International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 14, No.1 (Aug-2023)

http://dx.doi.org/10.12785/ijcds/140148

A Security Algorithm for Images Based on 2D Logistic Map Using Bit-level and Pixel-level Image Encryption Approaches

Manzoor Ahmad Lone*[1] and Shaima Qureshi[2]

[1,2]*Department of CSE, NIT, Srinagar (JK), India*

Received 12 Jun. 2022, Revised 23 May 2023, Accepted 22 Jun. 2023, Published 01 Aug. 2023

Abstract: This paper presents a new chaos-based image encryption method using a hybrid effect of bit-level and pixel-level image encryption principles to form an encrypted digital image. In the proposed encryption scheme, the 2D logistic map generates two pseudo-random chaotic streams that are employed in an efficacious way to use the bit-level and pixel-level ideologies to encrypt the plain image. The two chaotic sequences produced by the 2D logistic map are used to create two LSB-based bit-matrices to form a bit-level perspective that helps in the scrambling of the image. Furthermore, the same two chaotic streams of the 2D logistic map are used in a cross manner at the pixel level to diffuse the image and finally form a strong cipher image. The experimental numerical results, standard reference value tests, and comparative analysis with the existing encryption methods support and validate the reliability and robustness of the proposed encryption approach.

Keywords: Chaos, bit-level, encryption, 2D logistic map, pixel-level, security.

1. INTRODUCTION

Parallel to the escalating advancement in the computer and internet world, information security is a serious threatening issue. To protect image information loss, various image encryption schemes have been suggested by applying different techniques, such as wavelet transform [1], [2], [3], [4], [5], chaos theory [6], [7], [8], [9], [10], [11], [12], [13], [14], compressed sensing [15], [16], [17], [18], and DNA coding [19], [20], [21], [22], [23]. The encryption systems based on chaos theory possess several strong characteristic features, such as high initial condition sensitivity, unpredictability, ergodicity, and high randomness [24]. The chaotic streams generated by the chaotic maps are perplexing and very difficult to explore and predict, thus increasing the security of a cryptosystem. To deal with information security issues, chaos theory has become an attractive field for a wide class of researchers to design and develop cryptosystems based on chaotic maps. Compared to image encryption schemes using chaos theory at the pixel-level, less research is carried out on the bit-level encryption schemes [25]. The advantage of the bit-level encryption approach is that it helps in the confusion and diffusion operations while encrypting images. Some of the different bit-level techniques suggested to encrypt the images in the literature are [26], [27], [25], [28], [29], [30], [31]. In [30], authors proposed an image encryption approach in which for every pixel element the encoding of 4-higher order bits take place, and the 4-lower order bits are kept unchanged. In [32], a bit-level image encryption scheme is suggested by the authors using the Arnold map and the logistic map. The Arnold map is applied to perform bit-level permutation and the chaotic logistic map is used for the diffusion operation. In [25], authors suggested a bit-level image encoding method by employing the improved 1-dimensional logistic map and the Sine map. In [31], authors proposed a bit-level digital image encrypting scheme based on chaos theory using the piece wise linear chaotic map. In [33], authors proposed a bit-level encryption method for images using the FCLN (Fully-connected-like network) and change in the pixels of edges. FCLN copies a fully connected neural network, which changes both positions and values of the pixel elements. In [34], authors suggested the encryption procedure for digital images employing bit-level shuffling, Arnold transformation, and the dynamic overlap diffusion using the 5D-hyperchaotic system. The Arnold transformation is applied to shuffle and modify the position and magnitude of the pixel in an image to achieve better results. The authors in [35] use bit-level confusion and multiplication diffusion exploiting plaintext and chaotic system. Flip shuffling, binary tree, and circle indexing shuffling with the multiplication diffusion process help in generating the enigmatic encrypted image. In [36], a novel procedure for the encryption of digital images is suggested using the 5D-hyperchaotic map, pixel-level with bit-level image shuffling and DNA coding. The encryption approach also uses DNA complementary rules and DNA-XOR operations to improve the security the system. Further, other different methods and strategies are combined to

E-mail address: mahmadlone@gmail.com, shaima@nitsri.net*

develop image encryption algorithms that encrypt digital images based on confusion and diffusion operations and safely transfer the encrypted data from one place to another over public open networks. The authors in [37] employ the hyper-chaotic Lorenz system and a hash function to develop a secure encryption method for images. The authors in [38] combined the 6-dimensional hyper-chaotic map, and the Fibonacci Q-matrix to produce a secure cipher image. To encrypt a digital image, the 6D hyper-chaotic map is applied to create confusion in the elements of the image and the Fibonacci Q-matrix is applied to generate diffusion in the image. The authors in [39] proposed a novel encryption procedure for images by fusing the new 2-dimensional Hénon sine map and DNA encoding approach. The pixel elements are permuted using the 2D-Hénon sine map and diffused by applying the DNA encoding rules. The authors in [40] achieved simultaneous permutation and diffusion by applying chaotic theory and DNA encoding approaches for the safe and secure communication of gray-scale images over public networks. The authors in [41] introduced a gray-scale image encryption method by utilizing an enhanced 2D-LSMM (2D-Logistic sine chaotic map) and dynamic DNA encoding approach. The sine map input is governed by the logistic map, and the coding and operational standards of DNA streams are decided by the 2D LSMM.

The above literature study inspired the authors to propose a chaos-based image encryption procedure by employing a joint effect of bit-level and pixel-level encryption strategies to generate a cipher image. Due to the following points, the 2D logistic map and bit-level image encryption are used in the proposed scheme:

i). In the chaos map family, the chaotic 2D logistic map exploits the intrinsic characteristic features of chaos theory.

ii). The proposed system utilizes the 2-dimensional logistic map in the image encryption process, because it is neither too simple like the 1D logistic map nor complicated like 3D or more higher-dimensional chaotic maps. The 1D logistic map possesses low key space, periodic and blank window problems, and is also vulnerable to attacks [42], [43]. For example, by choosing a plain text attack, the authors in [44] crack a 1D chaotic map. On the contrary, the higher dimensional chaotic maps are complicated and their implementation is difficult in the programming domain. Thus, we choose the 2D logistic map in the proposed system.

iii). As little image encryption research is established in the bit-level direction as compared to pixel-level image encryption, this motivated the authors to propose an image encryption system using bit-level image encryption in coordination with pixel-level encryption to impose a hybridized effect of both approaches on the security of digital images.

In the proposed image encryption scheme, the 2D logistic map generates two chaotic sequences that are employed in an effective way to use bit-level and pixel-level perspectives to encrypt a digital image. The two chaotic streams created by the 2D logistic map are utilized to frame two LSB-based binary matrices $X_{bin_{[M\times N]}}$ and $Y_{bin_{[M\times N]}}$ that form the bit-level encryption basis to shuffle the elements of the image. Simultaneously, the same two chaotic streams created by the 2D logistic map are applied in a cross manner at the pixel-level to diffuse the pixels in the image. Thus, a hybrid effect of both the modes is imposed in the encryption of a digital image in the proposed encryption system to form a reliable cipher image. Also, the proposed encryption method uses the input image to formulate the initial key values of the 2D logistic map that boosts the security and key space of the proposed scheme. The method shows a high sensitivity to any approximate alteration (Δ) in the key parameters of the system. A little alteration in initial conditions (x_0, y_0) or in controlling parameters $(\alpha_1, \alpha_2, \beta_1, \beta_2)$ brings an avalanche in the cipher images. Thus, it can resist different cryptanalytic attacks efficiently. Further, all the key parameters contained by the 2D logistic map generate an immense key cardinality to counter against exhaustive attacks.

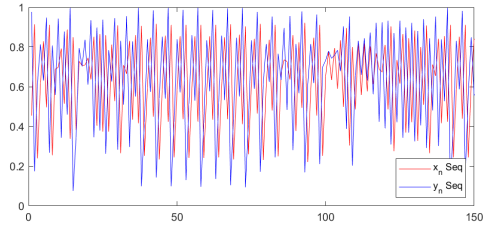

Figure 1. x_n and y_n chaotic plots of 2D logistic map

The remainder of the article is assembled as: Section 2, elaborates the mathematical background of the 2D logistic map. Section 3, describes the proposed encryption procedure. The numerical result findings are delineated in Section 4 and the conclusion is drawn in Section 5.

2. 2D LOGISTIC MAP

The chaotic maps show extremely high sensitive nature by making a small change in their initial value conditions. A small approximate change in initial value parameters leads to an unexpected outcome. Thus the system becomes very difficult to judge and explore. The following formula represents the mathematical relation of the 2D logistic map [45]:

$$\begin{cases} x_{n+1} &= \alpha_1 x_n(1-x_n) + \beta_1 y_n, \\ y_{n+1} &= \alpha_2 y_n(1-y_n) + \beta_2 x_n^2 + x_n y_n \end{cases} \quad (1)$$

where $\alpha_1, \alpha_2, \beta_1,$ and β_2 act as key parameters in the system. The scheme depicts chaotic nature and produces two chaotic streams x_n and $y_n \in (0, 1]$, when $2.75 < \alpha_1 \leq 3.4$, $2.75 < \alpha_2 \leq 3.45$, $0.15 < \beta_1 \leq 0.21$ and $0.13 < \beta_2 \leq 0.15$. Figure 1 represents the plots of x_n and y_n sequences developed by the 2D logistic map.

3. PROPOSED ENCRYPTION METHOD

The stepwise description of the suggested encryption method is given below, and the layout in Figure 2 reflects

the flow chart of the suggested method.

Algorithm 1: The proposed procedure:

Input: Original image ($[im^o]_{M\times N}$), keys.
Output: Cipher image (im^E).
1) The two initial values of 2D chaotic map are created on the similar pattern of [46], by using the the input image im^o as shown follows:

$$x_0 \leftarrow \frac{1}{M\times N\times 255}\left(\sum im^o\right), \quad (2)$$

$$y_0 \leftarrow \frac{x_0}{2}. \quad (3)$$

2) Use Eq.(1) to generate x_n and y_n chaotic streams, respectively.
3) Scale the x_n and y_n sequences in the range of $[0-255]$, and then transform them into $M\times N$ matrices, say $[X]_{M\times N}$ and $[Y]_{M\times N}$, respectively.
4) Convert each element of $[X]_{M\times N}$ matrix into binary string and store the LSB of each binary string in a binary matrix say $[X_{bin}]_{M\times N}$ at the respective positions of corresponding pixels.
5) Similarly, like **step-4**, convert $[Y]_{M\times N}$ matrix into $[Y_{bin}]_{M\times N}$.
6) Use the first LSB-based bit-matrix $[X_{bin}]_{M\times N}$ to apply the first level of shuffling in the image with the help of the following pseudo-code:

$inx \leftarrow 1;$
for $indi \leftarrow 1 : M$
for $ind\,j \leftarrow 1 : N$
if $\left([X_{bin}]_{(indi,ind\,j)} == 1\right)$
$Temp_{(inx)} \leftarrow [im^o]_{(indi,ind\,j)};$
$inx = inx + 1;$
end if
end for
end for
for $indi \leftarrow 1 : M$
for $ind\,j \leftarrow 1 : N$
if $\left([X_{bin}]_{(indi,ind\,j)} == 0\right)$
$Temp_{(inx)} \leftarrow [im^o]_{(indi,ind\,j)};$
$inx = inx + 1;$
end if
end for
end for

Finally, reshape $Temp$ vector into a matrix of size $M\times N$, say $[im^{o'}]_{M\times N}$.
7) Perform the XOR operation between $[im^{o'}]_{M\times N}$ and $[Y]_{M\times N}$ as shown below:

$$[im^{o''}]_{M\times N} \leftarrow \left([im^{o'}]_{M\times N} \oplus [Y]_{M\times N}\right). \quad (4)$$

This step induces the first level of diffusion in the image on the basis of pixel-level criteria.
8) Use the second LSB-based bit-matrix $[Y_{bin}]_{M\times N}$ to achieve the another level of shuffling in $[im^{o''}]_{M\times N}$. Thus, bit-level criteria is again applied by using the same pseudo-code as shown in **Step-6**, but instead of $[X_{bin}]$ and $[im^o]$ use

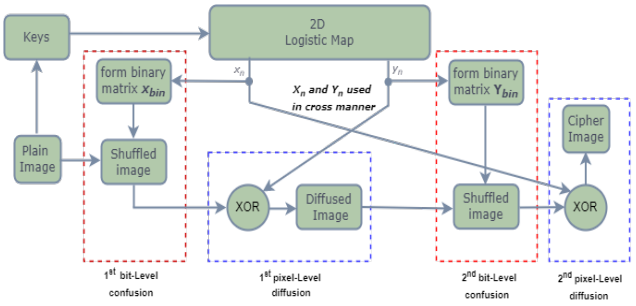

Figure 2. Flow chart of proposed encryption approach

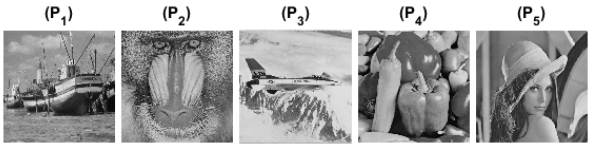

Figure 3. Plain images: P_1(Boat), P_2(Baboon), P_3(Jet), P_4(Pepper), P_5(Lena).

$[Y_{bin}]$ and $[im^{o''}]$, respectively. Let the final output of this step be represented as $[im^{o'''}]_{M\times N}$.
9) Perform the XOR operation between $[im^{o'''}]_{M\times N}$ and $[X]_{M\times N}$, as shown below:

$$[im^E]_{M\times N} \leftarrow \left([im^{o'''}]_{M\times N} \oplus [X]_{M\times N}\right). \quad (5)$$

This step induces the second level of diffusion in the image on the basis of pixel-level criteria and produces the final cipher image im^E.

The image encryption phase follows the reverse order of all the operations involved in the encryption process to reconstruct the plain image.

4. Simulation Results

The experimental numerical outcomes are obtained using the Matlab software platform on a machine with Windows 10 operating system. Standard gray-scale images of 256×256, as shown in Figure 3 are used to find the simulation results.

A. Key Space

Encryption systems with high key space can counter the brute force attacks effectively and efficiently. A reliable key space should be $\geq$ 128-bit key length [47] to resist exhaustive attacks . With a computer precision of 10^{-15}, the total key space of the suggested scheme becomes 2^{299}. Besides, in the proposed system, the 2D logistic map initial key values also rely upon the gray image of the 2^{8MN} key size. Thus, we can infer that the suggested encryption scheme has a substantial cardinal number for key space.

B. Key Sensitivity

In an efficient encryption method, a little alteration in secret keys should produce an avalanche in the ciphers,

TABLE I. Key sensitivity results of pepper image (changing one parameter at one instance): NPCR and UACI results between correct key encrypted image and incorrect key encrypted image.

	$x_0 + 10^{-15}$	y_0	α_1	α_2	β_1	β_2
	x_0	$y_0 + 10^{-15}$	α_1	α_2	β_1	β_2
	x_0	y_0	$\alpha_1 + 10^{-15}$	α_2	β_1	β_2
	x_0	y_0	α_1	$\alpha_2 + 10^{-15}$	β_1	β_2
	x_0	y_0	α_1	α_2	$\beta_1 + 10^{-15}$	β_2
	x_0	y_0	α_1	α_2	β_1	$\beta_2 + 10^{-15}$
NPCR	99.5956	99.5682	99.6506	99.6216	99.6353	99.6292
UACI	33.5338	33.4688	33.4022	33.5471	33.4986	33.4679

and enigmatic images should be displayed in the decryption phase. In the simulation, only one key is slightly changed among the key set, and it is observed that false images, as shown in Figure 4 are generated in the decryption process. In addition, for pepper image, the simulated quantitative results of key sensitivity for NPCR and UACI indicators determined with the help of Eq. (8), and Eq. (9), respectively, are listed in Table I. The results displayed in Figure 4 and Table I signify that the suggested system is extremely sensitive sensitive to an approximate variation (Δ) in the secret key parameters.

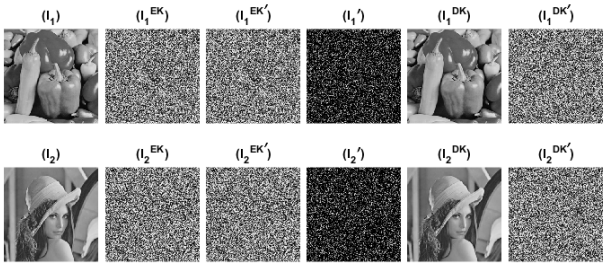

Figure 4. Key sensitivity: (I_1, I_2) plain images, ($I_1{}^{EK}$, $I_2{}^{EK}$) encrypted images by correct key, ($I_1{}^{EK'}$, $I_2{}^{EK'}$) encrypted images by incorrect key, ($I_1{}'$, $I_2{}'$) difference between correct key and incorrect key encrypted images, ($I_1{}^{DK}$, $I_2{}^{DK}$) decrypted images of ($I_1{}^{EK}$, $I_2{}^{EK}$) by correct key, respectively, ($I_1{}^{DK'}$, $I_2{}^{DK'}$) decrypted images of ($I_1{}^{EK}$, $I_2{}^{EK}$) by incorrect key, respectively.

C. Information Entropy

This indicator determines the randomness present in an image. Eq. (6) depicts the mathematical relation of information entropy:

$$E(I) = \sum_{a=0}^{T} p(I_a) log_2 \frac{1}{p(I_a)}, \quad (6)$$

where $T = 2^n - 1$, and $p(I_a)$ is the probability of I_a. The theoretical reference value of $E(I)$ in a 256 gray-scale image is 8 [47]. The proposed encryption system's numerical outcomes of entropy are very nearby to reference value 8, as revealed in Table II, thus justifying the randomness in the cipher image.

D. Correlation Analysis

The correlation amid the adjoining pixels in a cipher image should be mitigated extremely by a good encryption approach [24]. The correlation coefficient $\varphi_{(a,a')}$ is given as follows:

$$\varphi_{(a,a')} = \frac{S \times \varrho_{(a,a')}}{\sqrt{\sum_{s=1}^{S} (a_s - E_a)^2} \sqrt{\sum_{s=1}^{S} (a'_s - E_{a'})^2}}, \quad (7)$$

where S =size of image, $\varrho_{(a,a')}$=$E((a - E_a)(a' - E_{a'}))$, $E_a = \frac{1}{S} \sum_{s=1}^{S} a_s$, and (a, a') is the adjacent pixel pair. The numerical findings exhibited in Table III and the plots depicted in Figure 5 justify that the suggested system can resist statistically-based attacks.

TABLE II. Information entropy results

Image	Boat	Baboon	Jet	Pepper	Lena	Avg.
$E(I)$	7.9974	7.9976	7.9972	7.9974	7.9975	7.9974

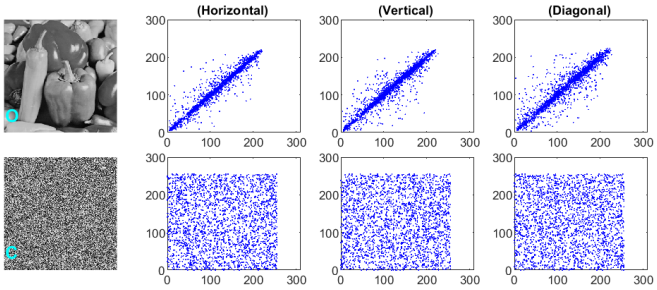

Figure 5. Correlation plots of Input image(O) and Cipher image(C)

TABLE III. Correlation coefficient results

Corr.	Boat	Baboon	Jet	Pepper	Lena	Avg.
HC	0.0065	0.0010	-0.0006	-0.0008	0.0006	0.0013
VC	0.0090	-0.0010	-0.0046	0.0079	-0.0017	0.0019
DC	-0.0028	0.0008	0.0012	0.0016	0.0040	0.0010

E. Differential Attack

An effective image encryption scheme should show high resistance to this type of attack. The two indicators, namely NPCR and UACI, determine the ability of an encryption system to withstand against differential attacks [7]. If I' and I'' are the two ciphered images with a minute variation in their plain image, then NPCR and UACI indicators are evaluated by the following relations, respectively:

$$NPCR = \frac{\sum_{a_x,a_y} Q_{(a_x,a_y)}}{M \times N} \times 100\%, \quad (8)$$

$$Q_{(a_x,a_y)} = \begin{cases} 1 & \text{if } I'_{(a_x,a_y)} \neq I''_{(a_x,a_y)}, \\ 0 & \text{otherwise} \end{cases}$$

$$UACI = \frac{1}{(M \times N)} \left[\sum_{a_x,a_y} \frac{|I'_{(a_x,a_y)} - I''_{(a_x,a_y)}|}{2^8 - 1} \right] \times 100\%. \quad (9)$$

The numerical results depicted in Table IV justify that the proposed system can efficiently counter differential attacks.

TABLE IV. Results of NPCR and UACI indicators

		$\mathcal{N}^*_{0.05}$	$\mathcal{N}^*_{0.01}$	$\mathcal{N}^*_{0.001}$		$V^{*-}_{0.05}, V^{*+}_{0.05}$	$V^{*-}_{0.01}, V^{*+}_{0.01}$	$V^{*-}_{0.001}, V^{*+}_{0.001}$ [48]
Image	NPCR	99.5693	99.5527	99.5341	UACI	33.2824, 33.6447	33.2255, 33.7016	33.1594, 33.7677
Boat	99.6048	√	√	√	33.5484	√	√	√
Baboon	99.6475	√	√	√	33.5239	√	√	√
Jet	99.6338	√	√	√	33.6443	√	√	√
Pepper	99.6048	√	√	√	33.5139	√	√	√
Lena	99.5792	√	√	√	33.5168	√	√	√
Average=	99.6140	√	√	√	33.5495	√	√	√

TABLE V. Chi-square test results

		$L^{(0.1)}$	$L^{(0.05)}$	$L^{(0.01)}$ [48]
Name	χ^2 value	284.3359	293.2478	310.4574
Boat	237.8828	√	√	√
Baboon	221.9922	√	√	√
Jet	254.4689	√	√	√
Pepper	236.6250	√	√	√
Lena	229.1016	√	√	√
Avg.	236.0141	√	√	√

TABLE VI. PSNR results of noise and crop attacks

	Varying density of salt and pepper noise					
Image	0.002	0.005	0.05	0.1	0.15	0.3
Boat	35.1573	31.6333	21.1400	18.1359	16.2977	13.1957
Baboon	36.4025	33.0076	22.6461	19.6919	17.9866	14.9905
Jet	35.2942	32.0068	21.7036	18.9549	17.1032	14.1125
Pepper	36.2745	32.0341	22.4918	19.4267	17.5184	14.5885
Lena	35.8149	31.8934	22.4115	19.2533	17.5263	14.4854

	Occlusion loss				
	5%	10%	20%	30%	50%
Boat	20.9188	17.9152	15.0169	13.2056	11.0186
Baboon	22.6173	19.6135	16.7697	14.9729	12.7342
Jet	21.9921	18.9090	15.9517	14.1629	11.9327
Pepper	22.3044	19.3289	16.3344	14.5634	12.3295
Lena	22.1537	19.1913	16.3435	14.5271	12.3082

F. Histogram Analysis

The histogram plot of an original image has spikes at many areas, indicating more pixels in that interval. In a cipher image, this information should be absent, and a cipher image should yield a flattened surface histogram. In the proposed system, compared to original image histograms, the cipher histogram plots are uniformly distributed, as shown in Figure 6. Thus, it confirms that the proposed can resist histogram attacks. Moreover, the quantitative investigation of the flatness of a histogram is measured by the Chi-square test [48] and is given by Eq. (10):

$$\chi^2_{im^E} = \sum_{a=0}^{255}[(\mathrm{Ob}_a - \mathrm{Ex}_a)^2 / \mathrm{Ex}_a], \qquad (10)$$

where a represents intensity value, Ob_a and Ex_a represent the observed and expected frequency of a, respectively. Mathematically Ex_a is given by $(M \mathrm{x} N)/2^8$. The numerical outcomes of the χ^2 test of the encrypted image successfully pass the theoretical values of all the three significance levels as shown in Table V, thus confirming the uniform distribution of histogram in a cipher image.

G. Noise and Cropping Attack

In transmitting information, noise attacks and occlusion attacks can degrade the encrypted data and lead to data loss. Thereby, an encryption system needs to have adequate ability to counter such types of attacks. The results in Figure 7 and Figure 8 show the potential of the suggested image encryption system to withstand noise and crop attacks, respectively. The outcomes in Figure 7 and Figure 8 imply that the deciphered images are visually observable up to noise density $d = 0.3$ and crop window =50%. Furthermore, the quantitative results of the PSNR parameter listed in Table VI between the original image and the image deciphered from the attacked cipher determine the strength of the suggested algorithm to counter such types of attacks. Eq. (11) defines the mathematical relation of PSNR:

$$PSNR = 10 \times log_{10}\left[\frac{(2^8-1)^2}{MSE(I, I')}\right], \qquad (11)$$

$$\text{where} \quad MSE = \frac{1}{M \times N}\sum_{a_x=0}^{N-1}\sum_{a_y=0}^{M-1}[I_{(a_x,a_y)} - I'_{(a_x,a_y)}]^2.$$

5. Comparison

The system configuration indicated in section-4 is employed to examine the performance speed of the suggested image encryption approach. For 256×256 images, the average running time of the proposed approach during the encryption and decryption process is $0.5787762s$. Furthermore, the comparison of the various parameters such as NPCR and UACI, information entropy, key space, and correlation coefficients of the proposed encryption system with some existing schemes shown in Table VII, Table VIII, Table IX, and Table X, respectively, are acceptable and are in parallel with the present existing encryption methods. Therefore, it endorses the robustness, performance, and effectiveness of the suggested encryption scheme.

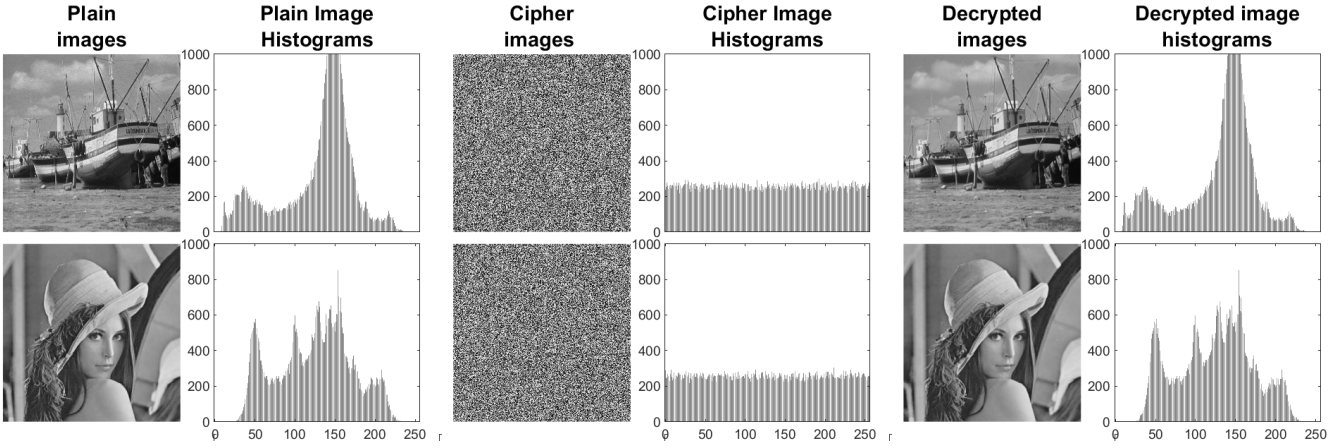

Figure 6. Histogram plots of plain and encrypted images

TABLE VII. Comparison analysis of differential attack indicators with existing schemes

	NPCR						UACI					
Image	[40]	[38]	[39]	[33]	[34]	**Proposed**	[40]	[38]	[39]	[33]	[34]	**Proposed**
Boat	99.2500	99.6078	99.6170	99.6153	-	99.6048	33.3928	33.4188	33.6609	33.4669	-	33.5484
Baboon	99.1051	99.5941	99.5925	99.6063	99.5948	99.6475	33.2517	33.4610	33.3822	33.4619	33.4382	33.5239
Jet	99.4176	99.6017	99.6231	-	-	99.6338	33.5254	33.5053	33.6358	-	-	33.6443
Pepper	98.4975	99.6033	99.6078	99.6139	99.6086	99.6048	32.9483	33.4274	33.4953	33.4685	33.4728	33.5139
Lena	99.5193	99.6246	99.6200	-	-	99.5792	33.5851	33.4226	33.4169	-	-	33.5168
Avg.	99.1579	99.6063	99.6121	-	-	99.6140	33.3407	33.4470	33.5182	-	-	33.5495

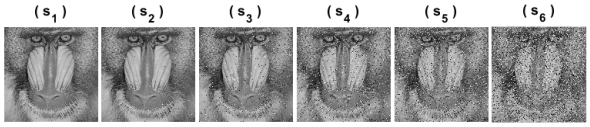

Figure 7. Noise analysis: d (density of salt and pepper noise) in $(s_1) - (s_6)$ is $0.002, 0.005, 0.05, 0.10, 0.15,$ and, 0.30, respectively.

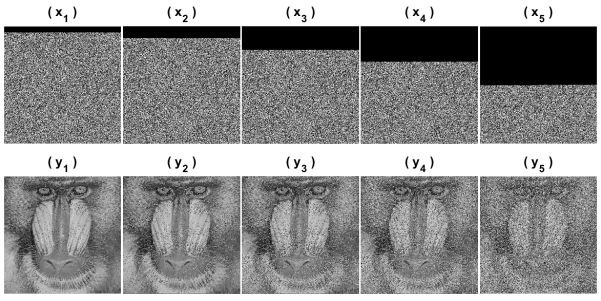

Figure 8. Crop analysis: In $(x_1) - (x_5)$ Crop window = $5\%, 10\%, 20\%, 30\%$ and 50%, respectively. $(y_1) - (y_5)$ decrypted images of $(x_1) - (x_5)$, respectively.

TABLE VIII. Comparison analysis of entropy with existing schemes

Image	[40]	[38]	[39]	[33]	[34]	**Proposed**
Boat	7.9941	7.9976	7.9971	7.9976	-	7.9974
Baboon	7.9938	7.9975	7.9971	7.9977	7.9976	7.9976
Jet	7.9974	7.9972	7.9970	-	-	7.9972
Pepper	7.9958	7.9970	7.9974	7.9974	7.9973	7.9974
Lena	7.9975	7.9972	7.9976	-	7.9972	7.9975
Avg.	7.9957	7.9973	7.9972	-	-	7.9974

TABLE IX. Key space comparative results

Algorithm	Key space
Proposed	2^{299}
[47]	2^{232}
[40]	2^{240}
[7]	2^{186}
[48]	2^{219}
[37]	2^{428}
[33]	2^{248}
[12]	2^{298}
[39]	10^{112}
[34]	10^{240}

TABLE X. Correlation coefficient comparison

Algo.	Corr.	Boat	Baboon	Jet	Pepper	Lena	Avg.
[40]	HC	0.0073	0.0059	0.0062	0.0037	0.0023	0.0051
	VC	0.0109	0.0041	0.0074	0.0258	0.0019	0.0100
	DC	0.0016	0.0028	0.0009	0.0079	0.0011	0.0029
[38]	HC	0.0138	0.0065	0.0229	0.0211	0.0069	0.0142
	VC	0.0093	0.0337	0.0103	0.0129	0.0479	0.0228
	DC	3.4412×10^{-6}	0.0244	0.0100	0.0013	0.0075	0.0086
[39]	HC	0.0001	0.0026	0.0028	0.0016	0.0056	0.0025
	VC	0.0031	0.0009	0.0041	0.0031	0.0037	0.0035
	DC	0.0015	0.0052	0.0010	0.0034	0.0032	0.0029
[33]	HC	-0.0040	0.0061	-	-0.0032	-	-
	VC	-0.0190	-0.0006	-	-0.0028	-	-
	DC	0.0008	-0.0005	-	-0.0006	-	-
[34]	HC	-	-0.0061	-	0.0045	-0.0094	-
	VC	-	0.0032	-	0.0063	-0.0038	-
	DC	-	0.0105	-	-0.0044	0.0044	-
Prop.	HC	0.0065	0.0010	-0.0006	-0.0008	0.0006	0.0013
	VC	0.0090	-0.0010	-0.0046	0.0079	-0.0017	0.0019
	DC	-0.0028	0.0008	0.0012	0.0016	0.0040	0.0010

6. Conclusions and Future Work

A chaos theory based new image security procedure exploiting a hybrid impact of bit-level and pixel-level image encryption ideas is proposed in this article. The 2D logistic map produces two pseudo-random chaotic streams that are utilized in an efficacious and ingenious way to operate bit-level and pixel-level image encryption approaches to confuse and diffuse image pixels, and frame a reliable cipher image. To enhance the security and keyspace of the proposed system, the initial key values of the 2D logistic map are related with the input image. In such relations, a small change in initial conditions produces false ciphers, and consequently, we are unable to recover the true image in the decryption phase. Further, the numerical results, satisfactory results of theoretical reference value tests, high sensitivity towards change in initial value parameters, and the comparative analysis with the existing encryption schemes confirm and justify the reliability of the proposed method. In future research, the suggested algorithm in this paper can be utilized in medical images, multimedia communication, commerce, and other areas to encrypt digital images.

References

[1] A. B. Joshi, D. Kumar, D. Mishra, and V. Guleria, "Colour-image encryption based on 2d discrete wavelet transform and 3d logistic chaotic map," *Journal of Modern Optics*, vol. 67, no. 10, pp. 933–949, 2020.

[2] M. A. Khan, J. Ahmad, Q. Javaid, and N. A. Saqib, "An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps and substitution box," *Journal of Modern Optics*, vol. 64, no. 5, pp. 531–540, 2017.

[3] C. Li and X. Yang, "An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos," *Optik*, vol. 260, p. 169042, 2022.

[4] P. Rakheja, R. Vig, and P. Singh, "Asymmetric hybrid encryption scheme based on modified equal modulus decomposition in hybrid multi-resolution wavelet domain," *Journal of Modern Optics*, vol. 66, no. 7, pp. 799–811, 2019.

[5] H. Zhong and G. Li, "Multi-image encryption algorithm based on wavelet transform and 3d shuffling scrambling," *Multimedia Tools and Applications*, pp. 1–20, 2022.

[6] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and dna encoding," *IEEE access*, vol. 7, pp. 36 667–36 681, 2019.

[7] M. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dynamics*, vol. 99, no. 4, pp. 3041–3064, 2020.

[8] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[9] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Computers & Mathematics with Applications*, vol. 59, no. 10, pp. 3320–3327, 2010.

[10] Y. Luo, J. Yu, W. Lai, and L. Liu, "A novel chaotic image encryption algorithm based on improved baker map and logistic map," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22 023–22 043, 2019.

[11] A. Y. Niyat, M. H. Moattar, and M. N. Torshiz, "Color image encryption based on hybrid hyper-chaotic system and cellular automata," *Optics and Lasers in Engineering*, vol. 90, pp. 225–237, 2017.

[12] J. Wu, X. Cao, X. Liu, L. Ma, and J. Xiong, "Image encryption using the random frdct and the chaos-based game of life," *Journal of Modern Optics*, vol. 66, no. 7, pp. 764–775, 2019.

[13] J. Wu, Z. Liu, J. Wang, L. Hu, and S. Liu, "A compact image encryption system based on arnold transformation," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2647–2661, 2021.

[14] Y. Zhou, Z. Hua, C.-M. Pun, and C. P. Chen, "Cascade chaotic system with applications," *IEEE transactions on cybernetics*, vol. 45, no. 9, pp. 2001–2012, 2014.

[15] J. Wang, Q.-H. Wang, and Y. Hu, "Image encryption using compressive sensing and detour cylindrical diffraction," *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1–14, 2018.

[16] X. Wang and Y. Su, "Image encryption based on compressed sensing and dna encoding," *Signal Processing: Image Communication*, vol. 95, p. 116246, 2021.

[17] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Optics and Lasers in Engineering*, vol. 121, pp. 203–214, 2019.

[18] G. Ye, M. Liu, and M. Wu, "Double image encryption algorithm based on compressive sensing and elliptic curve," *Alexandria Engineering Journal*, vol. 61, no. 9, pp. 6785–6795, 2022.

[19] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using dna cryptography," *Information Security Journal: A Global Perspective*, vol. 29, no. 2, pp. 91–101, 2020.

[20] V. Folifack Signing, T. Fozin Fonzin, M. Kountchou, J. Kengne, and

Z. Njitacke, "Chaotic jerk system with hump structure for text and image encryption using dna coding," *Circuits, Systems, and Signal Processing*, vol. 40, no. 9, pp. 4370–4406, 2021.

[21] S. Patel, K. Bharath, and R. Kumar, "Symmetric keys image encryption and decryption using 3d chaotic maps with dna encoding technique," *Multimedia Tools and Applications*, vol. 79, no. 43, pp. 31 739–31 757, 2020.

[22] T.-Y. Wu, X. Fan, K.-H. Wang, C.-F. Lai, N. Xiong, and J. M.-T. Wu, "A dna computation-based image encryption scheme for cloud cctv systems," *IEEE Access*, vol. 7, pp. 181 434–181 443, 2019.

[23] G. Xiao, M. Lu, L. Qin, and X. Lai, "New field of cryptography: Dna cryptography," *Chinese Science Bulletin*, vol. 51, no. 12, pp. 1413–1420, 2006.

[24] M. A. Lone and S. Qureshi, "Rgb image encryption based on symmetric keys using arnold transform, 3d chaotic map and affine hill cipher," *Optik*, p. 168880, 2022.

[25] C. Pak, K. An, P. Jang, J. Kim, and S. Kim, "A novel bit-level color image encryption using improved 1d chaotic map," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 12 027–12 042, 2019.

[26] A.-V. Diaconu, "Circular inter–intra pixels bit-level permutation and chaos-based image encryption," *Information Sciences*, vol. 355, pp. 314–327, 2016.

[27] G. Nandeesh, P. Vijaya, and M. Sathyanarayana, "An image encryption using bit level permutation and dependent diffusion," *Int J Comput Sci Mob Comput*, vol. 2, no. 5, pp. 145–154, 2013.

[28] L. Teng and X. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive," *Optics Communications*, vol. 285, no. 20, pp. 4048–4054, 2012.

[29] X. Wang and H.-l. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Optics Communications*, vol. 342, pp. 51–60, 2015.

[30] T. Xiang, K.-w. Wong, and X. Liao, "Selective image encryption using a spatiotemporal chaotic system," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 17, no. 2, p. 023115, 2007.

[31] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.

[32] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Information Sciences*, vol. 181, no. 6, pp. 1171–1186, 2011.

[33] Y. Sheng, J. Li, X. Di, Z. Man, and Z. Liu, "Bit-level image encryption algorithm based on fully-connected-like network and random modification of edge pixels," *IET Image Processing*, 2022.

[34] J. Wang, J. Li, X. Di, J. Zhou, and Z. Man, "Image encryption algorithm based on bit-level permutation and dynamic overlap diffusion," *Ieee Access*, vol. 8, pp. 160 004–160 024, 2020.

[35] C.-L. Li, Y. Zhou, H.-M. Li, W. Feng, and J.-R. Du, "Image encryption scheme with bit-level scrambling and multiplication diffusion," *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18 479–18 501, 2021.

[36] S. Sun, "A novel hyperchaotic image encryption scheme based on dna encoding, pixel-level scrambling and bit-level scrambling," *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1–14, 2018.

[37] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1319–1333, 2018.

[38] K. M. Hosny, S. T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix," *Electronics*, vol. 10, no. 9, p. 1066, 2021.

[39] J. Wu, X. Liao, and B. Yang, "Image encryption using 2d hénon-sine map and dna approach," *Signal Processing*, vol. 153, pp. 11–23, 2018.

[40] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Optics and Lasers in Engineering*, vol. 90, pp. 146–154, 2017.

[41] J. Zheng and L. Liu, "Novel image encryption by combining dynamic dna sequence encryption and the improved 2d logistic sine map," *IET Image Processing*, vol. 14, no. 11, pp. 2310–2320, 2020.

[42] I. S. Sam, P. Devaraj, and R. Bhuvaneswaran, "An intertwining chaotic maps based image encryption scheme," *Nonlinear Dynamics*, vol. 69, no. 4, pp. 1995–2007, 2012.

[43] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61 334–61 345, 2021.

[44] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1d chaotic map," *Signal processing*, vol. 144, pp. 444–452, 2018.

[45] Q. Zhang, L. Liu, and X. Wei, "Improved algorithm for image encryption based on dna encoding and multi-chaotic maps," *AEU-International Journal of Electronics and Communications*, vol. 68, no. 3, pp. 186–192, 2014.

[46] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37 855–37 865, 2021.

[47] P. Ayubi, S. Setayeshi, and A. M. Rahmani, "Deterministic chaos game: a new fractal based pseudo-random number generator and its cryptographic application," *Journal of Information Security and Applications*, vol. 52, p. 102472, 2020.

[48] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12 452–12 466, 2020.

Manzoor Ahmad Lone
Manzoor Ahmad Lone is enrolled as sponsored research scholar in Computer Science and Engineering department, NIT, Srinagar (J&K), India. His research interests are Image processing, Image Encryption and Chaos theory.

Dr. Shaima Qureshi
Dr. Shaima Qureshi is working as an Associate Professor in the Computer Science and Engineering department, NIT, Srinagar (J&K), India. Her areas of research include Mobile Networks, Algorithms, Machine learning and Image Encryption.