IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 7 August 2023, accepted 24 September 2023, date of publication 27 September 2023, date of current version 4 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3320031

RESEARCH ARTICLE

Digital Images Security Technique Using Hénon and Piecewise Linear Chaotic Maps

MOHAMMAD MAZYAD HAZZAZI[1], NADEEM IQBAL[2], AND ATIF IKRAM[2,3]

[1]Department of Mathematics, College of Science, King Khalid University, Abha 61421, Saudi Arabia
[2]Department of Computer Science and IT, The University of Lahore, Lahore 54000, Pakistan
[3]Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, Kuala Terengganu 21300, Malaysia

Corresponding author: Nadeem Iqbal (nadeem.iqbal537@gmail.com)

This work was supported by the Deanship of Scientific Research, King Khalid University, through the Research Group's Program, under Grant R. G. P. 2/5/44.

ABSTRACT The security of images has become a hot research area due to the widespread usage of the digital images all over the world. Literature review on chaotic image cryptography, on the other hand, indicates that many constructs have been employed for the realization of confusion operation while developing the image ciphers. To enhance the computational time, this study proposes a novel image cipher based on two chaotic maps and rectangle as a scrambler. As the given grayscale image is input, it is scrambled through dynamically generated rectangles. As a modus operandi, these rectangles are created in the given image with various dimensions and different location. The pixels lying on the boundary of the rectangle are rotated clockwise and anticlockwise with an arbitrary amount. These operations have been repeated a number of times to get the scrambling effects. The scrambled image has been further subjected to an XOR operation for embedding the diffusion effects in it. Two chaotic maps of Hénon and piecewise linear chaotic map have been used for the generation of random numbers. These numbers help in deciding the size, location, clockwise/anticlockwise movement of the pixels and the amount with which these pixels have to be rotated. The performance analysis and the machine simulation validate that the suggested cipher is sufficient enough to thwart the varied cryptanalytic attacks. In particular, we gained the computational speed of 0.5156 seconds and the information entropy of 7.9975. Besides, we posit that it has the ample prospects for its real world application.

INDEX TERMS Chaos, cryptanalysis, cybersecurity, decryption, encryption, geometric figure.

I. INTRODUCTION

The software and hardware products have changed the entire complexion of the world. No single niche of the world is there which has not received some kind of effect due to the revolution of computing. In all of this, digital images assume a special significance. One can regularly see the numerous kinds of images on daily basis. They are being generated, analyzed, saved and transmitted from one corner of the world to another corner. Normally, we have no concern about the safety of these images. But occasionally, we encounter such situations where an extreme caution is required while dealing with these images. For instance, the image of some spy, the image of the blueprint of a new missile etc. So, we need to adopt some serious measures to tackle this immediate menace.

When we investigate the kinds of measures, the scientists and researchers have taken, we come to know that encryption has been used as a solution for the problem under consideration. In particular, the ciphers like IDEA, RSA, AES, DES etc., has been developed to safeguard the precious data. But unluckily, these ciphers can encrypt the text data only [1]. Whereas, the nature of problem we are concerned with, is the image data. Images have diametrically opposite properties as compared their textual counterpart. For instance, they have powerful interpixel connection which must be dismantled with a robust encryption algorithm. Besides, there are an enormous amount of pixels in a very little image or photo.

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

Moreover, high redundancy exists among pixels of these digital images. So, different set of paraphernalia is required to cope with the kind of the problem we are confronting with. Fortunately, the theory of chaos and its ramifications in guise of varied chaotic maps and systems have done a great job in spawning random numbers with an excellent chaoticity. The random numbers given by these maps carried out diffusion and confusion operations over given image pixel values. These chaotic maps exist in one-, two- and higher-dimensions. The maps with maximum two dimensions are categorized as low-dimension maps and the ones with greater than two dimensions are dubbed as high-dimension chaotic maps. The low dimensional chaotic maps are easy to install but their produced random numbers are not much random at all [2]. In contrast to that, the high-dimensional chaotic maps are difficult to build but the numbers they produce are much random which are very fit for the enterprise of cryptography.

Image cryptographers have produced tens of hundreds of image cryptosystems using the constructs of DNA [3], [4], automatons [5], mathematical figures [6], [7], non-disclosure agreements [8], puzzles [9], chess pieces [10], magic squares [11], [12], optics [13], [14] etc. For example the work [15] developed 2D Hénon-Sine map (2D-HSM) and applied this map in spawning the chaotic data. Moreover, DNA codes were employed to boost the efficiency of diffusion and permutation. To evaluate this scheme, differential attack analysis, statistical attack analysis and computational complexity were carried out. Besides, an image encryption scheme comprising of three stages have been given in [16]. Rule 30 cellular automata has been employed in the first stage for the generation of the first encryption key. In the second state, an S-box was utilized whose design consists of the constructs like modular inverses, transformation and permutation. In the third and last stage, Lorenz system's solution was done for getting second encryption key. Apart from that, the work [17] created a generalized fusion fractal structure through the fusion of two 1D fractals acting as the seed functions out of the greater range of fractal functions. Moreover, the authors of the study [17] designed PLFF through the combination of Lambda and Phoenix fractals. Then, image cipher using PLFF fractal function was developed which exploited the pseudo-random number (PRN) sequences in the capacity of a secret key. For evaluating the performance of this cipher, varied security parameters like UACI, NPCR, histogram variance, correlation, information entropy etc., were employed.

Although much research has been carried out on the niche of chaotic image cryptography, still many works have been broken by the cryptanalysts by spotting varied loopholes in their design principles. For example, the cryptanalytic work [18] spotted various lacunas in the study [19]. The work [19] developed a permutation-rewriting-diffusion (PRD) for purpose of encryption thus boosting the relationship between diffusion and permutation. Apart from that, key stream was related pixels square sum of given plain image. Security risks spotted by [18] were two in number. Firstly, diffusion and rewriting operations were carried out through the notion of modular addition which is tantamount to the one-step diffusion operation. Secondly, diffusion matrix and rewriting parameters were independent of given plain image. Separate attack method was employed to break the security. First of all, equivalent diffusion process was broken through modulo subtraction operation on decrypted image and ciphertext of black image (an image consisting of all zero intensity values). Further, the underlying rule of permutation was decoded through the construction of numerous images with same square sum of pixels. Lastly, some suggestions were given to improve the security effects. An other work [20] using Brownian motion and discrete dynamical chaotic maps was cryptanalyzed by [21]. The particular attacks which were carried out were chosen-plaintext attack, chosen-ciphertext attack and known-plaintext attack. In particular, one chosen cipher image, one chosen plain image and just one pair of ciphertext and plaintext were taken to launch this attack. Apart from that, the work [21] developed an enhanced image cipher using the Basin chaotic map, Brownian motion and Gingerbread man map.

After getting inspiration from the above discussion, this work aims to craft an other grayscale image cipher using the piecewise linear chaotic map and Hénon map. Mathemtical figure rectangle has been used to embed confusion effects in the suggested cipher. In particualr, these rectangles will be formed iteratively in the given grayscale image. The random numbers given by the chaotic maps would decide the top left and bottom right corners to these rectangles. Besides, one random number would decide the direction in which the pixels of the selected rectangle would be moved. Apart from that, one more stream would decide the amount with which these movement has to be carried out.

The remaining research article has been set like this. Section II describes the preliminaries of this study. In these preliminaries, Hénon and Piecewise linear chaotic maps have been described. The proposed image cipher has been described in detail in the Section III. Section IV takes six test images and applies the suggested framework upon them to demonstrate the do-ability of the work. In Section V, detailed performance and security analyses have been carried out by using varied validation metrics. Lastly, in the Section VII, conclusion has been drawn with the essential remarks for the future research directions.

II. PRELIMINARIES

This section has been written to give an overview of fundamental building blocks upon which this work depends. Theory of chaos is a major breakthrough in the intellectual history of mankind [22]. According to this theory, the faintest tempering in the primitive and initial states of the systems causes to render diametrically different outputs. Following this revolutionary idea, mathematicians and the scientists alike, have crafted dozens of chaotic systems/maps to spawn streams of chaotic numbers [23], [24], [25]. These

systems and maps are intrinsically furnished with marvelous characteristics of aperiodicity, pseudo-randomness, unpredictability, large key space, mixing, ergodicity and plaintext sensitivity [9]. The perusal of literature reveals the fact that these maps are available in the form of two dimensions, one dimension, and more than two dimensions. This work employs two maps whose explanation is given below.

A. HÉNON MAP

The scientist Hénon (in 1976) developed this map. It is a 2D map meaning that it would render two arrays of chaotic data. The mathematical equations of this map are [26], [27]

$$\begin{aligned} p_{n+1} &= 1 - ap^2(n) + q(n), \\ q_{n+1} &= bp(n) \end{aligned} \tag{1}$$

In the above equations, $n = 0, 1, 2, \ldots$. Moreover, a and b correspond to the system parameters of this map. When conditions are met $a \in (0.54, 2)$ and $b \in (0, 1)$, this map shows its chaotic behavior.

B. PIECEWISE LINEAR CHAOTIC MAP

This is a 1D map. In mathematical parlance, it is defined as follows [28], [29]

$$s_i = F(s_{i-1}, \eta) = \begin{cases} \dfrac{s_{i-1}}{\eta}, & \text{if } 0 < s_{i-1} < \eta \\ \dfrac{s_{i-1} - \eta}{2 - \eta}, & \text{if } \eta \le s_{i-1} < 0.5 \\ F(1 - s_{i-1}, \eta), & \text{if } 0.5 \le s_{i-1} < 1 \end{cases} \tag{2}$$

For $\eta \in (0, 0.5)$ and $i = 1, 2, 3, \ldots$ we get the required behavior of chaoticity. Additionally, it renders even distribution and has nice properties of ergodicity.

III. PROPOSED IMAGE ENCRYPTION SCHEME

Researchers have employed varied constructs to carry out the operation of permutation and scrambling over the plaintext images. The current research endeavor has attempted to use the rectangle as a scrambler for the pixels of the given input grayscale image I. The suggested image cipher comprises of some stages. Firstly, the input plain image I is given to the system. To embed the plaintext sensitivity in the very core of the proposed algorithm, the average value *avg* of all the pixels have been calculated. This average value, in turn, tempers one of the initial values of the Hénon map, i.e., $p(0)$. Secondly, both the chaotic maps, i.e., Hénon map and the PWLCM have been iterated for $2mn + n_0$ times to get the streams $\{p(t)\}_{t=1}^{2mn+n_0}$, $\{q(t)\}_{t=1}^{2mn+n_0}$, $\{s(t)\}_{t=1}^{2mn+n_0}$ of random numbers. Thirdly, these streams have been translated into the required range of numbers so that the proposed logic of the image cipher can be implemented. The new streams of random numbers have been named as $\{u(t)\}_{t=1}^{mn}$, $\{v(t)\}_{t=1}^{mn}$ and $\{mask(t)\}_{t=1}^{mn}$. Fourthly, a structure *Point* has been defined which would characterize the *abscissa* and *ordinate* of the randomly selected pixel from the given image. Besides, an array *array* of *Point* has been defined which would model the top left corner and bottom right corner of the dynamically generated rectangles in the given input image. Fifthly, the confusion and scrambling operations have been done upon the given input image I with the help of *array*. Sixthly, the diffusion effects have been injected using the mask image *mask* to get the final cipher image I_1.

A. GETTING INITIAL VALUES OF CHAOTIC SYSTEM

Step 1: Provide the algorithm the grayscale plain image I (with size $m \times n$). For introducing the plaintext sensitivity, find the average value *avg* of all the pixels' intensity values. Now, the following equation has been used to update the initial key $p(0)$ of the chaotic system (1) being employed.

$$p(0) = p(0) + \frac{avg}{2^{80}} \tag{3}$$

Step 2: As the systems (1) and (2) are looped $(2mn + n_0)$ times, $\{p(t)\}_{t=1}^{2mn+n_0}$, $\{q(t)\}_{t=1}^{2mn+n_0}$, $\{r(t)\}_{t=1}^{2mn+n_0}$ have been obtained. Moreover, value of $n_0 \ge 500$. These n_0 are normally considered as the immature random data. Hence, to avoid any ill effect, these values have been bypassed.

Step 3: In the Step 2, the chaotic data is not in line with the peculiar logic this study has envisioned. Hence, the streams p, q and s are gone through the set of equations (4). So, we got revised streams of arbitrary data named as u, v and *mask*.

$$\begin{cases} u(i) = floor(mod(abs(p(i)) - floor(abs(p(i))) \times \\ 10^{14}, m - 3)) + 1, \\ v(i) = floor(mod(abs(q(i)) - floor(abs(q(i))) \times \\ 10^{14}, 3n - 3)) + 1, \\ mask(i) = floor(mod(abs(s(i)) - \\ floor(abs(s(i))) \times 10^{14}, 256)) \end{cases} \tag{4}$$

where $1 \le i \le 2mn$.

Step 4: Here we will define a structure called *Point* like below:

Definition 1: struct Point
{
int abscissa
int ordinate
}

Let *array* be the linear array of points *Point* with the size of $[1 \times 2mn]$. Fill this array with the points u and v like this.

$$\begin{cases} array(i).abscissa = u(i), \\ array(i).ordinate = v(i) \end{cases} \tag{5}$$

where $1 \le i \le 2mn$.

B. IMAGE ENCRYPTION PROCEDURE

Input the gray scale image I of size $m \times n$. Call the Algorithm 1 with the parameters I, *array* and *mask* to realize the purpose of scrambling over the given image and the diffusion operations.

Algorithm 1 *ImageEncryptionBasedOnRectangleBasedSramber (IERBS)*

Input: *I, array, mask*
Output: I_1

1: $[m \times n] \leftarrow size(I)$
2: **for** $i \leftarrow 1$ to $2mn$ by 2 **do**
3: **if** $array(i).abscissa < array(i+1).abscissa$ *and* $array(i).ordinate < array(i+1).ordinate$ **then**
4: $TA \leftarrow [\,]$
5: $TA(1 : array(i+1).ordinate - array(i).ordinate + 1) \leftarrow I(array(i).abscissa, array(i).ordinate : array(i+1).ordinate)$
6: $TA \leftarrow horzcat(TA, I(array(i).abscissa + 1 : array(i+1).abscissa - 1, array(i+1).ordinate)^T)$
7: $TA \leftarrow horzcat(TA, (I(array(i+1).abscissa, array(i).ordinate : array(i+1).ordinate)))$
8: $TA \leftarrow horzcat(TA, (I(array(i).abscissa + 1 : array(i+1).abscissa - 1, array(i).ordinate)^T))$
9: $direct \leftarrow mod(array(i).abscissa, 2)$
10: $amount \leftarrow mod(array(i).ordinate, 256) + 1$
11: **if** $direct = 0$ **then**
12: $slice \leftarrow circshift(TA, amount)$
13: **else**
14: $slice \leftarrow circshift(TA, -amount)$
15: **end if**
16: **end if**
17: $I \leftarrow RectangleBasedScrambler(I, slice, array)$
18: **end for**
19: $I_1 \leftarrow \oplus(I, mask)$

Algorithm 2 *RectangleBasedScrambler*

Input: *I, slice, array*
Output: I'

1: $I(array(i).abscissa, array(i).ordinate : array(i+1).ordinate) \leftarrow slice(1 : array(i+1).ordinate - array(i).ordinate + 1)$
2: $I(array(i).abscissa + 1 : array(i+1).abscissa - 1, array(i+1).ordinate) \leftarrow slice(array(i+1).ordinate - array(i).ordinate + 2 : array(i+1).ordinate - array(i).ordinate + 2 + array(i+1).abscissa - array(i).abscissa - 2)^T$
3: $I(array(i+1).abscissa, array(i).ordinate : array(i+1).ordinate) \leftarrow slice(array(i+1).ordinate - array(i).ordinate + 2 + array(i+1).abscissa - array(i).abscissa - 1 : array(i+1).ordinate - array(i).ordinate + 2 + array(i+1).abscissa - array.abscissa(i) - 1 + array(i+1).ordinate - array(i).ordinate)$
4: $I(array(i).abscissa + 1 : array(i+1).abscissa - 1, array(i).ordinate) \leftarrow slice(array(i+1).ordinate - array(i).ordinate + 2 + array(i+1).abscissa - array(i).abscissa - 1 + array(i+1).ordinate - array(i).ordinate + 1 : array(i+1).ordinate - array(i).ordinate + 2 + array(i+1).abscissa - array(i).abscissa - 1 + array(i+1).ordinate - array(i).ordinate + 1 + array(i+1).abscissa - array(i).abscissa - 2)^T$
5: $I' \leftarrow I$

Here the Algorithm 1 will be explained in a step by step fashion.

Step 1: Line 1 of the algorithm calculates the size $[m \times n]$ of the input image I.

Step 2: The *for* loop spanning the lines (2 - 18) performs the confusion operation over the pixels of the input image. The *for* loop iterates for $2mn$ times and increases its index i by 2 (Line 2) in each iteration.

Step 3: The *if* condition at line 3 checks whether the point $(array(i).abscissa, array(i).ordinate)$ is located at the left and upper position relative to the point $(array(i+1).abscissa, array(i+1).ordinate)$? If this is the case then process of scrambling has been carried out.

Step 4: Line 4 initializes an empty array TA. A slice of pixel values starting from $array(i).ordinate$ to $array(i+1).ordinate$ columns from the $array(i).abscissa^{th}$ row has been copied to the temporary array TA. In the same way, other three sides of the rectangle has been copied to the temporary array TA using the *horzcat* function.

Step 5: Line 9 introduces a new variable *direct* (for direction of sliding of pixels) which takes the value either 1 or 0. It is to be noted that variable $array.abscissa(i)$ has been used for this purpose.

Step 6: Lines (11 - 15) slide the pixels of the temporary array TA in a circular fashion clockwise or anti-clockwise (depending upon the truth or falsity of the condition at line 11)

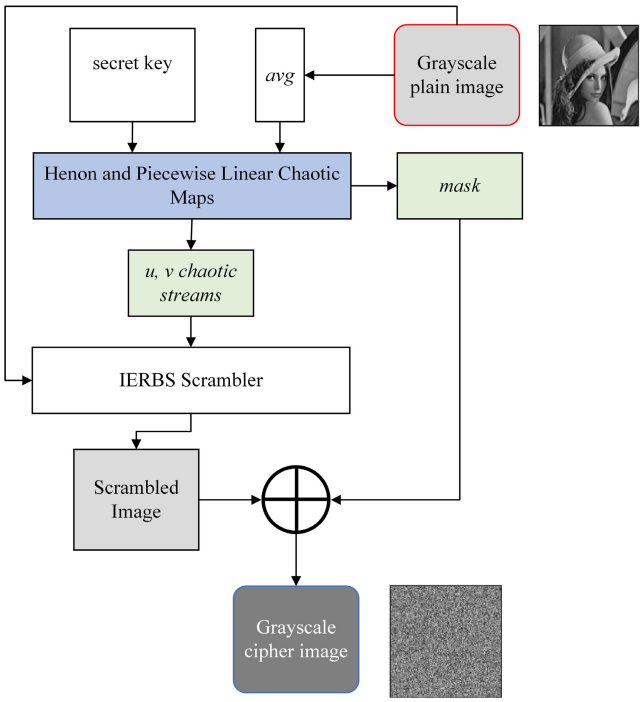


FIGURE 1. Proposed image cipher based on IERBS Scrambler.

with the amount of *amount*. The resultant pixels have been copied into the array *slice*.

Step 7: Line 17 calls the Algorithm 2 (*RectangleBasedScrambler*) with the parameters I, *slice* and *array*.

Step 8: Lines (1 - 4) of Algorithm 2 replace the original pixels of the input image I with the scrambled pixels contained in the array *slice*. This algorithm lastly assigns the scrambled image I to the new image I' which, in turn, is sent to the caller Algorithm 1.

Step 9: Lastly, in the line 19 of Algorithm 1, diffusion effects have been carried out by the XOR function between the scrambled image I and the mask image *mask* to get the final cipher image I_1. It is to be noted that symbol $\oplus$ corresponds to the XOR operation.

Example 1: In order to better appreciate the suggested scrambling operation based on the construct of rectangle, we give here an example. Figure 2a shows the randomly selected rectangle of the given plain image. Further, for this particular iteration of the algorithm, the values of the variables *direct* and *amount* happen to be 0 and 3 respectively. So, the scrambling operation has slided the pixels of the selected rectangle clockwise with the amount of 3 (Figure 2b).

The decryption algorithm is very trivial in its character and orientation. Its reason is that just the inversion of the steps of the encryption algorithm would yield the decryption algorithm. Moreover, it is to be noted that the private key cryptography has been adopted in this study.

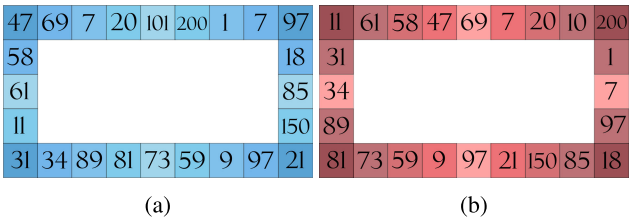


FIGURE 2. Illustration of scrambling. (a) Randomly selected rectangle of pixels from the given plain image (b) Rectangle after the rotation of pixels with the parameters of *direct* = 0 and *amount* = 3.

IV. SIMULATION OF THE SUGGESTED ALGORITHM

This section is meant for the simulation of the suggested algorithm in the previous section. For this end, six test images of Lena, Moon, House, Girl, White and Black have been taken. It is to be noted that the images White and Black would demonstrate the defiance of the cipher against the Chosen plaintext, known plaintext and ciphertext only attacks. We can see the test images in the Figure 3. As the encryption algorithm got applied over them one by one, the results have been drawn in the Figure 4. Besides, the images after the decryption have been shown in the Figure 5. One can see that the cipher images give no clue to the information contained by the original test images. Additionally, the decrypted images are 'verbatim' to the original test images. These both phenomena suggest the prowess and work-ability of the suggested encryption and decryption algorithms.

V. PERFORMANCE AND SECURITY ANALYSES

In this section, various evaluation metrics would be applied to objectively assess the quality of the image cipher developed in this research work. Moreover, this work has chosen these state of the art works [30], [31], [32], [33] to carry out the comparison of the different validation metrics between these published works and the suggested work.

A. COMPUTATIONAL TIME ANALYSIS

One of the chief contributions of this study is that the novel image cipher consumes very less time as compared to the many published works in the literature. This project has been completed using the tool of MATLAB R2016a and the Windows operating system. Besides, Intel(R) Core(TM) i5-4210U CPU @ 1.70 GHz 2.40 GHz is the processor's details. Moreover, 8 GB memory is installed in the said computer system. According to the Table 1, Lena image takes 0.5196 seconds for its encryption. Moreover, the average time taken for all the images is 0.5156 seconds. Apart from that, the comparison with other published works shows that the suggested work beats these works [30], [31] as far as the computational time is concerned.

B. FLOATING FREQUENCY

The prime job of any image cipher is to diffuse and confuse the pixels of the given images in such a way that they fashion uniformly in all the columns and rows. The notion of floating

FIGURE 3. Normal test images:(a) Lena; (b) Moon; (c) House; (d) Girl; (e) White; (f) Black.

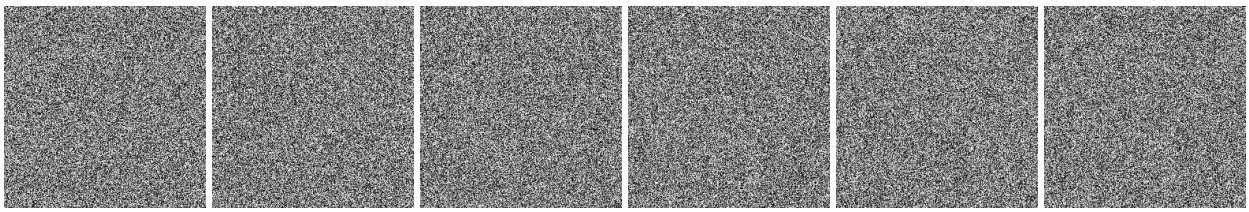


FIGURE 4. Images after encryption: (a) Lena; (b) Moon; (e) House; (f) Girl; (c) White; (d) Black.

FIGURE 5. Images after decryption: (a) Lena; (b) Moon; (c) House; (d) Girl; (c) White; (d) Black.

TABLE 1. Encryption speed of suggested algorithm and comparison with others.

Algorithm	Image	Speed (sec)
Proposed	Lena	0.5196
	Moon	0.5039
	House	0.5390
	Girl	0.5234
	White	0.4890
	Girl	0.5189
	Average	**0.5156**
Ref. [30]	Baboon	2.0
Ref. [31]	-	0.54
Ref. [32]	Lena	0.3493
Ref. [33]	Lena	0.16

frequency investigates it in a systematic way [34]. In case, the pixels of the image are not diffused and confused in a proper way, this parameter will expose them so that the image cryptographer may finetune his/her algoirthm. In the security parameter of floating frequency, windows comprising of 256 elements extracted from the cipher and plain images are scrutinized. In this scrutiny, it is judged that upto what extent the pixels' intensities are differing with each other. For this purpose, notions of column floating frequency (*CFF*) and row floating frequency (*RFF*) are used. This parameter is determined through the following three-pronged mechanism.

1) Windows (256 pixels) are extracted from the given image. These windows form the columns and the rows.
2) Now column floating frequency and row floating frequency are determined from each window.
3) The graphs of *RFF* and *CFF* are drawn after their mean values are determined.

Figure 6 shows the results in a graphical form about *CFF* and *RFF* for the cipher and plain Lena image. For the Figure 6a, floating frequency graph of Lena plain image has been shown against columns 1 to 256. One can note that relatively more pixels are there with same pixels' intensity values. So, we posit that results of *CFF* are low for the windows which have been selected. Whereas, Figure 6b is showing lesser number of pixels having the same values of intensity. By putting same idea in different parlance, more number of pixels exist with distinct intensity value in all the columns of the given image. This fact indicates that suggested image cryptosystem enjoys better effects of security. Additionally, it explains the reason that there are higher values of *CFF*. Moreover, 162 and 126 are values

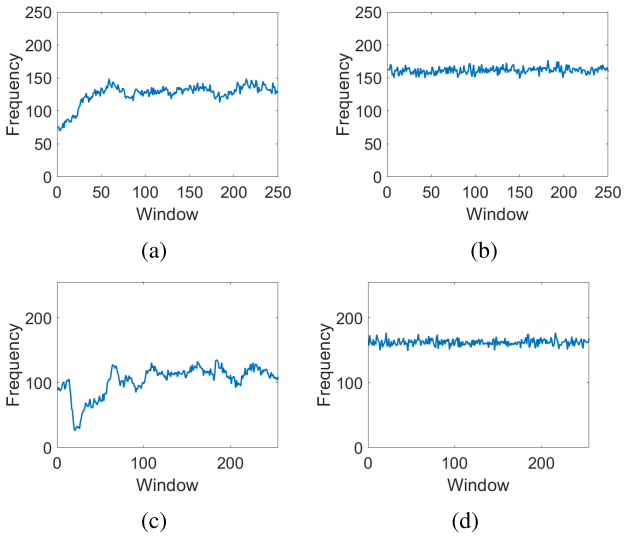


FIGURE 6. Column, row floating frequency for different images and their mean value: (a) Column floating frequency of plaintext image, 126; (b) Column floating frequency of ciphertext image, 162; (c) Row floating frequency of plaintext image, 107; (d) Row floating frequency of ciphertext image, 161.

of means for plain and cipher images of Lena respectively. If we convert these numerics in the percentage, they become $\frac{128}{256} \times 100\% = 49\%$ and 63% respectively. No doubt, better percentage of *CFF* in encrypted image is symptomatic of plausible effects of security. Similarly, Figures 6c and 6d demonstrate *RFF* for plain image Lena and its cipher form with average values of 107 and 161 in a respective way. 42% and 63% are calculated as their values in form of percentage. Of course, higher percentage of *RFF* in cipher images is better for image ciphers.

C. ENTROPY ANALYSIS

Entropy or information entropy (IE) is a frequently used metric to judge the effectiveness and defiance of the ciphers from the hackers' community. In this analysis, the extent with which the pixels of the given image are scattered is measured. The maximum value of entropy for a 256 grayscale image is calculated as 8. If the entropy value of cipher image is very nearly close to this ideal value 8, it indicates that the cipher has sufficiently confused and diffused the pixels of the given image. It, in turn, signals towards the high security effects. The mathematical formula for the notion of entropy was discovered in 1949 which is as below.

$$IE(s) = \sum_{i=0}^{2^n-1} p(s_i) log \frac{1}{p(s_i)} \tag{6}$$

here $IE(s)$ refers to the information entropy for the signal s. Table 2 shows the results of entropy for the selected images. Suggested algorithm is better than [30] vis-à-vis information entropy. The images chosen by this study have the dimensions of 256 × 256. For images with the larger size, this metric naturally provides better results and, of course, for the images with lesser sizes, we will get the poorer results.

TABLE 2. Entropy results.

Study	Images	Plain	Cipher
Ours	Lena	7.5835	7.9975
	Moon	6.7093	7.9973
	House	6.5148	7.9973
	Girl	6.8449	7.9974
	White	0.0	7.9974
	Black	0.0	7.9973
	Average	**4.6088**	**7.9974**
Ref. [30]	Baboon		7.9966
Ref. [31]	-		7.9999
Ref. [32]	Lena		7.99918
Ref. [33]	Lena		7.9992

TABLE 3. LSE results for the cryptic images.

Image	Value of entropy	Result
Lena	7.902613	Passed
Baboon	7.902976	Passed
Brain	7.902589	Passed
Tree	7.902279	Passed
White	7.902387	Passed
Black	7.902890	Passed

D. LOCAL SHANNON ENTROPY (LSE)

To curb numerous attacks potentially launched by the cryptanalytic community, image ciphers are expected to spread the pixels of the given image in a random fashion. The notions of LSE performs this job. In it, it is measured that up to what extent the picture pixels have been randomized [35]. For the given image I and the q non-overlapping blocks D_1, D_2,..., D_q with the S_C pixels selected in a random fashion, the idea of *LSE* is normally translated in the following way.

$$\overline{H_{q,S_C}(I)} = \sum_{j=1}^{q} \frac{H(D_j)}{q} \tag{7}$$

In this equation, $H(D_j)$ corresponds to Shannon entropy for image block D_j and its mathematical formula is

$$H(D_j) = \sum_{r=1}^{M} p(r) log \frac{1}{p(r)} \tag{8}$$

here, M refers to the total pixels; $p(r)$ renders probability of r^{th} value. According to the advices given in [36], the parameters (q, S_C) are provided with the pairs of values (30, 1936). Moreover, for the value of α as 0.05, the best value of *LSE* is found as 7.902469317 and a cipher image is declared for passing test if the condition given in the interval $7.901901305 \leq LSE \leq 7.903037329$ is fulfilled. Table 3 gives the results of *LSE* for the cryptic images. One can note that all the given test images passed *LSE*'s test. This phenomenon validates the fact that the novel image cipher is furnished with good properties of chaoticity for the cryptic images.

TABLE 4. Differential attack results for the security parameters of NPCR and UACI.

Image	NPCR(%)	UACI(%)
Lena	99.6378	33.5921
Moon	99.6167	33.4908
House	99.6306	33.6086
Girl	99.5937	33.6930
White	99.6209	33.6623
Black	99.6098	33.6089
Average	**99.6183**	**33.6093**

E. DIFFERENTIAL ATTACK ANAYSIS

This attack is very technical in its approach and orientation. In this attack strategy, hackers manage two copies (samples) of the plain images. One sample is simple whereas in other sample, a very minute change in the pixel intensity value is introduced. Now both of these samples are encrypted by invoking encryption algorithm. Pixel intensity values of these two samples form a hidden relationship whose further investigation leads hackers to the discovery of the secret key. To cope with this attack, researchers have invented security parameters of *NPCI* and *UACI*. Their full names expand as number of pixels change rate and unified average changing intensity. Apart from that, corresponding mathematical equations of these two notions go like this.

$$NPCR = \frac{\sum_{f,g} R(f,g)}{m \times n} \times 100\%$$

The pair (m, n) of values refers to the size of the image we are dealing with. Furhter, $R(f, g)$ is mathematically expressed as

$$R(f,g) = \begin{cases} 1, & \text{if } Cipher(f,g) \neq Cipher'(f,g), \\ 0, & \text{if } Cipher(f,g) = Cipher'(f,g) \end{cases}$$

$$UACI = \sum_{f,g} \frac{|Cipher(f,g) - Cipher'(f,g)|}{255 \times m \times n} \times 100\%$$

In the above equation, the variables *Cipher* and *Cipher*$'$ denote cipher images with no change in pixel values and with a change in pixel values respectively. Moreover, the Table 4 shows our experimental results of these metrics against chosen test images. Values 99.6378% & 33.5921% and 99.6183% & 33.6093% have been calculated for the Lena image and average value of all six test images. These values are sufficiently close to ideal values. Hence, we posit that suggested novel image cipher is furnished with a requisite capability to thwart the possible threats of differential attack. Moreover, the suggested work beats the works [30], [33] and [30], [31], [32], [33] regarding the metrics of NPCR and UACI respectively.

Image cryptographers are not satisfied with the results we have presented in our study regarding the differential attack. They sometimes resort to the more tighter analysis in which notion of critical values [37] is employed for images with other sizes. These other sizes are normally taken as 256×256, 512×512 and 1024×1024. One can see findings of NPCR and UACI in the accompanying Tables 6 and 7.

TABLE 5. Comparison of the differential attack results with other published works to change the cited works.

Scheme	Image	NPCR(%)	UACI(%)
Suggested	Lena	99.6183	33.6093
Ref. [30]	Lena	99.60	36.11
Ref. [31]	-	99.62	33.46
Ref. [32]	Lena	99.61937	33.44153
Ref. [33]	Lena	99.6040	33.4736

TABLE 6. Critical values (percentages) for NPCR randomness test.

Size	$N^*_{0.05}$	$N^*_{0.01}$	$N^*_{0.001}$
256×256	99.5693	99.5527	99.5341
512×512	99.5893	99.5810	99.5717
1024×1024	99.5994	99.5952	99.5906

TABLE 7. Theoretical results (percentages) for UACI randomness test.

Size	$\frac{u^{*-}_{0.05}}{u^{*+}_{0.05}}$	$\frac{u^{*-}_{0.05}}{u^{*+}_{0.05}}$	$\frac{u^{*-}_{0.05}}{u^{*+}_{0.05}}$
256×256	33.2824	33.7016	33.6777
	33.6447	33.2254	33.1593
512×512	33.5541	33.5825	33.6156
	33.3729	33.3445	33.3114
1024×1024	33.5088	33.5230	33.5395
	33.4182	33.4040	33.3875

TABLE 8. Critical values against NPCR randomness test.

Size	Image	NPCR value	0.05 level	0.01 level	0.001 level
256×256	Lena	99.6098	Pass	Pass	Pass
	Moon	99.6123	Pass	Pass	Pass
	House	99.6089	Pass	Pass	Pass
	Girl	99.6288	Pass	Pass	Pass
	White	99.6093	Pass	Pass	Pass
	Black	99.6176	Pass	Pass	Pass
512×512	Lena	99.6189	Pass	Pass	Pass
1024×1024	Lena	99.6292	Pass	Pass	Pass

More precisely, the Table 6 shows the critical values of $N^*_{0.05}, N^*_{0.01}, N^*_{0.001}$. Cryptographers have set these thresholds to judge the randomness of the pixels of cipher images. If values of the security parameter NPCR against two cipher images becomes lesser than N^*_α, then the wo cipher images in question would not be treated as sufficiently randomized along with significance of α-level. As the Table 8 suggests, NPCR's results for all levels of confidence fulfill the critical (theoretical) criterion of randomness of NPCR for the given sizes of 256×256, 512×512 and 1024×1024. Regarding the other security parameter of UACI, critical value U^*_α is made up of two segments of U^{*+}_α and U^{*-}_α according to the Table 7. If UACI results do not fall within the interval $(U^{*-}_\alpha, U^{*+}_\alpha)$, Null hypothesis gots rejected. As the Table 9 shows, UACI results qualify critical benchmarks designed for UACI randomness test. Hence, we asset that the pixels of the cipher images produced by the suggested encryption technique are sufficiently randomized.

F. KEY SPACE

Large key space is a guarantee that the cipher would be saved from the brute force attack. In such attack anatomy,

TABLE 9. Critical values for the randomness test of UACI.

Size	Image	UACI value	$\frac{u^{*-}_{0.05}}{u^{*+}_{0.05}}$	$\frac{u^{*-}_{0.05}}{u^{*+}_{0.05}}$	$\frac{u^{*-}_{0.05}}{u^{*+}_{0.05}}$
256×256	Lena	33.5045	Pass	Pass	Pass
	Moon	33.6189	Pass	Pass	Pass
	House	33.3009	Pass	Pass	Pass
	Girl	33.4090	Pass	Pass	Pass
	White	33.3009	Pass	Pass	Pass
	Black	33.4090	Pass	Pass	Pass
512×512	Lena	33.5098	Pass	Pass	Pass
1024×1024	Lena	33.4845	Pass	Pass	Pass

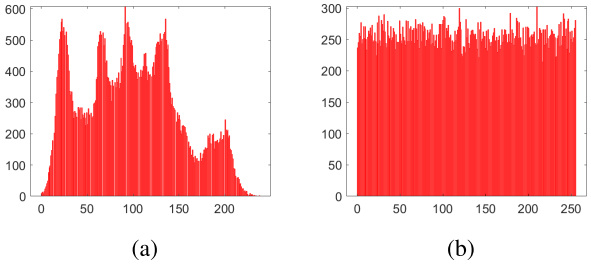
TABLE 10. Key space of suggested technique and contrasting analysis with some other techniques.

Scheme	Key space
Ours	$10^{84} \approx 2^{279}$
Ref. [30]	-
Ref. [31]	10^{144}
Ref. [32]	2^{430}
Ref. [33]	-

the hackers permute all possible keys of cryptosystem. In this way, the one which is actual, is spotted. The cryptographers are of the view that 2^{100} is least key space for potential brute force attack to be withstood. The precision of the system upon which the current project has been carried out is 10^{-14}. Moreover, system parameters and initial values of chaotic systems are $\{a, b, \eta\}$ and $\{p_0, q_0, s_0\}$. The key space has been found as $10^{14\times6} = 10^{84} \approx 2^{279}$. Since, $2^{100} \ll 2^{279}$, hence the suggested image cipher is safe from threats of brute force attack. Additionally, current work, unfortunately, couldn't beat any of the other works regarding this metric.

G. KEY SENSITIVITY

A nice cipher is always extremely key sensitive. The faintest tempering in any value of the key should result into a categorically different result. Here, this property of the suggested image cryptosystem would be demonstrated. Our modus operandi would be something like this. A cipher image would be generated by applying the secret key in the encryption algorithm. Now, the same key would be applied in encryption with a very minute change in one of the variables of the key. The change in the pixels' values would be calculated. If this change is very large, then we can say that the cipher is very sensitive to the key. The secret key of the cipher is $\{a, b, \eta, p_0, q_0, s_0\}$ (say Key_0). By using this key, the Lena image in Figure 3a has been encrypted. After it, a very small tempering of 10^{-14} is made in one of the variables, i.e., p_0 of the secret key. To put in other words, let $p_0{}' = p_0 + 10^{-14}$. In this way, other key set we got is $\{a, b, \eta, p_0{}', q_0, s_0\}$ (say Key_1). The same Lena image of Figure 3a has been encrypted by using this new key Key_1. The resultant effects upon the pixels have been shown in the Table 11. The difference rates have been computed between the cipher images by the untempered key Key_0 and the tempered keys $Key_k (k = 1, 2, \ldots 12)$. 99.62% calculates to be average result which beats the results given in the studies [38], [39]. Therefore, suggested cipher is more sensitive to the secret key.



(a) (b)

FIGURE 7. Histogram analysis for image of Lena. (a) Plain image (b) Cipher image.

H. STATISTICAL ANALYSIS

Correlation coefficient and histogram analyses are usually done with this heading.

1) HISTOGRAM ANALYSIS

Images are composed of tiny pixels. These pixels have different intensity values. Histogram gives us number of pixels for each intensity value in a systematic fashion. Plain and cipher images' histograms are different. For the plain image, the histogram has a curved bar over it. Whereas, for the cipher image, its histogram has a smooth bar. This smoothness of bar acts as a great resistance to the potential hackers. The more smooth the bar of a histogram of a cipher image is, the better it is. One can see that the histogram of the plain image has a curved bar whereas that of cipher one is very smooth (Figure 7). Hence, the suggested cipher is immune from the attack of histogram. Moreover, Figure 8 shows the histograms of the cipher and plain White and Black images. We can see the single vertical lines for the histograms of White (Figure 8b) and Black (Figure 8f) images since these two images have a single intensity values of 255 and 0 respectively.

The inspection of these bars through a naked eye is not sufficient. There must be some dispassionate criterion to assess the curved- and smoothness of these bars. Fortunately, the idea of variance has proved very handy to address this issue. The larger variance values denote poor security effects and vice versa [40], [41]. Table 12 shows findings of historam for cipher images of Lena, Moon, House, Girl, White and Black. According to the table, 256.4197 is average variance value for all the chosen images. Besides, 256.9921 comes out to be the variance value for the Lena image. Both of these metrics are better than 264.37 [42]. Hence, the suggested work is more secure.

2) CORRELATION COEFFICIENT ANALYSIS

Pixels of plain images are abundantly related with each other. Actually, this relationship is the underlying cause that the plain images have some underlying sense. As the cipher is applied over the plain images, its pixels undergo a radical

TABLE 11. Rates of difference between two images produced by minutely distinct keys.

Secret security keys	Difference rates(%)					
	Lena	Moon	House	Girl	White	Black
$Key_1(p_0' = p_0 + 10^{-14})$	99.5963	99.6185	99.6190	99.5998	99.6289	99.6178
$Key_2(q_0' = q_0 + 10^{-14})$	99.5894	99.6178	99.6039	99.6194	99.6098	99.6180
$Key_3(s_0' = s_0 + 10^{-14})$	99.6043	99.5990	99.6609	99.5823	99.6288	99.6289
$Key_4(a' = a + 10^{-14})$	99.6398	99.6187	99.6590	99.5806	99.6199	99.6223
$Key_5(b' = b + 10^{-14})$	99.6212	99.6287	99.6390	99.6287	99.6022	99.6097
$Key_6(\eta' = \eta + 10^{-14})$	99.6312	99.6290	99.6127	99.5936	99.6234	99.6123
$Key_7(p_0' = p_0 - 10^{-14})$	99.5963	99.6185	99.6190	99.5998	99.6193	99.6122
$Key_8(q_0' = q_0 - 10^{-14})$	99.5894	99.6178	99.6039	99.6194	99.6229	99.6112
$Key_9(s_0' = s_0 - 10^{-14})$	99.6043	99.5990	99.6609	99.5823	99.6129	99.6100
$Key_{10}(a' = a - 10^{-14})$	99.6398	99.6187	99.6590	99.5806	99.6222	99.6189
$Key_{11}(b' = b - 10^{-14})$	99.6212	99.6287	99.6390	99.6287	99.6123	99.6309
$Key_{12}(\eta' = \eta - 10^{-14})$	99.6312	99.6290	99.6127	99.5936	99.6321	99.6299
Average	**99.62**	**99.63**	**99.63**	**99.60**	**99.62**	**99.62**
Average of all	**99.62**	-	-	-		

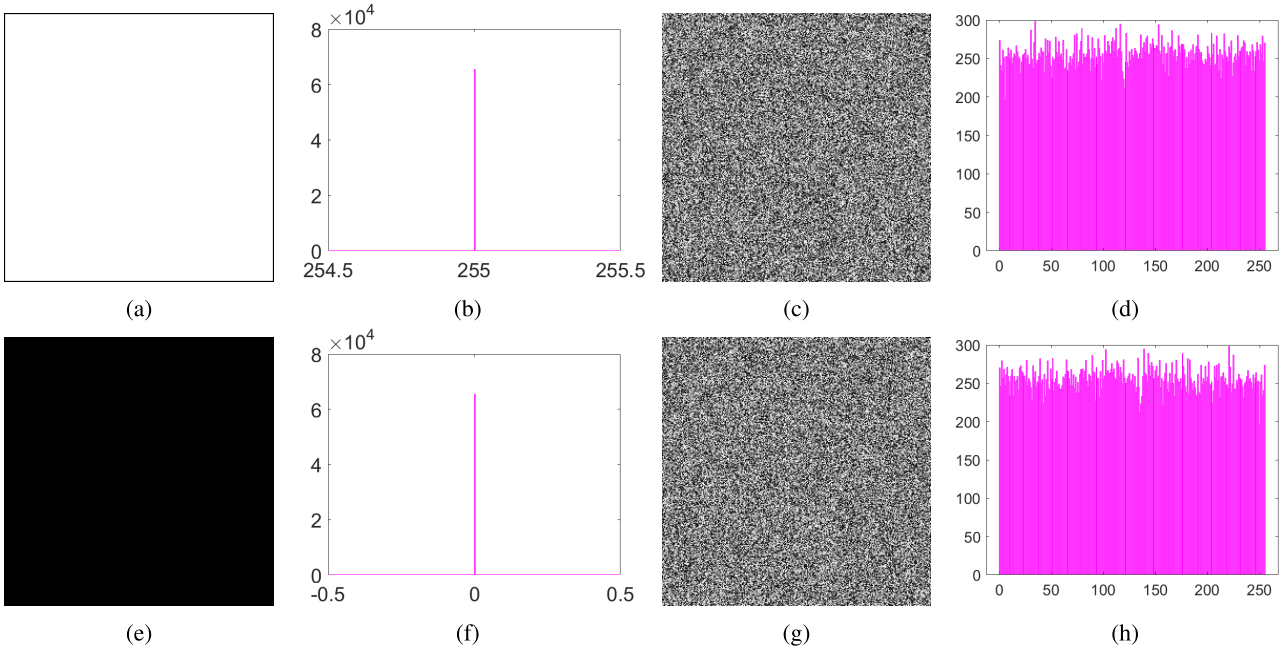


FIGURE 8. Histogram analysis of black and white images along with their cipher versions:(a) White image; (b) White image's histogram; (c) Cipher White image; (d) Histogram of cipher White image; (e) Black image; (f) Black image's histogram; (g) Cipher Black image; (h) Histogram of cipher Black image.

change in their intensity values and their locations. In this way, the strong connection between the neighboring pixels dismantles. To assess the correlation among the pixels, the following formula is employed. (CC) [43]:

$$CC = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right)\left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}} \tag{9}$$

In this formula, N represents number of pixels in totality in given image. Additionally, x and y denote total pixels' intensity values. Correlation distribution of pixels of cipher and plain images have been drawn in Figure 9. Apart from that, three orientations have been catered, i.e., diagonally, horizontally and vertically. Table 13 depicts this coefficient between two adjacent pixels for cipher and plain images of Lena. According to this table, value of this metric is almost equal to one for the original plain image and almost equal to zero for cipher image. Apart from that, a comparison has also been carried out in the Table 14. We can note that the results are comparable.

It is to be noted that 5,000 pairs of pixels have been chosen randomly from the given images and the formula has been applied over them. The results vary wildly. The reason of this stems from the fact that sometimes such pairs are chosen which produce better results and vice versa.

TABLE 12. Cipher images histogram varaince results.

Algorithm	Lena	Moon	House	Girl	White	Black	**Average**
Proposed	256.9921	259.3459	258.6641	253.7267	255.8788	253.9107	**256.4197**
Ref. [42]	264.37	-	-	-	-	-	-

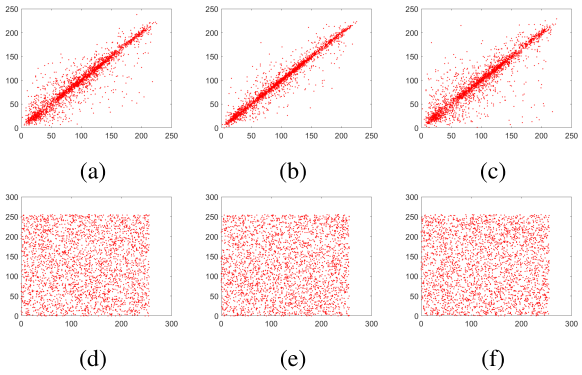


FIGURE 9. Correlation distribution for the test image of Lena: (a) plain image, horizontal; (b) plain image, vertical; (c) plain image, diagonal; (d) cryptic image, horizontal; (e) cryptic image, vertical; (f) cryptic image, diagonal.

TABLE 13. Correlation coefficient's findings.

Image	Correl. dire.		
	H	V	D
Plain image of Lena	0.9145	0.9345	0.9390
Encrypted Lena image	-0.0076	0.0047	0.0072

I. CHOSEN PLAINTEXT, KNOWN PLAINTEXT AND CIPHERTEXT ONLY ATTACKS ANALYSES

Cryptanalysts have many ways to break the cryptosystems. Out of these ways, chosen plaintext, known plaintext and ciphertext only attacks are normally launched by them [44]. Let us describe here one by one the modus operandi of each of these attacks. In ciphertext only attack, hackers have few ciphertexts at their disposal. Whereas, in the known plaintext attack, they have few pairs of ciphertexts and plaintexts. Apart from that, in the dynamics of chosen plaintext attack, they have full control on the encryption paraphernalia and hence, can have as many ciphertexts as they wish. Here, if it is demonstrated that suggested image cryptosystem is defiant to chosen plaintext attack, then defiance of ciphertext only and known plaintext only attacks are trivially guaranteed. The reason of this stems from the fact that ciphertext only and known plaintext attacks constitute ''subset'' of chosen plaintext attack.

In order to launch chosen plaintext attack, hackers may select a special kind of image, say Black image (Figure 10a) to encrypt it for tracing secret key which has been used. As soon as the Black image gets encrypted (Figure 10b), random numbers employed in encryption scheme are retrieved. After it, hackers may select any plain image of interest say the image of Lena and encrypt it (Figure 10c) through the launch of known plaintext attack, along with key employed in encryption operation of Black image. The potential hacker would be disappointed since the cipher image of Lena could not be decrypted using the key (Figure 10d). Similarly, same process was carried out upon some other special image White (Figures 10e to 10h). These phenomena signal towards the intrinsic defiance of suggested image cryptosystem against chosen plaintext, known plaintext and ciphertext only attacks.

J. PEAK SIGNAL TO NOISE RATIO (PSNR) ANALYSIS

PSNR objectively assesses the magnitude of the difference of pixel values between the cipher and plain images. Its mathematical formula is

$$\begin{cases} PSNR = 20log_{10}(^{255}/_{\sqrt{MSE}})dB \\ MSE = \dfrac{1}{m \times n}\displaystyle\sum_{f=1}^{m}\sum_{g=1}^{n}(Plain(f,g) - Cipher(f,g))^2 \end{cases} \tag{10}$$

In this formula, m and n refer to the length and the width of the given images. Besides, $Plain(f, g)$ and $Cipher(f, g)$ denote the intensity values of the pixels of the plain and cipher images at the address (f, g). Additionally, MSE refers to the mean squared error. Greater value of MSE is better for the security effects. Further, the lesser value of $PSNR$ is desirable. Its reason is that both these parameters have been reciprocally interrelated. Table 15 shows the $PSNR$ results by the proposed work and other numerous works published in the literature. According to the table, the results of $PSNR$ are infinite (∞) when the formula is applied over the plain and cipher images. We will infer from this phenomenon that cipher and plain images are exactly the same owing to the reality of $MSE = 0$. It also means that there is no loss between the restored and the plain images. Here 'O-C' refers to the original and cryptic images, and 'O-D' to the original and decrypted images. Moreover, $PSNR$ results for Lena by suggested work is the best when it is compared with other works [30], [45], [46], [47]. Therefore, we can say that the current study is better than the others.

K. MEAN ABSOLUTE ERROR (MAE)

This is an other powerful security parameter to judge the effectiveness of the image ciphers. As the plain image is subjected to the encryption algorithm, its pixels undergo a sweeping change in the pixels values and their locations. This is the job of this parameter to objectively gauge this departure. As an input to this notion, plaintext and ciphertext images are

TABLE 14. Metric of correlation coefficients and its contrasting analysis.

Type of image	Encryption scheme	Correlation direction		
		Horizontal	Vertical	Diagonal
Plain image of Lena		0.9145	0.9345	0.9390
Encrypted Lena image	Suggested	-0.0076	0.0047	0.0072
	Ref. [30]	0.0005	0.1313	-0.0047
	Ref. [31]	0.0013	-0.0009	-0.0023
	Ref. [32]	0.0033	0.0070	0.0027
	Ref. [33]	0.0002	0.0022	-0.0015

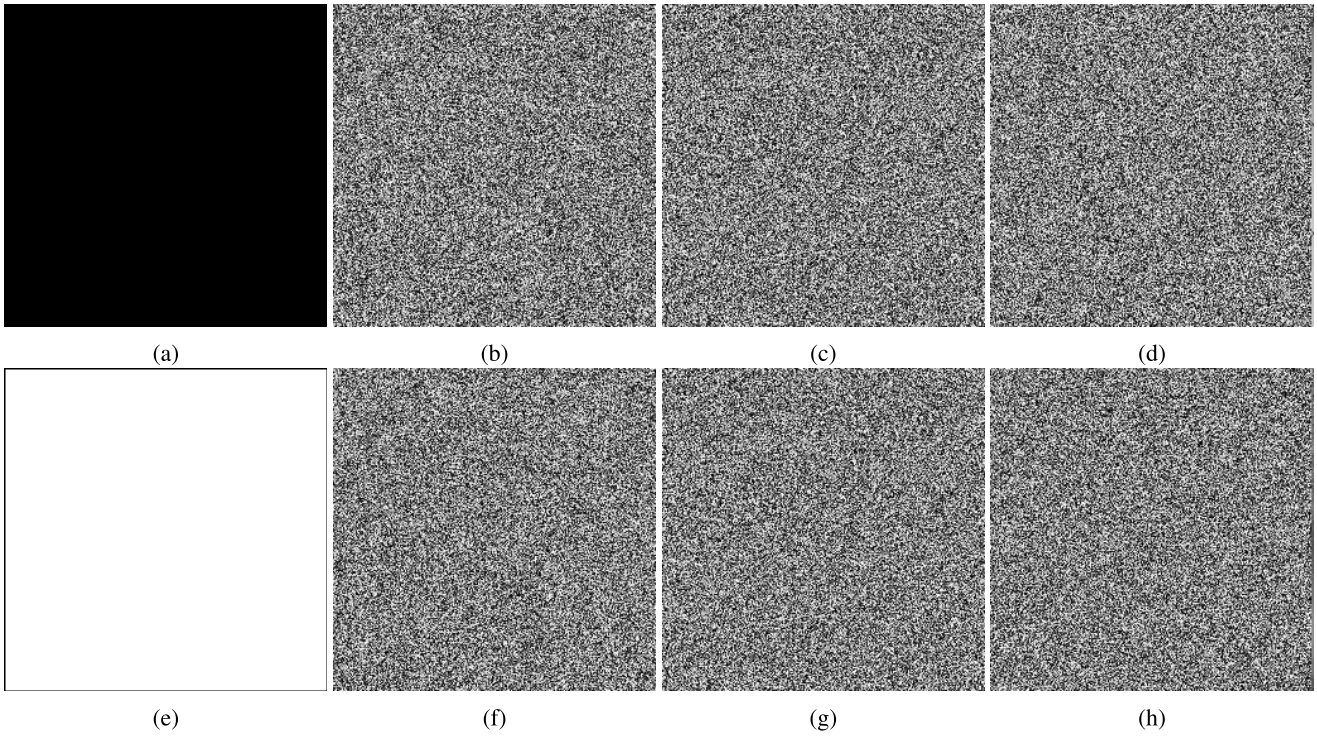


FIGURE 10. Using black and white images, demo of defiance of chosen plaintext attack :(a) Black image; (b) Cipher Black image; (c) Cipher Lena image; (d) Decrypted Lena image with possible secret key from the Black image; (e) White image; (f) Cipher White image; (g) Cipher Lena image; (h) Decrypted Lena image with possible secret key from White image.

TABLE 15. Peak signal to noise ratio results.

		Lena	Moon	House	Girl	White	Black	**Average**
Ours	PSNR (O-D)	∞	∞	∞	∞	∞	∞	∞
	PSNR (O-C)	8.5212	10.1721	8.8406	8.2582	9.8725	8.2009	**8.9776**
Ref. [48]	PSNR (O-C)	19.8469	-	-	-	-	-	-
Ref. [49]	PSNR (O-C)	9.2736	-	-	-	-	-	-

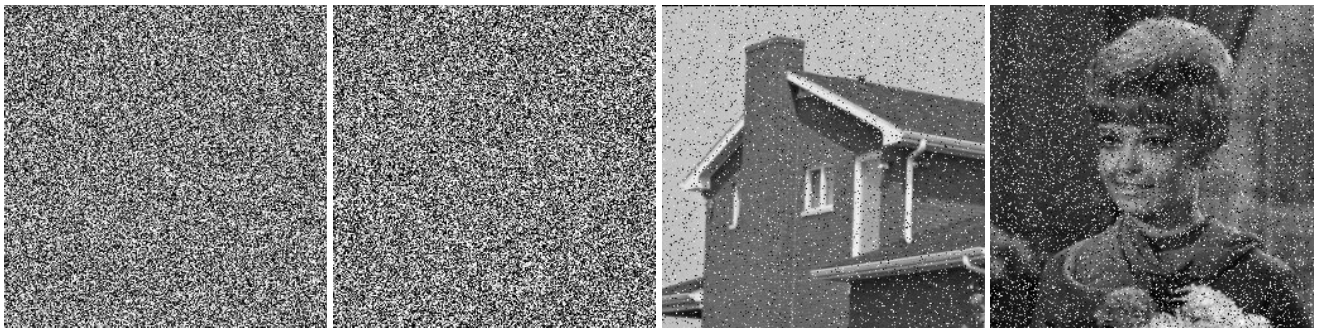
provided. Below is the equation.

$$MAE = \frac{1}{m \times n} \sum_{x=1}^{m} \sum_{y=1}^{n} abs(Cipher(x, y) - Plain(x, y)) \tag{11}$$

In this formula, *Plain* and *Cipher* refer to the plaintext and ciphertext images respectively, (m, n) being the size of these images. The greater the value of this security parameter, the better it is. Table 16 shows the obtained results by the suggested scheme. The results are better than the one given in [50].

L. DATA CROP AND NOISE ATTACKS

As the cipher images are generated, they are normally transmitted through the vulnerable channels. Sometimes, they undergo the attacks of noise and data crop. In noise attack, some kind of noise gets added to the cipher images which caused to change the pixel intensity values. On the destination side, when the original plaintext images are generated, they do not reflect the exact images. The reason is that noise damages some of the intensity values of the pixels as said earlier. To demonstrate the defiance of the cipher from this attack, this study has artificially added noise with different intensities as shown in the Figure 11.



(a) (b) (c) (d)

FIGURE 11. Defiance from the Pepper & Salt noise attack:(a) Cipher House image with noise density of 0.1; (b) Cipher Girl image with noise density of 0.2; (c) Output image from (a); (d) Output image from (b).

(a) (b) (c) (d)

FIGURE 12. Defiance from the data loss attack: (a) Cipher House image with data loss; (b) Cipher Girl image with data loss; (c) Output House image from (a); (d) Output Girl image from (b).

In particular, noise intensities of 0.1 and 0.2 were added in the cipher pictures of House and the Girl. Further, the Figures 14c and 14d show that the plain images can be identified easily. This phenomenon refers to the fact that the suggested image cipher can defy the noise attacks. In crop attack, as the name suggests, some portion of the cipher image is damaged during its transmission from the source to destination. For the experimentation purpose, we have cropped a significant amount of pixels data from the two cipher images (Figure 12a and 12b). As the decryption algorithms were applied over these cropped images, we can see the output in the Figures 12c and 12d. Again, these restored images can be easily identified. So, we assert that the suggested image ciphers have the sufficient power to withstand the possible attacks of crop and noise over them.

VI. OTHER ATTACKS

A. IMAGE ROTATION ATTACK ANALYSIS

Hackers, sometimes, launch an image rotation attack upon the image cryptosystems to have an illegal access over the original image. In this particular attack, the given cipher image is rotated with some degree say r^o. The cipher image is rotated in the reverse direction through the usage of relevant pixels which are located along the vertical and horizontal directions. For the horizontal orientation, first non-zero value of pixel from rightmost margin is determined. Apart from that, the distance of this non-zero value of pixel from leftmost margin is also computed. Same operations are carried out in the vertical direction as well.

TABLE 16. Mean absolute error results.

Image	MAE
Lena	81.8970
Moon	82.1093
House	75.8449
Girl	80.5834
White	83.9981
Black	81.4921
Average for all images	**80.9875**
Ref. [50]	79.354
Ref. [30]	84

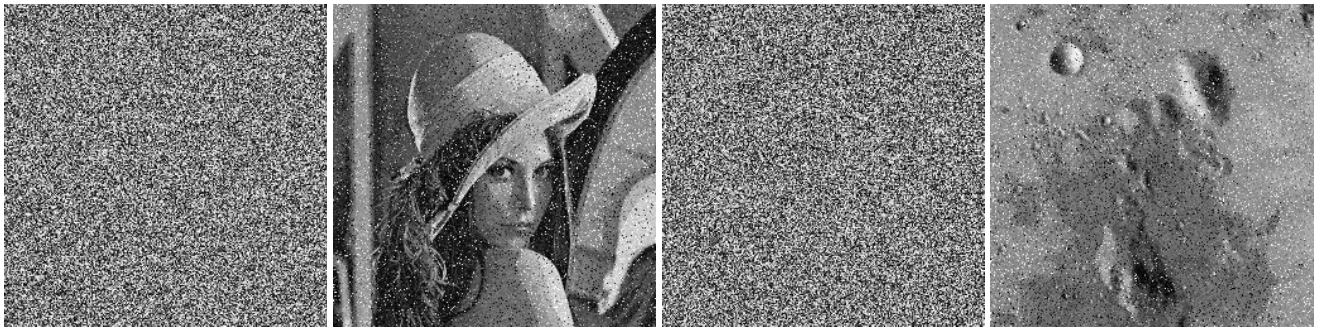
Following formulae are employed to calculate the rotation degree r'^o.

$$r'^o = \tan^{-1}(\frac{x}{y}) \tag{12}$$

$$rr^o = \begin{cases} -r'^o & \text{if } 0^o < r^o < 90^o \\ -(180 - r')^o & \text{if } 90^o < r^o < 180^o \\ -(270 - r')^o & \text{if } 180^o < r^o < 270^o \\ -(360 - r')^o & \text{if } 270^o < r^o < 360^o \end{cases} \tag{13}$$

(a) (b) (c) (d)

FIGURE 13. Demo of rotation attack analysis for the cipher image: (a) Cipher image of Lena with rotation of 15^o; (b) Decrypted image from (a); (c) Cipher image of Moon with rotation of 45^o; (d) Decrypted image from (c).



(a) (b) (c) (d)

FIGURE 14. JPEG compression attack on cipher images: (a) Cipher image of Lena; (b) Decrypted image from (a); (c) Cipher image of Moon; (d) Decrypted image from (c).

TABLE 17. Image rotation and JPEG attacks analyses.

Work	Attack	Image	PSNR
Proposed	Image rotation	Lena	15.7780
		Moon	14.8734
	JPEG Compression	Lena	13.0865
		Moon	14.5698
Ref. [51]	Image rotation	Lena	9.739
Ref. [52]		Lena	26.5053
Ref. [53]	JPEG Compression	Baboon	15.0854
Ref. [54]		Airplane	16.4162

In these equations, rr^o and r^o correspond to reverse rotation degree and attacker degree of rotation respectively. Moreover, x and y denote the vertical and horizontal distances of the two corner of the given image from the top left corner. Figures 13a and 13c show the cipher images after the rotation degrees of 15^o and 45^o respectively. Apart from that, the Figures 13b and 13d demonstrate the decrypted images. One can see that the retrieved images can be easily identified. This fact demonstrates that the suggested image cipher is potent enough to defy the potential rotation attacks. In order to objectively measure the quality of decrypted images, the security parameter of PSNR is also employed by the image cryptographers. The Table 17 shows values of PSNR for the images of Lena and Moon. A relatively bigger value of PSNR shows that the decrypted image has more resemblance to the original images. Moreover, comparison has also been carried out with [51] and [52]. The results of the suggested work are better than [51].

B. JPEG ATTACK ANALYSIS

Sometimes, JPEG compression attack is also launched by the hackers on the cipher images. In this particular attack dynamics, the given cipher image is compressed in the JPEG format. Now, the compressed version of the given cipher image is decrypted by invoking the decryption algorithm. Figure 14 demonstrates the defiance of the proposed image cipher against the JPEG attack. One can easily identify the original plain images although they have been blurred to some extent. Table 17 shows the results against this important security parameter. Unluckily our work couldn't beat both the studies [53], [54].

VII. CONCLUSION

Security of images is a hot research area. In particular, in the last two decades, hundreds of image ciphers have been developed for securing the precious images data. This project has employed the construct of rectangle to realize the operation of confusion —one of the primary requirements for the enterprise of encryption. Hénon and piecewise linear

chaotic maps have been used for the generation of random numbers. They facilitated in carrying out the confusion and diffusion operations on the pixels' data of the given images. The geometric figure of rectangle has been created iteratively within the scope of the given grayscale image. The top left and bottom right corners characterize the size and location of these rectangles. Now on each iteration, the pixels along the boundary of rectangle are rotated clockwise/anticlockwise for an arbitrary amount of numbers. This operation has been iterated for a number of times to embed the confusion effects in the given image. The security analysis and the machine experimentation gave very promising results which indicate that the suggested image cipher is defiant to the multifarious threats being launched from the cryptanalysis community. Hence, we posit that the suggested cipher can be applied to solve the real world problems. The incorporation of plaintext sensitivity feature is very trivial in its approach and orientation. In the future, to cement the security of the cipher, both SHA coding and DNA encoding would be carried out.

REFERENCES

[1] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, Aug. 2022.

[2] M. G. A. Malik, Z. Bashir, N. Iqbal, and Md. A. Imtiaz, "Color image encryption algorithm based on hyper-chaos and DNA computing," *IEEE Access*, vol. 8, pp. 88093–88107, 2020.

[3] Q. Liang and C. Zhu, "A new one-dimensional chaotic map for image encryption scheme based on random DNA coding," *Opt. Laser Technol.*, vol. 160, May 2023, Art. no. 109033.

[4] H. Li, T. Li, W. Feng, J. Zhang, J. Zhang, L. Gan, and C. Li, "A novel image encryption scheme based on non-adjacent parallelable permutation and dynamic DNA-level two-way diffusion," *J. Inf. Secur. Appl.*, vol. 61, Sep. 2021, Art. no. 102844.

[5] Y. Dong, G. Zhao, Y. Ma, Z. Pan, and R. Wu, "A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata," *Inf. Sci.*, vol. 593, pp. 121–154, May 2022.

[6] X. Wang, Y. Su, M. Xu, H. Zhang, and Y. Zhang, "A new image encryption algorithm based on Latin square matrix," *Nonlinear Dyn.*, vol. 107, no. 1, pp. 1277–1293, Jan. 2022.

[7] Y. Zhao, R. Meng, Y. Zhang, and Q. Yang, "Image encryption algorithm based on a new chaotic system with Rubik's cube transform and Brownian motion model," *Optik*, vol. 273, Feb. 2023, Art. no. 170342.

[8] A. Ikram, M. A. Jalil, A. B. Ngah, N. Iqbal, N. Kama, A. Azmi, A. S. Khan, Y. Mahmood, and A. Alzayed, "Encryption algorithm for securing non-disclosure agreements in outsourcing offshore software maintenance," *Comput., Mater. Continua*, vol. 73, no. 2, pp. 3827–3860, 2022.

[9] N. Iqbal, S. Abbas, M. A. Khan, T. Alyas, A. Fatima, and A. Ahmad, "An RGB image cipher using chaotic systems, 15-puzzle problem and DNA computing," *IEEE Access*, vol. 7, pp. 174051–174071, 2019.

[10] I. Hadjadj and A. Gattal, "An image encryption-based method for handwritten digit recognition," in *Proc. 12th Int. Conf. Inf. Syst. Adv. Technol. (ICISAT)*. Cham, Switzerland: Springer, 2023, pp. 18–26.

[11] N. Rani, V. Mishra, and S. R. Sharma, "Image encryption model based on novel magic square with differential encoding and chaotic map," *Nonlinear Dyn.*, vol. 111, no. 3, pp. 2869–2893, Feb. 2023.

[12] M. U. Hassan, A. Alzayed, A. A. Al-Awady, N. Iqbal, M. Akram, and A. Ikram, "A novel RGB image obfuscation technique using dynamically generated all order-4 magic squares," *IEEE Access*, vol. 11, pp. 46382–46398, 2023.

[13] S. Jiao, J. Feng, Y. Gao, T. Lei, and X. Yuan, "Visual cryptography in single-pixel imaging," *Opt. Exp.*, vol. 28, no. 5, pp. 7301–7313, 2020.

[14] P. Zheng, J. Li, Z. Li, M. Ge, S. Zhang, G. Zheng, and H. Liu, "Compressive imaging encryption with secret sharing metasurfaces," *Adv. Opt. Mater.*, vol. 10, no. 15, Aug. 2022, Art. no. 2200257.

[15] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon-Sine map and DNA approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018.

[16] W. Alexan, M. ElBeltagy, and A. Aboshousha, "RGB image encryption through cellular automata, S-box and the Lorenz system," *Symmetry*, vol. 14, no. 3, p. 443, Feb. 2022.

[17] M. Ahmad, S. Agarwal, A. Alkhayyat, A. Alhudhaif, F. Alenezi, A. H. Zahid, and N. O. Aljehane, "An image encryption algorithm based on new generalized fusion fractal structure," *Inf. Sci.*, vol. 592, pp. 1–20, May 2022.

[18] R. Chen, L. Liu, and Z. Zhang, "Cryptanalysis on a permutation–rewriting–diffusion (PRD) structure image encryption scheme," *Multimedia Tools Appl.*, vol. 82, no. 3, pp. 4289–4317, Jan. 2023.

[19] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dyn.*, vol. 94, no. 1, pp. 745–756, Oct. 2018.

[20] M. Khan, F. Masood, A. Alghafis, M. Amin, and S. I. B. Naqvi, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," *PLoS One*, vol. 14, no. 12, Dec. 2019, Art. no. e0225031.

[21] N. Munir, M. Khan, A. Al Karim Haj Ismail, and I. Hussain, "Cryptanalysis and improvement of novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," *Multimedia Tools Appl.*, vol. 81, no. 5, pp. 6571–6584, Feb. 2022.

[22] P. Snaselova and F. Zboril, "Genetic algorithm using theory of chaos," *Proc. Comput. Sci.*, vol. 51, pp. 316–325, Jan. 2015.

[23] M. Alawida, J. S. Teh, A. Mehmood, A. Shoufan, and W. H. Alshoura, "A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8136–8151, Nov. 2022.

[24] A. Elghandour, A. Salah, and A. Karawia, "A new cryptographic algorithm via a two-dimensional chaotic map," *Ain Shams Eng. J.*, vol. 13, no. 1, Jan. 2022, Art. no. 101489.

[25] M. Ma, Y. Yang, Z. Qiu, Y. Peng, Y. Sun, Z. Li, and M. Wang, "A locally active discrete memristor model and its application in a hyperchaotic map," *Nonlinear Dyn.*, vol. 107, no. 3, pp. 2935–2949, Feb. 2022.

[26] P. Ping, F. Xu, Y. Mao, and Z. Wang, "Designing permutation–substitution image encryption networks with Henon map," *Neurocomputing*, vol. 283, pp. 53–63, Mar. 2018.

[27] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, "A chaos based image encryption scheme using digit-level permutation and block diffusion," *IEEE Access*, vol. 6, pp. 67581–67593, 2018.

[28] Y. Luo, R. Zhou, J. Liu, Y. Cao, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, Aug. 2018.

[29] K. K. Raghuvanshi, S. Kumar, S. Kumar, and S. Kumar, "Investigation of piecewise linear chaotic map as a diffusion model for image encryption," *Multimedia Tools Appl.*, vol. 82, pp. 36325–36342, Mar. 2023.

[30] F. Masood, W. Boulila, A. Alsaeedi, J. S. Khan, J. Ahmad, M. A. Khan, and S. U. Rehman, "A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and logistic Gaussian map," *Multimedia Tools Appl.*, vol. 81, no. 21, pp. 30931–30959, Sep. 2022.

[31] X. Gao, J. Mou, S. Banerjee, Y. Cao, L. Xiong, and X. Chen, "An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1535–1551, Apr. 2022.

[32] Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, M. A. A. Sibahee, V. O. Nyangaresi, D. G. Honi, A. I. Abdulsada, and X. Jiao, "Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map," *IEEE Access*, vol. 10, pp. 26257–26270, 2022.

[33] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Inf. Sci.*, vol. 539, pp. 195–214, Oct. 2020.

[34] S. Janakiraman, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Lightweight chaotic image encryption algorithm for real-time embedded system: Implementation and analysis on 32-bit microcontroller," *Microprocessors Microsyst.*, vol. 56, pp. 1–12, Feb. 2018.

[35] X. Wang and S. Gao, "Application of matrix semi-tensor product in chaotic image encryption," *J. Franklin Inst.*, vol. 356, no. 18, pp. 11638–11667, Dec. 2019.

[36] D. H. ElKamchouchi, H. G. Mohamed, and K. H. Moussa, "A bijective image encryption system based on hybrid chaotic map diffusion and DNA confusion," *Entropy*, vol. 22, no. 2, p. 180, Feb. 2020.

[37] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Opt. Laser Technol.*, vol. 114, pp. 224–239, Jun. 2019.
[38] A. Kulsoom, D. Xiao, Aqeel-ur-Rehman, and S. A. Abbas, "An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules," *Multimedia Tools Appl.*, vol. 75, no. 1, pp. 1–23, Jan. 2016.
[39] Aqeel-ur-Rehman, X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," *Optik-Int. J. Light Electron Opt.*, vol. 153, pp. 117–134, Jan. 2018.
[40] Z.-L. Zhu, W. Zhang, K.-W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," *Inf. Sci.*, vol. 181, no. 6, pp. 1171–1186, Mar. 2011.
[41] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[42] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process.*, vol. 155, pp. 44–62, Feb. 2019.
[43] N. Iqbal, M. Hanif, S. Abbas, M. A. Khan, and Z. Ul Rehman, "Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102809.
[44] S. Jiao, T. Lei, Y. Gao, Z. Xie, and X. Yuan, "Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging," *IEEE Access*, vol. 7, pp. 119557–119565, 2019.
[45] C. Zhu, "A novel image encryption scheme based on improved hyper-chaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, Jan. 2012.
[46] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 995–1015, Oct. 2014.
[47] N. Taneja, B. Raman, and I. Gupta, "Combinational domain encryption for still visual data," *Multimedia Tools Appl.*, vol. 59, no. 3, pp. 775–793, Aug. 2012.
[48] A. Ihsan and N. Doğan, "Improved affine encryption algorithm for color images using LFSR and XOR encryption," *Multimedia Tools Appl.*, vol. 82, no. 5, pp. 7621–7637, Feb. 2023.
[49] S. Mansoor and S. A. Parah, "HAIE: A hybrid adaptive image encryption algorithm using chaos and DNA computing," *Multimedia Tools Appl.*, vol. 82, pp. 28769–28796, Feb. 2023.
[50] B. Norouzi, S. M. Seyedzadeh, S. Mirzakuchaki, and M. R. Mosavi, "A novel image encryption based on hash function with only two-round diffusion process," *Multimedia Syst.*, vol. 20, no. 1, pp. 45–64, Feb. 2014.
[51] A. A. Elsadany, A. Elsonbaty, and E. A. A. Hagras, "Image encryption and watermarking in ACO-OFDM-VLC system employing novel memristive hyperchaotic map," *Soft Comput.*, vol. 27, no. 8, pp. 4521–4542, Apr. 2023.
[52] S. E. El-Khamy and A. G. Mohamed, "An efficient DNA-inspired image encryption algorithm based on hyper-chaotic maps and wavelet fusion," *Multimedia Tools Appl.*, vol. 80, pp. 23319–23335, Jan. 2021.
[53] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A color image encryption technique using block scrambling and chaos," *Multimedia Tools Appl.*, vol. 81, pp. 505–525, Sep. 2022.
[54] K. M. Hosny, S. T. Kamal, and M. M. Darwish, "A novel color image encryption based on fractional shifted Gegenbauer moments and 2D logistic-sine map," *Vis. Comput.*, vol. 39, no. 3, pp. 1027–1044, Mar. 2023.

MOHAMMAD MAZYAD HAZZAZI received the Ph.D. degree in mathematics from the University of Sussex, Brighton, U.K. He is currently an Assistant Professor with the Department of Mathematics, King Khalid University, Abha, Saudi Arabia. He has more than 30 research publications in various international research journals. His current research interests include cryptography and coding theory.

NADEEM IQBAL received the M.S. degree in theorem proving from the National University of Sciences and Technology (NUST), Islamabad, Pakistan, and the Ph.D. degree from the National College of Business Administration and Economics (NCBA&E). He is currently an Assistant Professor with the Department of Computer Science and IT, The University of Lahore (UOL), Lahore, Pakistan. He is an accomplished researcher in the field of cyber security, with a strong foundation in computational science and engineering. His current research interests include cryptography, where he has made significant contributions to enhancing the security of digital systems and data protection. His research extends to various facets of cyber security, including encryption algorithms, data science, and the philosophical aspects of mathematics. His academic excellence is underscored by his outstanding GRE scores, showcasing his exceptional analytical and problem-solving skills. His passion for knowledge and continuous learning is evident through his attainment of the IBM professional certification in data science. With a rich academic background and a keen interest in algorithms, data science, and the philosophy of mathematics. He stands as a dedicated researcher and scholar in the field of cyber security and making valuable contributions to the ever-evolving landscape of digital security.

ATIF IKRAM received the master's degree in computer science from the University of South Asia, Pakistan, and the master's degree in quality management from Superior University, Lahore, Pakistan. He is currently pursuing the Ph.D. degree in computer science with Universiti Malaysia Terengganu, Malaysia. He is an Assistant Professor with the Department of Computer Science, The University of Lahore, Lahore Campus, Pakistan. He has more than 13 research publications in various international research journals and conferences. His current research interests include empirical software engineering (ESE), machine learning, data science, and eLearning.