INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

A Novel Fast Color Image Encryption Algorithm based on 2D-Hybrid Maps

S Syed Suhaila[1]*, V Pradeep[2]

1 Assistant Professor, Department of Computer Science and Engineering, Alagappa Chettiar Government College of Engineering and Technology, Karaikudi, Tamil Nadu, India
2 Assistant Professor, Department of Electrical and Electronics Engineering, Alagappa Chettiar Government College of Engineering and Technology, Karaikudi, Tamil Nadu, India

OPEN ACCESS

Received: 14.12.2021
Accepted: 19.02.2022
Published: 14.03.2022

Citation: Suhaila SS, Pradeep V (2022) A Novel Fast Color Image Encryption Algorithm based on 2D-Hybrid Maps . Indian Journal of Science and Technology 15(10): 457-467. https://doi.org/10.17485/IJST/v15i10.2348

* **Corresponding author**.

syedsuhaila63@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objectives: To design a fast and efficient color image encryption technique using 2D Duffing, Henon and Tinkerbell maps. **Methods:** The presented work employs the confusion-diffusion-confusion structure for encryption. Pixel-level scrambling is undertaken in the first phase of confusion, and the scrambled image is diffused using the Exclusive-OR operation. Finally, bit-level permutation is used for improved security. This work makes use of the 44 samples from the USC-SIPI image database. **Findings:** The presented color image encryption technology's performance is quantitatively compared with two recent techniques and observed that the proposed work reduces time by 81.2%. **Novelty:** This work employs a confusion-diffusion-confusion framework which increases algorithmic security by 47.8%. Further, a novel key generation scheme is designed to generate dynamic and input image-sensitive keys. **Applications/Improvements:** The simple Exclusive-OR operation-based diffusion that is devised significantly minimizes encryption time, thereby making it ideal for real-time applications.

Keywords: Encryption; Chaos; Sensitivity; Entropy; Histogram

1 Introduction

Owing to the rapid progression in communication technology, the Internet has become the primary carrier of multimedia data. Sensitive data in a form of digital image is continually being transmitted through the Internet by various financial organizations, the military and medical practitioners besides personal use by the individuals worldwide [(1)]. Of critical concern is the confidentiality of sensitive image data travelling through a public network. Cryptographic techniques effectively safeguard multimedia data against security attacks [(2)]. Because pictures have distinct intrinsic characteristics that differ from text, classical cryptographic algorithms are not ideal for image encryption [(3)]. Chaos is a non-linear dynamic system phenomenon that is imbued with significant properties such as ergodicity, strong sensitivity to control parameters, and an unpredictable random nature. Chaos is a key field of investigation in picture encryption because of its interrelation with cryptography [(4)].

In recent years, numerous chaos-based cryptosystems have been presented by researchers. Zhongyue Liang et al. [5] proposed a novel medical image encryption technique based on genetic computation and a 5D chaotic system. The technique employs diffusion-scrambling architecture. The DNA operation for diffusion and scrambling is carried out by following sorted chaotic sequences. The technique achieved wider keyspace and introduced high randomness in the ciphered picture but the 5D system increases computation time. Supriyo De et al. [6] developed an image encryption scheme that generates a pseudo-random chaotic sequence using a 2D ecological map. Additionally, the logistic map is used to execute image substitution. In spite of correlation reduction, this technique is vulnerable to statistical attacks. Karim H. Moussa et al. [7] introduced a parameters-based picture encryption algorithm using a 3D hopped map and histogram equalization. Chaos is applied for both pixel value transformation and pixel position permutation, and the security of the algorithm further enhanced by column and row rotation operations. However, the key size is not adequate enough to withstand brute force attacks. Aesha Elghandour et al. [8] suggested a cryptographic method for image encipherment, based on a piecewise nonlinear map. The confusion-diffusion framework is employed, with the logistic map adopted in the confusion process and the permuted image masked using the piecewise map. The scheme, however, is susceptible to chosen plain image and cipher image attacks. Mustafa Kamil Khairullah et al. [9] presented an encryption algorithm based on the two chaotic maps designed. The maps exhibit great parameter sensitivity and hence perform well against differential attacks. The sequence uniformity test results showed skewness in the distribution of quadratic and logistic maps.

Sadiq A. Mehdi [10] proposed an image cryptosystem that uses a new 4D hyper-chaotic autonomous mechanism. The system applies two positive Lyapunov exponents, which makes it most sensitive to the starting values. The scrambling process employed is not optimal, rendering it ineffective against noise attacks. Zijing Gao et al. [11] developed an image cipher based on enhanced sine and tent chaotic maps with expanded parameters. The scheme adopts the scrambling-diffusion model of picture encryption. The anti-attack ability of the proposed scheme is strong, despite its vulnerability to occlusion stacks. Shamsa Kanwal et al. [12] posited an encryption framework based on colorcodes and chaos. The linear piecewise map and the Hill cipher are used in the permutation and substitution phases, respectively. The technique, which enhances the diffusion process through the use of the logistic map, excels against statistical attacks. The PSNR values indicate that the quality of the decrypted image is compromised. Chao Yang et. al. [13] designed a 2D collapse mapthat is used in S-Box construction. The newly constructed S-box is used in the forward substitution and reverse substitution phases of the image encryption process. The two diffusion operations in opposite directions enhance the stability of the technique. From the visual comparison of decrypted images, it is perceived that the system poorly performs against 1/16 and 1/32 sized cropping attacks. Most of the cryptosystems studied in the literature can only be used for grayscale images.

Yaghoub Pourasad et al. [14] developed a novel digital image cryptosystem based on wavelet transform and chaos theory. The system employs wavelet transform to decompose image and extract wavelet coefficient, which reduces amount of calculation in confusion. The technique is fast but the map's chaotic orbit is simple, hence it can be predicted by non-linear prediction approach. Yong Zhang [15] introduced a cipher with identical procedure for encryption and decryption operations that uses Henon map to generate keys and lifting transformation for diffusion. The unified scheme achieved an average of 0.55% maximum relative error for ciphered images. The feedback operation is vaguely defined in the system. Adélaïde Nicole et al. [16] presented a secure image encryption technique using Lorenz system and DNA coding. This technique performs zigzag operation to combine the three sequences of Lorenz system and subsequently used in encryption. The system shows high level sensitivity on keys variation. The algorithm is time consuming hence not ideal for real time applications. Thus, it is of interest to design a fast color image encryption algorithm based on hybrid maps. The major benefits of the newly suggested technique include a larger key space, input picture sensitivity, good permutation property, and suitability for practical application.

2 Two Dimensional Chaotic Maps

This work employs the 2DDuffing, Henon and Tinkerbell maps, which are explained below.

2.1 2D Duffing map

The Duffing map is a discrete dynamical system. The 2D Duffing map may be defined as follows [17]

$$\begin{aligned} x_{n+1} &= y_n \\ y_{n+1} &= -bx_n + ay_n - y_n^3 \end{aligned} \tag{1}$$

where a and b are the system control parameters. The 2D Duffing map exhibits chaotic behaviour at a=2.75 and b=0.2. The trajectory of the 2D duffing map for the constant parameters (a=2.75 and b=0.2) and starting values (x_1=0.1933 and y_1=0.8087) is shown in Figure 1.

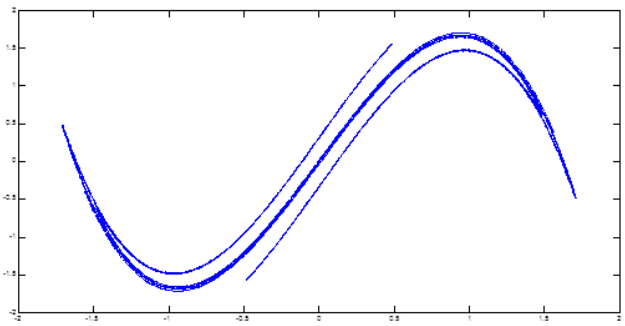

Fig 1. The trajectory of 2D the Duffing map

2.2 2D Henon map

The 2D Henon map may be defined as follows [18]

$$\begin{aligned} x_{n+1} &= y_n + 1 - ax_n^2 \\ y_{n+1} &= bx_n \end{aligned} \tag{2}$$

where a and b are the system control parameters. The 2D Henon map exhibits chaotic behaviour at a=1.4 and b=0.3. The trajectory of the 2D Henon map for the parameters (a=1.4 and b=0.3) and starting values (x_1=0.0 and y_1=0.0) is shown in Figure 2.

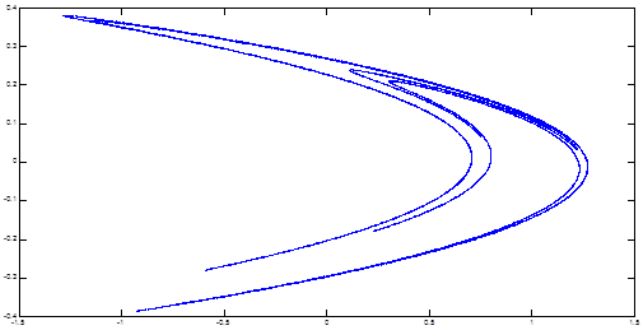

Fig 2. The trajectory of the 2D Henon map

2.3 2D Tinkerbell map

The Tinkerbell map may be defined as follows [19]

$$\begin{aligned} x_{n+1} &= x_n^2 - y_n^2 + ax_n + by_n \\ y_{n+1} &= 2x_n y_n + cx_n + dy_n \end{aligned}$$

where a, b, c and d are the system control parameters. The 2D Tinkerbell map shows chaotic behaviour when a=0.9, b=-0.6013, c=2.0 and d=0.5. The trajectory of the 2D Tinkerbell map for the constant parameters (a=0.9, b=-0.6013, c=2.0 and d=0.5) and starting values (x_1=-0.72 and y_1=-0.64) is shown in Figure 3.

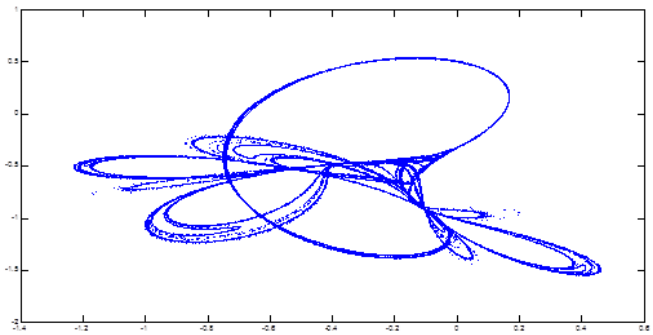

Fig 3. The trajectory of the 2D Tinkerbell map

3 Image Encryption and Decryption Algorithm

3.1 Key Generation

The initial values for the Duffing, Henon, and Tinkerbell maps are the secretkeys of the proposed algorithm. The technique is especially powerful against plaintext-based threats because of these input image-based keys.

The secret keys are obtained by using the following Eqns. (4) – (9).

$$x_1 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} R(i,j) + \sum_{i=1}^{M}\sum_{j=1}^{N} G(i,j)}{2 \times M \times N \times 2^8} \tag{4}$$

$$x_2 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} G(i,j) + \sum_{i=1}^{M}\sum_{j=1}^{N} B(i,j)}{2 \times M \times N \times 2^8} \tag{5}$$

$$x_3 = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} B(i,j) + \sum_{i=1}^{M}\sum_{j=1}^{N} R(i,j)}{2 \times M \times N \times 2^8} \tag{6}$$

$$y_1 = x_1 \bigoplus x_2 \tag{7}$$

$$y_2 = x_2 \oplus x_3 \tag{8}$$

$$y_3 = x_3 \quad \oplus \quad x_1 \tag{9}$$

where R, G, and B represent the red, green, and blue components, respectively.

3.2 The Encryption algorithm

The scheme utilizes the three 2D chaotic (Duffing, Henon, and Tinkerbell) maps in the encryption operation, along with the confusion-diffusion-confusion structure. Confusion renders the relationship between the values of the cipher image and encryption key as difficult as possible. There is a likelihood of the statistical structure of the plain image disintegrating into the long-range statistics of the cipher image during diffusion, with the two sharing a complicated relationship. In this work, confusion is realized through permutation and diffusion through substitution.The encryption operation comprises the following steps.

Step 1: Input the original image (P) of W×Hdimensions (W width pixels and H height pixels), using a color image with dimensions of 256×256.

Step2: Generating pseudo-random sequences: Set the chaotic map's initial seeds and system control parameters. Iterate the Duffing, Henon, and Tinkerbell maps 70536 times. Discard the first 5000 starting values to avoid transient effects.

Step 3:Pixel-level scrambling: Use the pseudo-random sequences generated by the Duffing map in step 2 for pixel scrambling. The process changes the position of each pixel.

Step4:Pixel -level substitution: Use the pseudo-random sequences generated by the Henon map in step 2 for pixel substitution. The process changes the value of each pixel.

Step 5:Bit-levelscrambling: Use the pseudo-random sequences generated by the Tinkerbell map in step 2 for bit scrambling. The process changes the position of each bit. The output is the cipher image, C. Figure 4 shows a block diagram of the encryption operation.

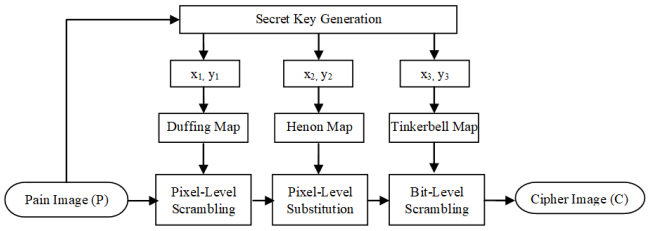

Fig 4. Block diagram of theproposed system

Pseudocode

```
% Reading image from a database
Read Image ('P')
Reshape 2D P into 1D P
%Generate Pseudo-Random Sequence
   [M, N]=size (P)
   [X, Y]=zeros (M, N)
   [X, Y]= map (arguments)
  Preprocessing(X, Y)
X=mod(X*10^14,256)
Y=mod(Y*10^14,256)
%Pixel Level Scrambling
      P1=shuffle P at pixel level based on index of ascending order chaotic sequences obtained in step 4.
%Pixel Level Substitution
   P'=de2bi (P)
   X=de2bi (X)
   SP1=bitxor (P', X)
%Bit Level Scrambling
       C=shuffle SP at bit level based on index of ascending order chaotic sequences obtained in step 4.
       C=bi2de(C)
 Reshape 1D C into 2D C
```

By executing the encryption algorithm in reverse order, the plain image can be effectively recovered.

4 Experimental Results and Security Analysis

4.1 Key Space analysis

Secret keys are crucial to the strength of any encryption scheme. Key space refers to the total number of possible keys that can be formed by utilizing all possible combinations of the secret keys [20]. The key space should be sufficiently large in order to withstand a brute force attack. The precision of the map's starting values is 10^{-14} in each test. The proposed technique offered 10^{126} key spaces, which is good enough to resist key-based attacks.

4.2 Key Sensitivity analysis

The security strength of a cipher is more depends on sensitivity of its secret key [21]. The key sensitivity of the suggested cryptosystem is tested as follows.The following keys are used to encrypt test image-1: $x_1 = 0.1933$, $y_1 = 0.8087$, $x_2 = 0$, $y_2 = 0$, $x_3 = 0.72$ &$y_3 = 0.64$. The encrypted image is then decrypted using the slightly modified keys, $x_1 = 0.193300000000000000001$, $y_1 = 0.8087$, $x_2 = 0$, $y_2 = 0$, $x_3 = 0.72$ and$y_3 = 0.64$. Figure 5 shows how a tiny change in the key resulted in a noise-like image during the decryption process, which demonstrates the keysensitivity of the proposed method.

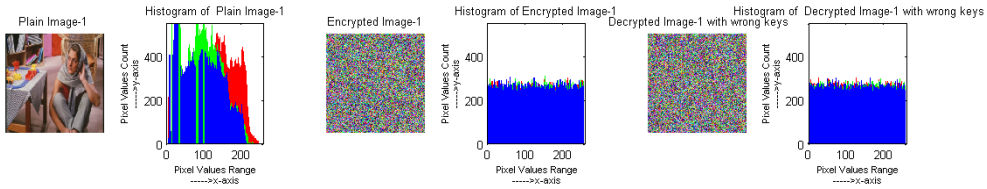

Fig 5. Key sensitivityresults

4.3 Histogram analysis:

A histogram shows the distribution of color intensity values for an image, and cryptanalysts can benefit from the statistical information offered. An efficient encryption operation must destroy statistical patterns [22]. Figure 6 illustrates the histograms of five test input images and their corresponding encrypted images. The proposed encryption operation distributes the pixel values in the cipher image much more uniformly, and is indicative of the system's strength.

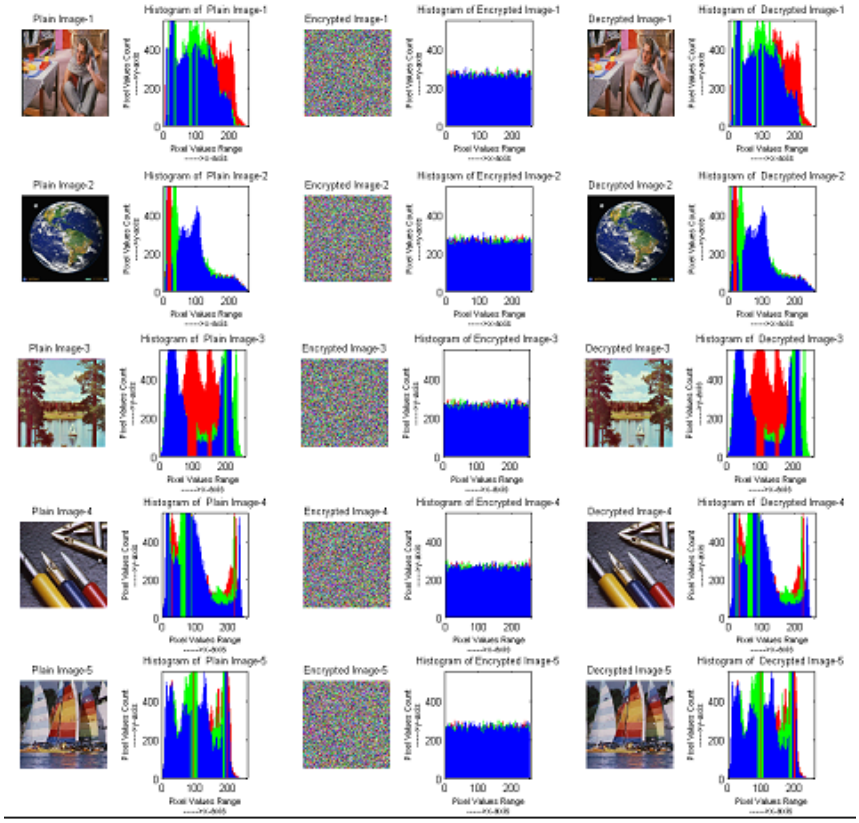

Fig 6. 4Histogram results

4.4 Correlation analysis

The degree of correlation between adjacent pixels of the input plain image is high. The encryption operation must lower the correlation value to almost zero to prevent statistical attacks [23]. The correlation coefficient is obtained using Eqn. (10), where x and y are the color component values of adjacent pixels in the image, N is the total number of adjacent pixels selected from the image, and r_{xy} is the correlation coefficient. The correlations of adjacent pixels in the input and cipher images for three directions are given in Figure 7 and Table 1.

$$
\begin{aligned}
r_{xy} &= \frac{E(x-E(x)(y-E(y))}{\sqrt{D(x)}\sqrt{D(y)}} \\
\mathrm{E(x)} &= \frac{1}{N}\sum_{i=1}^{N} x_i \\
\mathrm{E(y)} &= \frac{1}{N}\sum_{i=1}^{N} y_i \\
\mathrm{D(x)} &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\
\mathrm{D(y)} &= \frac{1}{N}\sum_{i=1}^{N} (y_i - E(y))^2
\end{aligned}
\tag{10}
$$

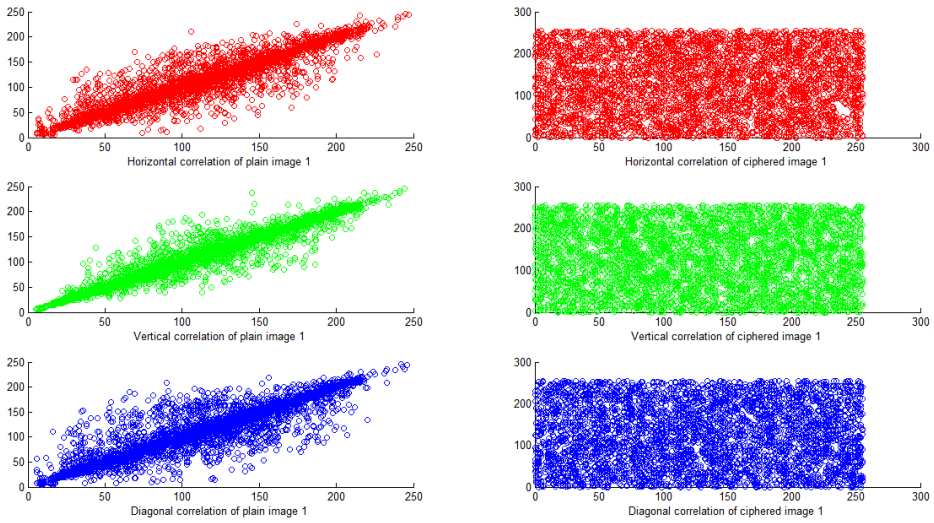

Fig 7. Correlation Coefficient analysis

Table 1. Correlation coefficient results

Image	Correlation Coefficient				
	Direction	Plain image	Proposed	[24]	[25]
Image-1	**Horizontal**	0.9253	0.0130	0.1134	0.0582
	Vertical	0.9591	0.0078	0.1078	0.0249
	Diagonal	0.8905	-0.0043	0.1050	0.0888
Image-2	**Horizontal**	0.9462	-0.0045	0.1044	0.0309
	Vertical	0.9323	-0.0008	0.1067	0.0480
	Diagonal	0.9038	0.0051	0.1015	0.0649
Image-3	**Horizontal**	0.9556	0.0013	0.1008	0.0608
	Vertical	0.9590	-0.0045	0.1064	0.0571
	Diagonal	0.9284	-0.0096	0.1025	0.0266

Continued on next page

Table 1 continued

	Horizontal	0.9691	-0.0019	0.1068	0.0569
Image-4	**Vertical**	0.9600	-0.0150	0.1037	0.0680
	Diagonal	0.9505	-0.0116	0.1141	0.0500
	Horizontal	0.9363	-0.0062	0.1021	0.0402
Image-5	**Vertical**	0.9357	-0.0082	0.1056	0.0314
	Diagonal	0.8766	-0.0017	0.1086	0.0769

4.5 Anti-differential attack analysis

In this type of attack, the value of one pixel in the input image is adjusted and its effect on the cipher image studied. The essential criteria for determining the effectiveness of the cipher against an anti-differential attack are the UACI and the NPCR (Unified Averaged Changed Intensity and Number of Changing Pixel Rate).The optimal UACI and NPCR values are 33.4635% and 99.6094%, respectively [26]. The UACI and NPCR are obtained according to the following Eqns (11) and (12).:

$$\mathrm{UACI} = \frac{1}{W \times H}\left[\sum_{i=1}^{W}\sum_{j=1}^{H}\frac{CI_1(i,j) - CI_2(i,j)}{255}\right] \tag{11}$$

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{W}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\% \tag{12}$$

$$\mathrm{D(i,j)} = \left\{ \begin{array}{l} 0 \text{ if } CI_1(i,j) = CI_2(i,j) \\ 1 \text{ if } CI_1(i,j) \neq CI_2(i,j) \end{array} \right\}$$

Where CI1 and CI2are ciphered-images whose respective original images are differed by single bit. The UACI and NPCR value gained by the presented methods are given inTable 2.

Table 2. UACI and NPCR results

Image	Metrics	Proposed	[24]	[25]
Image-1	**UACI (%)**	33.4586	30.1906	32.8531
	NPCR (%)	99.5368	94.6309	97.5502
Image-2	**UACI (%)**	33.4594	30.9192	32.2646
	NPCR (%)	99.5421	94.1673	98.1152
Image-3	**UACI (%)**	33.4457	31.3094	32.1990
	NPCR (%)	99.5759	94.4571	97.1899
Image-4	**UACI (%)**	33.4314	31. 9266	32.6143
	NPCR (%)	99.5040	94.7026	97.2706
Image-5	**UACI (%)**	33.4655	30.5176	32.0782
	NPCR (%)	99.5246	94.2741	97.0801

4.6 Information entropy

The unpredictability of the cipher image pixels is measured using information entropy. An entropy value of 8 indicates that the pixel values are highly random, and is measured as shown below [27]

$$Entropy = \sum_{i=0}^{255} P(r_i) log_2 P(r_i) \tag{13}$$

The likelihood of the occurrences of r_i is denoted by $P(r_i)$The entropy values of the ciphered test images are shown in Table 3.

4.7 Encryption time

The time taken to encrypt an image is critical to determining the practical usability of a cryptosystem. The running time was estimated on a desktop computer with the Windows7 OS, a 4 GB DDR3 RAM and an IntelCorei3 @ 3.20GHz processor. The encryption time taken by the suggested technique for an image sized 256 × 256 is shown in Table 4.

Table 3. Entropy results

Image	Correlation Coefficient			
	Original	Proposed	(24)	(25)
Image1	7.6724	7.9990	7.8212	7. 8277
Image2	5.5439	7.9991	7.8497	7. 8851
Image3	7.7390	7.9991	7.8960	7. 8537
Image4	7.5734	7.9989	7.8836	7. 8132
Image5	7.6370	7.9991	7.8461	7. 8808

Table 4. Encryption time results

Scheme	Time in seconds (Image Size (256×256))
Proposed	0.1422
(24)	0.9894
(25)	0.7571

4.8 Dataloss attack (Cropping)

When images are transmitted through the public network, they are vulnerable to data loss attack (cropping). A successful cipher must be robust against cropping attacks [28]. To show the strength of presented algorithm against the data loss attacks, the encrypted plain image-5 is cropped by size 32×32, 64×64, and 96×96 blocks and then decrypted. Figure 8 shows the results of data loss attack experiment, proving that the decrypted image contents are recognizable, which means that the proposed scheme resists the attack to a good extent.

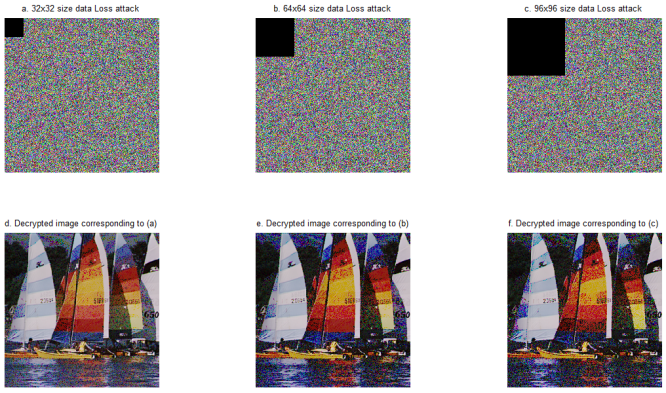

Fig 8. Data loss attack with different degrees (32×32, 64×64, and 96×96)

5 Discussion

Using metrics such asthe UACI, NPCR, information entropy, correlation coefficient, and encryption time, detailed security tests were undertaken. Tables 1, 2, 3 and 4 summarize the findings of a comparison with two (Madhu Sharma scheme and Sundara Krishnan et al.'s scheme) contemporary methodologies. Figure 5 shows how a tiny change in the key resulted in a noise-like image during the decryption process, which demonstrates the key-sensitivity of the proposed method. The proposed technique generated 10^{126} key spaces, which is sufficient to withstand brute force attacks. The proposed encryption method distributes the pixel values in the cipher image far more equally, as observed in the histograms (Figure 6), indicating that the new scheme is not vulnerable to statistical assaults. The suggested method achieved the best UACI and NPCR values (33.50% and 99.60%, respectively), indicative of its efficacy in preventing differential attacks. The dual scrambling procedure significantly reduces the correlation in all three directions (nearly 0) and achieves ideal optimal entropy values (almost 8), revealing no statistical information in the ciphered image. Overall, it is concluded that the presented strategy outperformed the other two techniques in terms of results. The limitation of the presented approach is that it can be applied only on jpeg images. For future work, it is

planned to extend this algorithm to work for other formats such as tiff, bitmap, gif, png and eps.

6 Conclusion

This work has presented a novel secure color image encryption scheme based on 2D hybrid chaotic maps. It introduced a confusion-diffusion-confusion framework for encryption that resulted in optimum entropy values (close to 8). It employed a novel key generation method that generated extremely sensitive keys and a bigger key space (10^{126}). For substitution, the system employed a simple Exclusive-OR operation that significantly reduced running time and hence makes it ideal for real-time Internet applications.

References

1) Wang X, Chen S, Zhang Y. A chaotic image encryption algorithm based on random dynamic mixing. *Optics & Laser Technology*. 2021;138:106837–106837. Available from: https://dx.doi.org/10.1016/j.optlastec.2020.106837.
2) Moafimadani SS, Chen Y, Tang C. A New Algorithm for Medical Color Images Encryption Using Chaotic Systems. *Entropy*. 2019;21(6):577–577. Available from: https://dx.doi.org/10.3390/e21060577.
3) Kamal ST, Hosny KM, Elgindy TM, Darwish MM, Fouda MM. A New Image Encryption Algorithm for Grey and Color Medical Images. *IEEE Access*. 2021;9:37855–37865. Available from: https://dx.doi.org/10.1109/access.2021.3063237.
4) He Y, Zhang YQ, He X, Wang XY. A new image encryption algorithm based on the OF-LSTMS and chaotic sequences. *Scientific Reports*. 2021;11(1). Available from: https://dx.doi.org/10.1038/s41598-021-85377-1.
5) Liang Z, Qin Q, Zhou C, Wang N, Xu Y, Zhou W. Medical image encryption algorithm based on a new five-dimensional three-leaf chaotic system and genetic operation. *PLOS ONE*. 2021;16(11):e0260014–e0260014. Available from: https://dx.doi.org/10.1371/journal.pone.0260014.
6) De S, Bhaumik J, Giri D. A secure image encryption scheme based on three different chaotic maps. *Multimedia Tools and Applications*. 2022;81(4):5485–5514. Available from: https://dx.doi.org/10.1007/s11042-021-11696-0.
7) Moussa KH, Naggary AIE, Mohamed HG. Non-Linear Hopped Chaos Parameters-Based Image Encryption Algorithm Using Histogram Equalization. *Entropy*. 2021;23(5):535–535. Available from: https://dx.doi.org/10.3390/e23050535.
8) Elghandour A, Salah A, Karawia A. A new cryptographic algorithm via a two-dimensional chaotic map. *Ain Shams Engineering Journal*. 2022;13(1):101489–101489. Available from: https://dx.doi.org/10.1016/j.asej.2021.05.004.
9) Khairullah MK, Alkahtani AA, Baharuddin MZB, Al-Jubari AM. Designing 1D Chaotic Maps for Fast Chaotic Image Encryption. *Electronics*. 2021;10(17):2116–2116. Available from: https://dx.doi.org/10.3390/electronics10172116.
10) Mehdi SA. Image encryption algorithm based on a novel 4d chaotic system. *International Journal of Information Security and Privacy*;2021(4):15–15. Available from: https://ideas.repec.org/a/igg/jisp00/v15y2021i4p118-131.html.
11) Gao Z, Liu Z, Wang L. An image encryption algorithm based on the improved sine-tent map. *Discrete Dynamics in Nature and Society*. 2021. Available from: https://doi.org/10.1155/2021/9187619.
12) Kanwal S, Inam S, Cheikhrouhou O, Mahnoor K, Zaguia A, Hamam H. Analytic Study of a Novel Color Image Encryption Method Based on the Chaos System and Color Codes. *Complexity*. 2021;2021:1–19. Available from: https://dx.doi.org/10.1155/2021/5499538.
13) Yang C, Wei X, Wang C. S-Box Design Based on 2D Multiple Collapse Chaotic Map and Their Application in Image Encryption. *Entropy*. 2021;23(10):1312–1312. Available from: https://dx.doi.org/10.3390/e23101312.
14) Pourasad Y, Ranjbarzadeh R, Mardani A. A New Algorithm for Digital Image Encryption Based on Chaos Theory. *Entropy*. 2021;23(3):341–341. Available from: https://dx.doi.org/10.3390/e23030341.
15) Zhang Y. A new unified image encryption algorithm based on a lifting transformation and chaos. *Information Sciences*. 2021;547(3):307–327. Available from: https://doi.org/10.1016/j.ins.2020.07.058.
16) Telem ANK, Fotsin HB, Kengne J. Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems. *Multimedia Tools and Applications*. 2021;80(12):19011–19041. Available from: https://dx.doi.org/10.1007/s11042-021-10549-0.
17) NagaSrinivasu P, Rao CS. A Multilevel Image Encryption based on Duffing map and Modified DNA Hybridization for Transfer over an Unsecured Channel. *International Journal of Computer Applications*. 2015;120(4):1–4. Available from: https://dx.doi.org/10.5120/21212-3915.
18) Sheela SJ, Suresh KV, Tandur D. Image encryption based on modified Henon map using hybrid chaotic shift transform. *Multimedia Tools and Applications*. 2018;77(19):25223–25251. Available from: https://dx.doi.org/10.1007/s11042-018-5782-2.
19) Prathi R, Renuga D. A chaos based image encryption using tinkerbell map functions. *International Conference on Electronics, Communication and Aerospace Technology*. 2018. Available from: https://doi.org/10.1109/ICECA.2018.8474891.
20) SundaraKrishnan K, Raja SP, Jaison B. A Symmetric Key Multiple Color Image Cipher Based on Cellular Automata, Chaos Theory and Image Mixing. *Information Technology and Control*. 2021;50(1):55–75. Available from: https://dx.doi.org/10.5755/j01.itc.50.1.28012.
21) Tutueva AV, Karimov AI, Moysis L, Volos C, Butusov DN. Construction of one-way hash functions with increased key space using adaptive chaotic maps. *Chaos, Solitons & Fractals*. 2020;141:110344–110344. Available from: https://dx.doi.org/10.1016/j.chaos.2020.110344.
22) Banik A, Shamsi Z, Laiphrakpam DS. An encryption scheme for securing multiple medical images. *Journal of Information Security and Applications*. 2019;49:102398–102398. Available from: https://dx.doi.org/10.1016/j.jisa.2019.102398.
23) Ghadirli HM, Nodehi A, Enayatifar R. An overview of encryption algorithms in color images. *Signal Processing*. 2019;164:163–185. Available from: https://dx.doi.org/10.1016/j.sigpro.2019.06.010.
24) Sharma M. Image encryption based on a new 2D logistic adjusted logistic map. *Multimedia Tools and Applications*. 2020;79(1-2):355–374. Available from: https://dx.doi.org/10.1007/s11042-019-08079-x.
25) Krishnan KS, Jaison B, Raja SP. An efficient novel color image encryption algorithm based on 3D Lü chaotic dynamical system and SHA-512. *International Journal of Wavelets, Multiresolution and Information Processing*. 2020;18(05):2050042–2050042. Available from: https://dx.doi.org/10.1142/s0219691320500423.
26) Yu J, Guo S, Song X, Xie Y, Wang E. Image Parallel Encryption Technology Based on Sequence Generator and Chaotic Measurement Matrix. *Entropy*. 2020;22(1):76–76. Available from: https://dx.doi.org/10.3390/e22010076.

27) Ramasamy P, Ranganathan V, Kadry S, Damaševičius R, Blažauskas T. An Image Encryption Scheme Based on Block Scrambling, Modified Zigzag Transformation and Key Generation Using Enhanced Logistic—Tent Map. *Entropy*. 2019;21(7):656–656. Available from: https://dx.doi.org/10.3390/e21070656.
28) Mariel L, Y H, Tiedeu A, Kom G. A robust and fast image encryption scheme based on a mixing technique. *Security and Communication Networks*. 2021. Available from: https://doi.org/10.1155/2021/6615708.