test	Success
Linear Complexity Test	Success
Binary Matrix Rank Test	Success
The Overlapping Template Matching Test (length= 4, Blocks =4,8)	Success
The Non-Overlapping Template Matching Test (length=4, Blocks= 4,8)	Success
Maurer's Universal Statistical Test	Success
Longest Runs of ones in a Block Test (Block=8)	Success
The Runs Test	Success

Table 1. Examine uncertainty in chaotic sequences made by skew tent map through NIST statistical tests

To examine the randomness of the selected range for $I \in (0, 1)$ NIST statistical test suite is applied as proposed in [81]. The randomness tests are passed for chaotic range as shown in Table 1.

To practically applied in security applications, the chaotic maps should also be sensitive to initial conditions. The chaotic sequence groupings for skew tent map is plotted for initial conditions I=0.4, q_0= 0.700000000000 and I=0.4, q_0= 0.700000000001 as shown in fig. 6(a). The graph shows that all cycles remained identical for initial runs, and then eventually started to phase out with each other. Similarly, in fig. 6(b) we plot chaotic sequence by changing the value of I i.e. I=0.400000000000, q_0= 0.7 to I=0.400000000001, q_0= 0.7. The graph shows that cycles are identical from start but then eventually after an increasing number of iterations both sequences are identifiable.

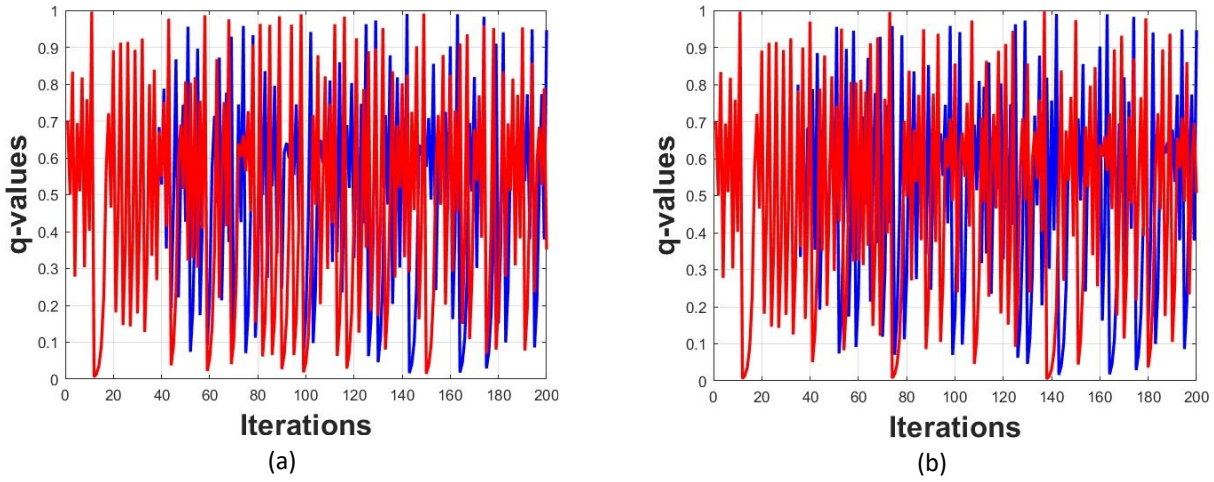


Fig. 6. Chaotic sequence of a skew tent map with preliminary conditions (a) I=0.4, q_0= 0.700000000000 and I=0.4, q_0= 0.70000000000; (b) I=0.400000000000, q_0= 0.7 and I=0.400000000001, q_0= 0.7

Likewise, the remaining two chaotic maps (logistic map and TD-ERCS) used in the encryption scheme exhibits equivalent characteristics as skew tent map. The logistic map employed in the algorithm will be mathematically given as [82]

$$q_n = oq_{n-1}(1 - q_{n-1}), \tag{2}$$

Here $q_0 \in (0, 1)$ and $o \in (3,6,4)$ are the initial input parameters.

TD-ERCS is the third chaotic map and gives two chaotic sequences mathematically expressed as [83]

$$\begin{cases} q_n = -\dfrac{2k_{n-1}y_{n-1} + q_{n-1}(\mu^2 - k_{n-1}^2)}{\mu^2 + k_{n-1}^2} \\ k_n = \dfrac{2k'_{n-m} - k_{n-1} + k_{n-1}k'^2_{n-m}}{1 + 2k_{n-1}k'_{n-m} - k'^2_{n-m}} \end{cases}, \tag{3}$$

where

$$k'_n = \frac{q_n}{q_n}\mu^2,$$

$$y_n = k_{n-1}(q_n - q_{n-1}) + y_{n-1},$$

$$k_{n-m} = \begin{cases} \dfrac{q_{n-1}}{y_{n-1}}\,\mu^2\,, if\ n < m, \\ \dfrac{q_{n-m}}{y_{n-m}}\mu^2, if\ n \geq m, \end{cases}$$

Where (μ, q_0, β, m) are initial seed parameters with $q_0 \in [-1, 1]$, $\tan\beta \in (-\infty, \infty)$, $\mu \in (0.05, 1)$ & $m = 2, 3.....n$ and with these initial parameters.

$$y_0 = \mu\sqrt{1 - q_0^2},$$

$$k'_0 = \frac{q_0}{y_0}\mu^2,$$

$$k_0 = \frac{tan\beta + k'_0}{1 - k'_0\, tan\beta},$$

2.2 S_8 elliptic curve S-boxes

Elliptic curve cryptography has been extensively applied in the development of powerful cryptosystems. Azam et al. [84] presented an algorithm to yield 8x8 S-boxes by applying the elliptic curve over a finite field. These S-boxes are used as a catalyst to create new S_8 Elliptic Curve S-boxes. Hussain et al. [30] by the application of symmetric group S_8 proposed an algorithm to construct a collection of cryptographically potent S-boxes. An S_8 symmetric group is a group of permutations of order 40328. The fundamental architecture of this algorithm is based on the permutation operation that is incorporated in the algebraic construction of the resultant substitution

box. We will propagate with the action of the S_8 symmetric group on ECs to yield 40320 unique S-boxes of equal strength and features.

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

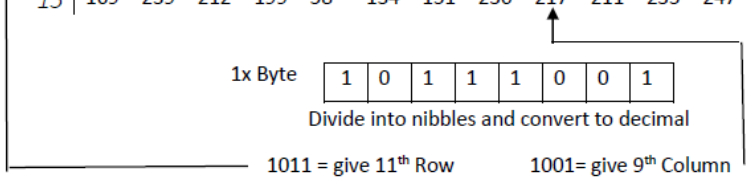


Fig. 7. Process for S-box transformation

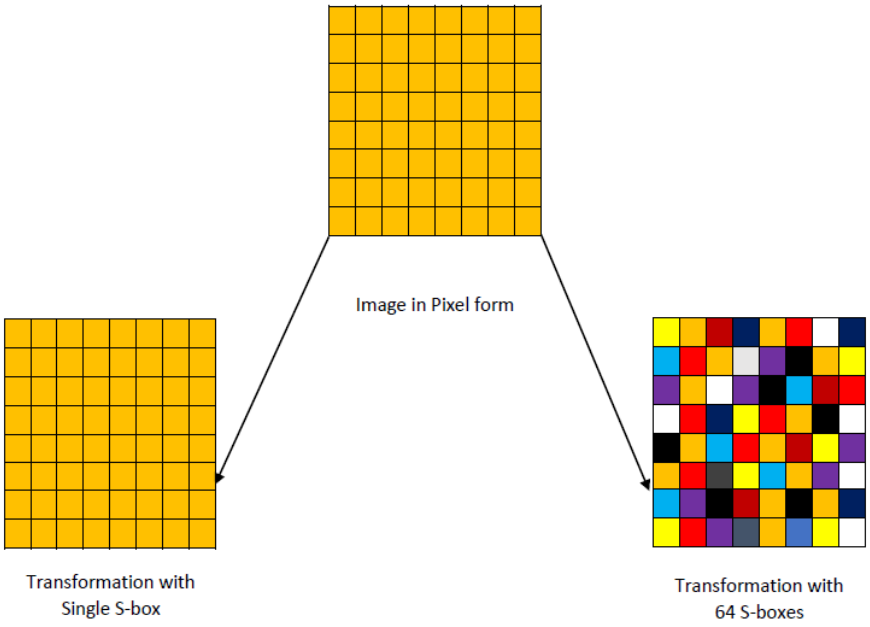


Fig. 8. Transformation effect through S-box

An image is a combination of pixels and in GF(2^8) every pixel can be represented in 8 bits with each element belong to GF(2^8). Consider an element of S-box represented by one byte and then divide it into two nibbles and further convert 4bits into decimal form as shown in fig 7. The first value is reflected as the row number (11^{th}) and the second value (9^{th}) as the column number. The element at the junction of the 11^{th} row and 9^{th} column is further swapped with the pixel on a plain text image. Similarly, S-box will be transverse for the whole image.

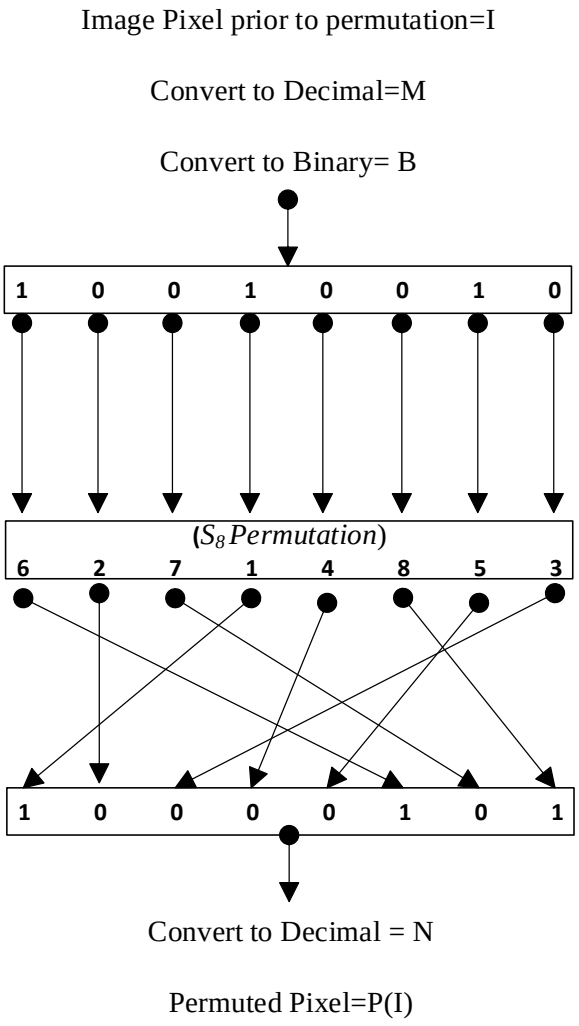


Fig. 9. Permutation for single pixel

2.3 Problem statement

The cryptosystem constructed by the application of a single S-box does not hold sufficient resilience as well as efficiency to cope with modern applications. Multimedia content such as

digital images possesses correlated data so multiple S-boxes will create high confusion and diffusion. We consider an 8x8 image with 64 pixels and the correlation among pixels is 1 as shown in fig.8. The transformation of the image is accomplished by a single S-box as well as by using a combination of 64 different S-boxes. fig. 8 reveals that a single S-box transformation does not improve correlation though multiple S-boxes enhanced correlation and shift pixel colors. The probability of two pixels with similar colors is very minimal. Image transformation through multiple S-boxes can give optimal value and able to achieve the desired security using a fewer number of encryption rounds.

3 Proposed encryption algorithm

Application of S_8 permutations and permutation of a particular type on elliptic curve S-boxes is a basic step to acquire confusion and diffusion between ciphertext and secret key and plaintext and ciphertext. The process of substitution along with permutation on an individual pixel is illustrated in fig. 7 and fig. 9. It is evident that S_8 permutation will completely alter the decimal value of image pixel and after application on S-box will also yield an entirely different S-box. It is indicated by the application of S_8 the algebraic properties of new S-boxes remain the same and become a vital characteristic in the development of a resilient cryptosystem. The multimedia content or data is taken in the form of an eight-bit length and introduces a cyclic shift along with substitution and permutation. The process is described below.

3.1 Encryption

As shown in fig. 10 digital image represented by P with dimensions a x b x c is fed as an input to an encryption algorithm. where a and b represents the number of rows and columns and c denotes the number of frames in a color image. A color image contains three frames and the grayscale image has only one frame. The pixel of an image at a certain point is denoted as $P(i,j,m)$ and for ease consider $P(i,j,m)$ as $P(i,j)$ where i,j,m represent ith row, jth column and mth frame. The pixel of the grey image has a range of [0 255] and can be represented in 1 byte or 8 bits. The proposed image encryption algorithm constitutes three major steps i.e. cyclic shift, permutation and substitution. A separate collection of hidden keys is used during the execution of these steps.

Suppose q_o and I will be the initial values resulted from a chaotic sequence q by the application of skew tent chaotic map. The initial values $q_o=k_1$, $I=k_2$ are the first two secret keys of

the offered encryption scheme. The length of a chaotic sequence is ($a*b*c$) with an initial range between [0 1]. To deploy our proposed algorithm, the range will be amplified by multiplying sequence with 100 and further limit value below 255 by applying modulo 8. We convert and represent each pixel of image $P(i,j)$ into a binary of 8 bits termed as $P_b(i,j)$. Now further we perform left cyclic shift of q_x bits and termed cyclic shifted image as $P_c(i,j)$ where x=1,2,3….a*b*c. Such as suppose P_b(i,j)=11011011 and q_x=3 then P_c(i,j)=10111011 is the result after cyclic shift.

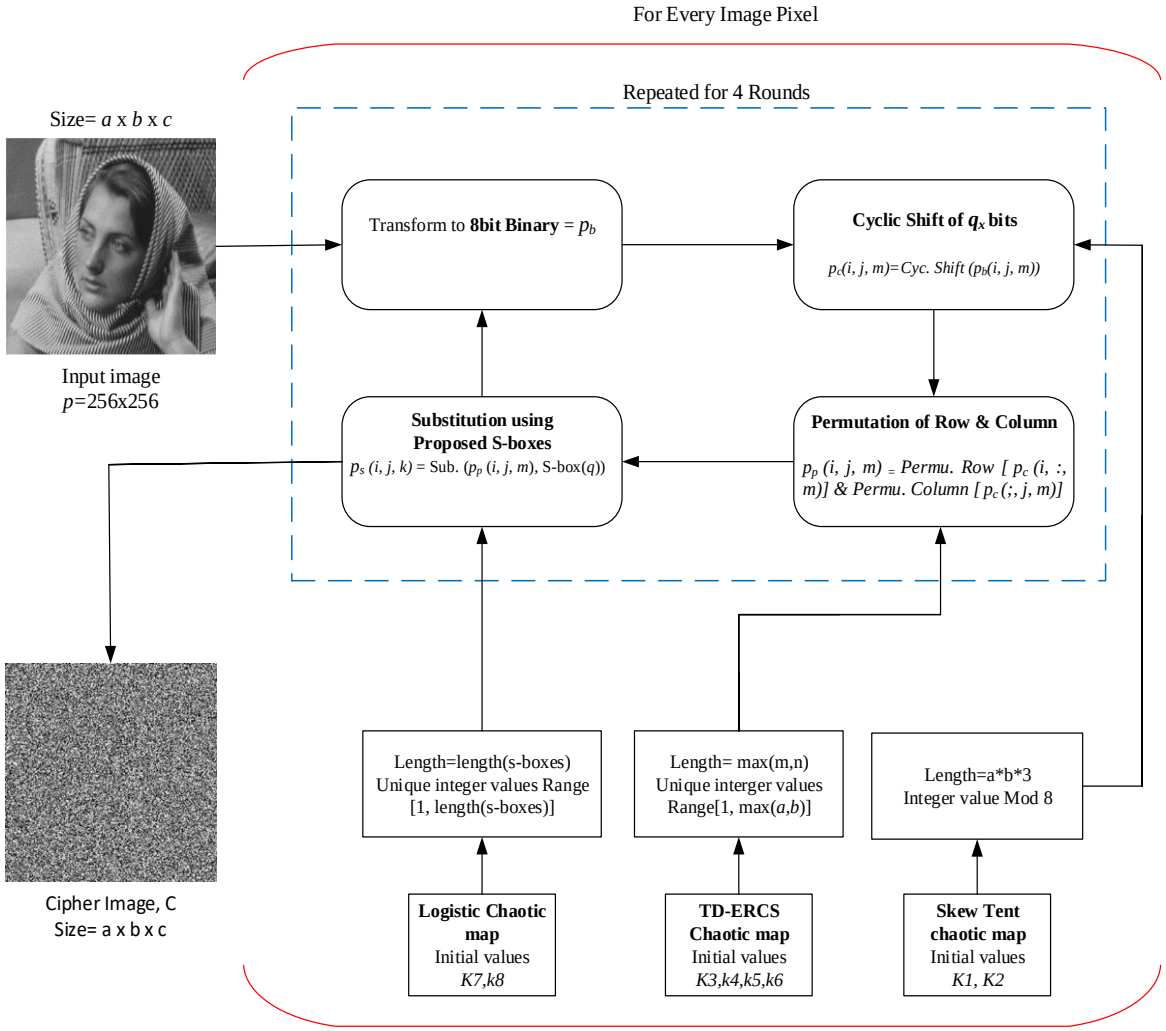


Fig. 10. Flowchart of proposed encryption algorithm with a unique set of keys deployed in each of three modules

We consider two chaotic sequences r and s with initial values of q_0, $tan\ \beta$, μ & m resulted from the application of TD-ERCS chaotic map. These four initial values were deemed to be the subsequent four secret keys of the suggested encryption scheme i.e. k_3, k_4, k_5 and k_6 respectively.

Additionally, only one chaotic sequence is required so we utilize sequence *r*. The range of *r* is [1, max (*a*,*b*)] where max(*a*,*b*) is the length of *r*. The initial range of chaotic sequence [-1,1] is expanded to [0,2] and further multiply sequence with 100 *max (*a*,*b*) but also restricting in range [1, max(*m*,*n*)]. Besides vector *r* only possess unique values from 1 to max (*m*, *n*). Simultaneously in step 2 binary value of the cyclic shifted pixel of the image is again altered into decimal and represented as $P_d(i,j)$. Regarding chaotic sequence *r* permutation of rows and columns will be done on $P_d(i,j)$ and resulted in a permuted image P_p. For instance, if the initial three values of chaotic sequence *r* are (42,86,11) then the initial three rows of P_d will be position at (42,86,11) rows of P_p. By the action of row and column permutation on P_d we get permuted image P_p.

$$\begin{cases} P_p(:, r(i)) = P_d(:, i), \ \forall\, i \in a, \\ P_p(y(i), :) = P_{p_1}(j, :), \ \forall\, j \in b, \end{cases} \tag{4}$$

Suppose q_0 and *o* be the initial values of another chaotic sequence *t* resulted from a chaotic logistic map. These two initial values are the subsequent two secret keys of the suggested encryption scheme i.e. $k_7$and k_8. The length of a chaotic sequence is *a*b*c* under modulo η and η is the overall amount of S-boxes employed in the algorithm. As done previously the initial range of chaotic sequence [0 1] has been amplified with 100* η and restricting under modulo η. Let S_p be the number of S-boxes generated via the symmetric group of permutation. The amount of S-boxes employed will depend upon the number of applications. The high profile applications, for example, will require 256 S-boxes and low profile applications on the other hand need only 128 S-boxes to attain the desired security. Although the larger number of S-boxes increases the computational complexity of the algorithm. In the third step, each image pixel P_p is substituted with one of the substitution boxes as per the substitution process shown in fig. 7.

$$P_s(i,j) = sbox\left(P_p(i,j), S_{t(q)}\right), \quad \forall\, i \in a, \forall j \in b, \forall q \in (1,2, \dots a * b * c) \tag{5}$$

Two parameters are required for this step image pixels P_p and substitution boxes. To make the algorithm more secure selection of each S-boxes to encrypt image pixels is done by using chaotic sequence *t*. Now the result obtains from this substitution is I_s and we again perform cyclic shift and similar operations. The above three steps are further repeated for four rounds until we acquire the resultant encrypted image *C* of the identical size as the original.

3.2 Decryption Stage

The decryption is identical to the encryption algorithm but in reverse order. In decryption the cipher image of size *a*b*c* is fed as input and operations of cyclic shift, substitution and permutation are performed in reverse order. Whereas the same set of secret keys are used to decrypt the cipher image.

During the initial step, every pixel of cipher image *C* is substituted by the application of inverse S-box substitution. Inverse S-box substitution on cipher image *C* is presented as follows.

$$P_{is}(i,j) = inv\_sbox\big(C(i,j), S_{t(q)}\big), \quad \forall\, i \in a, \forall j \in b, \forall q \in (1,2,\dots a * b * c) \tag{6}$$

The inv_sbox is a function that takes two parameters i.e image pixels, S-box and performs inverse substitution. Pixels of the cipher image is substituted through inverse substitution by applying different S-boxes. The S-boxes are selected through chaotic sequence *t* having initial values q_0 *and o* generated by the application of chaotic logistic map.

Following similar lines, the inverse of permutation is applied to image P_{i8} in accordance with the chaotic sequence *r*. The chaotic sequence *r* is generated by the application of TD-ERCS map with identical initial values utilized in the encryption scheme. We further obtain image P_{ip} as a result of this inverse permutation. For instance, if the initial three values of chaotic sequence *r* are (42,86,11) then the initial three rows of P_{i8} will be positioned at (42,86,11) rows of P_{ip}. Through the action of the row and column permutation on P_{i8} we get inverse permuted image P_{ip}.

$$\begin{cases} P_{ip1}(:,i) = P_{i8}(:, y(i)), \ \ \forall\, i \in a, \\ P_{ip}(j,:) = P_{ip_1}(y(i),:), \forall\, j \in b, \end{cases} \tag{7}$$

In the third and final step, we convert image pixels of P_{ip} into binary form comprising 8 bits and denote binary representation as $P_{ip}(i,j)$. Besides this right cyclic shift of q_x bits is performed on the image and the result is denoted as $P_{ic}(i,j)$ where q=1,2,…..*a*b*c* and q is chaotic sequence results through the application of skew tent map with similar initial values as employed in encryption. Just like the encryption the above three steps are replicated for four rounds to decode cipher image *D*. The output is finally achieved in the form of the original image.

4 Results and discussion

To perform simulations analysis, the algorithm is fed with an image ‘barbera’ as a carrier image of size 256x256x1 i.e. there are 256 rows, 256 columns and one frame. Table 2 outlines secret

encryption keys that are preliminary values of the three chaotic maps engaged. The input image and its histogram are presented in fig. 11(a) and (c). The input image is now encrypted using the intended scheme and ocular results in fig. 11(b) reveal that encryption outcomes are notably strong. The histogram of the encrypted image is further plotted in fig. 11(d) and the flat histogram shows the resiliency of the proposed encryption scheme. Moreover, to investigate the effect on the correlation of pixels, one greyscale image is considered having a color value of 127. By plotting the histogram of this image in fig. 12(c) only one peak value is observed showing maxing autocorrelation of image pixels. The grey image is now further encrypted with the same set of keys using the proposed encryption scheme. This encryption results in fig. 12(b) render strong encryption outcomes for greyscale image despite an elevated autocorrelation present in the plain image. Flat histograms of the encrypted image in fig. 12(d) reveals the strength of our proposed cipher.

To present a comprehensive simulation analysis of the proposed scheme, the results of encryption after each step on the input image are presented. The proposed scheme offers three major steps performed in four rounds therefore *4x3=12* images are analyzed as shown in fig. 13. The first three images are from round one other three from round two and so on. By observing fig. 13(round1-a) after cyclic shift step the results are not properly concealed. The permutation step is further applied to the image and resultant fig. 13(round1-b) still shows little glimpses of the original image. The third step of nonlinear substitution is further applied and form fig. 13(round1-c) it is observed that the image is entirely obscure and no fragment of it exposes original information of an image. The rest of the figures shows encrypted images for the other three rounds. It is evident from visual results that the strength of the presented encryption scheme is very strong. The results are further substantiated in the next section through statistical analysis.

4.1 Elementary Statistical analysis

The statistical analyses further examine visual strength and give an overview of the working of the cryptographic framework. The results are compared with prevailing image encryption schemes.

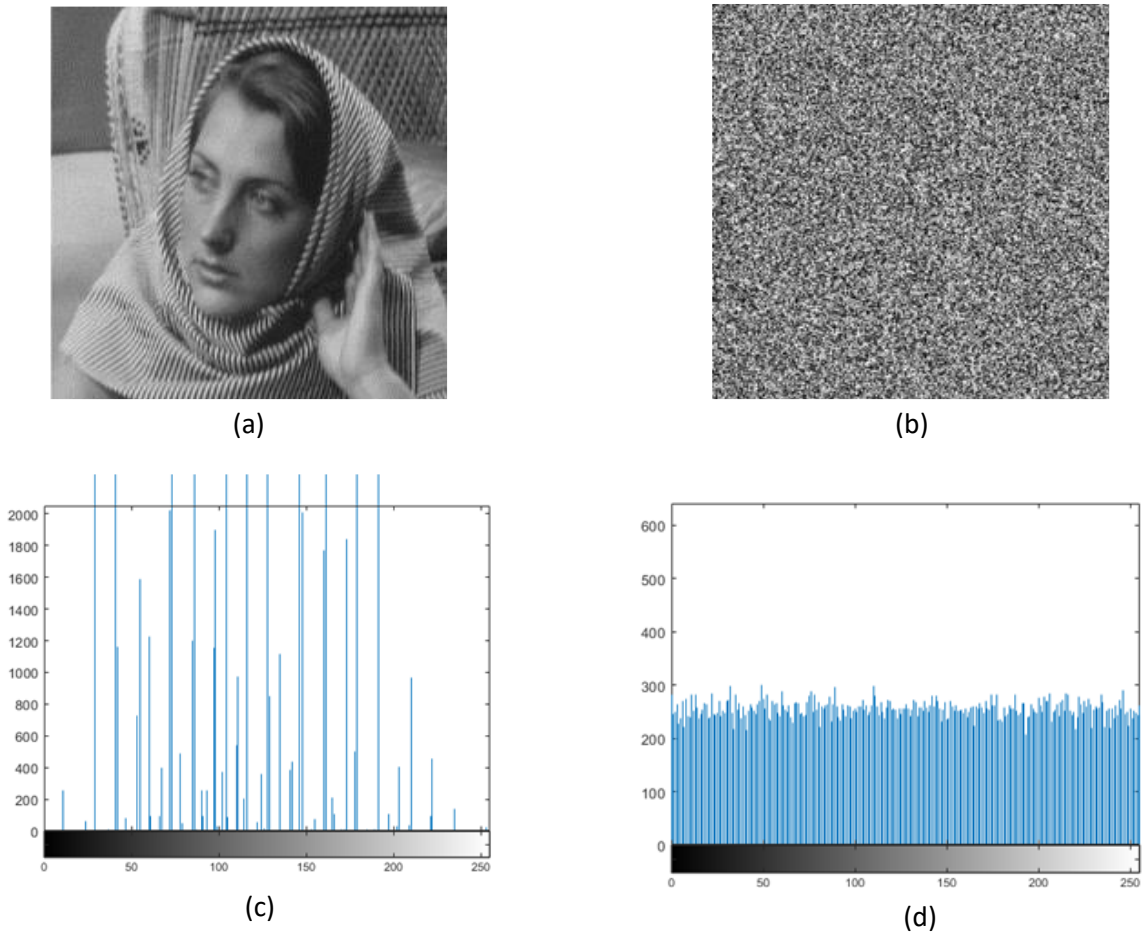


Fig. 11. Simulated results of the proposed encryption scheme with the histogram of an original and encrypted image

Parameters						
Chaotic Maps	q_0	$tan\beta$	μ	m	O	I
Skew tent chaotic map	0.4					0.8
TD-ERCS chaotic map	0.5	1	0.4	50		
Logistic chaotic map	0.5				3.7	

Table 2. Preliminary values for chaotic maps employed in the proposed encryption algorithm

4.1.1 Correlation

Correlation analysis is a cardinal tool to ascertain the resemblance between two images. Correlation is extremely beneficial in multimedia encryption applications, especially where cryptanalysis has added the edge of visually perceiving cipher images and extracting unauthorized details. The equation presents the correlation of an image as mentioned below.

$$Correlation = \sum_{i,j} \frac{(i-\alpha i)(j-\alpha j)\Psi(i,j)}{\varphi_i \varphi_j} \ , \tag{8}$$

i & *j* represent positions of row and column and ψ(*i*,*j*) is the value of a pixel at the ith row and jth column. α and φ both represent variance and standard deviation. The analysis ascertains perfect correlation by measuring similarity among two neighbor pixels for the entire image having range [- 1 1] with 1.

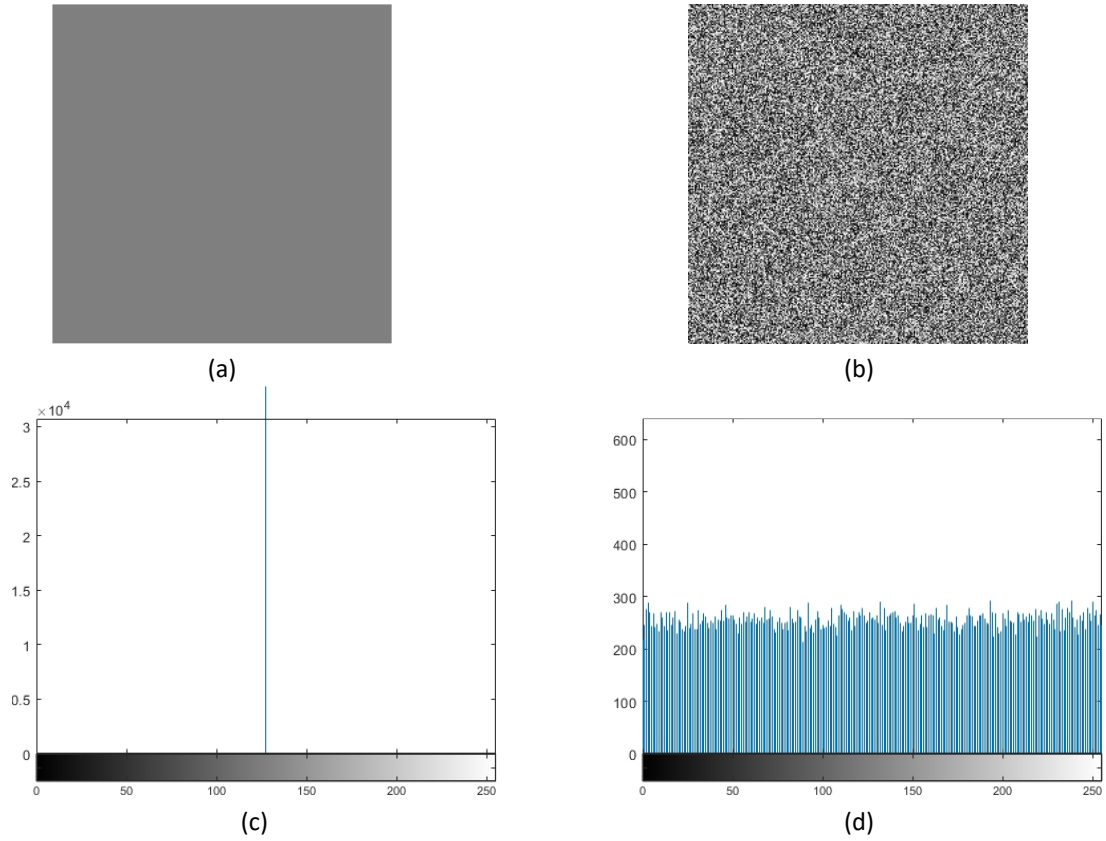


Fig. 12. Simulated outcomes of the proposed encryption scheme with histograms of an original and encrypted grayscale image

4.1.2 Entropy

Entropy is used to measure the texture and show randomness in a digital image. It is the amount of uncertainty of a random variable to occur in a random process. It is defined as

$$Entropy = -\sum P_r(\Psi(i,j)) \log_2 P_r\big(\Psi(i,j)\big), \tag{9}$$

i & *j* represent positions of row and column and ψ(*i*,*j*) is the pixel value at ith row and jth column. $P_r(i,j)$ represent the probability of image pixel. The entropy analysis demonstrates the randomness

of an image having 256 grayscales and a range [0 8]. The higher value of entropy reveals higher randomness.

4.1.3 Contrast

The viewer at certain times vividly identifies objects in encrypted images due to lack of high levels of diffusion. The contrast level determines that the encryption process is not effective and unable to generate the required amount of diffusion. The intensity among pixels is measured in accordance with some of the neighbors.

$$Contrast = \sum_{i,j} |i-j|^2 \ \Psi(i,j), \tag{10}$$

i & *j* represent positions of row and column and ψ(*i*,*j*) is the value of the pixel at ith row and jth column. Ranges of contrast values are [0 (size(Image)−1)2]. The constant image has a contrast value of zero and a larger value of contrast shows a larger deviation in image pixels.

4.1.4 Homogeneity

The homogeneity analysis measure characteristics of distribution showed by elements in the gray-level co-occurrence matrix (GLCM). GLCM measures pixel brightness values or gray levels by statistically process data. GLCM is expressed as,

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

i & *j* represent positions of row and column in image pixel. [0 1] represents the range of the homogeneity.

4.1.5 Energy

This energy analysis of an image quantifies the energy and provides the sum of squared elements of gray pixels in GLCM. The energy is expressed as

$$Energy = \sum_{i,j} \Psi(i,j)^2, \tag{12}$$

i & *j* represent positions of row and column in pixel of an image. [0 1] represents a range of energy and the energy of a constant image is one.

The above analyses are performed on the proposed encryption algorithm and outcomes are further equated with other related work as presented in the table. 3. The findings indicate that our proposed scheme has superior performance.

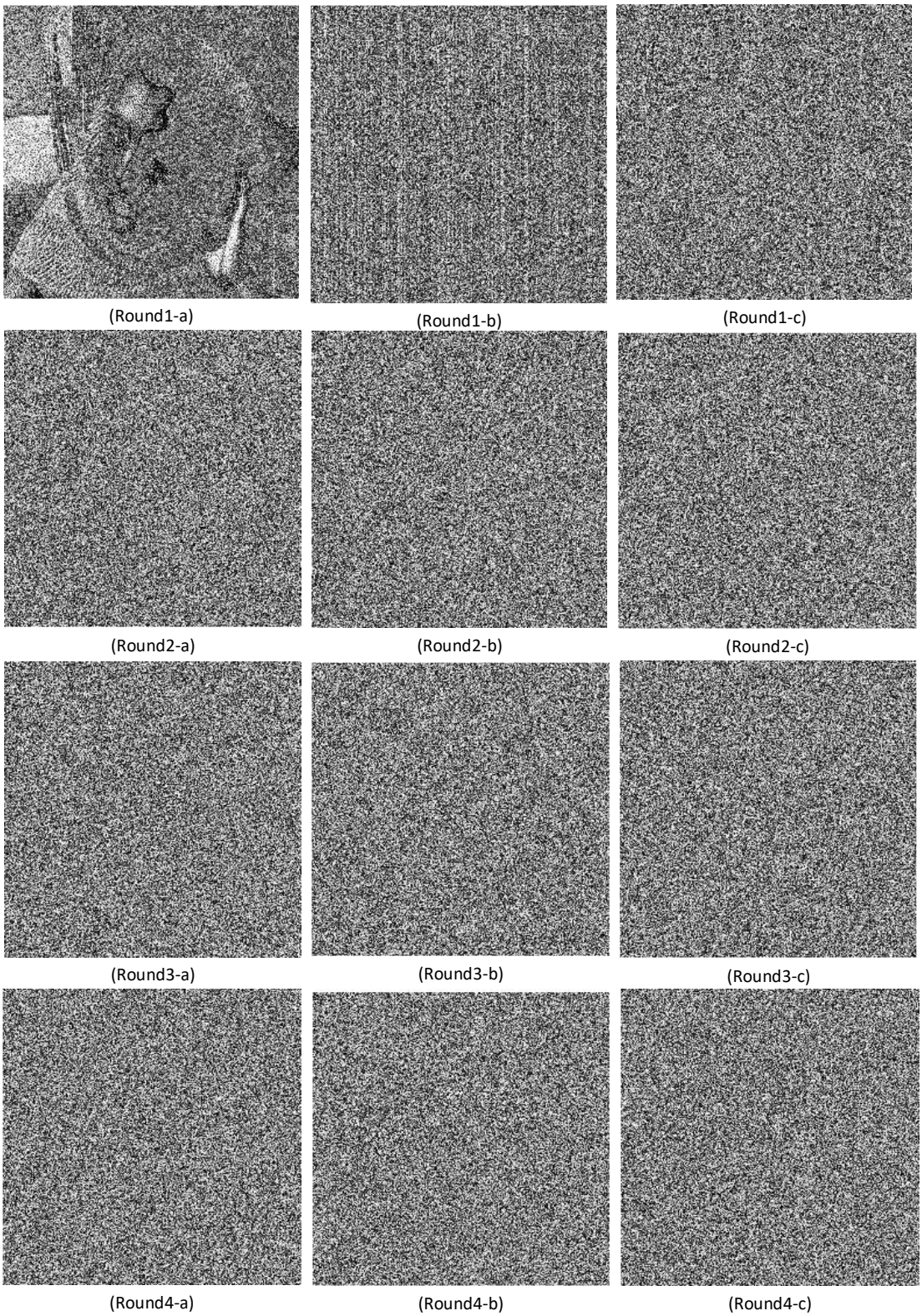


Fig. 13. Output images after each module during encryption rounds

Statistical Analysis (Lena Image)	**Ref.** [85]	**Ref.** [68]	**Ref.** [86]	**Ref.** [87]	**Ref.** [88]	**Ref.** [72]	**Proposed Scheme**
Entropy	7.9801	7.9973	7.9311	2.5643	7.9735	7.9521	7.9862
Contrast	8.6603	10.5325	8.0522	4.9454	8.1833	8.4587	10.4873
Energy	0.0674	0.0156	0.1984	0.4263	0.2132	0.3521	0.0156
Homogeneity	0.9102	0.3887	0.8365	0.5733	0.8251	0.9598	0.3906
Correlation	-0.0293	-0.0068	-0.0308	0.0439	0.0313	-0.0003	0.0012

Table 3. Comparison of Statistical analysis on an encrypted image with related work

4.2 Security and performance analysis

These analysis helps to determine the resilience, strength and performance of an encryption algorithm. A lot of recent work in encryption particularly image encryption lacks security and performance analysis and that's why it's difficult to determine the strength of these algorithms. These analyses are performed on the proposed encryption algorithm and results are equated with prevailing encryption schemes to benchmark the superior performance of the algorithm.

4.2.1 Analysis of sensitivity and space of encryption key

The total number of keys that can be deployed in an encryption algorithm is called keyspace. In this work, eight secret keys are derived from the preliminary conditions of three chaotic maps. The values and ranges of all eight secret keys are mentioned earlier. The average range of these security keys is sufficiently large. Suppose the average range of key is 10^{10} for all the eight keys, so there are 10^{80} possible keys nearly equivalent to 256 binary bits. The check this keyspace for all possible combinations a modern computer would require about 10^{20} years.

Keyspace alone is not adequate to ensure the effectiveness of a cipher and along with keyspace, key sensitivity should be attained as well. Key sensitivity is a property related to the decryption of cipher data such that it is not possible to decrypt the cipher if there is a minor change (even a single bit) of encryption and decryption keys. In this work, the input image is encrypted with secret keys shown in table 2 moreover resultant encrypted image is presented in fig. 11(b). Three different cases are considered to show the key sensitivity of our proposed encryption scheme. In the first case key k_5 is changed to $k_5=\mu=0.4$ to $k_5'=\mu=0.400000001$ and the rest of the seven keys remain the same. Fig. 14(a) represents the decrypted image and it is observed that decryption is not successful regardless of the tiny modification in only one key. In the second case

key k_3 is changed from $k_3=q_0=0.5$ to $k_3'=q_0=0.5000000001$ and for the third case $k_7=o=3.721546321451$ to $k_7'=o=3.721546321452$. The decrypted images of the second, and third cases are shown in fig. 14 (b) & 14(b). In all these cases decryption is failed despite a minor change in secret keys. The strong results evidently prove the key sensitivity of the proposed encryption algorithm.

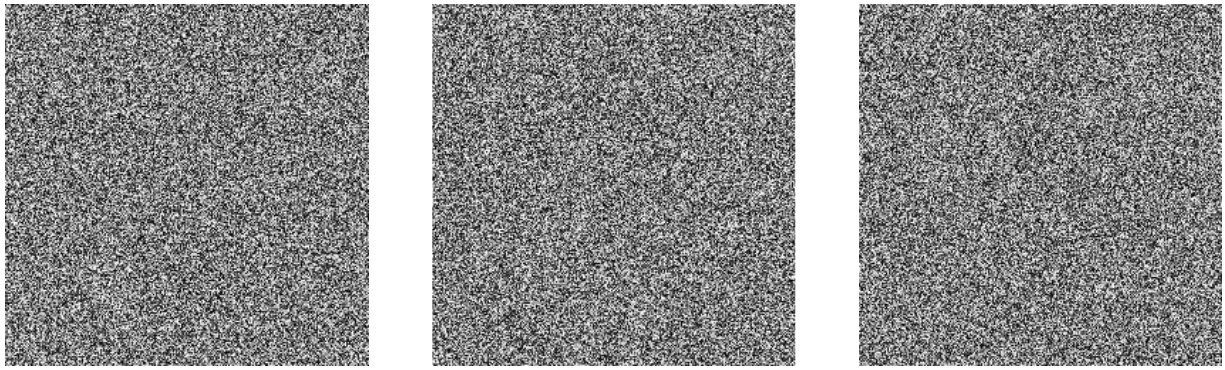


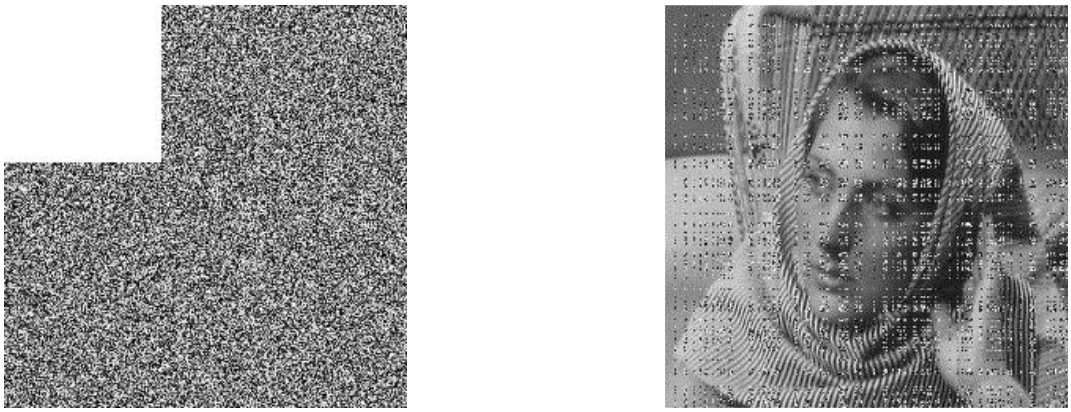
Fig. 14. Result of key sensitivity analysis with a minor change in encryption keys

4.2.2 Analysis of noise tolerance

The capability to resist noise is now one of the essential traits of all modern image encryption algorithms. The noise is added as a result of a wired or wireless channel and also deliberately by an unauthenticated user as well. As it's a well-established fact that data transmitted via channel could be affected by the channel noise. The majority of renowned ciphers are designed in a way that if cipher data is slightly corrupted they might unable to decrypt the data or image. To cater to this both error correction and error detection methods are applied to both transmitter and receiver. This will allow performing encryption and decryption successfully but enhances the computational complexity of the system and not pertinent especially for low profile applications. The low profile applications require more speed in contrast with security.

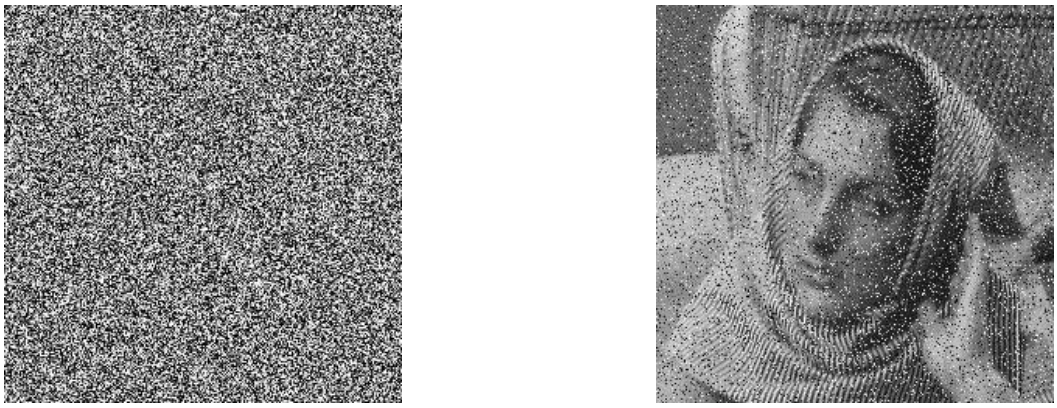
The proposed scheme can be used to decrypt the cipher image correctly with slight changes although the cipher image was induced with noise addition. Experiments have been performed on our cipher images by adding noise and then try to decrypt through the proposed algorithm. The input image is encrypted with secret keys as shown in table 2. Noises are added in these images and scenario-one first 10000 pixels of cipher image is corrupted with white ones as shown in fig. 15(a). Fig. 15(b) represents the decipher image obtain through decryption. It's clearly evident that

decryption is effective with only minor variations in the cipher image. Salt and pepper noise of density 0.2 is further added in cipher image as fig. 16 (a). The results in fig. 16(b) represents the decipher image and its evident that the resultant image is identifiable as the original image. In another scenario, the plaintext is considered an input to encryption. It's seen that if a few bits are corrupted or altered the whole text will be changed completely and cannot be recognized. This is very different from the image scenario. In that scenario, if some of the bits are corrupted, then the whole text will be changed completely. To understand the importance, suppose a law enforcement agency wants to disseminate the picture of a criminal through a mobile application. The picture is encrypted to avoid any unauthenticated access. In that case, even if the picture is corrupted through channel noise then even our proposed scheme may able to decrypt the photo. The other side recognizes the face of a criminal from the picture although the quality of the decipher image is not good. This is an important application of the proposed encryption algorithm.



(a) (b)

Fig. 15. Decryption results after noise addition in which100x100 pixels are corrupted or cropped



(a) (b)

Fig. 16. Decryption results after addition of salt and pepper noise of density 0.2 pixels in cipher image

4.2.3 NPCR and UACI Analysis

The number of pixels change rate (NPCR) and unified average changing intensity (UACI) are used to investigate the performance of an image encryption algorithm. The numbers of pixels changed in cipher image due to a single change in pixel of the plain image is measured through NPCR. Whereas UACI measures the average intensity among two cipher images produced as a result of a single shift in plain image. These two indicators are expressed as

$$NPCR = \frac{\sum_{x,y} O(x,y)}{M \times N} \times 100\%, \tag{13}$$

$$UACI = \frac{1}{M \times N} \sum_{x,y} \frac{|C_1(x,y) - C_2(x,y)|}{255} \times 100\%, \tag{14}$$

Where *M* and *N* are the width and height of cipher images C_1 and C_2 obtained through a single change of pixel in an input image. *D (x, y)* can be defined as

$$D(x,y) = \sum_{1}^{0} \quad \begin{matrix} if\ C_1(x,y) = C_2(x,y) \\ If\ C_2(x,y) \neq C_2(x,y) \end{matrix},$$

Image	**Lena**	**Barbara**	**Cameraman**	**Baboon**
NPCR(%)	99.565	99.591	99.262	99.583
UACI(%)	30.9131	29.4912	31.5723	29.7365

Table 4. NPCR and UACI for the proposed encryption algorithm

Analysis (Lena image)	**Ref. [89]**	**Ref. [90]**	**Ref. [91]**	**Proposed**
NPCR(%)	99.606	99.609	99.614	99.565
UACI(%)	33.4621	28.6181	28.6098	30.9131

Table 5. Comparison of NPCR and UACI with relevant approaches

Table 4. presents the result of NPCR and UACI using different images of size 256 x 256 and reveals that the algorithm is highly sensitive to small changes. Comparisons with other modern schemes have been done in table 5. depicted the excellent performance of the proposed approach.

4.2.4 Encryption Quality

The measurement techniques are used to gauge the performance of encryption algorithms such as mean-squared error (MSE), peak signal-to-noise ratio (PSNR) and structural similarity index (SSIM). The MSE measures the similarity whereas SSIM calculates the difference between two images. PSNR is the ratio between the original and encrypted images. These are mathematically expressed as

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [P(i,j) - C(i,j)]^2, \quad (15)$$

$$PSNR = 20log_{10}\left(\frac{255}{\sqrt{MSE}}\right), \quad (16)$$

Where $M \times N$ is the size of the image and P and C are both plaint and encrypted images respectively.

$$SSIM = \frac{(2\bar{P}\,\bar{C}+B_1)\,(2\sigma_{PC}+B_2)}{(P^2+C^2+B_1)\,(\sigma_P^2+\sigma_C^2+B_2)}, \sigma_C \quad (17)$$

Here $\bar{P}$, $\bar{C}$ is the mean of plain and encrypted image and σ_P and σ_C is the standard deviation of plain as well as encrypted image. Further σ_{PC} represents cross-correlation and $B_1 = (K_1\,O)^2$ and $B_2 = (K_2\,O)^2$, where O is dynamic range of pixel values and $K_1 = 0.02$ *and* $K_2 = 0.03$. It's evident from results in table 6. that the proposed scheme cohere sound encryption effect and quality.

Analysis	**Lena**	**Barbara**	**Cameraman**	**Ref. [92]**	**Ref. [93]**	**Ref. [94]**
PSNR	8.6098	9.0915	8.4143	7.87	8.1360	7.9709
SSIM	0.000513	0.0028	0.0021	0.0065	0.0165	0.0088
	Lena	**Barbara**	**Cameraman**	**Ref.** [68]	**Ref.** [95]	**Ref.** [92]
MSE	9026.4	8078.8	9442.1	9489.7	9325.6	9105

Table 6. Results of PSNR, SSIM and MSE analysis and comparison from recent approaches

4.2.5 Fixed-point ratio and gray average change value analysis

The fixed-point ratio is the percentage of pixels with no change after the image is encrypted. The encryption scheme aims to render the encrypted image as different from the original image. The

gray average change value calculates the gray level change of the encrypted image. These are expressed as

$$\begin{cases} BD(P,C) = \frac{\sum_{x=1}^{rows}\sum_{y=1}^{cols} k(x,y)}{rows \times Cols} \times 100\% \\ K(x,y) = \begin{cases} 1, p_{xy} = C_{xy} \\ 0, otherwise \end{cases} \end{cases}, \tag{18}$$

$$GAVE(P,C) = \frac{\sum_{x=1}^{rows}\sum_{y=1}^{cols}|C_{xy} - p_{xy}|}{rows \times colx}, \tag{19}$$

Where *P* and *C* represent plaintext and ciphertext image. The results in table 7. and table 8. depict superior performance of the proposed scheme.

Fixed-point ratio analysis	**Total no. of pixels**	**Number of fixed point**	**Rate of fixed point**
Lena	65,536	288	0.44%
Barbara	65,536	268	0.41%
Cameraman	65,536	245	0.37%
Baboon	65,536	273	0.42%
Ref. [96]	65,536	242	0.37%

Table 7. Fixed-point ratio analysis

Images	**Lena**	**Barbara**	**Cameraman**	**Baboon**
Change values of gray average	77.8327	74.2067	79.5131	74.8321
Ref. [96]	73.3558	-	-	69.9078

Table 8. Gray average change value analysis

4.2.6 Chi-Square analysis

Chi-square analysis inspects data variations from expected value and demonstrates uniformity in encrypted images. Chi-square (χ^2) is expressed as

$$\chi 2 = \sum_{j=1}^{256} \frac{(P_j - C_j)^2}{C_j}, \quad (20)$$

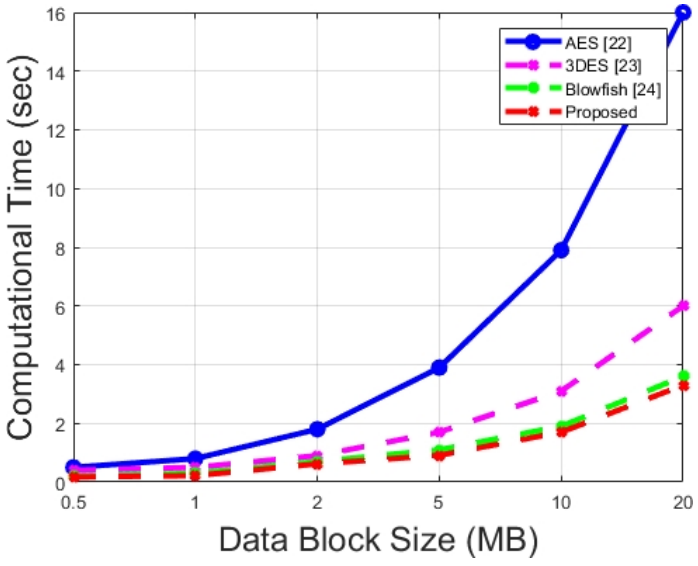
Here j is the gray value and P_j and C_j represent an observed and expected occurrence of each gray value between 0 to 255. Table 9. depicts that encrypted images from the proposed scheme yields uniform pixel distribution and excellent performance.

Images	**Lena**	**Barbara**	**Cameraman**	**Baboon**	**Ref.** [68]	**Ref.** [95]
Chi-square analysis	216.82	262.65	228.46	303.83	246.75	215.07

Table 9. Chi-square analysis

4.2.7 Computational complexity

All modern cryptographic schemes essentially require low computational complexity to synchronize with the latest low profile applications and innovative platforms. We reckoned the computational complexity of the proposed encryption scheme. This is done by measuring the computation and processing time required to encrypt an image of size 256x256. The input data is segregated into data blocks of various sizes before measuring computational time. The computational time for various blocks of data sizes functional in Electronic Codebook Mode. The results are further equated with prominent block ciphers as in fig. 16. The result reveals that our proposed encryption scheme exhibits superior performance. One basic reason is that our proposed scheme has only four rounds whereas all other algorithms have at least 12 rounds.



[30]

Fig. 16. Performance analysis of computation time with encryption algorithms for varying sizes

4.3 Cryptanalysis

The two most significant cryptanalysis strategies to verify the forte of any block cipher is linear and differential cryptanalysis. Our proposed algorithm has undergone both of them.

4.3.1 Linear Cryptanalysis

The imbalance of an event is tested by employing Linear approximation probability. $\acute{\Gamma}_q$ and $\acute{\Gamma}_q$ are two masks that are applied to the parity of both input and output bits. The linear approximation probability for any given S-box is specified as [97]

$$LProb. = max_{\acute{\Gamma}_q, \acute{\Gamma}_r \neq 0} \left| \frac{\{q/Y.\acute{\Gamma}_q = S(q).\acute{\Gamma}_r = \Delta r\}}{2^n} - \frac{1}{2} \right|, \tag{21}$$

where 2^n and Y are the total amount of elements and set of inputs. The procedures of active S-boxes are implemented. The $LProb_{max} = 2^{-4.21}$ and in four encryption rounds there are at least 128 S-boxes, $LProb.^{4r}{}_{max} = 2^{-4.21 \times 128} = 2^{-538.88}$. It's evident from derived results that a cryptanalyst differentiating a random permutation from the proposed encryption scheme is extremely difficult.

4.3.2 Differential Cryptanalysis

The differential at the input of a good nonlinear component S-box must have a uniform mapping with differential at the output. The inputs should uniquely correspond to output. The differential approximation probability is specified as [98]

$$DProb.(\Delta x \rightarrow \Delta y) = \left[\frac{\left\{ q \in \frac{Y}{S(q) \oplus S(q \oplus \Delta q)} \right\}}{2^m} = \Delta r \right], \tag{22}$$

Here Δq and Δr represent input and output differential. The procedures of active S-boxes are implemented. Now average differential probability is $DProb._{max} = 2^{-4.05}$ and in four encryption rounds there are at least 128 S-boxes $DProb.^{4r}{}_{max} = 2^{-4.05 \times 128} = 2^{-518.4}$. It's evident from derived results that the proposed encryption scheme is protected against differential cryptanalysis.

4.4 Other well-known attacks

Few other attacks are analyzed that might aid to break our proposed image encryption scheme. Suppose in these attacks the attacker knows both encryption and decryption algorithm. The attacks are examined as follows.

4.4.1 Cipher text-only attack

This attack is based on the fact that the intruder has access to ciphertext only. In our scenario, the attacker has access over cipher images and from the attacker's view, it is one of the hardest attacks. The decryption algorithm is used to decipher the accessible cipher image [99]. This is a preeminent effort to verify the right secret keys for decryption. The results of keyspace and key sensitivity analysis for our proposed algorithm show that it is highly unlikely to decipher images successfully in a meaningful time.

4.4.2 Known-plaintext attack

This known-plaintext assault is a cryptanalysis model where the intruder has access to both plaintext and accompanying ciphertext. In this scenario, the attacker has a set of plain images against their respective cipher images. The attacker tries to reveal secret keys with a pair of plain texts and ciphers text by decryption algorithm [99]. Our proposed algorithm has an excellent scheme of confusion and diffusion network. The permutations and no of S-boxes in each round make the algorithm highly resilient against this attack.

4.4.3 Chosen-plaintext attack

In this cryptanalysis model attackers select plaintext randomly to encrypt and get the corresponding ciphertext and reveal information to comprise the security of the algorithm. In this case, attackers choose any plain image to get corresponding cipher images. The attacker in this algorithm knows about both encryption and decryption [99]. The attacker selects plain images with the slightest differences and observes correlation between resulted cipher images. The security analysis executed earlier suggests that the proposed scheme is resilient for this attack.

The security and strength of the proposed algorithm are investigated through several security and performance metrics. The proposed scheme is compared with recent, related

encryption schemes and yields excellent performance. It is evident through results that the proposed scheme is highly resilient as compared to traditional schemes. Besides, it is feasible for real-time encryption applications due to its moderate computational requirements and noise resistant characteristics. The aim of this work is not intended for lossless encryption and to recover exact pixel values. As numerous multimedia applications and devices follow different storing and compression standards. However, the proposed decryption algorithm recovers with high PSNR values and fulfills major quality metrics. The proposed scheme tends to target noise-resistant and low-profile modern multimedia applications such as IoT, multimedia security applications, etc.

5 Conclusion

In this article, a unified algorithm is proposed to encrypt multimedia content. The algorithm incorporates the action of three distinct chaotic maps. The prescribed framework includes three standardized components left cyclic shift, permutation and substitution. These components are functional for four sets of rounds. Moreover, the offered scheme utilizes elliptic curves and S_8 symmetric group to design the confusion component. The input of each component is fed through the application of a distinct chaotic sequence generated via a chaotic map.

It is evident from the security performance analysis and simulation results that the proposed algorithm is secure against well-known attacks. Moreover, the image encryption algorithm has lower complexity and resistance against noise perturbation makes it viable to low profile applications. The algorithm is flexible and able to adapt to changes as desired. The modular approach followed through the SPN framework and the integration of chaotic maps into the system makes the algorithm feasible for a variety of applications. For instance, to enhance the resiliency of the algorithm amount of deployed S-boxes and the number of rounds of the algorithm can be increased or decreased. This depends on the target application but it also creates an additional computational load. The proposed scheme is an ideal candidate for modern image encryption applications and can be deployed to audio and video with minor modifications. In forthcoming, a cryptosystem to secure remote sensing big data will be investigated. Moreover, we intend to fuse the cryptosystem with a deep learning algorithm as well. Like all new proposals, it is highly recommended the analysis of our framework before immediate deployment.

7 References

[1] P. Dixit, A. K. Gupta, M. C. Trivedi, and V. K. Yadav, “Traditional and Hybrid Encryption Techniques: A Survey,” Springer, Singapore, 2018, pp. 239–248.

[2] S. Singh, A. K. Singh, and S. P. Ghrera, “A recent survey on data hiding techniques,” *Proc. Int. Conf. IoT Soc. Mobile, Anal. Cloud, I-SMAC 2017*, pp. 882–886, 2017.

[3] M. Faheem, S. Jamel, A. Hassan, Z. A., N. Shafinaz, and M. Mat, “A Survey on the Cryptographic Encryption Algorithms,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, 2017.

[4] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[5] J. Daemen and V. Rijmen, “The Design of Rijndael AES-The Advanced Encryption Standard Springer-Verlag,” 2001.

[6] N. Kumar, V. M. Mishra, and A. Kumar, “Smart grid security with AES hardware chip,” *Int. J. Inf. Technol.*, vol. 12, no. 1, pp. 49–55, 2020.

[7] M. Abomhara, O. Zakaria, O. O. Khalifa, A. . Zaidan, and B. . Zaidan, “Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard,” *Int. J. Comput. Electr. Eng.*, vol. 2, no. 2, pp. 223–229, 2010.

[8] S. Jahanzeb, H. Pirzada, A. Murtaza, T. Xu, and L. I. U. Jianwei, “Architectural Optimization of Parallel Authenticated Encryption Algorithm for Satellite Application,” *IEEE Access*, vol. 8, pp. 48543–48556, 2020.

[9] N. Ferguson, R. Schroeppel, and D. Whiting, “A simple algebraic representation of rijndael,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2001, vol. 2259, pp. 103–111.

[10] J. Fuller, W. Millan, and E. Dawson, “Multi-objective optimisation of bijective S-boxes,” *New Gener. Comput.*, vol. 23, no. 3, pp. 201–218, 2005.

[11] J. Cui, L. Huang, H. Zhong, C. Chang, and W. Yang, “An improved AES S-box and its performance analysis,” *Int. J. Innov. Comput. Inf. Control*, vol. 7, no. 5 A, pp. 2291–2302, 2011.

[12] L. Cui and Y. Cao, “A new S-box structure named affine-power-affine,” *Int. J. Innov. Comput. Inf. Control*, vol. 3, no. 3, pp. 751–759, 2007.

[13] M. Tran, D. K. Bui, and A. D. Duong, “Gray S-box for Advanced Encryption Standard,” pp. 253–258, 2008.

[14] E. S. Abuelyman, A. S. Alsehibani, and S. Arabia, “An Optimized Implementation of the S-Box using Residues of Prime Numbers,” vol. 8, no. 4, pp. 304–309, 2008.

[15] M. Ahmad, N. Mittal, P. Garg, and M. Maftab Khan, “Efficient cryptographic substitution box design using travelling salesman problem and chaos,” *Perspect. Sci.*, vol. 8, pp. 465–468, 2016.

[16] K. Kazlauskas, G. Vaicekauskas, and R. Smaliukas, “An Algorithm for Key-Dependent S-Box Generation in Block Cipher System,” *Inform.*, vol. 26, no. 1, pp. 51–65, May 2015.

[17] S. Picek and D. Jakobovic, “On the design of S-box constructions with genetic programming,” in *GECCO 2019 Companion - Proceedings of the 2019 Genetic and Evolutionary Computation Conference Companion*, 2019, pp. 395–396.

[18] C. P. Ruisanchez, “A New Algorithm To Construct S-Boxes With High Diffusion,” *Int. J. Soft Comput. Math. Control*, vol. 4, no. 3, pp. 41–50, 2015.

[19] D. Bikov, I. Bouyukliev, and S. Bouyuklieva, “Bijective S-boxes of different sizes obtained from quasi-cyclic codes,” *J. Algebr. Comb. Discret. Struct. Appl.*, vol. 6, no. 3, pp. 123–134, 2019.

[20] L. Mariot, S. Picek, A. Leporati, and D. Jakobovic, “Cellular automata based S-boxes,” *Cryptogr. Commun.*, vol. 11, no. 1, pp. 41–62, 2019.

[21] W. Z. Ü. I and E. Pasalic, “Constructions of Resilient S-Boxes with Strictly Almost Optimal Nonlinearity Through Disjoint Linear Codes,” vol. 60, no. 3, pp. 1638–1651, 2014.

[22] H. Isa, N. Jamil, and M. R. Z’aba, “Improved S-box construction from binomial power functions,” *Conf. Proc. - Cryptol. 2014 Proc. 4th Int. Cryptol. Inf. Secur. Conf. 2014*, vol. 9, pp. 131–139, 2014.

[23] E. Sakalauskas and K. Luksys, “Matrix Power S-Box Construction.,” *IACR Cryptol. ePrint Arch.*, vol. 2007, p. 214, 2007.

[24] V. S. Miller, “Use of Elliptic Curves in Cryptography,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 218 LNCS, pp. 417–426, 1986.

[25] B. N. Koblitz, “Elliptic Curve Cryptosystems,” vol. 4, no. 177, pp. 203–209, 1987.

[26] U. Hayat, N. A. Azam, and M. Asif, “A Method of Generating 8 × 8 Substitution Boxes Based on Elliptic Curves,” *Wirel. Pers. Commun.*, vol. 101, no. 1, pp. 439–451, 2018.

[27] U. Hayat and N. A. Azam, “A novel image encryption scheme based on an elliptic curve,” *Signal Processing*, vol. 155, pp. 391–402, 2019.

[28] C. Sapna Kumari and K. V. Prasad, “A novel S-Box generation of AES using elliptic curve cryptography (ECC),” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 4, pp. 749–765, 2019.

[29] N. A. Azam, U. Hayat, and I. Ullah, “Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field,” *Front. Inf. Technol. Electron. Eng.*, vol. 20, no. 10, pp. 1378–1389, 2019.

[30] I. Hussain, T. Shah, and H. Mahmood, “A New Algorithm to Construct Secure Keys for AES,” *Int. J. Contemp. Math. Sci. Vol. 5, 2010*, vol. 5, no. 26, pp. 1263–1270, 2010.

[31] H. Zhang, T. Ma, G. Bin Huang, and Z. Wang, “Robust global exponential synchronization of uncertain chaotic delayed neural networks via dual-stage impulsive control,” *IEEE Trans. Syst. Man, Cybern. Part B Cybern.*, vol. 40, no. 3, pp. 831–844, 2010.

[32] F. Yu *et al.*, “Chaos-Based Application of a Novel Multistable 5D Memristive Hyperchaotic System with Coexisting Multiple Attractors,” *Complexity*, vol. 2020, pp. 1–19, 2020.

[33] H. Lin and C. Wang, “Influences of electromagnetic radiation distribution on chaotic dynamics of a neural network,” *Appl. Math. Comput.*, vol. 369, no. 61971185, p. 124840, 2020.

[34] F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems,” *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, 2019.

[35] H. Liu, A. Kadir, and C. Xu, “Cryptanalysis and constructing S-Box based on chaotic map and backtracking,” *Appl. Math. Comput.*, vol. 376, p. 125153, 2020.

[36] M. A. Ben Farah, R. Guesmi, A. Kachouri, and M. Samet, “A new design of cryptosystem

based on S-box and chaotic permutation," *Multimed. Tools Appl.*, 2020.

[37] A. Shafique, "A new algorithm for the construction of substitution box by using chaotic map," *Eur. Phys. J. Plus*, vol. 135, no. 2, pp. 1–13, 2020.

[38] I. Hussain, "True-chaotic substitution box based on Boolean functions," *Eur. Phys. J. Plus*, vol. 135, no. 8, 2020.

[39] J. Ahmad, F. Masood, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel secure occupancy monitoring scheme based on multi-chaos mapping," *Symmetry (Basel).*, vol. 12, no. 3, pp. 1–16, 2020.

[40] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An Encryption Scheme Based on Discrete Quantum Map and Continuous Chaotic System," *Int. J. Theor. Phys.*, vol. 59, no. 4, pp. 1227–1240, 2020.

[41] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd EL-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci. (Ny).*, vol. 515, pp. 191–217, 2020.

[42] U. A. Waqas, M. Khan, and S. I. Batool, "A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images," *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 6891–6914, 2020.

[43] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, p. 107484, 2020.

[44] Y. Cao, "A new hybrid chaotic map and its application on image encryption and hiding," *Math. Probl. Eng.*, vol. 2013, 2013.

[45] A. Anees, I. Hussain, A. Algarni, and M. Aslam, "A robust watermarking scheme for online multimedia copyright protection using new chaotic map," *Secur. Commun. Networks*, vol. 2018, no. 2, 2018.

[46] H. Natiq, N. M. G. Al-Saidi, M. R. M. Said, and A. Kilicman, "A new hyperchaotic map and its application for image encryption," *Eur. Phys. J. Plus*, vol. 133, no. 1, 2018.

[47] A. Roy and A. P. Misra, "Audio signal encryption using chaotic Hénon map and lifting

wavelet transforms," *Eur. Phys. J. Plus*, vol. 132, no. 12, pp. 1–10, 2017.

[48] T. Omrani, R. Rhouma, and L. Sliman, "Lightweight cryptography for resource-constrained devices: A comparative study and rectangle cryptanalysis," *Lect. Notes Bus. Inf. Process.*, vol. 325, pp. 107–118, 2018.

[49] M. James and D. S. Kumar, "An Implementation of Modified Lightweight Advanced Encryption Standard in FPGA," *Procedia Technol.*, vol. 25, pp. 582–589, 2016.

[50] A. Bogdanov, F. Mendel, F. Regazzoni, V. Rijmen, and E. Tischhauser, "ALE: AES-based lightweight authenticated encryption," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 8424 LNCS, pp. 447–466, 2014.

[51] P. Li *et al.*, "Efficient implementation of lightweight block ciphers on volta and pascal architecture," *J. Inf. Secur. Appl.*, vol. 47, pp. 235–245, 2019.

[52] A. Biswas, A. Majumdar, S. Nath, A. Dutta, and K. L. Baishnab, "LRBC: a lightweight block cipher design for resource constrained IoT devices," *J. Ambient Intell. Humaniz. Comput.*, no. 0123456789, 2020.

[53] A. H. Bdair, R. Abdullah, S. Manickam, and A. K. Al-Ani, *Computational Science and Technology*, vol. 603, no. August. 2020.

[54] M. Qasaimeh, R. S. Al-Qassas, F. Moh`d, and S. Aljawarneh, "A Novel Simplified AES Algorithm for Lightweight Real-Time Applications: Testing and Discussion," *Recent Patents Comput. Sci.*, vol. 12, Dec. 2018.

[55] F. Ahmed and A. Anees, "Hash-Based Authentication of Digital Images in Noisy Channels," in *Robust Image Authentication in the Presence of Noise*, Springer International Publishing, 2015, pp. 1–42.

[56] F. Ahmed, A. Anees, V. U. Abbas, and M. Y. Siyal, "A noisy channel tolerant image encryption scheme," *Wirel. Pers. Commun.*, vol. 77, no. 4, pp. 2771–2791, 2014.

[57] O. Finko and D. Samoylenko, "Cryptographic System in Polynomial Residue Classes for Channels with Noise and Simulating Attacker," *Int. J. Sci. Res.*, vol. 1, no. 1, pp. 5–9, 2012.

[58] J. xin Chen, Z. liang Zhu, C. Fu, L. bo Zhang, and Y. Zhang, "An efficient image encryption scheme using lookup table-based confusion and diffusion," *Nonlinear Dyn.*, vol. 81, no. 3,

pp. 1151–1166, 2015.

[59] K. A. Kumar Patro and B. Acharya, “An efficient colour image encryption scheme based on 1-D chaotic maps,” *J. Inf. Secur. Appl.*, vol. 46, pp. 23–41, 2019.

[60] M. Li, P. Wang, Y. Liu, and H. Fan, “Cryptanalysis of a Novel Bit-Level Color Image Encryption Using Improved 1D Chaotic Map,” *IEEE Access*, vol. 7, pp. 145798–145806, 2019.

[61] Y. Li, C. Wang, and H. Chen, “A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation,” *Opt. Lasers Eng.*, vol. 90, no. October 2016, pp. 238–246, 2017.

[62] W. Zhang, H. Yu, Y. L. Zhao, and Z. L. Zhu, “Image encryption based on three-dimensional bit matrix permutation,” *Signal Processing*, vol. 118, pp. 36–50, 2016.

[63] C. Cao, K. Sun, and W. Liu, “A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map,” *Signal Processing*, vol. 143, pp. 122–133, 2018.

[64] W. Feng, Y. He, H. Li, and C. Li, “Cryptanalysis and Improvement of the Image Encryption Scheme Based on 2D Logistic-Adjusted-Sine Map,” *IEEE Access*, vol. 7, pp. 12584–12597, 2019.

[65] S. Jiao, W. Zou, and X. Li, “QR code based noise-free optical encryption and decryption of a gray scale image,” *Opt. Commun.*, vol. 387, no. September 2016, pp. 235–240, 2017.

[66] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, “An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata,” *Neural Comput. Appl.*, vol. 3, 2018.

[67] X. Chai, H. Wu, Z. Gan, Y. Zhang, Y. Chen, and K. W. Nixon, “An efficient visually meaningful image compression and encryption scheme based on compressive sensing and dynamic LSB embedding,” *Opt. Lasers Eng.*, vol. 124, no. January 2019, p. 105837, 2020.

[68] A. Qayyum *et al.*, “Chaos-Based Confusion and Diffusion of Image Pixels Using Dynamic Substitution,” *IEEE Access*, vol. 8, no. July, pp. 140876–140895, 2020.

[69] G. Cheng, C. Wang, and C. Xu, “A novel hyper-chaotic image encryption scheme based on quantum genetic algorithm and compressive sensing,” *Multimed. Tools Appl.*, pp. 29243–

29263, 2020.

[70] Y. Xian, X. Wang, X. Yan, Q. Li, and X. Wang, “Image Encryption Based on Chaotic Sub-Block Scrambling and Chaotic Digit Selection Diffusion,” *Opt. Lasers Eng.*, vol. 134, no. May, 2020.

[71] N. Sasikaladevi, K. Geetha, K. Sriharshini, and M. Durga Aruna, “H3-hybrid multilayered hyper chaotic hyper elliptic curve based image encryption system,” *Opt. Laser Technol.*, vol. 127, no. March, 2020.

[72] T. A. Al-Maadeed, I. Hussain, A. Anees, and M. T. Mustafa, “An image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes,” pp. 1–21, 2020.

[73] Y. Liu and J. Zhang, “A Multidimensional Chaotic Image Encryption Algorithm based on DNA Coding,” *Multimed. Tools Appl.*, vol. 79, no. 29–30, pp. 21579–21601, 2020.

[74] J. Ahmad, M. A. Khan, S. O. Hwang, and J. S. Khan, “A compression sensing and noise-tolerant image encryption scheme based on chaotic maps and orthogonal matrices,” *Neural Comput. Appl.*, vol. 28, no. s1, pp. 953–967, 2017.

[75] I. F. Elashry *et al.*, “Efficient chaotic-based image cryptosystem with different modes of operation,” *Multimed. Tools Appl.*, vol. 79, no. 29–30, pp. 20665–20687, 2020.

[76] K. A. K. Patro, B. Acharya, and V. Nath, “Secure, Lossless, and Noise-resistive Image Encryption using Chaos, Hyper-chaos, and DNA Sequence Operation,” *IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India)*, vol. 37, no. 3, pp. 223–245, 2020.

[77] A. Yaghouti Niyat and M. H. Moattar, “Color image encryption based on hybrid chaotic system and DNA sequences,” *Multimed. Tools Appl.*, vol. 79, no. 1–2, pp. 1497–1518, 2020.

[78] S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, “Breaking a chaotic image encryption algorithm,” *Multimed. Tools Appl.*, no. June 2018, 2020.

[79] 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.

[80] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” *Int. J. Bifurc. Chaos*, vol. 16, no. 8, pp. 2129–2151, 2006.

[81] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2001.

[82] N. Bacaër, "A short history of mathematical population dynamics," *A Short Hist. Math. Popul. Dyn.*, no. 1838, pp. 1–160, 2011.

[83] L. Y. Sheng, L. L. Cao, K. H. Sun, and J. Wen, "Pseudo-random number generator based on TD-ERCS chaos and its statistic characteristics analysis," *Wuli Xuebao/Acta Phys. Sin.*, vol. 54, no. 9, pp. 4031–4037, Sep. 2005.

[84] N. A. Azam, U. Hayat, and I. Ullah, "An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization," *Secur. Commun. Networks*, vol. 2018, pp. 1–9, 2018.

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

[86] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

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

[88] X. Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.

[89] S. Xiao, Z. J. Yu, and Y. S. Deng, "Design and Analysis of a Novel Chaos-Based Image Encryption Algorithm via Switch Control Mechanism," *Secur. Commun. Networks*, vol. 2020, pp. 30–32, 2020.

[90] Y. Zhang and Y. Tang, "A plaintext-related image encryption algorithm based on chaos," *Multimed. Tools Appl.*, vol. 77, no. 6, pp. 6647–6669, 2018.

[91] A. Kulsoom, D. Xiao, Aqeel-ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimed. Tools Appl.*, vol. 75, no. 1, pp. 1–23, 2016.

[92] M. A. Murillo-Escobar, M. O. Meranza-Castillón, R. M. López-Gutiérrez, and C. Cruz-

Hernández, “Suggested Integral Analysis for Chaos-Based Image Cryptosystems,” *Entropy*, vol. 21, no. 8, p. 815, 2019.

[93] A. A. Abdullatif, F. A. Abdullatif, and S. A. Naji, “An enhanced hybrid image encryption algorithm using Rubik’s cube and dynamic DNA encoding techniques,” *Period. Eng. Nat. Sci.*, vol. 7, no. 4, pp. 1607–1617, 2019.

[94] C. Xu, J. Sun, and C. Wang, “A novel image encryption algorithm based on bit-plane matrix rotation and hyper chaotic systems,” *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 5573–5593, 2020.

[95] J. Ahmad *et al.*, “A Partial Ligt-weight Image Encryption Scheme,” *2019 UK/China Emerg. Technol. UCET 2019*, pp. 1–3, 2019.

[96] T. Wang, L. Song, M. Wang, and Z. Zhuang, “A novel image encryption algorithm based on parameter-control scroll chaotic attractors,” *IEEE Access*, vol. 8, pp. 36281–36292, 2020.

[97] M. Matsui, “Linear cryptanalysis method for DES cipher,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 765 LNCS, pp. 386–397, 1994.

[98] E. Biham and A. Shamir, “Cryptanalysis of the Data Encryption,” p. 188, 1993.

[99] B. Schneier, “Applied Cryptography’Wiley,1996.”