IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 11 April 2023, accepted 1 May 2023, date of publication 10 May 2023, date of current version 17 May 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3275019

RESEARCH ARTICLE

A Novel RGB Image Obfuscation Technique Using Dynamically Generated All Order-4 Magic Squares

MAHMOOD UL HASSAN[1], **ASAAD ALZAYED**[2], **AMIN A. AL-AWADY**[1], **NADEEM IQBAL**[3], **MUHAMMAD AKRAM**[4], **AND ATIF IKRAM**[3,5]

[1]Department of Computer Skills, Deanship of Preparatory Year, Najran University, Najran 61441, Saudi Arabia
[2]Computer Science and Information Systems Department, College of Business Studies Public Authority for Applied Education and Training (PAAET), Safat 23167, Kuwait
[3]Department of Computer Science and IT, The University of Lahore, Lahore 54000, Pakistan
[4]Department of Computer Science, College of Computer Science and Information Systems, Najran University, Najran 61441, Saudi Arabia
[5]Faculty of Ocean Engineering Technology and Informatics, University Malaysia Terengganu, Kuala Terengganu 21030, Malaysia

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

This work was supported by the Deputy for Research and Innovation Ministry of Education, Saudi Arabia, under the Institutional Funding Committee with Najran University, Saudi Arabia, under Grant NU/IFC/2/SERC/-/47.

ABSTRACT Plethora of image encryption schemes exist in literature based on the construct of magic square for realizing the purpose of image obfuscation. This magic square carries out the scrambling project of the encryption. In these schemes, normally single and static magic square is implied. To render greater scrambling effects, this study proposes a novel image encryption scheme using all order-4 magic squares whose frequency reaches to the tune of 880. These magic squares have been dynamically selected to carry out the scrambling project. As the color image is input, it is broken into its gray scale red, green and blue components. These components are joined together to make a big gray scale image. Intertwining logistic map (ILM) has been used for the generation of random data. Besides, one more stream has been created through the arithmetic manipulation of the generated three streams. Streams generated by ILM has been used to realize the effects of confusion and diffusion. First and second streams out of the four streams randomly select the address from the big gray scale image to apply the randomly selected magic square by the third stream, in order to create the scrambling effects. The fourth and last stream of random numbers is used to create the diffusion effects in the scrambled image. Plaintext senstivity has been introduced by tempering the one initial value of the chaotic system through the usage of a characteristic of the given input color image. The experimentation and security analyses sections vividly demonstrate the strength, immunity from the diverse attacks and prospects for the real world application of the proposed image cipher. In particular, we got very promising stats of information entropy (7.9974) and computational time (0.9865 seconds). No doubt, they suggest the potential application of the proposed image cipher in some real world setting.

INDEX TERMS All order-4 magic squares, chaos, cyber security, decryption, encryption, secret key.

I. INTRODUCTION

Due to the proliferation of different software and hardware products, the complexion of the entire world has undergone a radical change. Be it industry, commerce, medicine, traffic, government &diplomacy, social life, the different gadgets are being used by the people in all walks of life. In all these affairs, digital images have become very important. These images are getting generated, saved and transmitted all over the world. In some situations, they happen to be extremely important and have strategic value as well. So, their safety and integrity from the potential

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Huang.

adversaries and hackers become an urgent challenge which must be coped with. Historically, the ciphers like DES, AES, RSA [1] have been employed to realize the said purpose. But they are incapicitated in the given scenario. The reason stems from the fact that they were designed for encrypting the text data. Whereas, the digital images contain diametrically distinct characteristics like large volume, tight interpixel connection and the high redundancy. Hence, to deal with this situation, we require an entirelyl different paraphernalia.

Fortunately, theory of chaos and the ensuing chaotic maps/systems have rendered a great job in spawning the random numbers which are utilized to carry out the diffusion and confusion operations necessary for cryptographic products. Chaotic maps are an excellent source for the generation of random numbers. Its reason is that they are heavily senistive to two entities. These are system parameters and initial conditions. Moreover, they have properties of ergodicity, mixing, unpredictability and randomness [2]. If we explore the literature of image cryptography, we will find that tens of hundreds of image cryptsystems have already been produced for safety and security of digital images [1], [2], [3], [4], [5], [6], [7], [8], [9], [10]. Different researchers come up with their unique idea for the materialization of confusion/scrambling and diffusion effects. They have used different instuments like nine palace [3], king [4], magic square [5], Rubik's cube [6], Latin squares [7], Sudoku [8], 15-puzzle [2], knight [9], Castle [10]. The fundamental idea for using these intruments was to scramble input plain image's pixels. In [3], color image encryption algorithm was developed based on the instruments of nine palace map and Cyclic Redundancy Check (CRC). The pixels were shuffled using the map. Moreover, the three planes of the given color image were translated into the binary matrices. These bits were shifted in a cyclic fasion through the usage of CRC code. Operation of XOR was made to gain the effects of diffusion. Moreover, work in [4] was based on random walk of chess piece king on large board of chess. The idea of 2D scrambled image was employed for this purpose. As the king walks on the large hypothetical chessboard, pixels lying on the plain image were transferred to scrambled image's different addresses. Lastly, the remaining pixels where shifted to empty positions of 2D scrambled image. Tinkerbell chaotic system was utilized for the random data. Both security analysis and simulation rendered very promising results. The authors of [5] used the construct of magic square to encrypt the given plaintext images. As a modus operandi of their work, a large number of random keys were created by the chaotic map and were fashioned as a matrix. This matrix was later on divided into a number of non-overlapping submatrices. Moreover, the concerned image was also sliced into a number of sub-images. Apart from that, are subimages were multiplied by magic square for rendering a yet other matrices' set. Finally, in order to give the encrypted image, an XOR operation was made on the two sets of matrices. The simulation and the performance evaluation gave very good results. A yet another image cipher was written based on the game of Rubik's cube [6]. For the effects of scrambling, bit-level encryption principle and Rubik's cube procedure were combined together in the 3D space. Moreover, by using contraction mapping principle, reducing as well as ascending dimension operations were carried out. They designed 2D diffusion structure which has the potential to disseminate a very minute change from plain image to cipher image. The computer experiments and evaluation proved validity and security of new cipher.

The work [11] designed a chaotic image encryption scheme using Hilbert curve, theory of matrix semi-tensor product and n-ary counting system. Confusion and diffusion effects were embedded in a parallel fashion. The simulation showed that the scheme was secured and could thwart the common attacks prevalent in the cryptanalysis community. In a yet another research endeavor [12], spatio-temporal chaos based Parameter Uncertainty Mixed Coupled Map Lattice (PUMCML) was developed. Moreover, using the Cantor set theory, Cantor diagonal matrix was created. Additionally, in order to generate the scrambled image, ordered rotation scrambling strategy for the reported matrix was employed. Finally, this scheme was demonstrated as more secured and better than the existing schemes. The study [13] developed an image cryptosystem uisng multiple chaotic systems. Moreover, dynamic diffusion and bit-combination scrambling was carried out. Lastly, the comparison with another state of the art schemes demonstrated that their proposed method was furnished with better security effects and could avert the varried attacks. An other study [14] has been carried out for reversible data hiding. Besides, based on ridge regression predictor, high precision error prediction algorithm has been given in this study [14]. Ridge regression, being a penalized least-square algorithm has the potential for the solution of the overfitting problem of least-square method. As a modus operandi of the proposed algorithm, 8 neighboring pixels of target pixel along with two distinct combinations were chosen as the training and the supporting sets in a respective way. The machine experiments demonstrated that suggested method beat existing adaptive reversible data hiding based on embedding performance and the prediction accuracy. Moreover, other studies of reversible data hiding using code division multiplexing has been conducted in [15]. Besides, the work [16] engineered a concealed attack using generative adversarial network and perceptual losses for a potent watermarking. Apart from that, the research [17] did a novel stereoscopic image description using the theory of Trinion fractional-order continuous orthogonal moments. An other study [18] developed a 3D model encryption method using 2D chaos map built through the fusion of semi-tensor product (STP) theory, infinite collapse (2D-LAIC) and logistic map. Moreover, XOR and STP processing were applied to the factional and integral part in order ot build a 3D model of the floating-point data type. Simulation results demonstrated that the suggested model contains good performance and effectiveness. The work [19] suggested an audio encryption algorithm using the theory of chaos namely AEA-NCS. Besides, a 2D-Logistic-nested-infinite-collapse (2D-LNIC) was developed through the combination of logistic map and infinite collapse map (1D-ICM). Apart from that, 2D-LNIC has nice chaotic features of attractor phase diagram and Lyapunov exponent. The job of the 2D-LNIC is spawning the keystream of random numbers. Evaluation results showed that AEA-NCS reduced the correlation of audio information in a marked way.

Cryptanalysis is a parallel project in which the exisiting ciphers are inspected for the possible lacunas, loopholes and other shortcomings in their design principles. Image ciphers are no exception. Many image ciphers have also been cracked and cryptanalyzed as the literature review indicates. For instance, the work given in [20] was broken by [21]. The scheme [20] was based on the multiple chaotic substitution boxes. Besides, only the confusion operation was implemented in this particular scheme. The scheme was cracked as the chosen-ciphertext and chosen-plaintext attacks were made over it. Resultantly, the secret key was retrieved. Later on, various statistical analyses were carried out to test the correctness of the data so recovered. In the same way, the encryption algorithm given in [22] was broken by the [23]. The algorithm [22] complied with the permutation-rewriting-diffusion (PRD) paradigm. This paradigm increased the potential relationship between the operations of diffusion and scrambling. Moreover, the random numbers were dependent over pixels square sum of input image. The loopholes identified by [23] were two in number. Firstly, the operations of diffusion and rewriting were carried out through the modular addition which is, actually equivalent to the single step diffusion. Secondly, the diffusion matrix and the rewriting parameters were independent of the given plain image. The attack dynamics adopted by [23] went like this. Diffusion process was broken by subtraction operation (modulo in nature) on given deciphered image and cipher-text image consisting of zero intensity values. Besides, potential permutation mechansim was revealed through the construction of many images containing same square sum of pixels. Apart from that, possible improvements in the Ye's scheme were recommended for increasing security. Some image encryption algorithms are very time consumging as the literature indicates. For example, the scheme given in [3] takes 20.915818 seconds to complete the encryption process. The current era needs smarter, efficient and more secure ciphers. No doubt, security and efficiency are interrelated in a reciprocal fashion. As we increase the security of the ciphers, they become more time consuming.

After the careful analysis of the above discussion, this study has endeavored to provide a smarter, efficient and more secured image cipher. Further, a proper balance has been striken to satisfy both the contradictory requirements as described earlier. We have used all the 880 4 × 4 magic squares to accomplish the project of confusion. The previous studies just used one or fewer magic squares [5], [24], [25], [26] to accomplish the project. Random numbers given by chaotic system will decide a particular magic square dynamically out of the 880 candidate magic squares for the task of confusion. This act of ours would create more complications to the potential hackers and other cryptanalytic savvy in sharply delineating his/her steps. This study has formulated the following hypothesis.

H_1: The set of all Order-4, 880 magic squares would abundantly scramble the pixels of the given image and hence would render the better results than many of the published works.

Having said that, nonethless, the main contributions of the work are as follows.

- To realize greater scrambling effects and hence more secuirty, all 880 4×4 magic squares have been employed to carry out the scrambling project of the proposed image encryption scheme.
- A very good computational time of 0.9865 seconds and an information entropy of 7.9974 have been achieved.
- A proper balance has been striken in the contradictory requirements of security and efficiency as the validation metrics indicate.

Remaining article has been outlines like this. Section II describes chaotic systems and all order-4 magic squares being used in the core of the proposed algorithm. In Section III, the way random data has been spawned and proposed image encryption and decryption schemes have been developed, are explained in detail. Section IV gives a computer experimentation of the proposed algorithm by taking four color images. Security analyses and performance have been done in the Section V. Lastly, the paper ends in Section VI after covering the necessary concluding remarks and probable future prospects of research.

II. PRELIMINARIES

In this section, the necessary preliminaries will be covered a little bit, the work upon which suggested encryption and decryption algorithms depend.

A. CHAOTIC SYSTEMS

Chaotic systems are basically the realization of the classical theory of chaos [27]. This theory talks about those systems which are extremely sensitive to the initial conditions characterizing those systems. To put it in the metaphor often dubbed as the Butterfly Effect that, "If butterfly flies its wing in Brazil, it can result into a tarnado in the Texas." Using this theory as said earlier, a lot of chaotic systems and maps have been developed. These maps comprise of one to many streams of random numbers. This work has employed intertwining logistic map [2].

$$\begin{cases} x(n+1) = [\,\mu \times k_1 \times y(n) \times (1 - x(n) + z(n)]\bmod 1 \\ y(n+1) = [\,\mu \times k_2 \times y(n) + z(n) \times 1/(1+x^2(n+1))]\bmod 1 \\ z(n+1) = [\,\mu \times (x(n+1) + y(n+1) + k_3) \times \\ \qquad \sin z(n)]\bmod 1 \end{cases} \tag{1}$$

Here $n = 0, 1, 2, 3, \ldots$, $0 < \mu \leq 3.999$, $|k_1| > 33.5$, $|k_2| > 37.9$, $|k_3| > 35.7$. This 3D map is furnished with better chaotic behavior in contrast to its predecessor logistic map. Besides, this map enjoys even distribution (Figures 1a to 1c) and contains no blank windows [2]. Apart from that, the Lyapunov exponents of ILM are all positive (Figure 1d) which signals towards the better chaotic behavior.

B. All ORDER-4 MAGIC SQUARES

Magic squares [28] are studied in the recreational mathematics. A magic square is an $n \times n$ square grid populated with distinct positive integers ranging from 1 to n^2, n being the number of cells on each side. These integers follow a very interesting rule that the sum of the integers in each row, column, diagonal and anti-diagonal is equal. This sum is often dubbed colloquially as *magic sum* or *magic constant* of the concerned magic square. A square grid with n cells on each side is said to have an order n. Normally, multiple magic squares exist for the given order. In our study, we have selected magic squares of order-4. There exist 880 magic squares of order-4 [28]. Below is a typical magic square of order-4. One can verify the above stated property of these squares. The *magic sum* or *magic constant* for this magic square is 34.

$$\begin{bmatrix} 4 & 5 & 12 & 13 \\ 7 & 16 & 1 & 10 \\ 14 & 11 & 6 & 3 \\ 9 & 2 & 15 & 8 \end{bmatrix}$$

The 880 magic squares of order-4 would perform the scrambling project in the proposed image cipher as described earlier.

III. PROPOSED IMAGE ENCRYPTION SCHEME

Suggested image cryptosystem has been written for the color images of any arbitrary size of $m \times n \times 3$. Chief contribution of this work is usage of all order-4 magic squares (880 in number) for the project of scrambling in the image encryption technology. Figure 2 illustrates the flowchart of suggested cryptosystem. After the RGB/color plaintext image is submitted to the system, it gets decomposed into blue, red and green channels. Then they are joined with each other to form a big image. The size of this big image becomes $m \times 3n$. Now for $3mn$ times, a particular *magic square* out of the 880 magic squares is randomly selected. This magic square scrambles the pixel values of a randomly selected 4×4 grid of pixels out of the given grayscale image. The drudgery of compiling all order-4 magic squares has been carried out in a separate source file of the coding. This file returns a randomly selected order-4 magic square to be used for the scrambling purpose. The diffusion effects have been realized by carrying out an XOR operation between the stream of random numbers given by the chaotic map and scrambled image. The plaintext senstivity has been achieved by taking the sum of the pixel color codes for red component of the input plain RGB image. This sum value later on alters one of the keys of the four dimensional chaotic map being used in the cipher. With each different input image, different streams of random numbers will be generated. In this way, any potential threat of the chosen plaintext attack would be averted.

A. GENERATION OF THE INITIAL VALUES OF THE CHAOTIC SYSTEM

Step 1: Input the color plain image *img* of size $m \times n \times 3$. Break this color image into its red, green and blue channels. Find the sum *sum* of pixel intensity values of red plane. Update the initial value $x(0)$ of the chaotic system (1) as follows.

$$x(0) = x(0) + \frac{sum}{2^{50}} \tag{2}$$

Step 2: As the system (1) is looped $(3mn + n_0)$ times, $\{x(t)\}_{t=1}^{3mn+n_0}$, $\{y(t)\}_{t=1}^{3mn+n_0}$, $\{z(t)\}_{t=1}^{3mn+n_0}$ get spawned. The value of the variable $n_0 \geq 500$. These n_0 values are overlooked and the remaining random data have been employed.

Step 3: The random numbers generated above are not fit to the algorithm we have conceived, so x, y and z are passed to the equations (3). In this way, updated streams of random numbers named as x, y and *magic_index* have been received. We can note that one more stream of random numbers *key_image* has been generated in equations (3) out of the streams of $\{x(t)\}_{t=1}^{3mn}$, $\{y(t)\}_{t=1}^{3mn}$, $\{z(t)\}_{t=1}^{3mn}$.

$$\begin{cases} x(i) = floor(mod(abs(x(i)) - floor(abs(x(i))) \times \\ 10^{14}, m-3)) + 1, \\ y(i) = floor(mod(abs(y(i)) - floor(abs(y(i))) \times \\ 10^{14}, 3n-3)) + 1, \\ magic\_index(i) = floor(mod(abs(z(i)) - \\ floor(abs(z(i))) \times 10^{14}, 880)) + 1, \\ key\_image(i) = mod(x(i) + y(i) + z(i), 256) \end{cases} \tag{3}$$

where $1 \leq i \leq 3mn$.

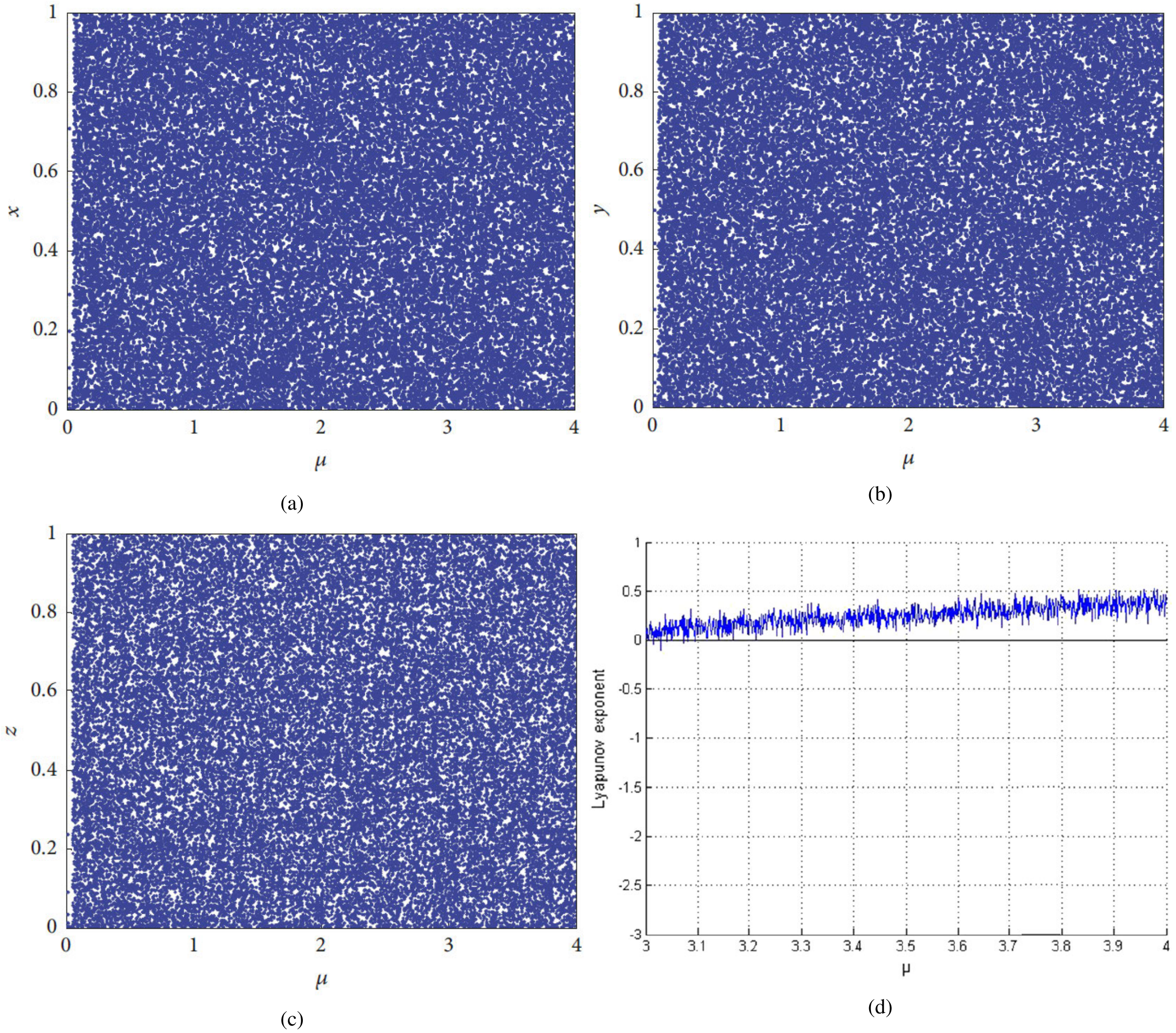
B. IMAGE ENCRYPTION PROCEDURE

Step 1:(Isolating and joining the channels of blue, red and green into a big gray scale image)

This is the assumption of this study that size of RGB image *img* is $m \times n \times 3$. Single gray scale image *img*1 of size $m \times 3n$ is obtained after the joining of channels green, red and blue colors.

Step 2: (Scrambling through magic square)

This is the "meaty" step of the proposed algorithm. The Algorithm 1, All Order-4 Magic Squares Based Scrambler



(a)

(b)

(c)

(d)

FIGURE 1. Intertwining logistic map with its streams' distribution: (a) Sequence *x* bifurcation diagram; (b) Sequence *y* bifurcation diagram; (c) Sequence *z* bifurcation diagram; (d) Lyapunov Exponents.

(AO4MSBS) has been called with the parameters $img1, x, y$ and $magic\_index$. At randomly selected starting address $(x(k), y(k))$ of the image $img1$, this algorithm scrambles the pixels of the image $img1$ with size $(x(k) : x(k) + 3, y(k) : y(k) + 3)$ using the *magic_selector* Algorithm 2 for $3mn$ times. In Step 2 of Algorithm 1, the algorithm *magic_selector* has been called with the parameter $magic\_index(k)$. As control passes to the Algorithm 2, the value of parameter $magic\_index(k)$ is copied in the variable *index* of the Algorithm 2. The variable *index* serves as an index to the *switch-case* structure of Algorithm 2. There exist 880 Order-4 magic squares, only the first two and the last one has been shown. The magic square corresponding to the variable *index* will be selected and will be returned to the calling Algorithm 1 with the variable *magic_square*. At line 3, a two-dimensional temporary array *temp* has been initialized. Now we have three entities at our disposal, *i.e.*, $img1(x(k) : x(k)+3, y(k) : y(k)+3)$, *magic_square* and *temp*. Magic square *magic_square* will act as a bridge between the entities $img1(x(k) : x(k) + 3, y(k) : y(k) + 3)$ and *temp*, *i.e.*, the pixels selected from the $img1(x(k) : x(k) + 3, y(k) : y(k) + 3)$ will be transferred to *temp* depending on the peculiar logic we have developed using the magic square. Lines(4-13) of Algorithm 1 fill the pixels selected from the $img1(x(k) : x(k) + 3, y(k) : y(k) + 3)$ to the two-dimensional array *temp*. The indices i, j of the nested loops of lines (4-5) provide all the addresses of the magic squares like (1, 1), (1, 2), (1, 3)..., (4,4). The $if - else$ selection structure of the lines (6-12) provides the row and column (row, col) of the array *temp* on which the pixel from the image

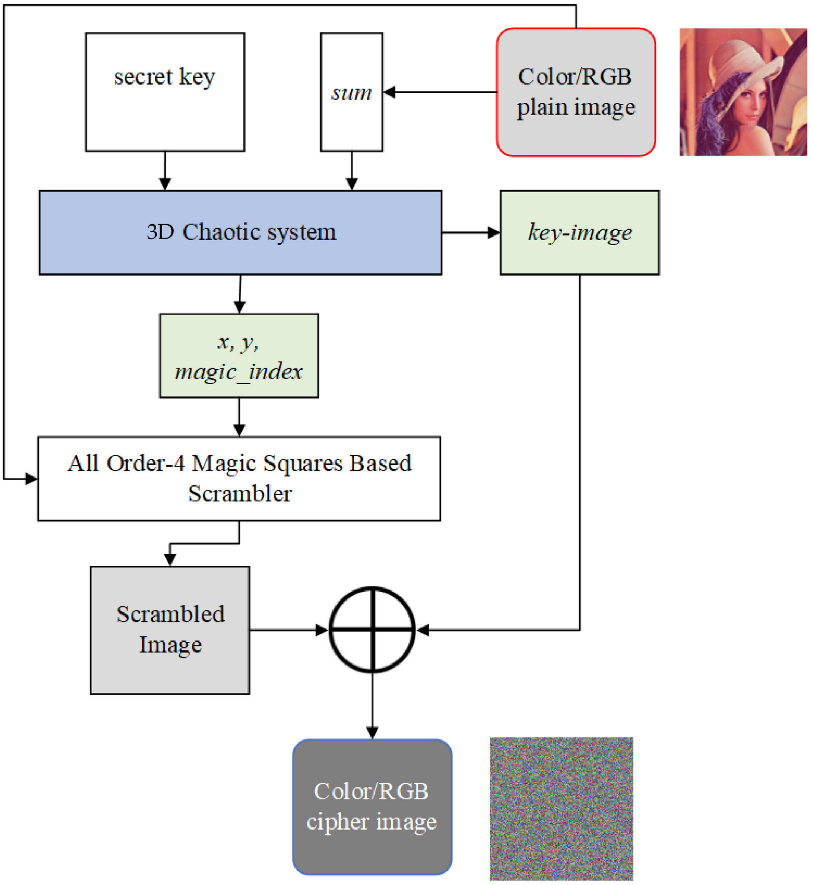


FIGURE 2. Proposed image cipher based on All Order-4 Magic Squares Based Scrambler.

$img1$ has to be transferred. If the entry $magic\_square(i,j)$ is a multiple of 4 then $(row, col) = (magic\_square(i,j)/4, 4)$ otherwise, $(row, col) = (\lfloor(magic\_square(i,j)/4\rfloor + 1, mod(magic\_square(i,j), 4)$. Lastly, the pixel of $img1$ at the address $(x(k)+i-1, y(k)+j-1$ is copied to the temporary array $temp$ at the address (row, col). After all the 16 pixels from the $img1$ are copied to the $temp$, the array $temp$ is copied to the $img1$ at the address $(x(k) : x(k)+3, y(k) : y(k)+3)$.

Step 3: (Diffusion)

Reshape the scrambled image $img2$ to the size $1 \times 3mn$. Carry out the operation of Exclusive-OR(XOR) to come up the effects of diffusion:

$$img3(i) = img2(i) \oplus key\_image(i) \qquad (4)$$

$i = 1, 2, 3, \ldots, 3mn$. Reshape $img3$ to the size $m \times 3n$.

Step 4: (Color image making)

Break the image $img3$ to its green, red and blue planes and join these planes to have a single encrypted RGB image $img4$. It is to be noted that its size will be the same as the size of input plain image, i.e., $m \times n \times 3$.

Example 1: To illustrate the lines (4-13) in a better way, here an example will be given by taking some intensity values. Figure 3 shows the four 4×4 matrices with the addresses of their entries at their subscripts. Matrix (1) is the matrix of pixel intensity values taken from the $img1$ at any address $(\{x_i\}_{i=1}^{m-3}, \{y_i\}_{i=1}^{3n-3})$. Matrix (2) is the matrix of a typical magic square generated at any of the selected magic index $(\{magic\_index_i\}_{i=1}^{3mn}$. Matrix (3) is the matrix of sixteen (16) integers. Lastly, the Matrix (4) is the resultant matrix after the pixels' data of Matrix (1) underwent the confusion effects.

C. IMAGE DECRYPTION PROCEDURE

Because suggested image encryption scheme has been developed through the philosophy of private key/symmetric, so the image decryption procedure will comprise of reversal of the steps of encryption procedure.

Step 1:(Breaking and mixing color channels into a big gray scale image)

Let's suppose that $m \times n \times 3$ are the dimensions of given plaintext picture img. Separate three channels of green, red and blue colors. As they are joined together with each other, the image $img1$ formed contains the size of $m \times 3n$.

Step 2: (Abolishing the effects of diffusion)

Reshape the scrambled image $img1$ to the size $1 \times 3mn$. Perform the bitwise Exclusive-OR operation to abolish effects of diffusion:

$$img2(i) = img1(i) \oplus key\_image(i) \qquad (5)$$

Algorithm 1 All Order-4 Magic Squares Based Scrambler (AO4MSBS)

```
Input: $img1, x, y, magic\_index$
Output: $img2$
for $k \leftarrow 1$ to $3mn$ do
    $magic\_square \leftarrow magic\_selector(magic\_index(k))$
    $temp \leftarrow zeros(4)$
    for $i \leftarrow 1$ to 4 do
        for $j \leftarrow 1$ to 4 do
            if $mod(magic\_square(i, j), 4) = 0$ then
                $row \leftarrow magic\_square(i, j)/4$
                $col \leftarrow 4$
            else
                $row \leftarrow \lfloor magic\_square(i, j/4) \rfloor + 1$
                $col \leftarrow mod(magic\_square(i, j), 4)$
            end if
            $temp(row, col) \leftarrow img1(x(k) + i - 1, y(k) + j - 1)$
        end for
    end for
    $img1(x(k) : x(k) + 3, y(k) : y(k) + 3) \leftarrow temp$
end for
$img2 \leftarrow img1$
```

Algorithm 2 *magic_selector*

```
Input: $index$
Output: $magic\_square$
switch $(index)$
case 1:
    $magic\_square = [1 \ 2 \ 15 \ 16; \ 12 \ 14 \ 3 \ 5; \ 13 \ 7 \ 10 \ 4; \ 8 \ 11 \ 6 \ 9]$
case 2:
    $magic\_square = [1 \ 2 \ 15 \ 16; \ 13 \ 14 \ 3 \ 4; \ 12 \ 7 \ 10 \ 5; \ 8 \ 11 \ 6 \ 9]$
    . . . . . . . . . . . . . . . . . . . . . . . .
    . . . . . . . . . . . . . . . . . . . . . . . .
    . . . . . . . . . . . . . . . . . . . . . . . .
case 880:
    $magic\_square = [7 \ 14 \ 4 \ 9; \ 15 \ 6 \ 12 \ 1; \ 2 \ 3 \ 13 \ 16; \ 10 \ 11 \ 5 \ 8]$
end switch
```

$i = 1, 2, 3, \ldots, 3mn$. $img2$ is the encrypted image only with the scrambling effects.

Step 3: (Unscrambling)

Reshape image $img2$ to the size of $m \times 3n$. Call the Algorithm 3 with the parameters $img2, x, y, magic\_index$. This algorithm nullifies the scrambling effects in the image $img2$ and returns the $img3$.

Step 4: (Color image making)

Break the image $img3$ to its red, green and blue components and mix these components to make single color/RGB plain image $img4$. Moreover, its size is $m \times n \times 3$. Of course, this is equal to the same one as that of original image's size.

IV. EXPERIMENTATION AND SIMULATION

To show the workability of the proposed image cryptosystem, here some chosen images will be taken and the practical demonstration of the image encryption and decryption algorithms will be presented. In particular, four color images of Brain, Tree, Lena and Baboon have been picked. The size of these images is 256 × 256. One can ake them from website of USC-SIPI Image Database. Besides, MATLAB 2016 version (standard 754) with 64-bit double-precision according to IEEE [29] has been employed for the machine experimentation.

To spark chaotic map for random data, system parameters and initial values taken are: $x(0) = 0.36$, $y(0) = 0.25$, $z(0) = 0.78$, $\mu = 1.5$, $k_1 = 35.5$, $k_2 = 38.2$, $k_3 = 36.0$. Figures 4, 5, 6 draw the plain input images, cipher output images and retrievedd images in a respective way. One can note that plaintext images have been thoroughly translated into the cloudy forms giving no faintest hint to the original images. This signals towards the successful idea of encryption and its implentation. Besides, these cipher images

Algorithm 3 All Order-4 Magic Squares Based Unscrambler (AO4MSBU)

```
Input: img2, x, y, magic_index
Output: img3
for $k \leftarrow 1$ to $3mn$ do
    $magic\_square \leftarrow magic\_selector(magic\_index(k))$
    for $i \leftarrow 1$ to 4 do
        for $j \leftarrow 1$ to 4 do
            if $mod(magic\_square(i, j), 4) = 0$ then
                $row \leftarrow magic\_square(i, j)/4$
                $col \leftarrow 4$
            else
                $row \leftarrow \lfloor magic\_square(i, j)/4 \rfloor + 1$
                $col \leftarrow mod(magic\_square(i, j), 4)$
            end if
            $temp(i, j) \leftarrow img2(x(k) + row - 1, y(k) + col - 1)$
        end for
    end for
    $img2(x(k) : x(k) + 3, y(k) : y(k) + 3) \leftarrow temp$
end for
$img3 \leftarrow img2$
```

$$\overset{(1)}{\begin{bmatrix} 100_{(1,1)} & 18_{(1,2)} & 203_{(1,3)} & 113_{(1,4)} \\ 143_{(2,1)} & 105_{(2,2)} & 69_{(2,3)} & 71_{(2,4)} \\ 88_{(3,1)} & 98_{(3,2)} & 101_{(3,3)} & 119_{(3,4)} \\ 212_{(4,1)} & 130_{(4,2)} & 144_{(4,3)} & 158_{(4,4)} \end{bmatrix}} \quad \overset{(2)}{\begin{bmatrix} 4_{(1,1)} & 5_{(1,2)} & 12_{(1,3)} & 13_{(1,4)} \\ 7_{(2,1)} & 16_{(2,2)} & 1_{(2,3)} & 10_{(2,4)} \\ 14_{(3,1)} & 11_{(3,2)} & 6_{(3,3)} & 3_{(3,4)} \\ 9_{(4,1)} & 2_{(4,2)} & 15_{(4,3)} & 8_{(4,4)} \end{bmatrix}}$$

$$\overset{(3)}{\begin{bmatrix} 1_{(1,1)} & 2_{(1,2)} & 3_{(1,3)} & 4_{(1,4)} \\ 5_{(2,1)} & 6_{(2,2)} & 7_{(2,3)} & 8_{(2,4)} \\ 9_{(3,1)} & 10_{(3,2)} & 11_{(3,3)} & 12_{(3,4)} \\ 13_{(4,1)} & 14_{(4,2)} & 15_{(4,3)} & 16_{(4,4)} \end{bmatrix}} \quad \overset{(4)}{\begin{bmatrix} 69_{(1,1)} & 130_{(1,2)} & 119_{(1,3)} & 100_{(1,4)} \\ 18_{(2,1)} & 101_{(2,2)} & 143_{(2,3)} & 158_{(2,4)} \\ 212_{(3,1)} & 71_{(3,2)} & 98_{(3,3)} & 203_{(3,4)} \\ 113_{(4,1)} & 88_{(4,2)} & 144_{(4,3)} & 105_{(4,4)} \end{bmatrix}}$$

FIGURE 3. An example of confusion: Matrix (1) is the randomly selected 4 × 4 matrix from the *img*1, Matrix (2) is a typical randomly selected 4 × 4 magic square, Matrix (3) is a 4 × 4 matrix for the sixteen entries, Matrix (4) is the confused matrix against the initially given Matrix (1) of the pixels data. One can see how the 16 numbers in the Matrix (1) have been scrambled in the Matrix (4). Matrices (2) and (3) have facilitated this process of scrambling. As a representative, the colors of the three integers in the input Matrix (1) have been made green. Similarly, the colors of three integers in the Matrix (2) have been made red.

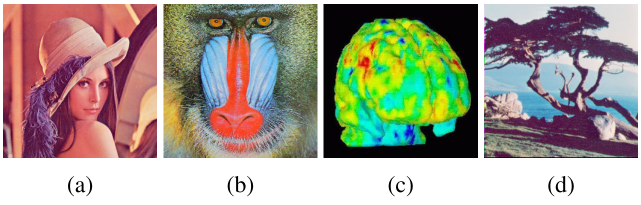

(a) (b) (c) (d)

FIGURE 4. Plaintext images: (a) Lena image; (b); Baboon image; (c) Brain image; (d) Tree image.

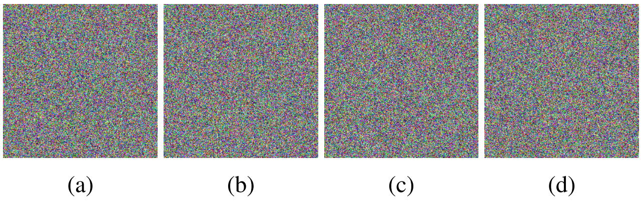

(a) (b) (c) (d)

FIGURE 5. The cipher output images: (a) Lena image; (b) Baboon image; (c) Brain image; (d) Tree image.

have been decoded into their original forms. This again validates the decryption machinery of the proposed work.

V. PERFORMANCE AND SECURITY ANALYSES

To show robustness of proposed image cryptosystem from the multifarious attacks of the hackers' community, a plethora of validation metrics have been developed. In the following subsections, few most popular will be used.

A. KEY SPACE

Brute-force attack is an attack crafted by antagonists. Dynamics of this attack goes like this. Hackers exhaust all the secret keys over the encryption algorithm in an ordered

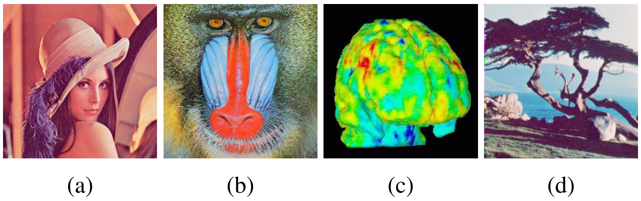


FIGURE 6. The decrypted/retrieved images: (a) Lena image; (b) Baboon image; (c) Brain image; (d) Tree image.

TABLE 1. A comparison of key space with some other schemes.

Algorithm	Key space
Ours	10^{98}
Ref. [32]	10^{195}
Ref. [31]	10^{88}
Ref. [33]	3.9402×10^{185}
Ref. [34]	10^{128}

way until the required key is identified. Its solution is a large key space. The minimum key space is 2^{100} [30] as set by the cryptographers. In this work, system parameters as well as initial values serve as key of image cipher. These system parameters and the initial values are 7. Key space becomes $10^{14\times 7} = 10^{98}$ if the number 10^{-14} is treated as the computer precision. This value is very promising to endure the threat of brute-force attack. Additionally, Table 1 makes a comparison of the key space between the proposed cipher and the ones published in the niche of image security. Our work beats studies given in [31] regarding the secuirty parameter of key space.

B. KEY SENSITIVITY

Encryption schemes which are very sensitive regarding the secret key are deemed more robust and secured. Hence, the reported feature must be cared for. This feature is shown like this. A very negligile alteration is made in secret key of cipher and output is obtained by invoking the encryption machinery. The results of the output should be radically different from those results which are obtained without making any modifications in the secret key.

We assume that $x(0), y(0), z(0), k_1, k_2, k_3, \mu$ constitute initial key set and we call it as K_0. Encryption algorithm got implemented on image of Lena (Figure 4). Now, a very negligible change 10^{-14} is done in $x(0)$ of secret key, *i.e.*, $x(0)' = x(0) + 10^{-14}$. It is to be noted that left over keys were not changed in this process. An other key set was obtained, *i.e.*, $x(0)', y(0), z(0), k_1, k_2, k_3, \mu$ and name it as K_1. Afterwards, through the usage of K_1, same image of Lena (Figure 4) has been encrypted. Apart from that, rates of difference (Table 2) were calculated between the encrypted images produced by K_0 and $K_t (t = 1, 2, \ldots 22)$. It is to be noted that keys K_0 and $K_t (t = 1, 2, \ldots 22)$ are different in a very slight way. 99.62% calculates to be average result which beats the results given in the studies [35], [36]. Therefore, suggested cipher is more sensitive to the secret key.

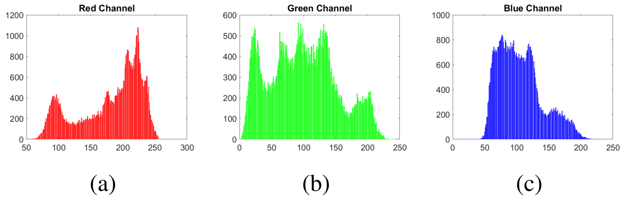


FIGURE 7. Plain Lena image histogram in different components. (a) red, (b) green, (c) blue.

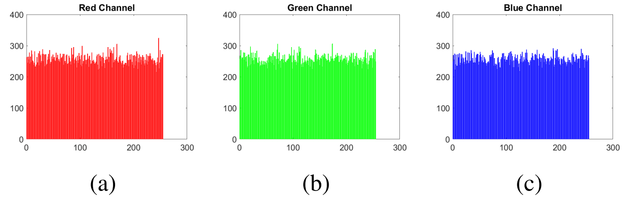


FIGURE 8. Cipher Lena image histogram in different components. (a) red, (b) green, (c) blue.

C. STATISTICAL ANALYSIS

Statistical attack is a frequently launched attack by the hackers upon the ciphers. To show the robustness of the suggested cipher against the statistical attack, two measures have been chosen in this study *i.e.*, the analyses of histogram analysis and correlation.

1) HISTOGRAM

Distribution of pixels' intensity values is depicted through an insrument called as histogram. Normally the bar of histogram of plaintext images is very slanting, running ups and downs. Such kinds of bars fascinate the cryptanaltic savvy since they are rich in the information of the image. These savvy can break the cipher through the histogram attack on it. As the image is encrypted, the ensuing histogram using cipher image has a very smooth and consistent bar which is very immune to histogram attack. Histogram analysis for the original and cipher images of Lena are shown in Figures 7 and 8 respectively. As it is very obvious from the figures that plain image has a dancing and slating bar over it. In contrast, the bar of encrypted images is much uniform and smooth in nature. This smoothness and uniformity of bar serves as a great barrier for future histogram attacks to succeed. Hence, we assert that the suggeste work is secured and robust.

Mathematicians use the notion of variance to objectively measure the value of variance for the given histogram. Small values of variance correspond to smoothness of bar and vice versa [37], [38]. Cipher images historam variance values of Baboon, Lena, Brain and Tree images are provided in Table 3. According to the table, 257.7601 has come out to be the average variance value for chosen images. Besides, our work beats the study [33]. Hence, we contend that the suggested work is efficient and secured.

2) CORRELATION COEFFICIENT ANALYSIS

Pixels of normal and plain images are strongly correlated with each other. So, thier correlation coefficient value is

TABLE 2. Difference rates between two images encrypted by slightly different keys.

Secret security keys	Difference rates(%)			
	Lena	Baboon	Brain	Tree
$Key_1(x'(0) = x(0) + 10^{-14})$	99.5963	99.6185	99.6190	99.5998
$Key_2(y'(0) = y(0) + 10^{-14})$	99.5894	99.6178	99.6039	99.6194
$Key_3(z'(0) = z(0) + 10^{-14})$	99.6043	99.5990	99.6609	99.5823
$Key_4(k_1{}' = k_1 + 10^{-14})$	99.6398	99.6187	99.6590	99.5806
$Key_5(k_2{}' = k_2 + 10^{-14})$	99.6212	99.6287	99.6390	99.6287
$Key_6(k_3{}' = k_3 + 10^{-14})$	99.6209	99.5965	99.6189	99.5909
$Key_7(\mu' = \mu + 10^{-14})$	99.6312	99.6290	99.6127	99.5936
$Key_8(x'(0) = x(0) - 10^{-14})$	99.5923	99.6134	99.6086	99.6109
$Key_9(y'(0) = y(0) - 10^{-14})$	99.6144	99.5623	99.6019	99.6094
$Key_{10}(z'(0) = z(0) - 10^{-14})$	99.6112	99.5897	99.6512	99.6016
$Key_{11}(k_1{}' = k_1 - 10^{-14})$	99.6143	99.6012	99.6698	99.6080
$Key_{12}(k_2{}' = k_2 - 10^{-14})$	99.6188	99.6298	99.6421	99.6111
$Key_{13}(k_3{}' = k_3 - 10^{-14})$	99.6297	99.6175	99.6256	99.5908
$Key_{14}(\mu' = \mu - 10^{-14})$	99.6287	99.6279	99.6164	99.6212
Average	**99.62**	**99.63**	**99.63**	**99.60**
Average of all	**99.62**	-	-	-

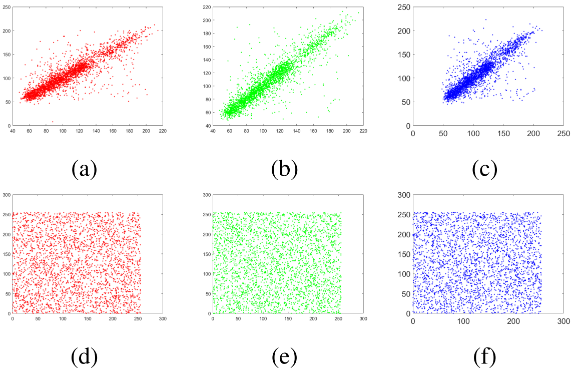
TABLE 3. Cipher images histogram varaince results.

Algorithm	Lena	Baboon	Brain	Tree	**Average**
Proposed	252.3987	266.7437	261.9081	249.9900	**257.7601**
Ref. [33]	264.37				

higher. As the plain image is submitted to image encryption algorithm, this strong correlation gets dismantled. Consequently, the coefficient value drops phenomenally. This value normally ranges from -1 to 1 inclusive. A value of zero refers that there exists no correlation among the consecutive pixels. In the same way, value of 1 or -1 indicates that the pixels are maximally correlated with each other. To show this feature of the suggested scheme, pairs of 5,000 randomly chosen pixels have been used for both the cipher and plain images. Moreover, this work was carried out in the diagonal, vertical and horizontal directions. The formula used for this purpose is (CC) [39]:

$$CC = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{\left(N\sum_{j=1}^{N} x_j^2 - \left(\sum_{j=1}^{N} x_j\right)^2\right)\left(N\sum_{j=1}^{N} y_j^2 - \left(\sum_{j=1}^{N} y_j\right)^2\right)}} \tag{6}$$

In this equation, total number of pixels contained by the image are referred to by the variable N. Besides, color values of the consecutive pixels have been denoted by x and y. Figure 9 has drawn correlation distribution of diagonally, horizontally and vertically neighboring pixels for encrypted and original Lena image. Table 4 depicts this coefficient between two adjacent pixels for cipher and plain images of Lena. According to this table, the value of this metric is almot equal to 1 against original image. Similarly, this value closes to zero for images which are encrypted/cipher. Figure 9 and the Table 4 shed light on the fact that potential relationship between the pixels of cipher and plain images has been dropped in a dramatic way.



(a) (b) (c)

(d) (e) (f)

FIGURE 9. Correlation distribution of neighboring pixels in the given channel and the image of Lena: (a) red component, horizontal, original image; (b) green component, vertical, original image; (c) blue component, diagonal, original image; (d) red component, horizontal, cipher image; (e) green component, vertical, cipher image; (f) blue component, diagonal, cipher image.

TABLE 4. Results of metric correlation coefficient.

Image	Component	Correlation direction		
		Horizontal	Vertical	Diagonal
Plain image of Lena	Red	0.9551	0.9263	0.9154
	Green	0.9503	0.9365	0.9276
	Blue	0.9423	0.9235	0.8721
Encrypted Lena image	Red	0.0023	0.0078	-0.0022
	Green	-0.0045	0.0044	0.0055
	Blue	-0.0042	0.0053	0.0023

Additionally, in order to demonstrate the superiority of the suggested work over the other published works [31], [32], [33], [34], a comparative analysis has also been made in the Table 5. No doubt, results of the suggested work are comparable.

D. RANDOMNESS ANALYSIS OF THE PROPOSED ALGORITHM

This is not sufficient just to produce the cipher images by subjecting their plain versions through some encryption algorithms. Rather, there must be some objective yardstick

TABLE 5. Comparitive analysis of correlation coefficients taking various encryption schemes.

Image	Encryption scheme	Correlation direction		
		Horizontal	Vertical	Diagonal
Plain image of Lena		0.9492	0.9288	0.9050
Encrypted Lena image	Suggested	-0.0021	0.0058	0.0019
	Ref. [32]	0.0079	-0.0054	0.0023
	Ref. [31]	-0.0082	-0.0128	-0.0012
	Ref. [33]	-0.0029	0.0013	-0.0026
	Ref. [34]	0.0007	-0.0015	-0.0007

TABLE 6. Statistical randomness results for chosen cipher images' *p* values.

Name	Lena	Baboon	Brain	Tree	Result
Frequency	0.708765	0.750987	0.599654	0.490976	Pass
Block Frequency (m = 128)	0.061987	0.045908	0.049543	0.069865	Pass
Cumulative Sums (Forward)	0.588960	0.709088	0.780970	0.783421	Pass
Cumulative Sums (Reverse)	0.820965	0.847643	0.809871	0.730976	Pass
Runs	0.070987	0.097865	0.290877	0.099342	Pass
Longest Run	0.484098	0.809865	0.929087	0.840976	Pass
Rank	0.306599	0.398564	0.865908	0.310987	Pass
FFT	0.500987	0.529800	0.718765	0.859087	Pass
Non Overlapping Template (m = 9, B = 000000001)	0.049865	0.099087	0.070987	0.200987	Pass
Overlapping Template (m = 9)	0.079087	0.099087	0.029873	0.088728	Pass
Universal	0.239808	0.209873	0.498765	0.270987	Pass
Approximate Entropy	0.798765	0.419087	0.698767	0.470745	Pass
Random Excursions	0.450987	0.590876	0.809712	0.490875	Pass
Random Excursions Variant	0.509087	0.498547	0.409887	0.909876	Pass
Serial (m = 8)	0.539879	0.790980	0.198701	0.309834	Pass
Linear Complexity	0.676287	0.489877	0.519082	0.690987	Pass

TABLE 7. Information entropy results.

Scheme	Images	Plain			Cipher			
		Red	Green	Blue	Red	Green	Blue	**Average**
Suggested	Lena	7.2507	7.5931	6.9659	7.9973	7.9973	7.9975	**7.9974**
	Baboon	7.6942	7.4637	7.7443	7.9971	7.9973	7.9974	**7.9973**
	Brain	7.2549	7.2704	6.7825	7.9973	7.9973	7.9976	**7.9974**
	Tree	7.2104	7.4136	6.9207	7.9975	7.9971	7.9974	**7.9973**
Ref. [32]	Lena							7.9975
Ref. [31]	Lena							7.9896
Ref. [33]	Lena							7.9971
Ref. [34]	Boats							7.9976

TABLE 8. Local Shannon entropy results for cipher images.

Images	Value of entropy	Outcome
Lena	7.902567	Passed
Baboon	7.902490	Passed
Brain	7.902299	Passed
Tree	7.902884	Passed

through which the intrinsic randomness among the pixels of the cipher image may be measured. Luckily NIST Test Suite [18], [19] serves this purpose. Significance level p for varied tests ought to surpass the threshold 0.01 in order to accept the randomness of bit sequences [40]. Table 6 shows the results for the four chosen images. One can note that the cipher images passed all the tests. This indicates that the pixels of the cipher images have been sufficiently randomized. This, in turn, signals towards the plausible security effects.

E. INFORMATION ENTROPY ANALYSIS

As plain image pixels are disturbed by the application of some encryption algorithm, they get scattered randomly in the entire image. To measure their arbitrariness, unpredictability and randomness, the concept of information entropy is very handy. This concept was given by Shannon [2] in the form of following mathematical formula in 1949:

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) log \frac{1}{p(m_i)} \tag{7}$$

In the above equation, information source m's entropy is being denoted by $H(m)$. Besides, $p(m_i)$ is probability of m_i. 8 comes out to be the peak value for the randomized images through the idealistic proportions with 256 gray values. Therefore, nice encryption algorithms are desired to render this value nearing to the value of 8. Results obtained can be observed in the Table 7. One can note that the average result is

TABLE 9. Average NPCR and UACI values for different images.

Images	NPCR(%)			UACI(%)		
	Red	Green	Blue	Red	Green	Blue
Lena	99.6076	99.6276	99.6160	33.5809	33.5765	33.5956
Baboon	99.6265	99.6499	99.6199	33.4759	33.4289	33.5765
Brain	99.6690	99.5678	99.6290	33.6278	33.4287	33.5576
Tree	99.5651	99.6197	99.6198	33.7289	33.4198	33.3177
Average	**99.6171**	**99.6163**	**99.6212**	**33.6034**	**33.4635**	**33.5119**
Average for all images		**99.6182**			**33.5263**	

TABLE 10. NPCR and UACI metrics and their comparison with various schemes.

Scheme	Average NPCR(%)	Average UACI(%)
Suggested	99.6171	33.5843
Ref. [32]	99.6063	33.2985
Ref. [31]	99.6090	33.4727
Ref. [33]	99.6067	33.5000
Ref. [34]	99.6200	33.6900

TABLE 11. 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 12. 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

nearly equal to 8. So, we assert that this new cipher is immune to this assault. Moreover, a comparison with other published works can be seen in the Table 7. Suggested algorithm is better than those in [31] and [33] vis-à-vis information entropy.

F. LOCAL SHANNON ENTROPY (LSE)

To fend off various assaults, an effective image encryption should randomly disperse the pixels of the provided image. The idea of local Shannon entropy serves as a more precise way to define how random the picture pixels are [41]. If we have some image *img* and t non-overlapping blocks B_1, $B_2, \ldots$, B_t with Q_C pixels are chosen arbitrarily, notion of *LSE* can be expressed as

$$\overline{H_{t,Q_C}(img)} = \sum_{i=1}^{t} \frac{H(B_i)}{t} \tag{8}$$

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

$$H(B_i) = \sum_{s=1}^{M} p(s) log \frac{1}{p(s)} \tag{9}$$

where M denotes number of pixels; $p(s)$ the probability of s^{th} value. In accordance with suggestions written in [42], two parameters (t, Q_C) are assgined the values (30, 1936). Besides, for $\alpha = 0.05$, *LSE*'s optimal value calculates to be 7.902469317 and a cipher image is thought of as passing test if the condition given in the interval $7.901901305 \leq LSE \leq 7.903037329$ is met. *LSE* results for chosen cipher images can be seen in the Table 8. All images successfully passed test of *LSE*. This indicates that the suggested image encryption algorithm has nice chaotic properties of cipher images.

G. PLAINTEXT SENSITIVITY (DIFFERENTIAL ATTACK)

Sometimes, to crack the cipher, a differential attack is planned over the ciphers. In this attack, two samples of the plain image are managed, one a simple plain image and the other with a very minute change in it, say a change of just single pixel. Now the cipher images for both of these plain images are obtained. Through a careful scrutiny of these cipher images, a hidden connection is revealed between them in the form of mathematical equation. On further manipulation, one may access the key with which the entire cipher operates. Two measures have been invented by cryptographers to cope with it. They are Unified Average Changing Intensity (*UACI*) and Number of Pixels Change Rate (*NPCR*). These measures investigate the aftermath repercussions on the cipher image as a very twist is introduced in given plaintext picture. Their mathematical formulas go like this

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{10}$$

where M and N correspond to image's dimensions. $D(i,j)$ can be defined by:

$$D(i,j) \quad = \begin{cases} 1, & if\ C(i,j) \neq C'(i,j); \\ 0, & if\ C(i,j) = C'(i,j). \end{cases} \tag{11}$$

$$UACI \ = \frac{1}{M \times N} \left[\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \right] \times 100\% \tag{12}$$

C and C' are respectively the ciphered images before and after one pixel of the plain image is changed. *NPCR* and *UACI* results of selected four images have been written in the Table 9. To get a single value, we have calculated the average values for the metrics *UACI* and *NPCR* against the channels of red, green and blue. These values are 33.5843%

TABLE 13. Critical values against NPCR randomness test.

Size	Image	NPCR value	0.05 level	0.01 level	0.001 level
256×256	Lena	99.6174	Pass	Pass	Pass
	Baboon	99.6321	Pass	Pass	Pass
	Brain	99.6219	Pass	Pass	Pass
	Tree	99.6015	Pass	Pass	Pass
512×512	Lena	99.6292	Pass	Pass	Pass
1024×1024	Lena	99.6208	Pass	Pass	Pass

TABLE 14. Critical values against UACI randomness test.

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	33.5860	Pass	Pass	Pass
	Baboon	33.4938	Pass	Pass	Pass
	Brain	33.5380	Pass	Pass	Pass
	Tree	33.4888	Pass	Pass	Pass
512×512	Lena	33.5187	Pass	Pass	Pass
1024×1024	Lena	33.4623	Pass	Pass	Pass

and 99.6171% in a respective way. The magnitude of these values have the sufficient capability to foil any threaat of differential attack. Besides, a comparative analysis has also been carried out for image of Lena with other works (Table 10). We can note that the suggested algorithm is better than [31], [32], and [33]. The Tables 11 and 12 show critical values [43] regarding the security parameters of NPCR and UACI respectively for the images with sizes 256 × 256, 512×512 and 1024×1024. In particular, critical values $N^*_{0.05}$, $N^*_{0.01}$, $N^*_{0.001}$(three significance levels) have been written in the Table 11. Its interpretation is that if the resutls of NPCR for two cryptic images evaluates to be less than N^*_α, these two encrypted images will not be randomazied with the significance of α-level. According to Table 13, for chosen images of proposed encryption scheme, values of NPCR for all levels of confidence meet critical (theoretical) benchmark of randomness test of NPCR for all sizes of 256 × 256, 512 × 512 and 1024 × 1024. As far as the parameter UACI is concerned, critical value U^*_α, comprises of two parts, i.e., U^{*+}_α and U^{*-}_α (Table 12). Null hypothesis is rejected, if UACI value does not fall between interval $(U^{*-}_\alpha, U^{*+}_\alpha)$. Table 14 vividly depicts that, given arbitrary sizes of images, values of UACI meet critical benchmarks set for the UACI randomness test.

H. CONTRAST AND ENERGY ANALYSES

Contrast analysis is an other metric to measure the intensity variations in the given image. To put it in other words, it assesses the pixels' heterogeneity in the images. Relatively higher values of this metric indicate that the images contain abundant levels of grey which, in turn, signals towards better effects of security. The validation metric contrast C for an image can be described mathematically as [44]

$$C = \sum_{g,h} |g - h|^2 \times q(g, h) \tag{13}$$

where the pair (g, h) denotes the intensity values of the given image. Apart from that, $q(g, h)$ denotes number with which gray-level co-occurrence matrices (*GLCM*) occur. Putting this in other words, it calculates the frequency with which a pixel with grayscale value g occurs in a spatial relationship to a pixel with the value of h. Table 15 depicts value of this security parameter through usage of the formula 13 against the cipher and plain images. The value 10.4872 comes out as an average value. Moreover, this value is better than 8.6448 [44]. Hence, suggested image cipher is more secured. Apart from that, an image's energy corresponds to sum of squared elements in gray level co-occurrence matrix which can be written as [44]

$$E = \sum_{g,h} q(g, h)^2 \tag{14}$$

where $q(g, h)$ refers to number of gray-level co-occurrence matrices which was mentioned before. Through this evaluation, intrinsic disorder lying in ciphertext image is measured. If this metric renders lower resutls, it indicates better encryption quality. Table 16 shows results of this security parameter for encrypted and the plain images. The table shows that for the plain images, its values are bigger. In contrast, for encrypted images, its values are smaller. Moreover, the average value comes out to be 0.0156. Besides, value 0.0156 is better than 0.165 given in the work [44]. These results once again indicate the better security effects rendered by the suggested work.

I. PEAK SIGNAL-TO-NOISE RATIO ANALYSIS

Encryption project entails the maximum difference between the two entities. These entities are cipher and plain images. Here a similarity yardstick termed as Peak-Signal-to-Noise Ratio (PSNR) is used for guaging this discrepancy between encrypted and original plain images. Mathematically, it is represented as

$$\begin{cases} PSNR = 20log_{10}(255/\sqrt{MSE})dB \\ MSE = \dfrac{1}{M \times N} \displaystyle\sum_{i=1}^{M} \sum_{j=1}^{N} (P_0(i,j) - P_1(i,j))^2 \end{cases} \tag{15}$$

In the above relationship, M and N denote the test image's size. Moreover, $P_0(i, j)$ and $P_1(i, j)$ are the pixel intensity values of plaintext and ciphertext images in a respective way. Apart from that, *MSE* stands for mean squared error. This mean squared error is magnitude of deviation between plaintext and ciphertext images. The larger value of *MSE* would cause to prodcue smaller value of *PSNR*, which in turn, augurs well for security effects. The *PSNR* values by various

TABLE 15. The results of contrast analysis.

Algorithm	Image	Plaintext		Ciphertext			
		Red	Green	Blue	Red	Green	Blue
Proposed	Lena	0.7594	1.0527	0.6394	10.4345	10.4843	10.4098
	Baboon	1.3652	1.9110	1.9198	10.5098	10.4708	10.5343
	Brain	0.6941	0.6156	0.4913	10.5143	10.5187	10.4398
	Tree	1.3287	1.2984	1.1209	10.5232	10.5209	10.4857
	Average for each component	**1.0369**	**1.2194**	**1.0429**	**10.4955**	**10.4987**	**10.4674**
	Average for all images		**1.0997**			**10.4872**	
Ref. [44]	Pepper					8.6448	

TABLE 16. The energy analysis results.

Algorithm	Image	Plaintext		Ciphertext			
		Red	Green	Blue	Red	Green	Blue
Proposed	Lena	0.1166	0.0699	0.1402	0.0156	0.0156	0.0156
	Baboon	0.0477	0.0464	0.0412	0.0156	0.0156	0.0156
	Brain	0.3286	0.2192	0.4219	0.0156	0.0156	0.0156
	Tree	1.0000	1.0000	1.0000	0.0156	0.0156	0.0156
	Average for each component	**0.4668**	**0.4656**	**0.4856**	**0.0156**	**0.0156**	**0.0156**
	Average for all images		**0.4727**			**0.0156**	
Ref. [44]	Pepper					0.165	

TABLE 17. PSNR results: 'O-C' denotes original and cryptic images; 'O-D' denotes original and decrypted images.

		Lena	Baboon	Brain	Tree
Ours	PSNR (O-D)	∞	∞	∞	∞
	PSNR (O-C)	8.7289	8.7654	7.9654	8.9950
Ref. [45]	PSNR (O-D)	96.2956			
	PSNR (O-C)	9.0348			
Ref. [47]	PSNR (O-C)	8.6878			
Ref. [46]	PSNR (O-C)	9.0486			

TABLE 18. The *MAE* results.

Image	MAE		
	Red	Green	Blue
Lena	84.2547	79.7435	71.2534
Baboon	75.6564	70.8223	78.3545
Brain	105.8223	108.1034	107.4454
Tree	77.7459	87.0987	81.9087
Average for each component	**85.8698**	**86.4420**	**84.7405**
Average for all images		**85.6841**	
Ref. [48]		79.354	

published schemes have been shown in Table 17. As the table shows, its value is infinite (∞) for the decrypted/restored and original plaintext image. This means that the decrypted image is verbatim to the original image because of $MSE = 0$. We can, moreover, infer that suggested cryptosystem is lossless. Besides, in terms of the similarity between cipher and original plain images, the *PSNR* results for the image of Lena through the proposed cipher is the best when it is compared with other works [45], [46]. Hence, we assert that suggested scheme is furnished with better effects of security.

J. MEAN ABSOLUTE ERROR (MAE)

Cryptographers and mathematicians have come up with a plethora of validation metrics to objectively assess their products. Mean absolute error is one of them. It measures deviation between two entities. These entities correspond to output cipher image and input plain image. Its mathematical description is

$$MAE_{R,G,B} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |C_{R,G,B}(i,j) - P_{R,G,B}(i,j)| \tag{16}$$

In the above equation, the cipher and plain images have been referred to by C and P in a respective way. Besides, M and N denote the dimensions of the images. Bigger value of *MAE* is better for effects of security. Table 18 gives results of *MAE* produced by our algorithm. We can see that the proposed cipher has rendered the better result than the one given in [48].

K. NOISE AND DATA LOSS THREATS

Real world is characterized by a lot of dangers and other uncertainities. In some situations, the cipher images suffer from the attacks like noise and data loss. The ciphers enduring these attacks witness more credibility in the sight of academicians and the practitioners. So foiling these two attacks should be an inbuilt feature of the nice image cryptosystems. Noise is occasionally added to the cipher images during their storage or transmission from one point to the other. In order to show robustness of suggested cipher vis-a-vis noise attack, noise densities of 0.1 and 0.2 have been mixed in the Lena and Baboon cipher images as shown in the Figures 10a and 10b. Upon applying the decryption algorithm upon these contaminated two images, the results have been depicted in Figures 10c and 10c. Clearly, the original visual information of these images is intact.

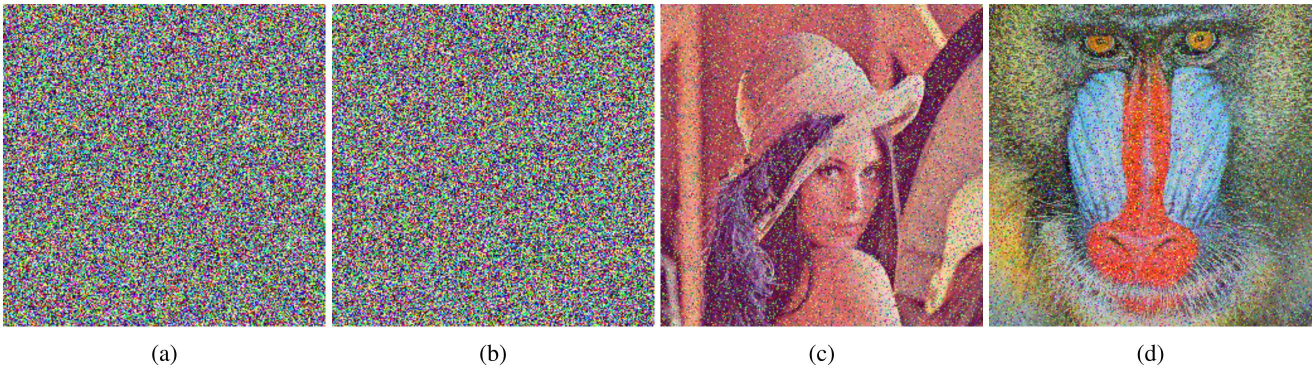

(a) (b) (c) (d)

FIGURE 10. Pepper & Salt noise attack:(a) Noise density 0.1 added in cipher Lena image; (b) Noise density 0.2 added in cipher Baboon image; (c) The retrieved/decoded image from (a); (d) The retrieved/decoded image from (b).

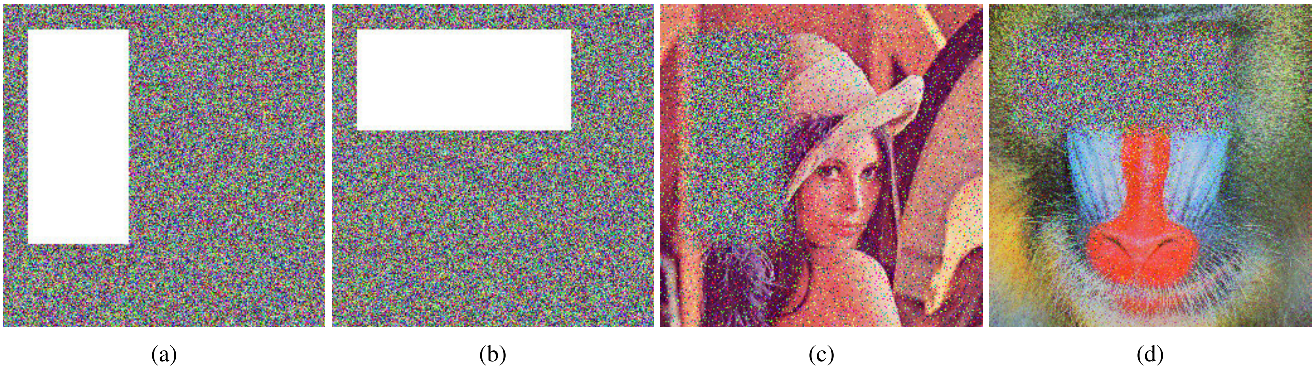

(a) (b) (c) (d)

FIGURE 11. Demo of immunity of data loss attack: (a) data loss of 170 × 80 in cipher Lena; (b) data loss of 80 × 170 in cipher Baboon image; (c) Decrypted Lena image from (a); (d) Decrypted Baboon image from (b).

Data loss/crop attack is also observed sometimes in the real world settings. As the cipher images are sent to the recipients, they come under the attack of data loss due to which problems may arise upon their retrieval through the decryption algorithm. Figures 11a and 11b plot the encrypted Lena and Baboon images with data cropping of 170 × 80, 80 × 170 respectively. In order show the capability of the suggested cipher for foiling this attack, these cropped images have been provided to the decryption machinery of this project.The retrieved/decoded images have been depicted in Figures 11c to 11d. We can note that the original cipher images are obvious from these figures. Hence, this is our assertion that the suggested cipher can thwart the potential crop attacks on the encrypted images during their storage or their transmission through the network.

L. COMPUTATIONAL TIME ANALYSIS

Security considerations is, no doubt, a prime concern while writing some cryptographic product. The ciphers having relatively lesser response time see more probability for the application in the real world. This project has been completed under settings of Intel(R) Core(TM) i5-4210U CPU @ 1.70 GHz 2.40 GHz. Additionally, 8 GB memory was utilized. Additinionally, the tool used was MATLAB R2016a and the underlying operating system was Windows 10.

TABLE 19. Encryption speed of suggested algorithm and comparison with others.

Algorithm	Image	Speed (sec)
Proposed	Lena	0.9865
	Baboon	0.9930
	Brain	1.0033
	Tree	0.9587
	Average	**0.9854**
Ref. [32]	Lena	2.5607
Ref. [49]	Lena	3.1143
Ref. [34]	-	0.067230

The Table 19 shows the computational time consumed for encrypting the given images. Besides, comparative analysis has also been made. Suggested scheme outperforms the works [32], [49].

VI. CONCLUSION

In order to boost the security effects, in this research, all order-4, 880 magic squares have been used to create the confusion effects in the big gray scale image formed by concatenating the three components of the input color plain image. Previous studies just employed a single static magic square. In contrast, we have used 880 dynamically selected random major squares for this purpose. The randomly selected magic squares have been applied on the image an arbitrary number of times. One keystream of random numbers has been used to select the magic squares out of the 880 magic squares. Two keystreams of random values decide address of gray scale image where the magic square has been applied. Diffusion effects have been created by carrying out an XOR operation between the scrambled image and the fourth stream of random numbers. To make the cipher speedier, we have not resorted to the lengthy hash codes for the introduction of the plaintext sensitivity, rather, sum of the pixels of the red component of the input color image tempers initial state of chaotic map. Simulation and performance analyses depict that the potential image cryptosystem is furnished with good security effects; it can withstand the cryptanalytic attacks and has promise for the real world application. The injection of DNA strands in the proposed algorithm for greater security effects may be one of the possible future research directions.

ACKNOWLEDGMENT

Authors would like to acknowledge the support of the Deputy for Research and Innovation Ministry of Education, Kingdom of Saudi Arabia for this research through a grant (NU/IFC/2/SERC/-/47) under the Institutional Funding Committee at Najran University, Kingdom of Saudi Arabia.

REFERENCES

[1] M. Hussain, N. Iqbal, and Z. Bashir, "A chaotic image encryption scheme based on multi-directional confusion and diffusion operations," *J. Inf. Secur. Appl.*, vol. 70, Nov. 2022, Art. no. 103347.

[2] 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.

[3] Z. Xiong, Y. Wu, C. Ye, X. Zhang, and F. Xu, "Color image chaos encryption algorithm combining CRC and nine palace map," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 31035–31055, Nov. 2019.

[4] N. Iqbal, S. Abbas, M. A. Khan, A. Fatima, A. Ahmed, and N. Anwer, "Efficient image cipher based on the movement of king on the chessboard and chaotic system," *J. Electron. Imag.*, vol. 29, no. 2, 2020, Art. no. 023025.

[5] R. H. Al-Hashemy and S. A. Mehdi, "A new algorithm based on magic square and a novel chaotic system for image encryption," *J. Intell. Syst.*, vol. 29, no. 1, pp. 1202–1215, Dec. 2019.

[6] H. Zhu, L. Dai, Y. Liu, and L. Wu, "A three-dimensional bit-level image encryption algorithm with Rubik's cube method," *Math. Comput. Simul.*, vol. 185, pp. 754–770, Jul. 2021.

[7] 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.

[8] S. A. Mehdi and A. A. Kadhim, "Image encryption algorithm based on a new five dimensional hyperchaotic system and sudoku matrix," in *Proc. Int. Eng. Conf. (IEC)*, Jun. 2019, pp. 188–193.

[9] M. Singh, A. Kakkar, and M. Singh, "Image encryption scheme based on Knight's tour problem," *Proc. Comput. Sci.*, vol. 70, pp. 245–250, Jan. 2015.

[10] N. Iqbal, R. A. Naqvi, M. Atif, M. A. Khan, M. Hanif, S. Abbas, and D. Hussain, "On the image encryption algorithm based on the chaotic system, DNA encoding, and castle," *IEEE Access*, vol. 9, pp. 118253–118270, 2021.

[11] X. Wang and S. Gao, "A chaotic image encryption algorithm based on a counting system and the semi-tensor product," *Multimedia Tools Appl.*, vol. 80, no. 7, pp. 10301–10322, Mar. 2021.

[12] W. Xingyuan, G. Suo, Y. Xiaolin, Z. Shuang, and W. Mingxu, "A new image encryption algorithm with Cantor diagonal scrambling based on the PUMCML system," *Int. J. Bifurcation Chaos*, vol. 31, no. 1, Jan. 2021, Art. no. 2150003.

[13] X. Wang, S. Gao, L. Yu, Y. Sun, and H. Sun, "Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion," *IEEE Access*, vol. 7, pp. 103662–103677, 2019.

[14] X. Wang, X. Wang, B. Ma, Q. Li, and Y.-Q. Shi, "High precision error prediction algorithm based on ridge regression predictor for reversible data hiding," *IEEE Signal Process. Lett.*, vol. 28, pp. 1125–1129, 2021.

[15] B. Ma and Y. Q. Shi, "A reversible data hiding scheme based on code division multiplexing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 9, pp. 1914–1927, Sep. 2016.

[16] Q. Li, X. Wang, B. Ma, X. Wang, C. Wang, S. Gao, and Y. Shi, "Concealed attack for robust watermarking based on generative model and perceptual loss," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 8, pp. 5695–5706, Aug. 2022.

[17] C. Wang, B. Ma, Z. Xia, J. Li, Q. Li, and Y.-Q. Shi, "Stereoscopic image description with trinion fractional-order continuous orthogonal moments," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 32, no. 4, pp. 1998–2012, Apr. 2022.

[18] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li, C. Wang, and X. Tang, "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Process.*, vol. 202, Jan. 2023, Art. no. 108745.

[19] R. Wu, S. Gao, X. Wang, S. Liu, Q. Li, U. Erkan, and X. Tang, "AEA-NCS: An audio encryption algorithm based on a nested chaotic system," *Chaos, Solitons Fractals*, vol. 165, Dec. 2022, Art. no. 112770.

[20] M. Khan, "A novel image encryption scheme based on multiple chaotic S-boxes," *Nonlinear Dyn.*, vol. 82, nos. 1–2, pp. 527–533, Oct. 2015.

[21] A. S. Alanazi, N. Munir, M. Khan, M. Asif, and I. Hussain, "Cryptanalysis of novel image encryption scheme based on multiple chaotic substitution boxes," *IEEE Access*, vol. 9, pp. 93795–93802, 2021.

[22] 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.

[23] R. Chen, L. Liu, and Z. Zhang, "Cryptanalysis on a permutation–rewriting–diffusion (PRD) structure image encryption scheme," *Multimedia Tools Appl.*, vol. 82, pp. 1–29, Jul. 2022.

[24] W. Zhong, Y. H. Deng, and K.-T. Fang, "Image encryption by using magic squares," in *Proc. 9th Int. Congr. Image Signal Process., Biomed. Eng. Informat. (CISP-BMEI)*, Oct. 2016, pp. 771–775.

[25] Y. Zhang, P. Xu, and L. Xiang, "Research of image encryption algorithm based on chaotic magic square," in *Advances in Electronic Commerce, Web Application and Communication*. Springer, 2012, pp. 103–109.

[26] J. Wang and L. Liu, "A novel chaos-based image encryption using magic square scrambling and octree diffusing," *Mathematics*, vol. 10, no. 3, p. 457, Jan. 2022.

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

[28] K. Ollerenshaw and H. Bondi, "Magic squares of order four," *Phil. Trans. Roy. Soc. London A, Math. Phys. Sci.*, vol. 306, no. 1495, pp. 443–532, 1982.

[29] W. Kahan, "IEEE standard 754 for binary floating-point arithmetic," *Lect. Notes Status IEEE*, vol. 754, no. 1776, p. 11, May 1996.

[30] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on Lorenz equation, gingerbreadman chaotic map and s8 permutation," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 3753–3765, Nov. 2017.

[31] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.

[32] N. Iqbal, M. Hanif, Z. U. Rehman, and M. Zohaib, "On the novel image encryption based on chaotic system and DNA computing," *Multimedia Tools Appl.*, vol. 81, no. 6, pp. 8107–8137, Mar. 2022.

[33] 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.

[34] T. Nestor, N. De Dieu, K. Jacques, E. Yves, A. Iliyasu, and A. A. El-Latif, "A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem," *Sensors*, vol. 20, no. 1, p. 83, Dec. 2019.

[35] 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.

[36] 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.

[37] 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.

[38] 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.
[39] 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.
[40] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Comput. Electr. Eng.*, vol. 54, pp. 471–483, Aug. 2016.
[41] 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.
[42] 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.
[43] M. Hanif, S. Abbas, M. A. Khan, N. Iqbal, Z. U. Rehman, M. A. Saeed, and E. M. Mohamed, "A novel and efficient multiple RGB images cipher based on chaotic system and circular shift operations," *IEEE Access*, vol. 8, pp. 146408–146427, 2020.
[44] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad, and M. A. Khan, "A novel image encryption based on Lorenz equation, gingerbreadman chaotic map and S_8 permutation," *J. Intell. Fuzzy Syst.*, vol. 33, no. 6, pp. 3753–3765, Nov. 2017.
[45] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, Jan. 2012.
[46] 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.
[47] 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.
[48] 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, 2014.
[49] Z. Bashir, N. Iqbal, and M. Hanif, "A novel gray scale image encryption scheme based on pixels' swapping operations," *Multimedia Tools Appl.*, vol. 80, no. 1, pp. 1029–1054, Jan. 2021.

MAHMOOD UL HASSAN received the B.S. degree (Hons.) in computer science from Hazara University, Pakistan, the M.S. degree in computer science from COMSATS University Islamabad, Pakistan, and the Ph.D. degree in computer science from the IIC University of Technology, Cambodia. He is currently an Assistant Professor with the Department of Computer Skills, Deanship of Preparatory Year, Najran University, Najran, Saudi Arabia. He has more than 40 publications in the areas of computer networks, image processing, and cloud computing in well reputed international journals and conferences. His research interests include *ad-hoc* networks, connectivity and coverage restoration in the wireless networks, image processing, and cloud computing.

ASAAD ALZAYED received the Ph.D. degree in software engineering from Lougbrough University, London, U.K. He is currently an Associate Professor with the Computer Science and Information System Department, Public Authority for Applied Education and Training, PAAET, Kuwait. He has more than 19 research publications in various international research journals and conferences. His research interests include requirements engineering, software usability, software development, and IT/business alignment.

AMIN A. AL-AWADY received the B.S., M.S., and Ph.D. degrees in computer science from the Faculty of Computer Science and Technology, Technical University of Wroclaw, Poland. He is currently an Assistant Professor with the Department of Computer Skills, Deanship of Preparatory Year, Najran University, Najran, Saudi Arabia. He has more than 15 publications in the areas of database systems, computer networks, and cloud computing in well reputed international journals and conferences. His research interests include database and distributed database systems, *ad-hoc* networks, connectivity and coverage restoration in the wireless networks, and cloud computing.

NADEEM IQBAL received the M.Phil. degree in computational science and engineering from NUST, Islamabad, Pakistan, and the Ph.D. degree in computer science from NCBA&E. He is currently an Assistant Professor with the Department of Computer Science and IT, The University of Lahore (UOL), Lahore, Pakistan. Prior to joining UOL, he worked in various academic institutions and has guided numerous undergraduate and master's students. His research interests include images cryptography, cyber security, image processing, and computer graphics.

MUHAMMAD AKRAM received the M.Sc. degree in computer science from the University of Azad Jammu & Kashmir and the M.S. degree in computer science from the Blekinge Institute of Technology, Sweden. He is currently pursuing the Ph.D. degree in ICT with Universiti Tenaga Nasional, Malaysia. He is also a Lecturer with the College of Computer Science and Information Systems (CCSIS), Najran University, Saudi Arabia. He is also the Director of the Program Accreditation Unit, CCSIS. He has more than 30 research publications in various international research journals and conferences. He is the author of two books. His research interests include human–computer interaction, web accessibility, software usability, cognitive radio, and agent-based modeling.

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 from Universiti Malaysia Terengganu, Malaysia. He is also 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 research interests include empirical software engineering (ESE), machine learning, data science, and e-learning.