Multimedia Tools and Applications (2022) 81:20585–20609
https://doi.org/10.1007/s11042-022-12268-6

A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box

Tahir Sajjad Ali[1] · **Rashid Ali**[1]

Received: 30 March 2021 / Revised: 20 August 2021 / Accepted: 14 January 2022 /
Published online: 11 March 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
In modern technological era image encryption has become an attractive and interesting field for researchers. They work for improving the security of image data from unauthorized sources. Chaos theory, due to its randomness and unpredictable behaviors, is considered favorite for the purpose of image encryption. This paper proposes a diffusion based image encryption algorithm by using chaotic maps. Firstly a chaotic map (piecewise linear chaotic map) is used for the generation of S-box, then it is used for the pixel values modification to generate element of non-linearity. After this these modified values are further diffused with another random sequence, generated by tent logistic chaotic map. Finally the color components of pre-encrypted image are mixed with each other so that the developed randomness uniformly distributed in them. For image data we develop non-linearity and diffusion by using S-box and then more randomness is added in the pre-encrypted image with the help of Boolean operation XOR. The use of this combination of chaotic maps along with S-box and Boolean operation XOR is a different technique, that provides satisfactory results for security aspects and also works efficiently.

Keywords Image encryption · Chaos · Chaotic system · Tent logistic map · Piecewise linear chaotic map · S-box

1 Introduction

21st century is the century of innovation and technology. In its early years, we saw a rapid progress in every aspect of life. Social media and communication sector revolutionized in previous two decades. Internet has completely changed the way of communication and socializing with each other. In many of our daily use internet applications like Facebook, WhatsApp, Video conferencing, Skype etc., we have to deal with digital images. Digital image communication is also used in some sensitive institutions like military image database, medical imaging system etc. Researchers use image based data to analyze,

✉ Tahir Sajjad Ali
tahir.sajjad@cust.edu.pk; tahirali.maths@gmail.com

[1] Capital University of Science and Technology, Islamabad, Pakistan

diagnose and resolve the real world problems. Tiwari et al. [48] proposed image based rapid pests detection and identication technique for soyabean crop. Dhiman et al. [14] proposed a computation approach for the analysis of medical images used for COVID-19 disease. Singh et al. [45] used fuzzy entropy approach for remotely sensed high resolution satellite images to analyze the difference and uncertainty representation.

Unfortunately, there are a few downsides to social networking. Some of these are cyber bulling [16] and online harassment [17]. Another damaging impact is privacy theft. Providing personal information on social sites can make users vulnerable to crime like identity theft, stalking, cyberbulling [57] etc. In all these sectors we need high level, reliable and robust security system to prevent illegal use of digital images from unauthorized sources.

In cryptography, traditional encryption techniques like AES [13], RSA [43], IDEA [37] etc. are used to encrypt text data. Structure of a digital image is quite different from text data. Digital images have redundancy, strong relationship with adjacent pixels, less avalanche effect, that is, a little change in attribute of pixel does not generate huge effect in quality of image and bulk of data. Therefore, ordinary used schemes of data encryption are not well suited for the encryption of digital images.

For the solution of the problems related to communication involving images, chaos theory has provided a potential platform. Chaotic maps have properties [4] such as sensitivity for initial condition, control parameters, unpredictable behavior, randomness and simple implementation on software and hardware. Due to their random and unpredictable behavior, these maps, automatically fulfill many cryptographic requirement for the security of encrypted data like confusion, diffusion, balancedness at bit level and avalanche effect. For these properties chaotic maps are widely used in cryptography. Chaos based encryption algorithms are considered as highly secure, robust, computationally powerful and possessing good complexity level to make cryptanalysis harder. To fulfill image encryption requirements many encryption techniques [6–8, 11] etc for digital images are developed to help out in providing good security and efficiency.

Chaos theory [31] was established in 1969 and since then, it has been playing a vital role in physics, mathematics, biology, engineering etc. In 1989 Matthews [33] gave the idea that under certain conditions some easy nonlinear iterative maps have the ability to generate chaotic sequences. He also derived a chaotic map and proposed that it could be helpful for cryptographic purposes. He had used logistic chaotic map to generate keystream for encryption purpose of secret information. Habutsu et al. [22] used a one dimensional chaotic map to generate a cryptosystem in 1991. His generated cryptosystem was based on tent map. He used this chaotic map to make a ciphertext from plaintext. Then in 1997 Fridrich [19] used two dimensional chaotic baker map for image encryption. He used substitution diffusion architecture for this purpose, where substitution and diffusion were taken separately. Chen et al. [10] and Mao [34] in 2004 used three dimensional cat map and baker map for the generation of permutation in image data. in 2005 Guan et al. [21] proposed image encryption scheme that uses two chaotic maps. He used two dimensional cat map and chen's map for generating permutation in pixel position and pixel value modification. Patidar et al. [39] proposed a modified substitution diffusion architecture in 2010. His modified architecture was more secure against chosen plaintext and known plaintext attacks. Stoyanov and Kordov proposed an image encryption method in 2014 that is based on chebychev polynomial together with chaotic maps [47] and rotation equation in [46]. Li et al. [30] proposed an image encryption scheme that uses modified tent map. Chai et al. [7] used improved genetic algorithm and STP for effective color image crypytosystem. In [8], the authors have proposed an efficient approach for encryption of double images into visually meaningful cipher image.

Recently scientists are working to improve the chaotic maps by removing their weaknesses, enhancing their chaotic behaviors and randomness. Then these modified and improved chaotic systems are used for the intensification of the security features in various encryption schemes. In this perspective [24] introduced improved tent-sine system and also used this map by employing a novel technique to construct a substitution box. Lu et al. [32] presented a new compound chaotic system (tent logistic system) that has a better chaotic performance, vast chaotic range and huge key space. He also used this chaotic map in a novel substitution box generation algorithm. Ali et al. used tent logistic tent system introduced by [1] for medical image signcryption [2] purpose to enhance the security and authentication of sensitive medical images.

The aim of this research is to propose an image encryption scheme that depends on the piecewise linear chaotic map (PWLCM) and a compound chaotic map. The PWLCM is employed to form a cryptographically strong substitution box (S-box) that is used for the value substitution of image pixels. Then compound chaotic system is used as pseudo random number generator to produce three chaotic sequences which are utilized to encrypt each component of color image individually. Another novel reversible self mixing operation based on Boolean operation XOR is performed that ensures further diffusion in image. The encryption process using compound chaotic system mainly used Boolean function XOR to mix the chaotic random sequence, substituted pixel value and preceding pixel value. The use of compound chaotic system, S-box, inclusion of random sequences and also implementation of reversible self mixing operation provide good performance for the encryption of color images.

The manuscript is organized as: Section 2 is based on the introduction of chaotic maps. Section 3 is concerned with the S-box. In this section algorithm for the generation of S-box using PWLCM and its role in cryptography is presented. In Section 4 the proposed image encryption and image decryption algorithms are presented. Section 5 is devoted for the presentation of the results and discussions with the help of examples and figures. Section 6 provides the detailed security analysis of the proposed scheme particularly key space analysis, distribution of pixels in original and cipher images, correlation analysis, information entropy, mean squared error, peak signal to noise ratio, complexity analysis and the speed analysis of proposed algorithm. Section 7 presents the conclusion of the above discussed work.

2 Chaotic maps

There are many chaotic systems, that are being used in the applications of information security. In this section we briefly describe some of the basic chaotic maps and then a dynamic compound chaotic system generated by the combining tent [59] and logistic chaotic map [38].

2.1 Logistic map

A chaotic system shows deterministic behavior. It is non-linear in nature. A famous example of one dimensional chaotic map is logistic map [36]. In this system, states change with iterations in a deterministic way. Logistic map is discrete time, one dimensional and non-linear map with quadratic non-linearity [38]. The logistic map has the following state equation:

$$y_{n+1} = f(y_n) = \mu y_n(1 - y_n), \tag{1}$$

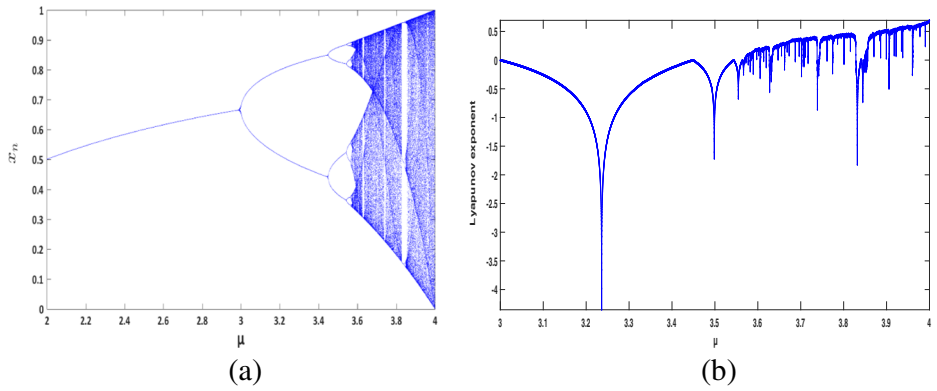

Fig. 1 **a** The bifurcation diagram of Logistic map, **b** Lyapunov exponent of Logistic map

where $y_0 \in (0, 1)$ shows the initial state of the chaotic system at any time n and $\mu \in (0, 4)$, is the system parameter also known as bifurcation parameter. The next state of the system is expressed by y_{n+1}, where n shows the discrete time (Fig. 1).

The behavior of logistic map highly depends on the value of control parameter μ. The chaotic behavior of (1) can be achieved for the μ between 3.567 and 4, where it shows a chaos with infinite period. In this range there are uncountable initial points y_0 that give non-periodic trajectories, no matter how much long time series created by $f(y_n)$, generated pattern never repeats itself.

Sequences generated in this way are highly sensitive to the initial condition y_0. The sensitive dependence on initial condition of a chaotic system is measured with the help of Lyapunov exponent [35]. Negative value of Lyapunov exponent expresses that the orbit converges with time, while its positive value shows that distance between nearby orbit increases with time. The Lyapunov exponent mostly shows a positive behavior for $\mu = 3.57$ to 4, that indicates the chaotic behavior of logistic map.

The logistic map also suffers from some shortcomings, like limited chaotic range, non uniform distribution and also periodic windows in its chaotic region.

2.2 Tent chaotic map

Another one dimensional discrete chaotic iterative map is tent map, that exhibit tent like shape in the bifurcation diagram as shown in the Fig. 2b. It is also known as triangle map and its mathematical model is as follows:

$$x_{n+1} = \begin{cases} rx_n & \text{if} \quad 0 < x_n < 0.5 \\ r(1 - x_n) & \text{if} \quad 0.5 \leq x_n < 1 \end{cases} \tag{2}$$

where the system parameter $x_0 \in (0, 1)$ and the control parameter $r \in (0, 2)$. The chaotic map (2) is simplistic and has linear equations but for certain parameter values it shows a complicated and chaotic behavior. The chaotic properties of tent map are shown in Fig. 2. The figure shows that the chaotic range of tent map (2) is from 2 to 4. Some drawbacks of tent map are short chaotic range and lackness in uniform distribution among the output state values.

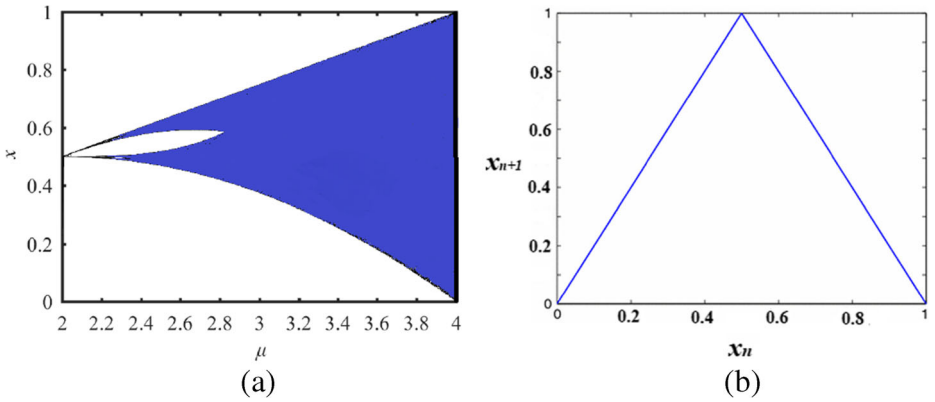

Fig. 2 **a** The bifurcation diagram of Tent map, **b** the diagram of Tent map function

2.3 Piecewise linear chaotic map

Piecewise linear chaotic map (PWLCM) is used as it has ample non linear dynamic action and a positive Lyapunov exponent as shown in Fig. 3. The multi-segmented map shows some fantastic dynamic properties like uniform invariant density function, large positive Lyapunov exponent, and random like behavior.

These properties are particularly valuable and useful for cryptographic purposes. A piecewise linear chaotic map is given by:

$$x_{n+1} = f(x_n, m) = \begin{cases} \dfrac{x_n}{m} & \text{if} \quad 0 \le x_n < m \\ \dfrac{x_n - m}{0.5 - m} & \text{if} \quad m \le x_n < 0.5 \\ \dfrac{1 - m - x_n}{0.5 - m} & \text{if} \quad 0.5 < x_n < 1 - m \\ \dfrac{1 - x_n}{m} & \text{if} \quad 1 - m \le x_n < 1 \end{cases} \tag{3}$$

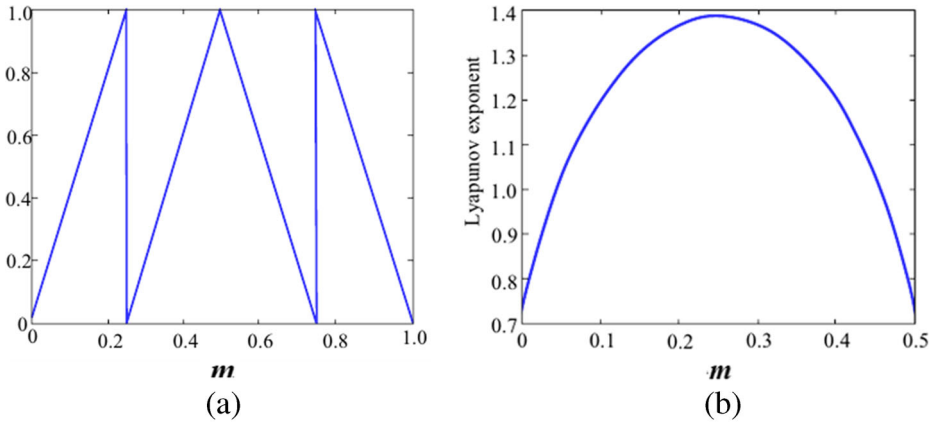

Fig. 3 **a** plot of piecewise linear chaotic map, **b** Lyapunov exponent

Here $x_0 \in [0, 1)$ is the initial state/initial condition and $m \in (0, 0.5)$ is the control parameter of chaotic map (3).

The output of PWLCM has uniformly continuous distribution, confusion and ergodicity. It can also be used to generate good chaotic sequences for making strong S-boxes.

2.4 The tent logistic system

For the solution of problems faced by logistic and tent maps, [32] suggested a new compound chaotic system by bringing together the tent and logistic map. Hence formed new system is named as tent logistic system. The mathematical form of this system can be presented as:

$$x_{n+1} = \begin{cases} \frac{4(9-\mu)}{9}(x_n)(1-x_n) + \frac{2\mu}{9}(x_n) & x_n < 0.5 \\ \frac{4(9-\mu)}{9}(x_n)(1-x_n) + \frac{2\mu}{9}(1-x_n) & x_n \geq 0.5 \end{cases} \tag{4}$$

Where $\mu \in [0, 9]$ is the system parameter of the chaotic map (4). For $\mu = 0$ the above equation behaves like logistic map, while for $\mu = 9$ the above described equation degenerates to form the tent chaotic map. Due to this both the logistic and tent chaotic maps can be considered as the special cases of this system. Figure 4 shows the bifurcation and state distribution diagram of said chaotic system. From this figure it is evident that the whole range $\mu \in [0, 9]$ has chaotic behavior, also this chaotic region is much greater than the logistic and tent map. The output of this system is uniformly distributed within [0, 1]

This chaotic system is more suitable for the use in cryptographic application as it provides a large chaotic range. Also if the control parameter is used as the secret key key space for the generation of random chaotic sequences, then this key space would be much large to resist brute force attacks. The output random sequence is uniformly distributed to give a good uniformly distributed random sequence.

2.4.1 NIST randomness test for tent logistic system

National Institute of standards and technology (NIST) has issued Federal Information Processing Standard for the random number generators. There are 16 tests in this test suit that

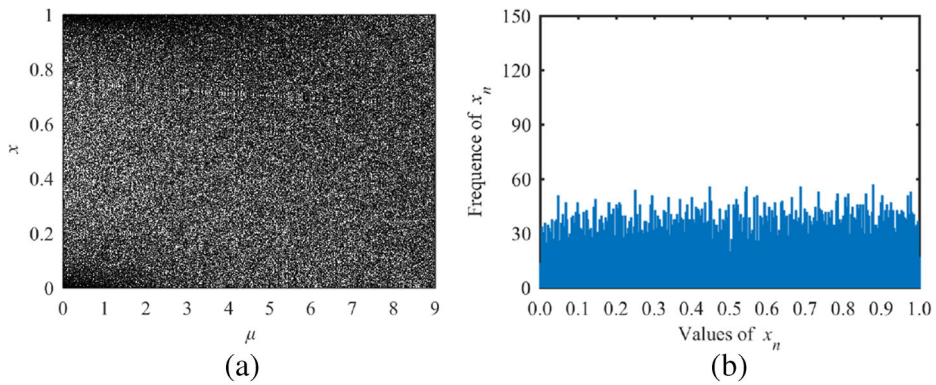

Fig. 4 **a** Bifurcation diagram of tent logistic chaotic map, **b** the state distribution of tent logistic chaotic map

focus on different sorts of randomness present in any sequence generated by pseudo random number generator. To apply the test first we design a pseudo random number generator of tent logistic chaotic map.

Algorithm 1 (*Pseudo Random Number Generator (PRNG)*)
Given the chaotic map (4), we construct a PRNG by executing the following steps.

1. *Set system's control parameter μ, the initial value x_0, the positive integer n_0 and the L the length of generated sequence.*
2. *Iterate the chaotic map (4) for L to get a random sequence.*
3. *Discard first n_0 values of above generated sequence to get rid of the harmful effects of transient process.*
4. *Use a non linear transformation (5) to convert the obtained random sequence X into integer sequence Y*

$$y_i = mod(floor(x_i \times 10^{14}), 256), \quad i = 1, 2, ..., (L - n_0), \tag{5}$$

where mod gives back the remainder after dividing by 256, while the floor(x) returns the largest integer less than or equal to x. Hence the output sequence $Y = [y_1, y_2, \ldots, y_{(L-n_0)}]$ lies in the range of [0, 255].
5. *Convert each y_i to binary number of size 8 bit. Hence a bit sequence is formed that is $B = \{b_1, b_2, \ldots, b_{8(L-n_0)}\}$.*
6. *Change the bit sequence to a single stream of length 100×10^6 bits.*
7. *Divide the bit sequence to 100 subsequences, of length 10^6 bit each.*

By using the above algorithm we have generated 100 sub sequences, each of length 10^6 bits.

These sequences are input in NIST statistical suite for their randomness and the obtained results are depicted in the Table 1. The obtained results shows that the sequences generated

Table 1 Statistical randomness tests results

Test #	NIST statistical test name	p. value	Pass Rate	Result
1	Frequency (monobit)	0.911413	99/100	✓
2	Block Frequency ($m = 128$)	0.897763	99/100	✓
3	The Run Test	0.202268	100/100	✓
4	Cumulative Sums (Forward)	0.637119	100/100	✓
5	Cumulative Sums (Reverse)	0.779188	100/100	✓
6	Longest Run of Ones	0.897763	98/100	✓
7	Non Overlapping Template ($m = 9$, $B = 000000001$)	0.045675	99/100	✓
8	Overlapping Template ($m = 9$)	0.834308	99/100	✓
9	Rank	0.401199	100/100	✓
10	DFT Spectral	0.574903	98/100	✓
11	Universal Statistical Test	0.236810	98/100	✓
12	Approximate Entropy ($m = 10$)	0.574903	99/100	✓
13	Random Excursions	0.554420	57/57	✓
14	Random Excursions Variant	0.474986	56/57	✓
15	Serial ($m = 16$)	0.935716	99/100	✓
16	Linear Complexity ($M = 500$)	0.090936	100/100	✓

from tent logistic chaotic map pass almost all the tests. Hence tent logistic map can be used as a potential platform for the generation of a good chaotic random sequence

3 S-boxes in cryptography

Substitution boxes, in short, S-boxes are considered as main component in many conventional algorithms of cryptography like DES [26], AES [13] etc. The design of S-box is based on Shannon's theory of confusion and diffusion [44]. S-boxes can also be used efficiently as look-up table for substitution in encryption and decryption processes [23]. The objective of such substitution boxes is to establish the element of non-linearity in the encrypted data and also to induce confusion and diffusion [44] in cipher. Use of S-box gives high resistance for linear and differential cryptanalysis. Cryptographically strong S-boxes play vital role in the design of a secure cryptosystem. They increase security level against known attacks. Many researchers have proposed different methods [5, 24, 29] to generate strong S-boxes. Chaotic maps, due to its properties [4] as ergodicity, sensitive to initial condition, randomness and ability to generate again with a key are potential platform for the generation of a strong S-box. In this section an algorithm for generating S-box using PWLCM (3) is presented. The following shows the proposed algorithm:

Algorithm 2 (*Chaotic S-box*)
For the chaotic map (3), the following steps lead to the creation of an S-box.

1. *Divide the interval* $[0.1, 0.9]$ *into* 256 *sub-intervals each of fixed length* $\triangle h$*, i. e.,* $\triangle h = (0.9 - 0.1)/256 = 0.003125$.
2. *Classify each sub-interval as* $L_0, L_1, ..., L_{255}$.
3. *Choose an arbitrary initial condition* x_0' *and* $m \in (0, 0.5)$ *for (3) to create a sequence* x_n *of the values lying in [0.1, 0.9].*
4. *Start a void array S.*
5. *Whenever an output value* x_n *lies in a particular interval* $L_i (i = 0, ..., 255)$*, give that sub-interval index* i *to S. Leave those values which do not belong to any sub-interval or giving repeated sub-interval index value.*
6. *Stop iterating PWLCM when it traverses all the sub-intervals* L_0 *to* L_{255}.
7. *Return the elements of array as S in the range of 0 to 255, containing 256 distinct integers.*

Note that in step 3, a slightly different value of x_0' will provide a totally different S-box. Thus, it is possible to create many S-boxes using the above stated algorithm. One such S-box is generated by setting parameter $x_0' = 0.76$ and with fixed value of $m = 0.15$ in (3). Table 2 displays the resulting S-box.

The properties of this S-box are tested using SET (S-box Evaluation Tool) [41]. It is observed that S-box is fairly balanced and holds reasonably strong cryptographic characteristics.

4 Proposed cryptosystem for digital images

In this section, we describe a new image encryption mechanism for the protection of digital images. In the proposed scheme initially an S-box is generated by PWLCM used as lookup

Table 2 S-Box

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

table for pixel substitution. Then three random sequences are generated and bitwise XOR is performed with substituted pixel values of each image component. The algorithm is based mainly on two secret keys k_1, k_2 containing the parameters of both PWLCM (3) and chaotic tent logistic map (4), that is $k_1 = (m,\ x_0')$, where $m \in (0,\ 0.5)$, $x_0' \in [0, 1)$ and $k_2 = (\mu_1,\ \mu_2,\ \mu_3,\ x_0,\ y_0,\ z_0)$, where $\mu_1,\ \mu_2,\ \mu_3 \in (0,\ 9)$ and $x_0,\ y_0,\ z_0 \in (0,\ 1)$ (Figs. 5, 6 and 7).

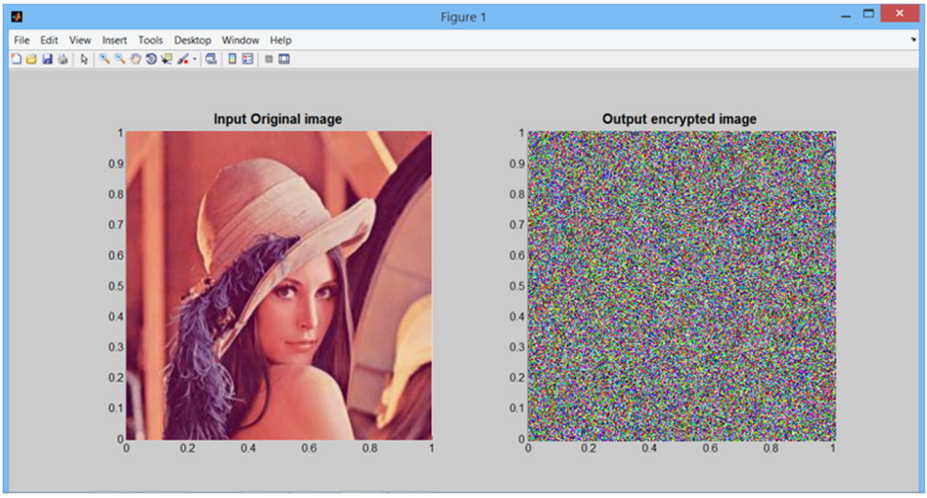

Fig. 5 User interface preview in real time encryption mechanism

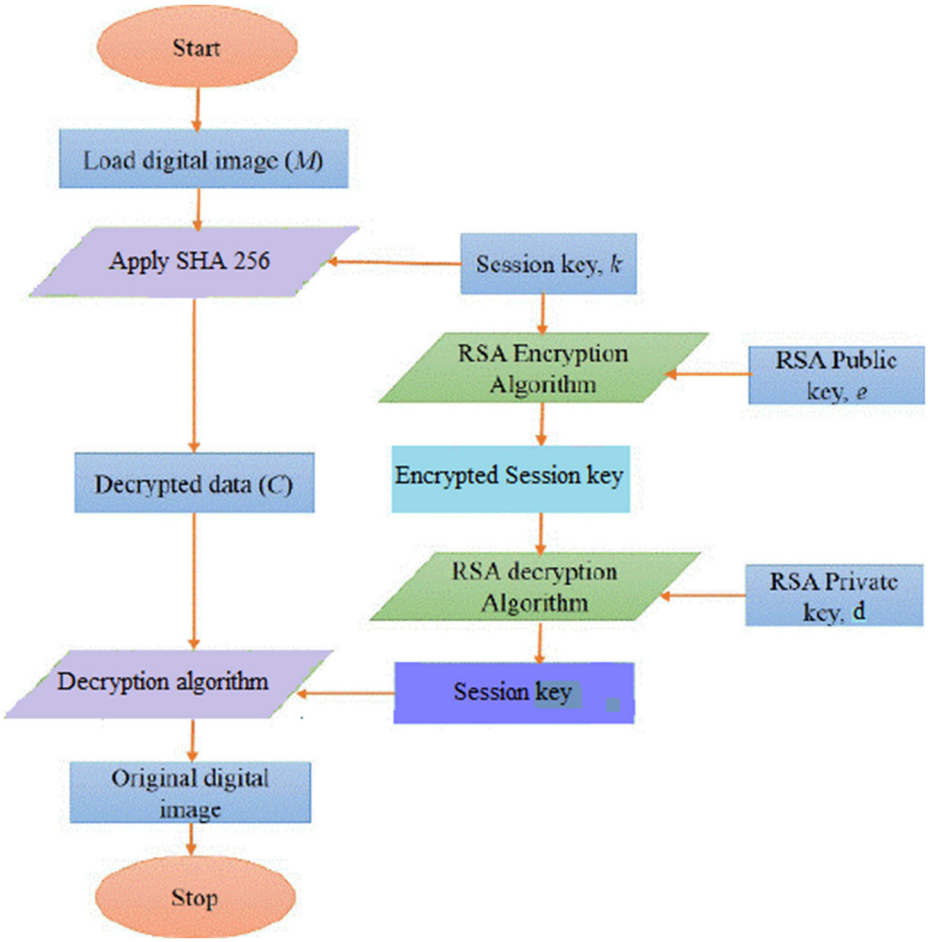

Fig. 6 Flow diagram of the proposed cryptosystem

4.1 Key management

The proposed cryptosystem is hybrid in nature, it uses a symmetric and asymmetric scheme for the security of images. For this purpose initial secret key is developed by using the plain image. SHA 256 is implemented on the image that gives 256 bits output.

$$H(I) = b_{255}\, b_{254} \ldots\, b_0 \tag{6}$$

This hash value will be used in the generation of secret keys. The output H_i is split into 8 bit blocks h_i as follows:

$$H_i = h_1|h_2|h_3| \ldots |h_{32}. \tag{7}$$

The initial states of used chaotic maps are derived from the above blocks as:

$$x_0' = \frac{h_1 \oplus h_5 \oplus h_9 \oplus h_{13} \oplus h_{17} \oplus h_{21} \oplus h_{25} \oplus h_{29}}{2^8} \tag{8}$$

$$x_0 = \frac{h_2 \oplus h_6 \oplus h_{10} \oplus h_{14} \oplus h_{18} \oplus h_{22} \oplus h_{26} \oplus h_{30}}{2^8} \tag{9}$$

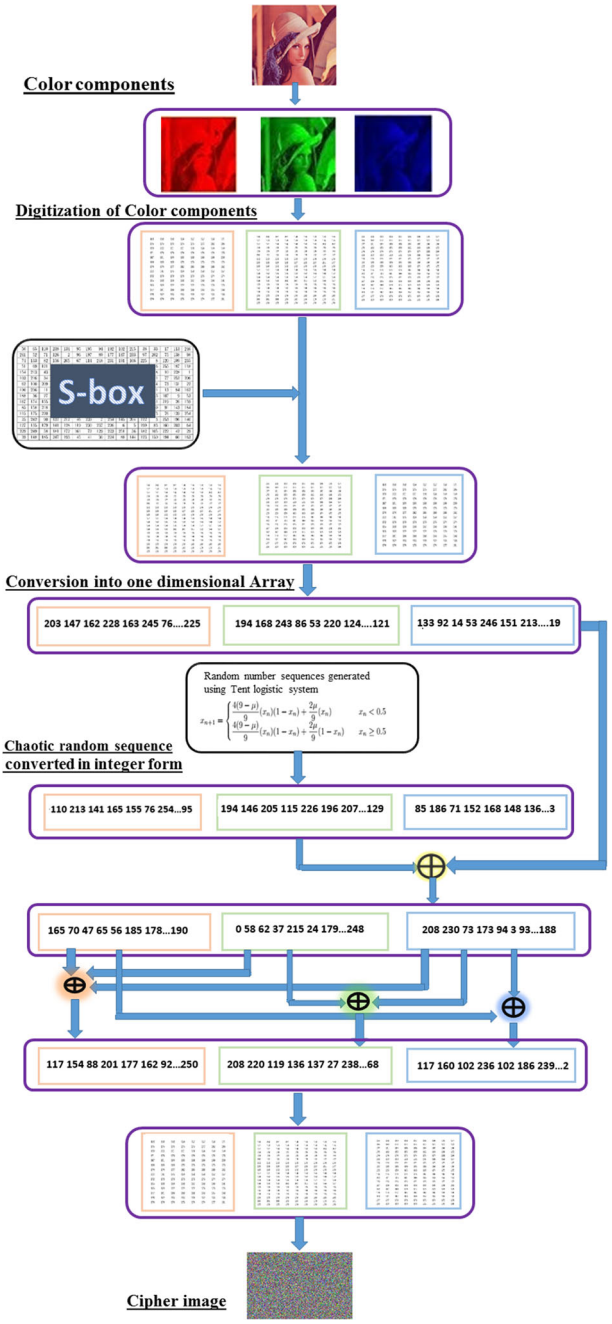

Fig. 7 Flow diagram of the proposed image encryption scheme

$$y_0 = \frac{h_3 \oplus h_7 \oplus h_{11} \oplus h_{15} \oplus h_{19} \oplus h_{23} \oplus h_{27} \oplus h_{31}}{2^8} \tag{10}$$

$$z_0 = \frac{h_4 \oplus h_8 \oplus h_{12} \oplus h_{16} \oplus h_{20} \oplus h_{24} \oplus h_{28} \oplus h_{32}}{2^8} \tag{11}$$

While the control parameters $m,\ \mu_1,\ \mu_2,\ \mu_3$ are formed as:

$$m' = 0.(b_{19} \times 2^{19} + \ldots b_1 \times 2^1 + b_0 \times 2^0)$$

$$m = \begin{cases} m' & m' < 0.5 \\ 1 - m' & m' \geq 0.5 \end{cases} \tag{12}$$

$$\mu_1 = (b_{23} \times 2^3 + \cdots + b_{20} \times 2^0).\ (b_{43} \times 2^{19} + \cdots + b_{24} \times 2^0) \bmod 9 \tag{13}$$

$$\mu_2 = (b_{47} \times 2^3 + \cdots + b_{44} \times 2^0).\ (b_{67} \times 2^{19} + \cdots + b_{48} \times 2^0) \bmod 9 \tag{14}$$

$$\mu_3 = (b_{71} \times 2^3 + \cdots + b_{68} \times 2^0).\ (b_{91} \times 2^{19} + \cdots + b_{72} \times 2^0) \bmod 9 \tag{15}$$

The secret random numbers $T_0,\ M_0$ and N_0 used in encryption are generted as:

$$T_0 = (b_{108} \times 2^{19} + \ldots b_{90} \times 2^1 + b_{89} \times 2^0) \bmod 256 \tag{16}$$

$$M_0 = (b_{128} \times 2^{19} + \ldots b_{110} \times 2^1 + b_{109} \times 2^0) \bmod 256 \tag{17}$$

$$N_0 = (b_{148} \times 2^{19} + \ldots b_{130} \times 2^1 + b_{129} \times 2^0) \bmod 256 \tag{18}$$

The SHA 256 value of plain image is encrypted by RSA encryption algorithm. The asymmetric encryption technique is adopted for the secure transmission of key. The receiver's public key is used to encrypt the hash value in (6). The receiver only use his private key for the decryption of the master key.

$$K_f = H_m^e \mod (r).$$

Here H_m is the master key, K_f is its related encrypted key and $(e,\ r)$ is the public key of receiver. For the decryption receiver uses his private key $(d,\ r)$ in the following relation to get the master key as:

$$H_m = K_f^d \mod (r).$$

After receiving H the receiver uses (7)–(18) to form the subkeys and then use them in decryption algorithm to get the secret image.

Algorithm 3 (*Image encryption algorithm*)
Input: *Image I, Secret keys* k_1, k_2, *Algorithm (2), PWLCM (3), tent logistic map (4).*
Output: *Encrypted image* C.

1. *Read the given secret image* I.
2. *Convert the color (RGB) image* I *into its primary color components i.e., Red, Green and Blue components.*
3. *Input* m *and* x_0' *from secret key* k_1 *in Algorithm (2) to generate an S-box, S.*
4. *Use S as lookup table, for the color components of* I *obtained in Step 1. That is, replace each entry* $m \in I$ *by* $S(m)$, $p_i \leftarrow S(m_i)$ *to get* $P = \{p_1, ..., p_N\}$.
5. *Change the substituted color components into 1 dimensional array of numbers.*
6. *Iterate the tent logistic map for initial state* x_0, y_0, z_0 *and control parameter* μ_1, μ_2, μ_3 *for* L *times.*
7. *Discard first* n_0 *values from* L *i.e.,* $L^* = L - n_0$ *to eliminate the harmful effects of transient process.*
8. *Convert the obtained sequence to 8-bit integer values using the relation*

$$\begin{aligned} x_i &= mod(floor(x_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \\ y_i &= mod(floor(y_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \\ z_i &= mod(floor(z_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \end{aligned}$$

   where mod gives back the remainder after dividing by 256, while the floor(x) gives the largest integer less than or equal to x. *Hence the output sequences lie in the range of [0, 255].*
9. *Pre encrypt each color component separability by using the above generated chaotic sequence as follows:*

   The scrambling process of the pre encrypted image's red component:

   for $i = 1$, $i{+}{+}$, $i = L^*$ **do**
   if $i = 1$, **then**
   $R'(i) \leftarrow R(i) \oplus X(i) \oplus T_o$
   else
   $R'(i) \leftarrow R'(i-1) \oplus R(i) \oplus X(i)$;
   end
   end

   The scrambling process of the pre encrypted images green component:

   for $i = L^*$, $i{-}{-}$, $i = 1$ **do**
   if $i = L^*$, **then**
   $G'(i) \leftarrow G(i) \oplus Y(i) \oplus M_o$
   else
   $G'(i) \leftarrow G'(i+1) \oplus G(i) \oplus Y(i)$;
   end
   end

The scrambling process of the pre encrypted images blue component:

for $i = 1$, $i{+}{+}$, $i = L^*$ **do**
  if $i = 1$, **then**
    $B'(i) \leftarrow B(i) \oplus Z(i) \oplus N_o$
  else
    $B'(i) \leftarrow B'(i-1) \oplus B(i) \oplus Z(i)$;
  end
end

10. *Mix pre encrypted color components to combine the diffusion effects as follows:*

$$\begin{aligned} R''(i) &= R'(i) \oplus G'(i) \oplus B'(i) \\ G''(i) &= G'(i) \oplus B'(i) \\ B''(i) &= R'(i) \oplus B'(i) \end{aligned}$$

11. *Convert R'', G'' and B'' into image form and concatenate these color components, to get ciphered image C.*

The ciphered image C can be converted back to its original image by using following decryption algorithm.

Algorithm 4 (*Image decryption algorithm*)
Input: *Cipher image C, Secret key k_1, k_2, Algorithm (2), PWLCM (3), tent logistic map (4).*
Output: *Original image I.*

1. *Read the cipher image C.*
2. *Convert the cipher image into its primary color components i. e., R'', G'', B''.*
3. *Transform these color components into their digital form and then reshape into one dimensional array form.*
4. *Re-mix color components as follows to get the pre decrypted image components R', G', B'*

$$\begin{aligned} R'(i) &= R''(i) \oplus G''(i) \\ G'(i) &= R''(i) \oplus B''(i) \\ B'(i) &= R''(i) \oplus G''(i) \oplus B''(i). \end{aligned}$$

5. *Iterate the tent logistic map for initial states x_0, y_0, z_0 and control parameters μ_1, μ_2, μ_3 for L times to get three chaotic random sequences.*
6. *Discard first n_0 values to eliminate the harmful effects of transient process.*
7. *Convert the obtained sequences to 8-bit integer values using these relations:*

$$\begin{aligned} x_i &= mod(floor(x_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \\ y_i &= mod(floor(y_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \\ z_i &= mod(floor(z_i \times 10^{14}), 256), \quad i = 1, 2, ..., L^*, \end{aligned}$$

   where mod gives back the remainder after dividing by 256, while the floor(x) gives the largest integer less than or equal to x. Hence the output sequences lie in the range of [0, 255].
8. *Perform the initial decryption using chaotic random sequences as follows:*

The unscrambling process of red component of Cipher image:

for $i = 1,\ i{+}{+},\ i = L^*$ **do**
  if $i = 1$, **then**
    $R'(i) \leftarrow R(i) \oplus X(i) \oplus N_o$
  else
    $R'(i) \leftarrow R'(i-1) \oplus R(i) \oplus X(i)$;
  end
end

The green component of the cipher image is unscrambled as follows:

for $i = L^*,\ i{-}{-},\ i = 1$ **do**
  if $i = L^*$, **then**
    $G'(i) \leftarrow G(i) \oplus Y(i) \oplus M_o$
  else
    $G'(i) \leftarrow G'(i+1) \oplus G(i) \oplus Y(i)$;
  end
end

The following shows the unscrambling procedure of the blue component of cipher image:

for $i = 1,\ i{+}{+},\ i = L^*$ **do**
  if $i = 1$, **then**
    $B'(i) \leftarrow B(i) \oplus Z(i) \oplus N_o$
  else
    $B'(i) \leftarrow B'(i-1) \oplus B(i) \oplus Z(i)$;
  end
end

9. *Convert the obtained one dimensional sequences into two dimensional array.*
10. *Input* k_1 *for* m *and* x_0' *in Algorithm (2) to generate an S-box and then generate its inverse S-box,* S^{-1}.
11. *By using inverse S-Box,* (S^{-1}) *as lookup table for substitute values, obtained after step 5. That is,* $m_i \leftarrow S^{-1}(p_i)$ *to get* $I = \{m_1, \ ..., m_N\}$.
12. *By converting resulting matrix I into image form, original image I is obtained.*

The validation of the proposed image encryption scheme is demonstrated by correctly recovering the original image from the encrypted image. The decryption algorithm correctly reverses all the effects performed during encryption and only the intended receiver can successfully recover the original image.

5 Results and discussions

For the demonstration of proposed scheme, we have applied Algorithms 3 and 4 on two different RGB image files in the following examples. These files are taken from the http://sipi.usc.edu/database/ that is also known as the USC-SIPI Image Database to analyze the utility and the do-ability of our proposed RGB image encryption scheme. All the related experiments and simulations have been performed in the environment of MATLAB.

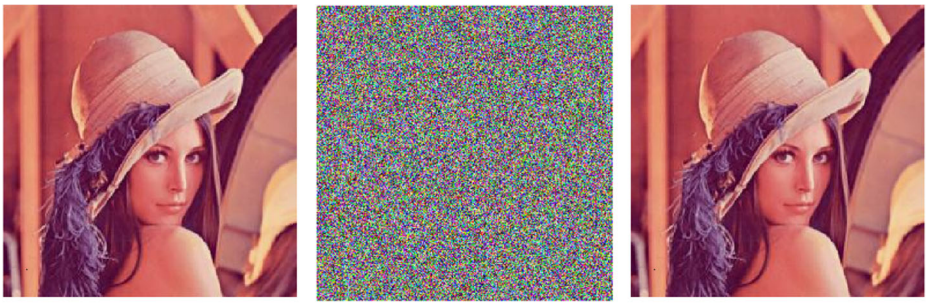

Fig. 8 Experimental results for the Lena image (**a**) Original image (**b**) Encrypted image (**c**) Decryption

Example 1 For image encryption we have selected the standard Lena 256×256 image. The original Lena image shown in the Fig. 8a is encrypted by using the proposed Algorithm 3. The resulting encrypted image is visible in Fig. 8b. The figure shows that the proposed encryption mechanism completely scramble the original image without leaving any clue to reveal the original information. The decryption is then performed by using the proposed image decryption Algorithm 4 and displayed in Fig. 8c. The decryption result indicates that the proposed scheme effectively works and perfectly recover the original image.

Example 2 In the next example we have taken a Pepper 256×256 image. The original image is shown in Fig. 9a, the encryption result is displayed in Fig. 9b. The encryption result signifies that the proposed technique generates a noise like structure that does not reveal any useful information about the original image. The decryption result using Algorithm 4 is presented in Fig. 9c. From the decryption result it is evident that the proposed scheme is able to give a flawless recovery.

6 Security analysis

The algorithm is capable for the use in real time application such as internet communication, multimedia systems etc. For the evaluation of the quality and performance of proposed

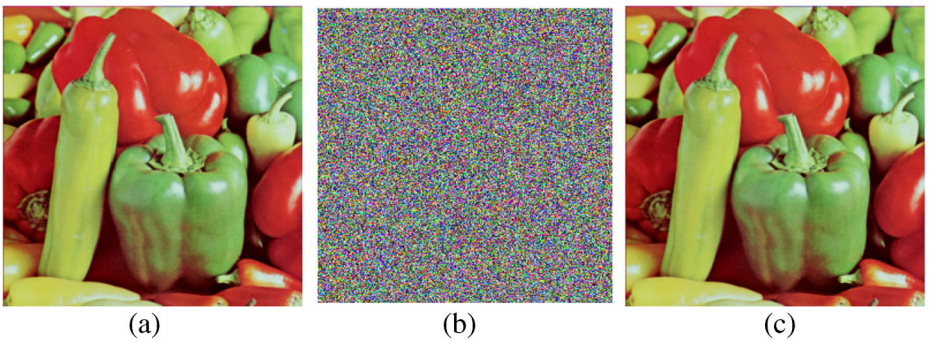

Fig. 9 Experimental results for the Pepper image (**a**) Original image (**b**) Encrypted image (**c**) Decryption

Table 3 Key space size comparison

Image encryption schemes	Key Space
Cuaric et al. [12]	2^{128}
Wang et al. [50]	2^{149}
Rehman et al. [42]	2^{209}
Guesmi et al. [20]	2^{256}
Proposed scheme	2^{398}

image encryption scheme, we apply different security measures and analysis indicators on it. This section is devoted to address the security properties of the proposed scheme.

6.1 Key space

Key space in a cryptosystem is considered an essential feature. It should be sufficiently large to withstand against brute force attack. In the proposed encryption algorithm, secret key is actually a pair $k = (k_1,\ k_2)$ having two secret keys used in encryption algorithm. These secret keys contain the parameters of used chaotic maps, *i.e.*, $k_1 = (x_0',\ m)$ for Chaotic map (3) and $k_2 = (x_0,\ \mu_1, y_0,\ \mu_2, z_0,\ \mu_3)$ for tent logistic map (4). In consonance with IEEE floating point precision [54] the precision of each key should be greater than 10^{-15}. We use precision level for chaotic map's parameters as 10^{-15}. Hence the keyspace size will be $(10^{15})^8 = 10^{120} \approx 2^{398}$. This keyspace is large enough to prevent brute force attack. The resulting keyspace is larger than minimum requirement [4] of key size 2^{100}. A comparison of key space using our proposed technique with some other state of the art schemes is also shown in Table 3.

6.2 Key sensitivity

Another essential requirement for an image encryption scheme is its highly sensitive behavior towards its secret keys. For a good encryption system, a single bit modification in secret key gives completely different encrypted result. In this research we have used PWLCM and tent logistic maps. These chaotic maps are highly sensitive to initial conditions and control parameters. If we take a very insignificant change in key or control parameter, the resulting generated random sequence will completely changed. Which in response gives entirely different encryption/decryption results.

In Fig. 10 two test images Lena and Peppers are used for key sensitivity analysis. First we encrypt them using key components $x_0 = 0.76$ and $m = 0.15$ for PWLCM and $x_0 = 0.479,\ \mu_1 = 4.5,\ y_0 = 0.596,\ \mu_2 = 6.2,\ z_0 = 0.964, \mu_3 = 7.9$ for tent logistic map. Figure 10c, g show the result of using slightly different key than original key, that is x_0 is changed from 0.479 to 0.47900000000000000009. Figure 10d, h depict the difference between the encryption results and modified key based encryption results. From these results it is evident that the encryption results are significantly change by taking a minor modification in any of the key component.

6.3 Distribution of pixels in cipher image

Image histogram shows that how pixels in an image are dispersed. From the above Example 1, Lena image, Fig. 8a is taken as original image, with size (256×256). Histograms of its

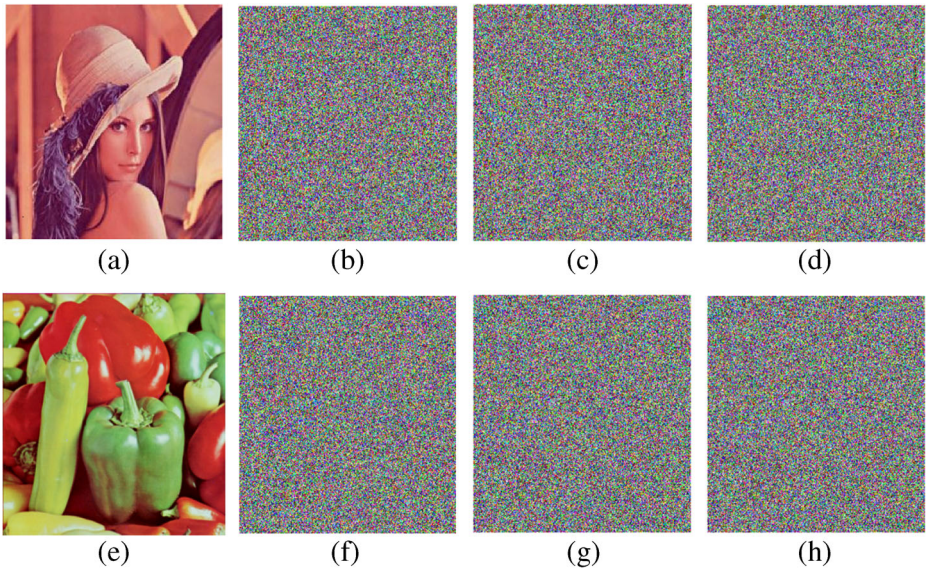

Fig. 10 Experimental results of proposed encryption method for the minor modification in the secret key: (**a**, **e**) original images of Lena and Peppers (**b**, **f**) encrypted images (**c**, **g**) encrypted images using slightly modified key (**d**, **h**) absolute intensity difference images

corresponding ciphered image components are shown in Fig. 11a, b, c. From the histogram it is clear that, there does not exist any clue to mount a statistical analysis attack on the encrypted image.

6.4 Correlation analysis of two adjacent pixels

The quantitative analysis for the evaluation of having high confusion and diffusion among neighboring pixels in plain image and the corresponding cipher image is evaluated by a test of correlation. We have examined the correlation in the adjacent pixels in Lena ciphered image. Figure 12 shows row-wise correlation in components of encrypted Lena image. For

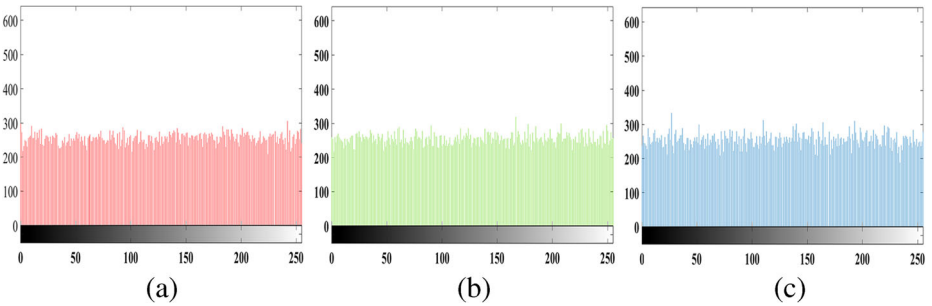

Fig. 11 Histogram of encrypted image (**a**) red component (**b**) green component (**c**) blue component

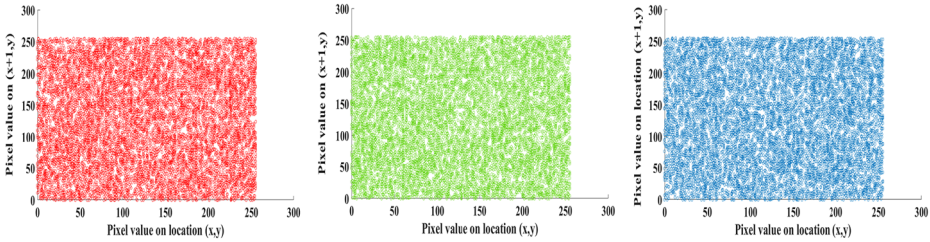

Fig. 12 Correlation (row-wise) in the encrypted Lena image (**a**) red component (**b**) green component (**c**) blue component

calculation of correlation coefficient in horizontal, vertical and diagonal in cipher image, the following relation [40] has been used.

$$C_r = \frac{(n\sum_{p=1}^{n} x_p y_p - \sum_{p=1}^{n} x_p \sum_{p=1}^{n} y_p)}{\sqrt{(n\sum_{p=1}^{n}(x_p)^2 - (\sum_{p=1}^{n} x_p)^2)((n\sum_{p=1}^{n}(y_p)^2 - (\sum_{p=1}^{n} y_p)^2)}} \tag{19}$$

where x_p and y_p are the values of the adjacent pixels in the image and n is the cumulative number of pixels taken for the calculation of correlation (19).

The values in resulting Table 4 tells that correlation coefficient of cipher image approaches to zero. Hence neighboring pixels in cipher image are almost uncorrelated.

6.5 Information entropy

This feature of analysis is used to test the randomness in the encrypted image. It also indicates an average amount of information contained in ciphered image. For the cipher image C the entropy value [55] can be computed with the formula:

$$H(C) = \sum_{i=o}^{2^N-1} P(c_i) log_2 \frac{1}{P(c_i)}. \tag{20}$$

Here $p(c_i)$ in (20) shows the probability of occurrence of symbol c_i in cipher image C. For exact random source emitting 256 symbols, the ideal value of entropy $H(C)$ is 8. If value of entropy less than 8 in cipher image then it means that there is a possibility of predictability of plain image. Which is dangerous for security of image encryption algorithm. In proposed algorithm entropy for ciphered image C, that is $H(C)$ is checked. The calculated value of entropy of ciphered image C with comparison to other images is shown in Table 5.

Table 4 Correlation coefficient of two neighboring pixels in original and ciphered image

Direction	Orig. Img.	Prop. Scheme	Wang et al. [49]	Wang et al. [50]	Zhang et al. [58]	Wei et al. [53]
Horizontal	0.9355	0.0019	0.0019	0.0037	0.0036	0.0042
Vertical	0.9093	0.0035	0.0038	0.0029	0.0023	0.0033
Diagonal	0.8815	0.0008	0.0019	0.0047	0.0039	0.0024

Table 5 Entropy values comparison

Encryption schemes	Entropy values
Fu et al. [18]	7.9880
Wu et al. [56]	7.9971
Choi et al. [11]	7.8198
Wu et al. [52]	7.9912
Proposed scheme	7.9959

The result shows that entropy of encrypted image is very near to ideal entropy value which is 8. It shows that amount of information leakage in proposed image encryption algorithm is almost zero. Hence it is secure enough.

6.6 Sensitivity analysis of the proposed algorithm

Number of pixel change rate (NPCR) and the unified average changing intensity (UACI) are used as the measuring criterion's for investigating the effect of varying one pixel of the plain image on the cipher image. These indicators are calculated by the following formulas:

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

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

Here w and h indicate the width and height of the cipher image respectively. X and X' are cipher images obtained from the original image and one pixel difference in the original image respectively. If X and X' are same then $K_{i,j} = 0$ otherwise 1. For the resistance against differential attacks, NPCR and UACI [51] values should be large and close to their optimum values. In this research, for Lena 256×256 image the calculated NPCR and UACI values are 99.62 and 33.46 respectively. The proposed scheme shows high performance for these indicators. Therefore it will provide well resistance against "known plaintext attacks" and "chosen plaintext attacks".

6.7 Noise and data loss attacks

A good encryption scheme also has the property to minimize the noise effects generated due to the pixel discrepancies in the decrypted image. For the capacity evaluation of our proposed method against the resistance of noise and data loss attacks, we use color Lena image as test case of size 256×256. The encrypted test image is noised by adding 1%, 5% and 10% salt and pepper noise as shown in the Fig. 11.

It is obvious from the figure that when the encrypted image encounter the salt and pepper noise, the decryption results retains a significant majority of original information and also contains a small portion of evenly distributed noise. The quantitative analysis for the difference between the plain image I_P and the decrypted image I_D is carried out by using peak signal to noise ratio (PSNR). While the mean square error (MSE) is used to measure

the cumulative squared error between the original image and the decrypted image. For the calculation of PSNR and MSE [5] of MN sized image, we use the following relations:

$$\text{PSNR} = 10.\log \frac{255^2}{\text{MSE}} \, (db), \tag{21}$$

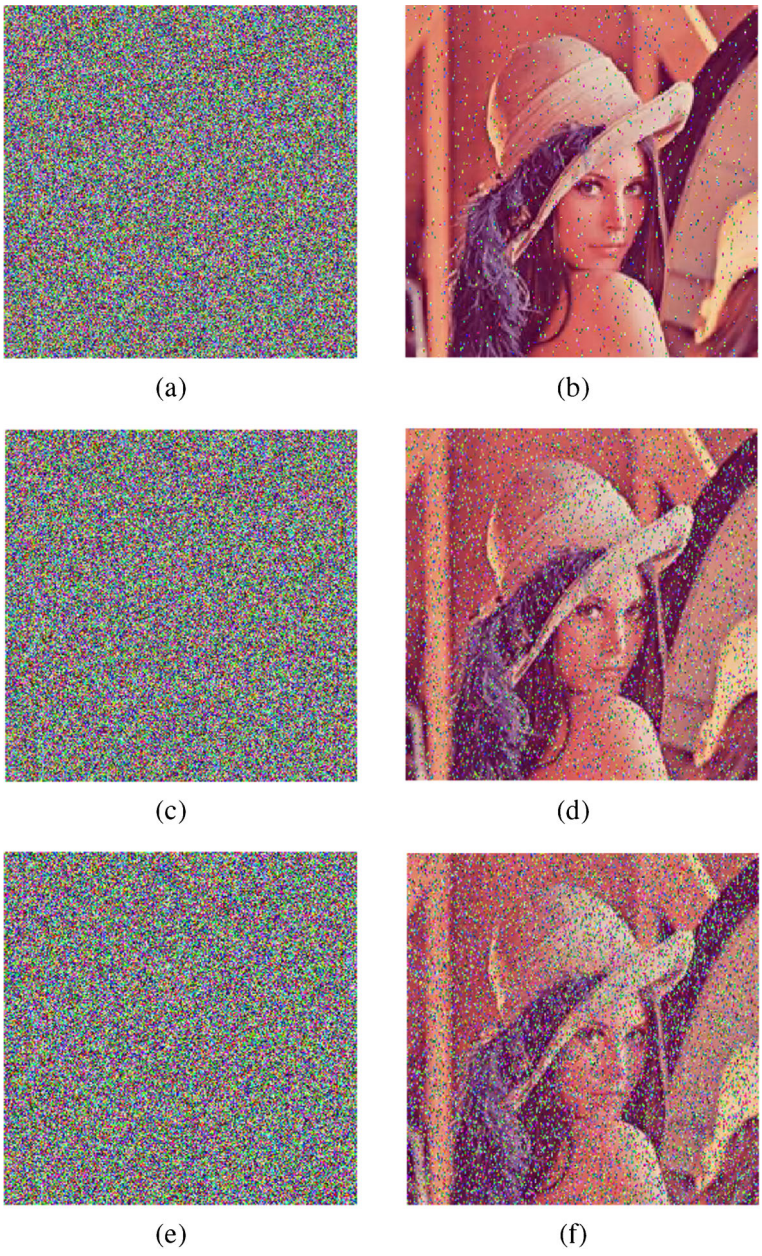

Fig. 13 Experimental results for the performance evaluation of data loss attacks: (**a**, **c**, **e**) cipher images with 1%, 5% and 10% salt and pepper noise, (**b**, **d**, **f**) decryption results of corresponding images using our scheme

Table 6 Performance of MSE and PSNR about salt and pepper noise

Salt & pepper noise	1%	5%	10%
MSE	392.49	1845.3	3357.43
PSNR	22.2370	15.5095	12.9098

$$\mathrm{MSE} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{i=0}^{N-1} (\mathrm{I}_P(i, j) - \mathrm{I}_D(i, j))^2. \tag{22}$$

The smaller MSE values calculated from (22) indicate the minimal error in the decryption results. Whereas the higher PNSR values obtained from (21) reveal the higher decrypted image fidelity against its original plain image (Fig. 13).

The calculated values of PSNR for these modified cipher images by 1%, 5% and 10% salt and pepper noise are shown in Table 6. The findings show that the encryption strategy provides reasonable efficiency for data loss and noise attacks.

6.8 Complexity analysis

There is a strong relationship between the complexity in the chaotic system and the robustness of the cryptosystem based on that chaotic system. In this research we have used two chaotic maps, the piecewise linear chaotic map (3) and tent logistic map (4). The chaotic map (3) is used to generate a random sequence of length MN, where as chaotic map (4) gives 3 random sequences, floor function is used to convert these values into integer form. The XOR function is used to generate randomness in the image and also to accumulate the generated randomness in different components of image. Thus the calculated complexity value for used chaotic maps and applied operations, is $14(MN) + 3\log_2(MN)$. The high complexity of the proposed scheme ensures good quality encryption results.

6.9 Encryption/decryption time

For any algorithm, security considerations are important but a good encryption algorithm should also robust and efficient. The running speed of encryption algorithm is an important aspect. Using our proposed algorithm, we have measured the encryption/decryption time of Lena image of size 256×256. The time analysis is done on CORE i7-3520M, 2.90GHz CPU with 8GB RAM notebook running on Windows 8, 64 bit operating system using Matlab R2013a (8.1.0.604). The average time taken by the proposed encryption/decryption algorithm for Lena image is 0.277 second.

6.10 Comparison

A deep and detailed overall comparison of the proposed scheme with other image encryption schemes is given below.

The comparison presented in Table 7 shows that the proposed scheme has better results for correlation analysis and key space while the performance against entropy analysis, NPCR and UACI is also comparable with many other state of the art encryption techniques.

Table 7 Properties comparison of cipher generated by taking Lena as test image

Algorithms	NPCR	UACI	Correlation	Keyspace	Entropy
Proposed scheme	99.62	33.46	0.002066	10^{120}	7.9959
Ali et al. [3]	99.6094	33.4635	0.0020	10^{90}	7.9984
Kanwal et al. [25]	99.61	33.46	0.002977	10^{84}	7.9990
Chai et al. [6]	99.63	–	0.0037	10^{51}	7.9983
Wu et al. [52]	100	33.47	0.00603	10^{112}	7.9912
Wang et al. [50]	99.5956	33.5512	0.0038	10^{56}	7.9975

7 Conclusion

In this study a novel and different technique for the encryption/decryption of color images is proposed based on S-box and chaotic system. Hybrid cryptographic approach is used for this purpose. It uses a plain image based master key for the generation of subkeys to encrypt the corresponding image. The master key is sent to the receiver by using the asymmetric cryptographic technique RSA after encrypting with the public key of the receiver. Encryption and decryption processes are carried out by using symmetric cryptographic approach. In encryption phase the generated S-box by PWLCM takes the substitution of image pixel values and hence generates confusion and diffusion in the image. The tent logistic system is used as PRNG for the generation of random chaotic sequence. Then a mixing technique employed for the mixing of this generated sequence with substituted image pixels values and their preceding values. Finally a self mixing operation on the components of image is used for stable noise like effects in the encrypted image.

The proposed algorithm has provided resistance to different types of cryptographic attacks as brute force attack, known plaintext attack, noise and data loss attacks etc. It is also capable of handling with different sizes and formats of images. The security analysis shows the practicability and effectiveness of proposed scheme. The proposed encryption scheme is based on multi chaotic maps, therefore it may require large memory and hence increase computational cost. As a future work, the image encryption and decryption coding algorithms can be further improved by using some recent work on the optimization of alogrithms and code design like [9, 15, 27, 28].

References

1. Alawida M, Samsudin A, Teh JS, Alkhawaldeh RS (2019) A new hybrid digital chaotic system with applications in image encryption. Sig Process 160:45–58
2. Ali TS, Ali R (2020) A novel medical image signcryption scheme using TLTS and Henon chaotic map. IEEE Access 8:71974–71992
3. Ali TS, Ali R (2020) A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimed Tools Applic 79(27):19853–19873
4. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifur Chaos 16(08):2129–2151
5. Asim M, Jeoti V (2008) Efficient and simple method for designing chaotic S-boxes. ETRI J 30(1):170–172
6. Chai X, Bi J, Gan Z, Liu X, Zhang Y, Chen Y (2020) Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. Sig Process 176:107684
7. Chai X, Zhi X, Gan Z, Zhang Y, Chen Y, Fu J (2021) Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption. Sig Process 183:108041

8. Chai X, Wu H, Gan Z, Han D, Zhang Y, Chen Y (2021) An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. Inf Sci 556:305–340
9. Chandrawat RK, Kumar R, Garg BP, Dhiman G, Kumar S (2017) An analysis of modeling and optimization production cost through fuzzy linear programming problem with symmetric and right angle triangular fuzzy number. In: Proceedings of sixth international conference on soft computing for problem solving. Springer, pp 197–211
10. Chen G, Mao Y, Chui CK (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons and Fractals 21(3):749–761
11. Choi J, Seok S, Seo H, Kim H (2016) A fast ARX model-based image encryption scheme. Multimed Tools Applic 75(22):14685–14706
12. Curiac DI, Volosencu C (2012) Chaotic trajectory design for monitoring an arbitrary number of specified locations using points of interest. Mathematics Problem in Engineering, 1–18
13. Daemen J, Rijmen V (2001) AES Proposal, Rijndael. National institute of standards and technology, FIPS-197
14. Dhiman G, Kaur A, Sharma V, Kautish S, Guo S, Slowik A, Anshu S, A V (2020) Special issue on computational approaches for COVID-19 disease medical image analysis. Current medical imaging, Bentham Science
15. Dhiman G, Kumar V (2019) Spotted hyena optimizer for solving complex and non-linear constrained engineering problems. In: Harmony search and nature inspired optimization algorithms. Springer, pp 857–867
16. Diomidious M, Chardalias K, Magita A, Koutonias P, Panagiotopoulou P, Mantas J (2016) Social and psychological effects of internet use. Acta Inform Med 24(1):66–68
17. Drebing H, Bailer J, Anders A, Wagner H, Gallas C (2014) Cyberstalking in a large sample of social network users: prevalence, characteristics and impact upon victims. Cyberpsychol Behav Soc Netw 17(2):61–67
18. Fu C, Lin B, Miao Y, Liu X, Chen J (2011) A novel chaos-based bit level permutation scheme for digital image encryption. Opt Commun 284(23):5415–5423
19. Fridrich J (1998) Symmetric ciphers based on two dimensional chaotic maps. Int J Bifur Chaos 8(6):1259–1284
20. Guesmi R, Farah MAB, Kachouri A, Samet M (2016) A novel chaos based image encryption using DNA sequence operation and secure hash algorithm SHA-2. Nonlinear Dynam 83(3):1123–1136
21. Guan ZH, Huang F, Guan W (2005) Chaos based image encryption algorithm. Phys Lett A 346(1–3):153–157
22. Habutsu T, Nishio Y, Sasase I, Mori S (1991) A secret key cryptosystem by iterating a chaotic map. In: Workshop on the theory and application of cryptographic techniques. Springer, Berlin
23. Hussain I, Shah T, Gondal MA, Mahmood H (2012) Analysis of S-Box in image encryption using root mean square error method. Zeitschrift fur natureforschung A 67(6–7):327–332
24. Jamal SS, Shaukat S et al (2019) Construction of cryptographic S-boxes based on mobius transformation and chaotic tent-sine system. IEEE Access 7:173273–173285
25. Kanwal S, Inam S, Cheikhrouhou O, Mahnoor K, Zaguia A, Hamam H (2021) Analytic study of a novel color image encryption method based on the chaos system and color codes. Complexity
26. Kammer RG (1999) Data encryption standard(DES), Federal information processing standards publication. FIPS PUB 46:3
27. Kaur S, Awasthi LK, Sangal AL, Dhiman G (2020) Tunicate swarm algorithm: a new bio-inspired based metaheuristic paradigm for global optimization. Eng Applic Artific Intell 90:103541
28. Kaur A, Dhiman G (2019) A review on search-based tools and techniques to identify bad code smells in object oriented systems. In: Harmony Search and Nature Inspired Optimization Algorithms. Springer, Singapore, pp 909–921
29. Khan M, Shah T, Batool SI (2015) Construction of S-box on chaotic Boolean function and its application in image encryption. Neural computing and application, https://doi.org/10.1007/s 00521-015-1887
30. Li C, Luo G, Chunbao Li KQ (2017) An image encryption scheme based on chaotic tent map. Nonlin Dynam 87(1):127–133
31. Lorenz EN (1969) Atmospheric predictability as revealed by naturally occuring analogues. Journal of Atmospheric Science. Bibcode: 1969JAtS.26.636L, 636–646
32. Lu Q, Zhu C, Wang G (2019) A novel S-box design algorithm based on a new compound chaotic system. Entropy 21(10):1004
33. Matthews R (1989) On the derivation of a 'chaotic' encryption algorithm. Cryptologia 8(1):29–41
34. Mao Y (2004) A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurc Chaos 14(14):3613–3624

35. Markus M, Hess B (1989) Lyapunov exponents of the Logistic map with periodic forcing. Comput Graph 13(4):553–558
36. Mankar VH, Das TS, Sarkar SK (2010) Discrete chaotic sequence based on logistic map in digital communication. National conference on emerging trends in electronics engineering and computing, E3c
37. Meier W (1994) On the security of IDEA block cipher. Advances in cryptology. In: Proceedings of eurocrypt, lecture notes in computer science, vol 765. Springer, Berlin, pp 371–385
38. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. Image Vis Comput 24(9):926–934
39. Patidar V, Pareek NK, Purohit G, Sud KK (2010) Modified substitution diffusion image cipher using chaotic standard and logistic map. Commun Nonlinear Sci Numer Simul 15(10):2755–2765
40. Pearson K (1895) Note on regression and inheritance in the case of two parents. Proc R Soc London 58(347–352):240–242
41. Picek S, Batina L, Jakobovic D, Ege B, Golub M (2014) S-box, SET, match: a toolbox for S-box analysis, Information security theory and practice, securing the internet of things. Ser Lect Notes Comput Sci 8501:140–149
42. Rehman AU, Liao X, Kulsoom A, Abbas SA (2015) Selective encryption for gray images based on chaos and DNA complementary rules. Multimed Tools Applic 74(13):4655–4677
43. Rivest RL, Shamir A, Adleman L (1977) A method for obtaining digital signatures and public-key cryptosystems. Association for computing machinery
44. Shannon CE (1949) Communication theory of secrecy systems. Bell Syst Tech J 28:656–715
45. Singh P, Dhiman G (2018) Uncertainty representation using fuzzy-entropy approach: special application in remotely sensed high-resolution satellite images (RSHRSIs). Appl Soft Comput 72:121–139
46. Stoyanov B, Kordov K (2015) Image encryption using Chebyshev map and rotation equation. Entropy 17:2117–2139
47. Stoyanov B, Kordov K (2014) Novel image encryption scheme based on Chebyshev polynomial and duffing map. The Scientific World Journal
48. Tiwari V, Gupta KG, Ojha M, Sharma A, Dhiman G (2021) Image-based rapid pests detection and identification on soybean crop: method for low-powered devices. Microprocessors and microsystems. Elsevier
49. Wang X, Lintao L, Yingqian Z (2015) A novel chaotic block image encryption algorithm based on dynamic random growth technique. Opt Lasers Eng 66:10–18
50. Wang X, Zhu X, Wu X, Zhang Y (2018) Image encryption algorithm based on multiple mixed hash functions and cyclic shift. Optics Lasers Eng 107:370–379
51. Wu Y, Noonan JP, Agaian S (2011) NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. J Select Areas Telecommun (JSAT) 1(2):31–38
52. Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ELGamal scheme. Sig Process 141:109–124
53. Wei et al (2012) A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J Syst Softw 85(2):290–299
54. Whitehead N, Fit-Florea A (2011) Precision performance: floating point and IEEE 754 compliance for NVIDIA GPUs rn (A + B) 21(1):18749–19424
55. Wu Y, Zhou Y, Saveriades G, Agaian S, Noonan JP, Natarajan P (2013) Local Shannon entropy measure with statistical tests for image randomness. Inform Sci 222:323–342
56. Wu Y, Zhou Y, Noonan JP, Agaian S (2014) Design of image cipher using latin squares. Inform Sci 264:317–339
57. Yuvaraj N, Srihari K, Dhiman G, Somasundaram K, Sharma A, Rajeskannan S, Masud M (2021) Nature-inspired-based approach for automated cyberbullying classification on multimedia social networking. Mathematical Problems in Engineering
58. Zhang Q, Guo L, Wei X (2010) Image encryption using DNA addition combining with chaotic maps. Math Comput Model 52(11):2028–2035
59. Zhou Y, Bao L, Chen CP (2014) A new 1D chaotic system for image encryption. Sig Process 97:172–182

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.