Nonlinear Dyn (2023) 111:2869–2893
https://doi.org/10.1007/s11071-022-07958-7

ORIGINAL PAPER

Image encryption model based on novel magic square with differential encoding and chaotic map

Narbda Rani · Vinod Mishra ·
Suvita Rani Sharma

Received: 8 June 2022 / Accepted: 28 September 2022 / Published online: 28 November 2022

Abstract In this paper, an encryption model for the grayscale and color images based on novel magic square, and differential encoding technique along with chaotic map has been proposed. The coordinate positions of the plain image have been randomized by implementing the 2D Arnold scrambling algorithm in confusion phase. The magic square constructed by a novel approach has been used to alter the pixel values of the original image. The differential encoding technique has been introduced in the model to raise the bit-level security. Further, the piece-wise linear chaotic map has been utilized in the diffusion phase to increase randomization for increasing the complexity. The visual analysis as well as histogram and correlation coefficient analysis has been performed to test the resistance of the proposed model against different kinds of statistical, entropy, and cropping attacks. The effect of information loss of the plain image hidden in the encrypted image has been investigated by trimming the one-third and one-fourth portion of the encrypted image. The proposed model has also been tested against the differential attacks by examining the NPCR and UACI scores. A comparison of the propounded model with the other existing encryption models has also been made for validation. The results show that the proposed model is advantageous and feasible for the image encryption-related applications.

Keywords Magic square · Differential encoding · Chaotic map · Scrambling · Encryption · Decryption

1 Introduction

The recent advancements in networking and communication technologies raises the demand to store and transmit data over the network which requires improvement in the application areas concerning cryptography, cybersecurity, etc. [72]. The data transmitted and stored using open network are prone to information leakage. With the increase in volume, velocity, and veracity of the multimedia data, it becomes necessary to enhance the security, confidentiality, and privacy of the information [38,57]. The requirement of confidentiality and authenticity of the information being downloaded, uploaded, and stored is one of the major issues in cloud data storage and encryption related applications. Thus, the need for securing the information from illegal and unlicensed access becomes a necessity [8]. Cryptography is a vital technique which guarantees the privacy of secret data by converting it to an unrecog-

N. Rani (✉) · V. Mishra
Department of Mathematics, Sant Longowal Institute of Engineering and Technology, Longowal, Sangrur 148106, Punjab, India
e-mail: narmadasharma1990@gmail.com
V. Mishra
e-mail: vinodmishra.2011@rediffmail.com

S. R. Sharma
Department of Computer Science and Engineering, Sant Longowal Institute of Engineering and Technology, Longowal, Sangrur 148106, Punjab, India
e-mail: suvita.sharma1204@gmail.com

nizable form. Both images and text are converted to an unreadable form using the process of encryption [53].

Images play a significant role as an essential multimedia resource in the modern big data era which constitutes a large amount of information [30,70]. Henceforth, the maintenance of integrity and security of images have become a major concern in many fields such as military, internet communication, multimedia systems, telemedicine, e-commerce, e-learning, banking, etc. [13,56,60]. The modern cryptographic applications offer a workable solution to the persisting issues of sharing images through internet.

In general, the image encryption model is divided into two parts: confusion and diffusion [17,23]. The randomness in the pixels of plain image is introduced in the confusion process, whereas the pixel values of the image are altered in the diffusion process by using various methods [19].

Frequently, mathematics plays a vital role in various cryptographic models for enhancing the level of security [40,44,63,67]. The researchers have utilized different techniques such as chaotic maps, matrix theory, wavelet theory, numerical techniques, magic cubes, transformation theory, elliptic curves, DNA encoding, etc., for encrypting images [10,43,50,52,64]. The matrix theory fulfills the requirement by using singular value decomposition, permutation, inverse of matrices, etc., in cryptographic models [43,45,68]. Most commonly, the special type of matrices named as magic squares raise the level of randomness in the encryption models to a higher extent [41]. In addition to matrix theory, the chaos maps have been widely used by the experimenters in the image encryption algorithms because of its unpredictability and sensitivity of initial state [25,49]. The shuffling and altering of image pixels have been performed in the confusion and diffusion phases, respectively, of the encryption algorithms by using different chaotic maps [32,37]. Despite this the sensitivity of chaotic maps to parameter initialization disturbs the stability of image encryption algorithms. Thus, the chaotic maps are required to be used in combination with other components to achieve the optimum extent of stability. Moreover, it is also necessary to introduce the new methods for construction of magic squares which are capable of raising the level of randomness in the image encryption models in comparison to the existing models.

In this work, a new approach for the generation of magic square has been instigated. The flexible structural features as well as complex arrangement of the elements of a novel magic square along with chaotic map and differential encoding enlighten the way toward the field of image encryption. The proposed model has been implemented on both color as well as grayscale images. The alteration in pixel values has been performed by taking advantage of elements and properties of newly constructed magic square which enhances the reliability and feasibility of the proposed model.

The rest of paper is outlined as under: The related work is outlined in Sect. 2. The motivation behind this work is elaborated in Sect. 3. The detailed description of all the phases of the proposed encryption and decryption model along with the construction of novel magic square is given in Sect. 4. The anatomization and detailed discussions of the proposed model are presented in Sect. 5. The conclusions procured from the work are delineated in Sect. 6.

2 Related work

A square matrix of order n, in which the elements alongside each row, each column, and each of the two main diagonals are sum up to a fixed constant is known as magic square [34]. The algebraic properties of magic squares enlighten the way toward different application areas illustrated as image processing, cryptography, game theory, graph theory, and appreciably more.

The researchers represented several methods for the construction of magic squares having fabulous mathematical characteristics. Li et al. showed the construction of pandiagonal magic squares of doubly even order using magic rectangles [29]. Lee et al. gave the necessary and sufficient condition for the non-singularity of regular magic squares by virtue of centro-skew matrices [28]. Chan et al. gave the method for the construction of singular and non-singular regular classical magic squares of odd order [6]. Liu et al. proved the non-singularity of the odd-order classical regular magic square generated using the centro-skew S-circulant matrix [31]. Miranda et al. gave a method for the generation of doubly even-order magic square along with the generalization of Durer′s magic square [33]. The growing need of randomness in cryptographic models motivated the researchers to introduce reliable method for the construction of magic squares.

The various types of chaotic maps are used in combination with other components for the improvement in security of image encryption models in case of both grayscale and color images by the researchers. Shuangyuan et al. instigated the image encryption technique based on matrix transformation by locating the possible changed region [48]. Pappachan and Baby proposed image encryption model using combination of magic square and Tinkerbell maps [36]. Zhong et al. came forward with the concept of Good Lattice Point (GLP) for image encryption algorithms by modifying the pixel values using magic square operations [69]. Sowmiya et al. utilized the elements of pandiagonal magic squares in the model generated to encrypt images [51]. Farhan et al. [9] generated the keys using magic square for color image encryption. Rageed and Sadiq [39] introduced the composition of magic square along with 3D-chaotic map to encrypt and decrypt color images. Hua et al. [21] propounded a color image encryption algorithm using orthogonal Latin squares and 2D chaotic map. Wang and Liu [55] performed the image encryption by associating the octree diffusing and magic square scrambling with chaotic maps. Senthilnayaki et al. propounded a medical image encryption model based on magic square and particle swarm optimization (PSO) [47].

From the earlier work, it has been concluded that the erstwhile image encryption models lack in efficiency due to tight correlation, high redundancy, and big data stream. Also, it is necessary to introduce more mathematically rigorous method for the construction of large order magic squares. Moreover, the image encryption models based on single component along with either chaotic map or magic square are resilient in spite of the models based on combination of more than two components. Henceforth, in this paper the mathematically strong method for the generation of large order magic squares is formulated. Furthermore, this novel magic square is used in association with chaotic maps and differential encoding technique for encryption of both color as well as grayscale images. The differential encoding is utilized for the first time in encryption model to enhance the bit-level security and complexity.

3 Motivation

It has been observed from the literature that the mathematical approaches are capable of generating a more secure encryption models in comparison to any other techniques. Also, the less frequent availability of mathematically rigorous methods for the construction of large order magic squares has been noticed by us. Moreover, the magic squares are capable of generating a more secure encryption algorithm on combining with other components such as chaotic maps, scrambling techniques, DNA encoding, wavelet algorithms, etc. In addition, with growing demands it is necessary to pay attention to some techniques which are not explored yet. The differential encoding is one such technique which has not been utilized widely in spite of its great ability to provide the bit-level privacy to the encrypted data. Hence, these limitations of the benchmark models motivate us to propose an image encryption model by combining the concepts of magic square and differential encoding technique with the chaotic maps. The instigation of a novel magic square raises the level of complexity and security by making use of its elements. Also, the differential encoding technique is used to enhance the bit-level security of the proposed encryption model. Thus, the integration of chaotic map with the magic square and differential encoding in the propounded encryption model efficiently neglects all the major shortcomings of the image encryption models.

4 Proposed encryption/decryption model

The proposed model for encryption and decryption of grayscale and color images has been instigated in this paper. Figure 1 shows the block diagram of the proposed encryption model. In the proposed model the encryption process comprises of two phases: confusion and diffusion. The scrambling technique has been used in the confusion phase to randomize the image pixels. Further, the diffusion phase has been accomplished using components: magic square, differential encoding technique, and chaotic map are explained in the following subsections.

4.1 Encryption model

All the phases of the encryption model have been explained in this subsection. The proposed model has been implemented on both grayscale and color images of different sizes. The systematic arrangement of all the components of the propounded image encryption model is shown in Fig. 1.

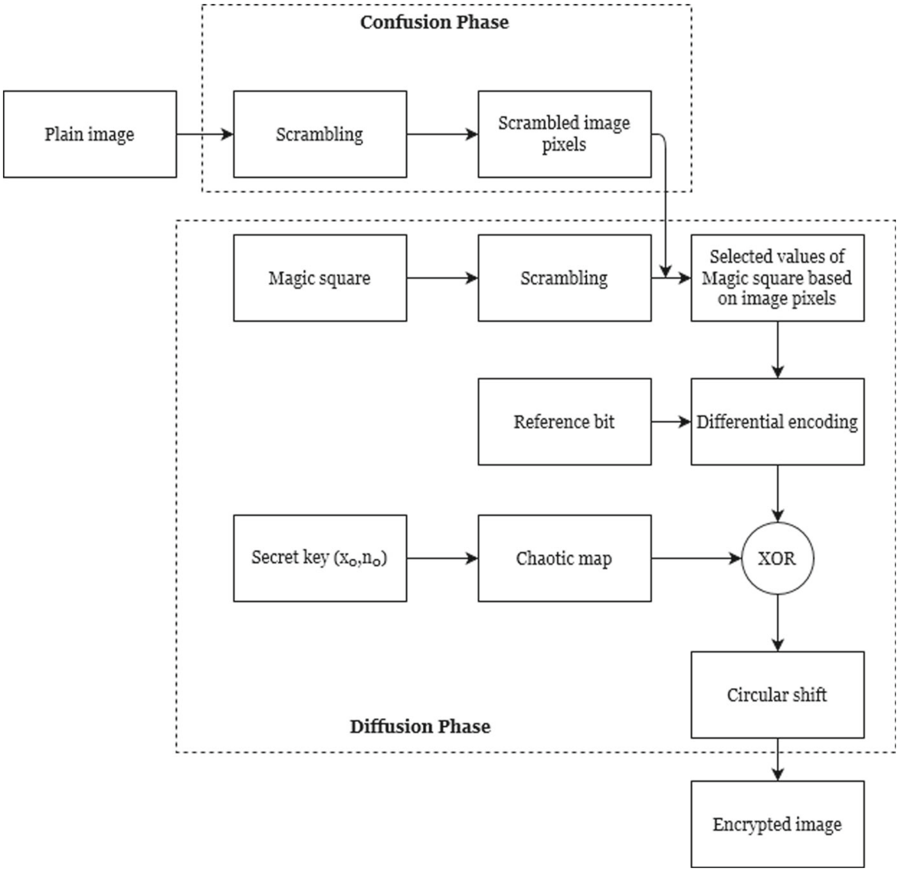


Fig. 1 Block diagram of proposed encryption model

4.1.1 Confusion phase

In this phase, the initial locations of the pixels in the plain image are changed to any other random location to increase the haphazardness at the starting point of the encryption process [17]. In the proposed encryption model the scrambling has been performed by implementing 2D Arnold map given in Algorithm 1.

Algorithm 1 Scrambling Algorithm

```
**Input:** Image ($img_{M \times N}$), where $M$ is the number of rows and $N$ is the number of columns, number of iterations ($itr$).
**Output:** Scrambling image ($scramble\_img$)
**Begin**
A=[1,1;1,2]
for $k = 1 : itr$
    for $i = 1 : M$
        for $j = 1 : N$
            $r = (A \times [i - 1; j - 1]) mod\ M$
            $scramble\_img(i, j) = img(r_1 + 1, r_2 + 1)$
        end
    end
end
```

4.1.2 Diffusion phase

The diffusion phase of encryption model is essential to alter the pixel values of the plain image for generating an encrypted image. The propounded model contains components in the diffusion phase: magic square, differential encoding technique, and chaotic map are explained as follows:

4.1.0.1 Magic square

The $n \times n$-array of n^2 numbers in which the sum of elements of each row, each column, main diagonal, and anti-diagonal is equal to a fixed constant is called as magic square and the fixed constant is termed as magic constant [42]. Mathematically, if $[a_{ij}]$ is a magic square of order n, then

$$\sum_{j=1}^{n} a_{ij} = k \ \text{ and } \ \sum_{j=1}^{n} a_{ji} = k \quad \forall \ i = 1, 2, 3, \ldots \tag{1}$$

$$\sum_{i=1}^{n} a_{ii} = k \ \text{ and } \ \sum_{i=1}^{n} a_{i,n-i+1} = k. \tag{2}$$

The utilization of magic squares in the encryption model raises the level of complexity and security of the encrypted image. Moreover, the level of security in the proposed encryption model has been escalated by combining the concept of magic square with other components. The elements of magic squares have been used to change the pixel values of the plain image in the proposed model. The doubly even-order magic square of order sixteen has been harnessed in the propounded model generated by using following novel approach:

Let us consider two sets $P = \{p_k \mid \forall\ 1 \le k \le \frac{n}{2}\}$ and $Q = \{q_l \mid \forall\ 1 \le l \le \frac{n}{2}\}$, where

$$p_k = \begin{cases} 4s+1 & \text{if } k \text{ is odd} \\ 4s+4 & \text{if } k \text{ is even} \end{cases} \quad \text{and}$$
$$q_l = \begin{cases} 4s+2 & \text{if } l \text{ is odd} \\ 4s+3 & \text{if } l \text{ is even} \end{cases} \tag{3}$$

for all $0 \le s \le \frac{n}{4} - 1$. Thus, the elements of first row of $A = [a_{ij}]_{n \times n}$ are given by

$$a_{1j} = \begin{cases} j & \text{if } j \in P \\ n^2 + 1 - j & \text{if } j \in Q \end{cases}. \tag{4}$$

Now, define

$$\delta_r = \begin{cases} n(n-r) + 1 - a_{1j} & \text{if } j \in P \\ n(n+r) + 1 - a_{1j} & \text{if } j \in Q \end{cases}$$
$$\text{for all } \ 1 \le r \le \frac{n}{2} - 1. \tag{5}$$

The filling of remaining first $\frac{n}{2} - 1$ number of rows of A, starting from second row, is performed by using the following procedure:

Let $s_1 = \{1, 2, 5, 6, \ldots\} = \{x_f \mid \forall\ 1 \le f \le \frac{n}{4}\}$ and $s_2 = \{3, 4, 7, 8, \ldots\} = \{y_g \mid \forall\ 1 \le g \le \frac{n}{4} - 1\}$ be any two sets, where

$$x_f = \begin{cases} 4h+1 & \text{if } f \text{ is odd} \\ 4h+2 & \text{if } f \text{ is even} \end{cases} \quad \text{and}$$
$$y_g = \begin{cases} 4h+3 & \text{if } g \text{ is odd} \\ 4h+4 & \text{if } g \text{ is even} \end{cases} \tag{6}$$

for $0 \le h \le \left\lfloor \frac{n}{8} - \frac{1}{2} \right\rfloor$.

Therefore, the elements of all the remaining rows starting from the second row and up to $\left(\frac{n}{2}\right)^{th}$ row are given by

$$a_{r+1,j} = \begin{cases} \delta_r & \text{if } r \in s_1 \\ n^2 + 1 - \delta_r & \text{if } r \in s_2 \end{cases}. \tag{7}$$

The elements of the lower half portion of matrix A, i.e., from $\left(\frac{n}{2} + 1\right)^{th}$ row to n^{th} row, are calculated by using the following expression

$$a_{n-i+1,j} = n^2 + 1 - a_{i,n-j+1}, \quad \text{for } \ 1 \le j \le n. \tag{8}$$

Therefore, the sum of elements of the first row (i.e. for $i = 1$) is

$$\begin{aligned} \sum_{j=1}^{n} a_{1j} &= \sum_{j \in P} j + \sum_{j \in Q} (n^2 + 1 - j) \\ &= \sum_{j \in P} j + \sum_{j \in Q} (n^2 + 1) - \sum_{j \in Q} j \\ &= \sum_{j \in Q} (n^2 + 1) \qquad \left\{ \because \sum p_k = \sum q_l \right\} \\ &= \frac{n(n^2+1)}{2}. \end{aligned} \tag{9}$$

The sum of elements of the i^{th} row, for $2 \le i \le \frac{n}{2}$, evaluated by considering two cases is given by

Case-I: when $r \in s_1$ then the row sum is

$$\begin{aligned} \sum_{j=1}^{n} a_{ij} &= \sum_{j=1}^{n} a_{r+1,j} \\ &= \sum_{j=1}^{n} \delta_r = \sum_{j \in P} \{n(n-r) + 1 - a_{1j}\} \\ &\quad + \sum_{j \in Q} \{n(n+r) + 1 - a_{1j}\} = (n^2 + 1) \\ &\quad \sum_{j \in P} (1) + (n^2 + 1) \sum_{j \in Q} (1) \\ &\quad - nr \sum_{j \in P} (1) + nr \sum_{j \in Q} (1) \\ &\quad - \left(\sum_{j \in P} a_{1j} + \sum_{j \in Q} a_{1j} \right) \\ &= (n^2 + 1) \left(\frac{n}{2}\right) + (n^2 + 1) \left(\frac{n}{2}\right) \\ &\quad - nr \left(\frac{n}{2}\right) + nr \left(\frac{n}{2}\right) \\ &\quad - \left(\sum_{j \in P} j + \sum_{j \in Q} (n^2 + 1 - j) \right) \qquad \{\text{from } (9)\} \end{aligned}$$

$$= \frac{n(n^2+1)}{2}. \tag{10}$$

Case-II: when $r \in s_2$ then the row sum is

$$\begin{aligned}
\sum_{j=1}^{n} a_{ij} &= \sum_{j=1}^{n} a_{r+1,j} = \sum_{j=1}^{n} \left(n^2+1-\delta_r\right) \\
&= \sum_{j\in P}\{n^2+1-n^2+nr-1+a_{1j}\} \\
&\quad + \sum_{j\in Q}\{n^2+1-n^2-nr-1+a_{1j}\} \\
&= \sum_{j\in P} nr - \sum_{j\in Q} nr + \left(\sum_{j\in P} a_{1j} + \sum_{j\in Q} a_{1j}\right) \\
&= nr\sum_{j\in P}(1) - nr\sum_{j\in Q}(1) \\
&\quad + \frac{n(n^2+1)}{2} \quad \{\text{from } (9)\} \\
&= nr\left(\frac{n}{2}\right) - nr\left(\frac{n}{2}\right) \\
&\quad + \frac{n(n^2+1)}{2} = \frac{n(n^2+1)}{2}.
\end{aligned} \tag{11}$$

Next, the sum of elements of each i^{th} row, for $\frac{n}{2}+1 \le i \le n$, is

$$\begin{aligned}
\sum_{j=1}^{n} a_{ij} &= \sum_{j=1}^{n} a_{n-i+1,j} = \sum_{j=1}^{n}\{n^2+1-a_{i,n-j+1}\} \\
&= (n^2+1)\sum_{j=1}^{n}(1) - \frac{n(n^2+1)}{2} \\
&\quad \left\{\because \sum_{j=1}^{n} a_{i,n-j+1} = \sum_{j=1}^{n} a_{ij}, \right. \\
&\qquad \left. \text{for} \quad 1 \le i \le \frac{n}{2}\right\} \\
&= \frac{n(n^2+1)}{2}.
\end{aligned} \tag{12}$$

The main diagonal elements of the matrix A are defined by

$$a_{ii} = (n+1)(i-1)+1, \quad \text{for} \quad 1 \le i \le n, \tag{13}$$

and their sum is evaluated by

$$\begin{aligned}
\sum_{i=1}^{n} a_{ii} &= \sum_{i=1}^{n}\{(n+1)(i-1)+1\} \\
&= (n+1)\sum_{i=1}^{n}(i-1) + \sum_{i=1}^{n}(1) \\
&= (n+1)\left(\frac{n(n+1)}{2} - n\right) + n \\
&= \frac{n(n^2+1)}{2}.
\end{aligned} \tag{14}$$

Similarly, the anti-diagonal elements of the matrix A are defined by

$$a_{i,n-i+1} = (n-1)i+1, \quad \text{for} \quad 1 \le i \le n \tag{15}$$

and their sum is

$$\begin{aligned}
\sum_{i=1}^{n} a_{i,n-i+1} &= \sum_{i=1}^{n}\{(n-1)i+1\} \\
&= (n-1)\frac{n(n+1)}{2} + n \\
&= \frac{n(n^2+1)}{2}.
\end{aligned} \tag{16}$$

The column-wise definition of the above-constructed matrix $A = [a_{ij}]_{n\times n}$ is given below:

For $j = 1$, the elements of matrix A are given by

$$a_{i1} = \begin{cases} n(i-1)+1 & \text{if} \;\; i \in P \\ n(n+1-i) & \text{if} \;\; i \in Q \end{cases} \tag{17}$$

and their sum is

$$\begin{aligned}
\sum_{i=1}^{n} a_{i1} &= \sum_{i\in P}\{n(i-1)+1\} \\
&\quad + \sum_{i\in Q}\{(n^2+1)-n(i-1)-1\} \\
&= n\sum_{i\in P}(i-1) + \sum_{i\in P}(1) + (n^2+1) \\
&\quad \sum_{i\in Q}(1) - n\sum_{i\in Q}(i-1) - \sum_{i\in Q}(1) \\
&= n\left(\frac{n(n+1)}{4} - \frac{n}{2}\right) + \frac{n}{2} + \frac{n(n^2+1)}{2} \\
&\quad -n\left(\frac{n(n+1)}{4} - \frac{n}{2}\right) - \frac{n}{2} \\
&= \frac{n(n^2+1)}{2}.
\end{aligned} \tag{18}$$

For $2 \le j \le \frac{n}{2}$, the elements of the matrix A are defined by

$$a_{ij} = a_{i,r+1} = \begin{cases} n^2+1-\delta'_r & \text{if} \;\; r \in s_1 \\ \delta'_r & \text{if} \;\; r \in s_2 \end{cases} \tag{19}$$

$$\text{where,} \quad \delta'_r = \begin{cases} a_{i1}+r & \text{if} \;\; i \in P \\ a_{i1}-r & \text{if} \;\; i \in Q \end{cases} \tag{20}$$

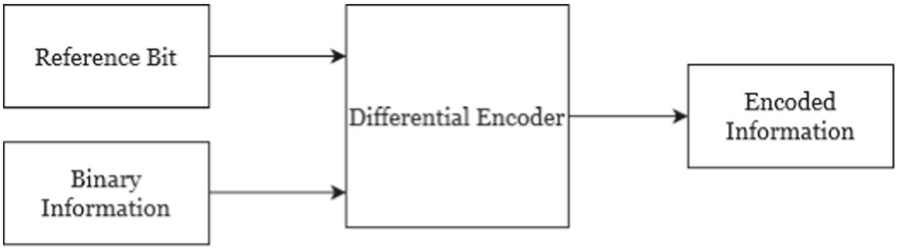


Fig. 2 Block diagram of differential encoding technique

and s_1, s_2, P, Q, r are same as defined previously and their sum is evaluated as below:

Case-I: when $r \in s_1$ then the sum of elements of each column is

$$\begin{aligned}\sum_{i=1}^{n} a_{ij} &= \sum_{i=1}^{n} a_{i,r+1} = \sum_{i=1}^{n}\{(n^2+1)-\delta'_r\}\\ &= (n^2+1)\sum_{i=1}^{n}(1) - \sum_{i\in P}(a_{i1}+r)\\ &\quad -\sum_{i\in Q}(a_{i1}-r)\\ &= n(n^2+1) - \frac{n(n^2+1)}{2} - r\left(\frac{n}{2}\right)\\ &\quad +r\left(\frac{n}{2}\right) = \frac{n(n^2+1)}{2}.\end{aligned} \tag{21}$$

Case-II: when $r \in s_2$ then the sum of elements of each column is

$$\begin{aligned}\sum_{i=1}^{n} a_{ij} &= \sum_{i=1}^{n} a_{i,r+1} = \sum_{i=1}^{n}\delta'_r\\ &= \sum_{i\in P}(a_{i1}+r) + \sum_{i\in Q}(a_{i1}-r)\\ &= \left(\sum_{i\in P} a_{i1} + \sum_{i\in Q} a_{i1}\right) + \sum_{i\in P} r - \sum_{i\in Q} r\\ &= \frac{n(n^2+1)}{2} + r\left(\frac{n}{2}\right)\\ &\quad -r\left(\frac{n}{2}\right) = \frac{n(n^2+1)}{2}.\end{aligned} \tag{22}$$

Now, for $\frac{n}{2}+1 \le j \le n$, the elements of the above-generated matrix A are given by

$$a_{i,n-j+1} = (n^2+1) - a_{n-i+1,j}\ \text{, for }\ 1 \le i \le n \tag{23}$$

and their sum is

$$\begin{aligned}\sum_{i=1}^{n} a_{ij} &= \sum_{i=1}^{n} a_{i,n-j+1} = \sum_{i=1}^{n}\{(n^2+1) - a_{n-i+1,j}\}\\ &\quad \left\{\because \sum_{i=1}^{n} a_{n-i+1,j} = \frac{n(n^2+1)}{2},\right.\\ &\quad \left.\text{for }\ 1 \le j \le \frac{n}{2}\right\}\\ &= (n^2+1)n - \frac{n(n^2+1)}{2} = \frac{n(n^2+1)}{2}.\end{aligned} \tag{24}$$

Hence, the matrix A constructed above is a magic square with magic sum $\frac{n(n^2+1)}{2}$.

Algorithm 2 for the construction of above-introduced new class of doubly even-ordered magic square is as under:

Algorithm 2 Construction Algorithm

```
Input: Order $n(= 4m)$ of magic square $A = [a_{ij}]_{n\times n}$.
Output: Magic square $A$ of order $n$.
Begin
for $s = 0 : n/4 - 1$
    for $k = 1 : n/2$
        if $k$ is even
            $p_k = 4s + 4$
        else
            $p_k = 4s + 1$
        end
        $P = [p_k]$
    end
end
for $s = 0 : n/4 - 1$
    for $l = 1 : n/2$
        if $l$ is even
            $q_l = 4s + 3$
        else
            $q_l = 4s + 2$
        end
        $Q = [q_l]$
    end
end
for $h = 0 : \lfloor \frac{n}{8} - \frac{1}{2} \rfloor$
    for $f = 1 : n/4$
        if($f\ mod\ 2 = 0$)
```

```
            $x_f = 4h + 2$
        else
            $x_f = 4h + 1$
        end
        $s_1 = [x_f]$
    end
end
for $h = 0 : \lfloor \frac{n}{8} - \frac{1}{2} \rfloor$
    for $g = 1 : \frac{n}{4} - 1$
        if($g \ mod \ 2 = 0$)
            $y_g = 4h + 4$
        else
            $y_g = 4h + 3$
        end
        $s_2 = [y_g]$
    end
end
for $j = 1 : n$
    if($j \in P$)
        $a_{1j} = j$
    else
        $a_{1j} = n^2 + 1 - j$
    end
end
for $r = 1 : (\frac{n}{2} - 1)$
    for $j = 1 : n$
        if($j \in P$)
            $\delta_r = n(n - r) + 1 - a_{1j}$
        else
            $\delta_r = n(n + r) + 1 - a_{1j}$
        end
    end
end
for $r = 1 : (\frac{n}{2} - 1)$
    for $j = 1 : n$
        if ($r \in s_1$)
            $a_{r+1,j} = \delta_r$
        else
            $a_{r+1,j} = n^2 + 1 - \delta_r$
        end
    end
end
for $i = (\frac{n}{2} + 1) : n$
    for $j = 1 : n$
        $a_{ij} = n^2 + 1 - a_{n-i+1,n-j+1}$
    end
end
```

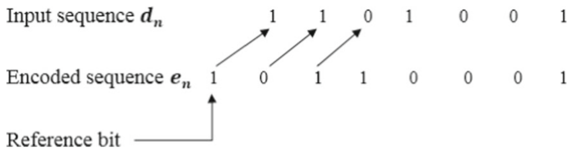


Fig. 3 Illustration of differential encoding technique used in encryption model

4.1.0.2 Differential encoding technique

The differential encoding technique is implemented to impart unambiguous signal reception. In this technique, the previous reference bit is XOR with next bit in the sequence to hide the bit information of the plain image [73]. In this paper, it has been applied to encode the elements of the magic square which raises the level of security and complexity of the encrypted image. The encoding and decoding formulas used in implementation of this technique have been given below:

$$e_n = d_n \oplus e_{n-1} \tag{25}$$

$$\tilde{d_n} = \tilde{e_n} \oplus \tilde{e}_{n-1} \tag{26}$$

where d_n, e_n, $\tilde{d_n}$ and $\tilde{e_n}$ are the input, encoded, receiver and decoded sequences.

The block diagram of the differential encoding technique is depicted in Fig. 2. The examples of the sequence employed in the encryption and decryption model generated by this technique are demonstrated in Figs. 3 and 4.

4.1.0.3 Chaotic map

The random behavior, vulnerability, and susceptibility features of the chaotic maps increase their demand in the image encryption models [11]. The sequences generated using Piece-wise Linear Chaotic Map (PWLCM) alter the pixel values of the plain image to a high extent. Moreover, the chaotic maps generate different sequences each time for the same image which makes it hard for the intruders to fetch any information related to the plain image from the encrypted image. Two secret keys n_0 (control parameters) and x_0 (initial value) are used for the generation of chaotic sequences.

The complete utilization of the above components in the encryption model is outlined in Algorithm 3 as under:

Algorithm 3 Encryption Algorithm

```
Input: Color ($img_{M\times N\times l}$) or Grayscale ($img_{M\times N}$) image, Secret key $key_1(n_0, x_0)$
Output: Encrypted image ($enc\_img$)
Begin
Step 1: The pixel values of $img$ are scrambled using Algorithm 1
Step 2: Convert the 2D image array to 1D array ($img\_1D$)
Step 3: Use the secret key $key_1(n_0, x_0)$ to generate the chaotic sequence
         $X_1 = x_0$
         for $i = 2 : M \times N$
             $X_1(i) = n_0 \times X_1(i-1) \times (1 - X_1(i-1))$
         end
Step 4: To convert the continuous chaotic values into discrete values use the equation
         $X_1 = \lfloor X_1 \times 10^{14} \rfloor \; mod \; 256$
Step 5: Convert the values of $X_1$ into binary form ($bin\_X_1$)
Step 6: Generate the doubly even order magic square ($MS$) of order 16 using algorithm 2.
Step 7: Scramble the elements of magic square using Algorithm 1 and convert it into 1D array ($m\_square$)
Step 8: for $i = 1 : M \times N$
     (a) $bin\_sq(i)$=binary value of ($m\_square$ ($img\_1D(i) + 1$))
     (b) Generate encrypted values ($enc$) by applying differential encoding in the values $bin\_sq(i)$ and $bin\_X_1$
     (c) Apply circular shift on $enc$ binary values and convert it into decimal values
     (d) Generate encrypted image ($e\_img$) by converting 1D array to 2D array end
Step 9: count_component=size($img$)
         if size(count_component,2)==3
             $l_1 = img(:, :, 1), l_2 = img(:, :, 2), l_3 = img(:, :, 3)$
             for $l_p, p = 1, 2, 3$
                 Repeat Steps 1 to 8
                 $c_p = e\_img$
             end
             $enc\_img_{color} = c_1 \,||\, c_2 \,||\, c_3$
         else
             $l = img$
                 Repeat Steps 1 to 8
                 $enc\_img_{gray} = e\_img$
         end
```

4.2 Decryption model

The decryption has been accomplished by applying the encryption algorithm in reverse order. Starting with the conversion of 2D encrypted image to 1D array, the reverse circular shift and XOR operation have been applied to fetch the encoded magic square values using chaotic maps in binary form. The reverse differential encoding technique is used to extract the actual selected entries of the magic square which are further used to fetch the pixel values of the plain image. The reverse scrambling algorithm has been used to restore the original positions of the pixels in the plain image from the encrypted image. The reverse of the scrambling process is depicted with the help of Algorithm 4 as below:

Algorithm 4 Reverse Scrambling Algorithm

```
Input: Scramble image ($scramble\_img_{M\times N}$), where $M$ is the number of rows and $N$ is the number of columns, number of iterations ($itr$).
Output: Unscrambling image ($unscramble\_img$)
Begin
A=[1,1;1,2]
for $k = 1 : itr$
    for $i = 1 : M$
        for $j = 1 : N$
            $r = (A \times [i-1; j-1]) mod \; M$
            $unscramble\_img(r_1 + 1, r_2 + 1) = scramble\_img(i, j)$
        end
    end
end
```

5 Results and discussions

In this paper, the proposed encryption and decryption model based on the integration of magic square and differential encoding with chaotic maps has been analyzed. The model has been investigated in MATLAB 2021a platform, on Windows 10 Pro operating system with Intel® Xenon® CPU E5-2650 v3 (2.30 GHz) and 8GB of RAM. The 20 grayscale and 10 color images have been investigated using the proposed

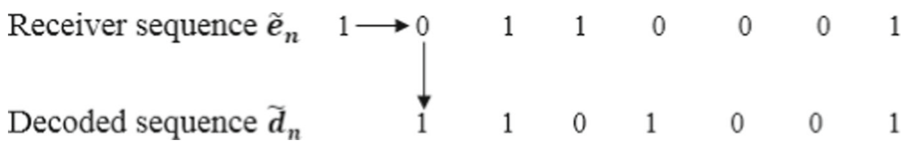

Receiver sequence $\tilde{e}_n$
1 → 0 1 1 0 0 0 1
Decoded sequence $\tilde{d}_n$
1 1 0 1 0 0 1

Fig. 4 Illustration of differential encoding technique used in decryption model

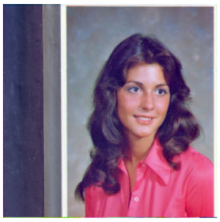
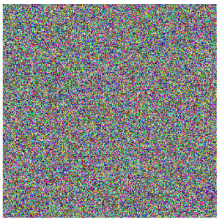
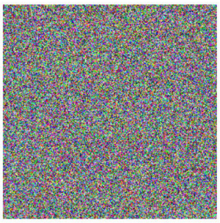
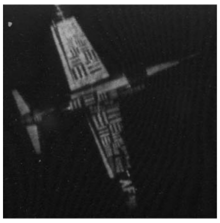
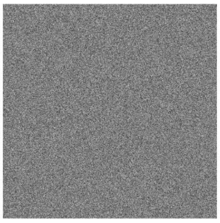
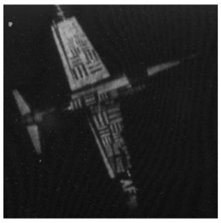
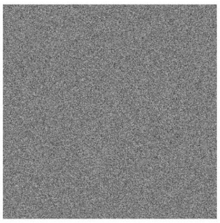
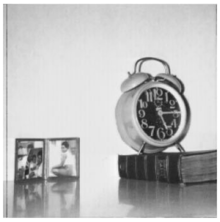
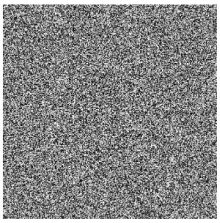
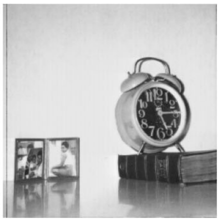
Image Name	Original Image	Encrypted Image	Decrypted Image
4.1.04			
4.1.05			
7.2.01			
5.3.01			
5.1.12			

Fig. 5 Encrypted and Decrypted test images

image encryption model while the results of only 17 images have been shown in the paper. The images available in USC-SIPI database have been utilized for the attestation of the propounded model [59]. The security, visual and statistical examination of the proposed model has been performed to confirm the resistance ability of the model against differential, entropy, visual, statistical, and cropping attacks. The grayscale and color images of resolution 256 × 256 pixels, 512 × 512 pixels, and 1024 × 1024 pixels have been considered for experimentation of the proposed model.

5.1 Visual analysis

The visual analysis is used to check the dissimilarity and similarity of the plain image with encrypted and decrypted image respectively. Figure 5 depicts the plain, encrypted, and decrypted grayscale and color images of different sizes using the proposed model. In case of color images, the component-wise encryption has been carried out using the proposed model. The encrypted images constitute the smooth distribution of the RGB and grayscale components. The visual inspection of the encrypted images shows that no information about structural outline of the plain image has been revealed. Also, a high visual similarity has been observed between decrypted and plain images.

5.2 Histogram analysis

The histograms invaded the demographic dissimilarity between the pixel values of the plain and encrypted images. The effectiveness of the resistance against statistical attacks of the encryption model is guaranteed by the even and smooth distribution plots [2].

In Figs. 6 and 7, the histograms of original and encrypted color and grayscale images are represented. The uneven distribution in the histogram of the plain images convey the useful information about the pixel values. The histograms of the encrypted images are uniformly distributed in the case of grayscale as well as color images which guarantee the strength of the proposed model to resist statistical attacks. The uniformity in the histograms is justified by using the chi-square test [17,23,35] to obtain the numerical results instead of visual spoofing and its values are calculated by the following formula:

$$\chi^2 = \sum_{i=1}^{N} \frac{(P_i - E_i)^2}{E_i}$$

where $E_i = \frac{MN}{256}$ and P_i represents the expected and observed frequencies of each level in the image and $i = 1, 2, 3, \ldots, 255$. Generally, for the different levels of significance the chi-square values are $\chi^2_{0.05}(255) = 293.2478$, $\chi^2_{0.01}(255) = 310.4574$ and $\chi^2_{0.1}(255) = 284.3359$.

In Table 1, the chi-square values of the encrypted image are less than the chi-square values of the plain image which proves the uniformity of histograms of encrypted images.

5.3 Key space analysis

The security of an image encryption model from the brute-force attacks is assured by the enough large size of key space. The required size of the key space must be greater than 2^{128} to resist the brute-force attacks effectively [39,46]. In the proposed image encryption model the key $k = (k_1, k_2, k_3, k_4)$ is used for the decryption process at the receiver end. Here, the sub-keys k_1, k_2, k_3, k_4 represent the size of key of the 2D Arnold

Table 1 Chi-square test values of color and grayscale test images

Image name	Type	Plain image	Encrypted image
4.1.01	Color	161648.19	247.78
4.1.02	Color	279285.98	258.29
4.1.03	Color	757390.70	257.11
4.1.04	Color	81482.60	244.15
4.1.05	Color	317258.15	252.90
4.1.08	Color	338837.91	254.36
4.2.07	Color	340999.44	247.75
5.1.09	Gray	135687.57	250.02
5.1.10	Gray	50862.54	258.48
5.1.11	Gray	220848.68	274.57
5.1.12	Gray	282061.56	241.40
5.2.08	Gray	298865.24	231.33
5.2.09	Gray	441857.81	266.74
7.1.01	Gray	1153566.31	273.24
5.3.01	Gray	709340.68	270.39
5.3.02	Gray	1974776.14	256.50
7.2.01	Gray	7199928.10	217.44

map used as scrambling technique, the size of key generated by magic square, the size of key produced by reference bits, and the size of key consisting of the parameters $n_0 = (n_1, n_2, n_3)$ as well as initial values $x_0 = (x_1, x_2, x_3)$ of the PWLCM map respectively. Further, if the size of each element of the magic square of order m is 2^b bits then the size of the sub-key k_2 is $(2^b)^{m^2}$. Also, if the computer precision is 10^{-15} then the size of key generated by each parameter and initial value in PWLCM is 10^{15} which means the size of sub-key k_4 is $(10^{15})^3 \times (10^{15})^3 \approx 2^{299}$. Hence, the total size of the key space is calculated as

$$\begin{aligned} & k_1 \times (2^b)^{m^2} \times k_3 \times (10^{15})^3 \times (10^{15})^3 \\ & \quad \approx k_1 \times (2^b)^{m^2} \times k_3 \times 2^{299} \\ & \quad = k_1 \times k_3 \times (2^{bm^2+299}) \end{aligned}$$

which is much larger than 2^{128}. This infers that the proposed model is capable of resisting brute-force attacks.

5.4 Key sensitivity analysis

The high sensitivity of the key in the encryption model guarantee the infeasibility of the brute force attack to decrypt the encrypted image. It means that the slightest changes made in the key used for decryption purpose do not allow the images to be get decrypted [4,65]. In the proposed model, the change in only a single parameter of the key $k = (k_1, k_2, k_3, k_4)$ do not allow the encrypted image to reveal any information

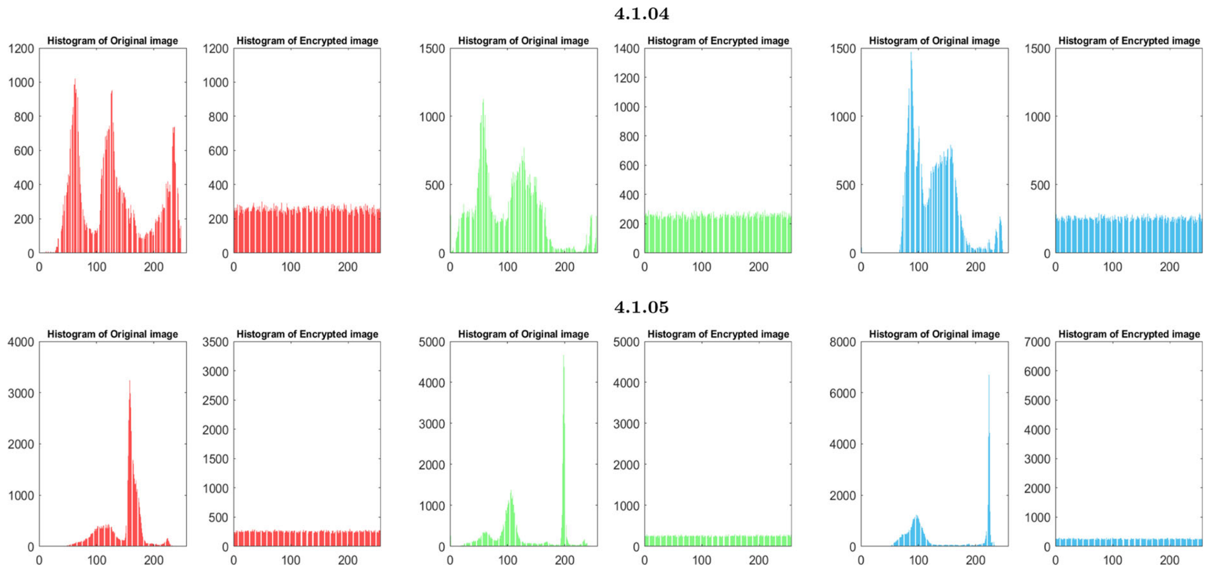


Fig. 6 Histograms of color test images

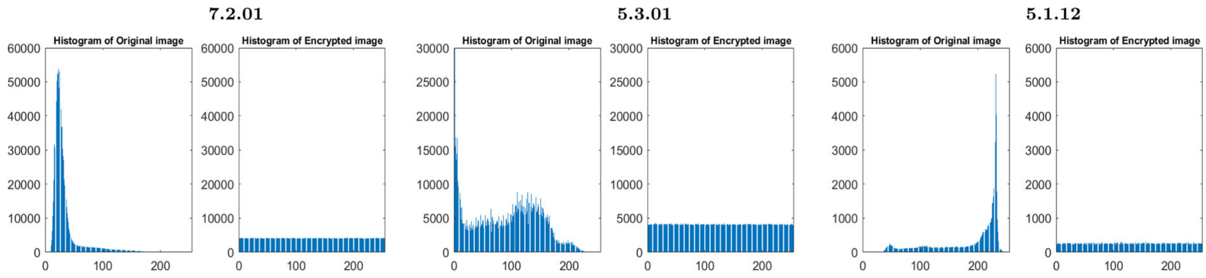


Fig. 7 Histograms of grayscale test images

related to the plain image. For instance, in case of RGB image if change the initial value $x_0 = (x_1, x_2, x_3)$ of the PWLCM from $x_1 = 0.157613081677548$, $x_2 = 0.970592781760616$, $x_3 = 0.957166948242946$ to $x_1 = 0.157613081977548$, $x_2 = 0.970592781960616$, $x_3 = 0.957166948942946$ then this modified key do not generate the original plain image. Similarly, the intruder will never be able to obtain the original plain image if two or more parameters of the key are changed. The results of the decrypted images after changing one, two and three parameters in the key of the image 4.1.04 (RGB image) and 5.1.12 (gray image) are shown in Fig. 8 which ensures that the proposed model efficiently resists the brute force attacks.

5.5 Speed analysis

The time taken for the execution of an algorithm is also a significant factor, with respect to enhanced security level. The times taken by the encryption and decryption algorithms of the proposed model are given in Table 2, in case of both grayscale and color test images. The average times taken for the encryption of grayscale images of sizes 256 × 256, 512 × 512 and 1024 × 1024 pixels are 2.3 s, 9.5 s and 38.5 s respectively. In the same way, the encryption times of 256 × 256 and 512 × 512 pixels color images are 6.75 s and 27.7 s, respectively. Also, their corresponding average decryption times in case of both grayscale as well as color images are 3.66 s, 14.95 s, 60.31 s, 11.07 s and 45.23 s. It has been concluded that the proposed model is faster in comparison to some erstwhile models [3,5,16,24,54,58,66]. Also, the proposed image encryption model is slower in comparison to the other state-of-the-art models [22,26,62,64]. The main reason is that in order to improve the encryption security of this encryption method the image is scrambled with complex chaotic map, and the alteration of image pixel values using the elements of proposed magic square, which greatly increases the encryption speed.

The comparative analysis of the average values of time taken for encryption and decryption of 256 × 256 grayscale images is represented in Table 3. The bold values indicate that the proposed model has better speed efficiency in comparison to erstwhile image encryption models. The data used for comparison of the algorithms introduced by Hu et al. [16], Wang and Liu [58], Zhan et al. [65], Chai et al. [5] has been taken from Yan et al. [62].

Table 2 Speed analysis of color and grayscale test images

Image	Type	Encryption time (in s)	Decryption time (in s)
4.1.01	Color	6.6579	11.1714
4.1.02	Color	6.8697	10.8531
4.1.03	Color	6.7266	11.1876
4.1.04	Color	6.8697	11.2047
4.1.05	Color	6.6579	10.9451
4.1.08	Color	6.7345	11.0839
4.2.07	Color	27.7834	45.0566
5.1.09	Gray	2.3498	3.6401
5.1.10	Gray	2.3713	3.6636
5.1.11	Gray	2.3765	3.6734
5.1.12	Gray	2.3537	3.6529
5.2.08	Gray	9.5224	14.7534
5.2.09	Gray	9.5346	15.3539
5.3.01	Gray	38.5357	60.9303
5.3.02	Gray	38.5562	59.7302
7.1.01	Gray	9.5179	14.7603
7.2.01	Gray	38.6883	60.2592

Table 3 A comparative analysis of average encryption and decryption speeds

Encryption model	Average encryption time (in s)	Average decryption time (in s)
Ayoup et al. [3]	7.32	–
Hu et al. [16]	14.83	14.96
Wang and Liu [58]	15.82	13.35
Zhan et al. [66]	38.39	36.98
Chai et al. [5]	10.79	10.73
Vidhya et al. [54]	10.44	–
Kumar et al. [24]	10.44	–
Proposed	**2.36**	**3.66**

5.6 Correlation coefficient analysis

The relation between the neighboring pixels of the plain and encrypted images is revealed by evaluating the correlation coefficients [12] horizontally, vertically and diagonally using the formula given below:

$$r(u, v) = \frac{\sum_{i=1}^{N}\left(\left(u_i - \frac{1}{N}\sum_{i=1}^{n} u_i\right)\left(v_i - \frac{1}{N}\sum_{i=1}^{N} v_i\right)\right)}{\sqrt{\sum_{i=1}^{N}\left(u_i - \frac{1}{N}\sum_{i=1}^{N} u_i\right)^2}\sqrt{\sum_{i=1}^{N}\left(v_i - \frac{1}{N}\sum_{i=1}^{N} v_i\right)^2}} \tag{27}$$

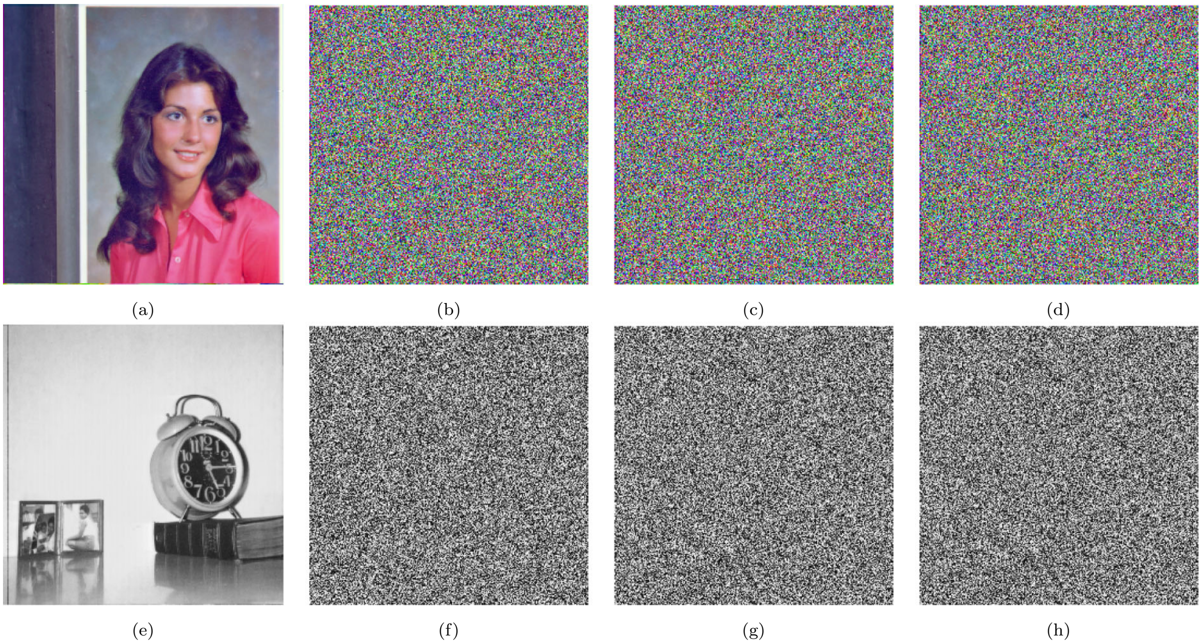


Fig. 8 **a**, **e** plain images "**4.1.04**" and "**5.1.12**"; **b**, **f** decrypted form of images with one key changed; **c**, **g** decrypted form of images with two keys changed; **d**, **h** decrypted form of images with three keys changed

where N is the size of the image and u, v are adjacent pixel values of the grayscale image or RGB components.

The average horizontal, vertical and diagonal correlation coefficients have been evaluated for both plain and encrypted images in this work. The correlation between neighboring pixels of the plain and encrypted images has been performed by randomly choosing 3000 pairs of neighboring pixels in opposite directions. The pixels value $(x + 1, y)$ with respect to the variable position (x, y) is considered for horizontal correlation. In the same way, the neighboring pixels $(x, y + 1)$ and $(x + 1, y + 1)$ have been used for vertical and diagonal correlation respectively over the value (x, y).

In Fig. 9, the average horizontal, vertical, and diagonal correlation scatter plot of the color images have been depicted. The linear relationship has been followed in the plots of plain image which infers the strong correlation between the neighboring pixel values. On the other hand, the weak correlation between the neighboring pixel values of the encrypted image in the figure shows that the statistical attacks get weaker against the proposed model.

Figure 10 represents the correlation coefficient scatter plots of the grayscale images. The plots of plain images show that the points are closely placed along the diagonal line which implies high correlation between the neighboring pixels. While the symmetrically distributed points in the plots of encrypted images depict the low correlational among the neighboring pixels. Thus, the proposed model greatly minimizes the correlation between the neighboring pixels of the encrypted image which enhances the resisting power of the proposed model against statistical attack.

The average values of correlation coefficients of the plain and encrypted images are indicated in Table 4. The negative values of the correlation coefficient of the encrypted images obtained by using the proposed model depicts the weak relationship among the neighboring pixels. This implies that the proposed model is highly resistant to statistical-based attacks.

5.7 Information entropy analysis

The distribution and randomness in the pixels of an image is measured by entropy parameter and is calculated using the formula shown as follows:

$$H(t) = \sum_{i=0}^{255} p(t_i) \log_a \left(\frac{1}{p(t_i)} \right) \tag{28}$$

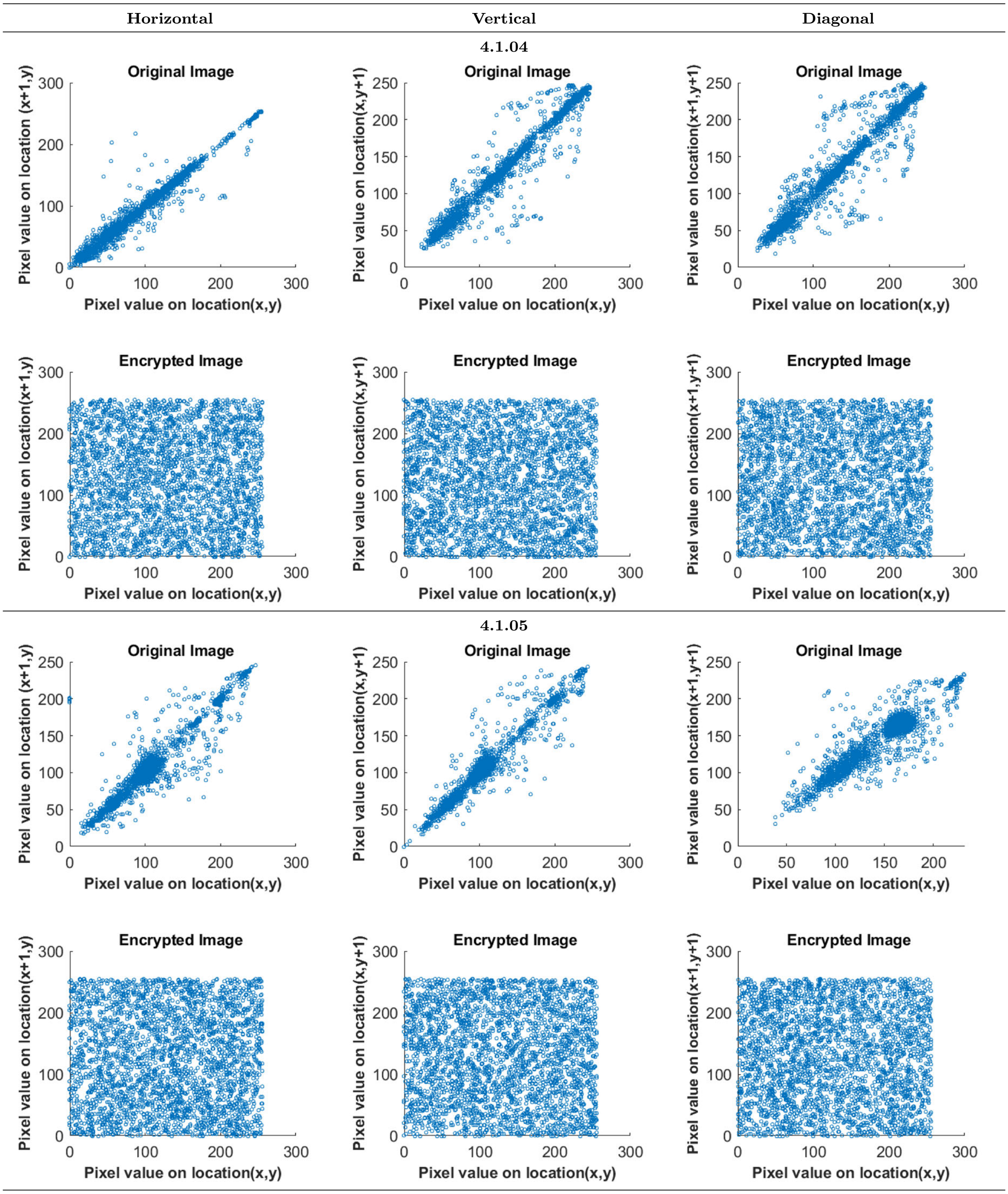


Fig. 9 Correlation between two adjacent pixels of plain and encrypted color test images

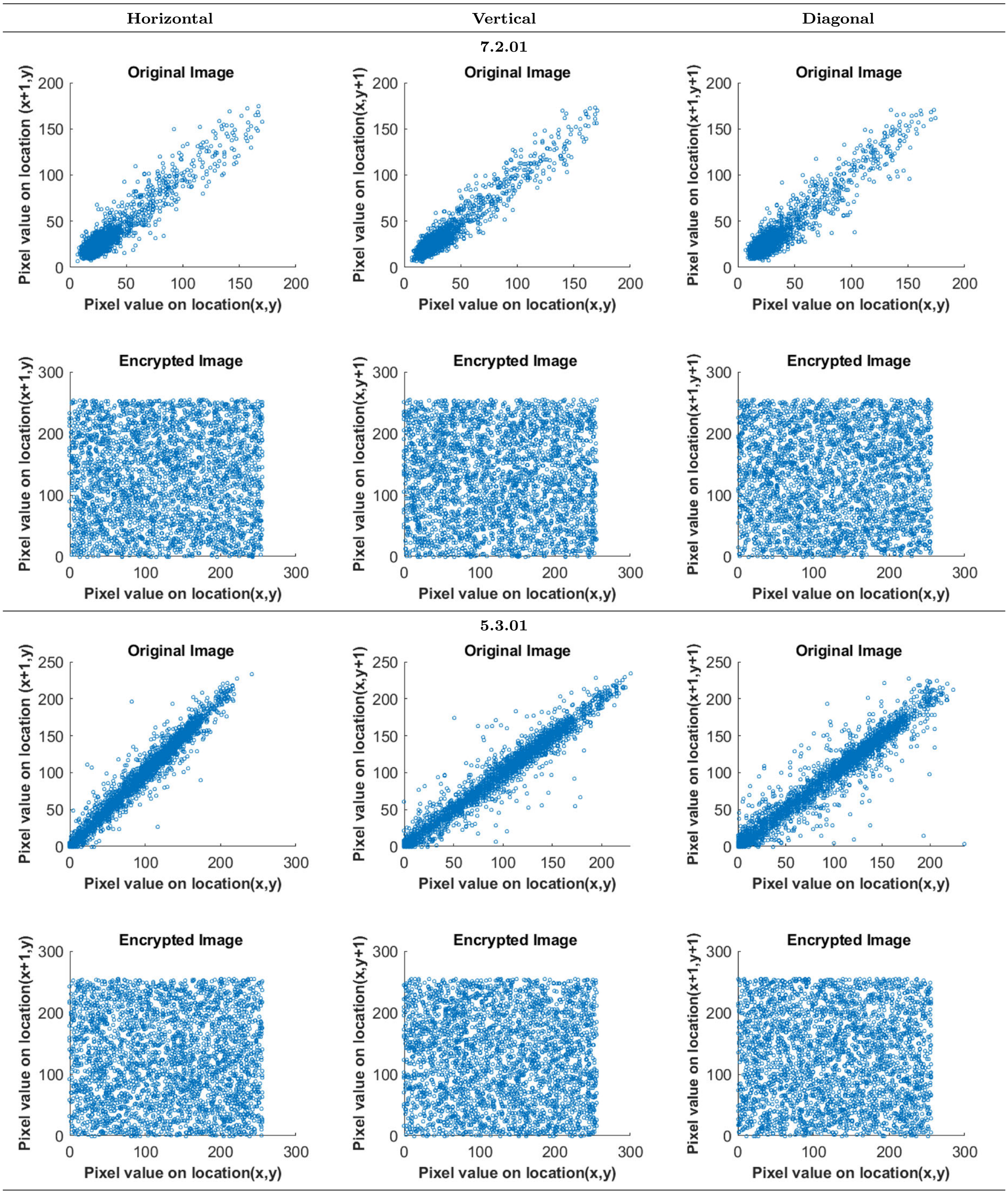


Fig. 10 Correlation between two adjacent pixels of plain and encrypted grayscale test images

Table 4 Correlation coefficients of color and grayscale test images

Image name	Type	Plain image			Encrypted image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
4.1.01	Color	0.9622	0.9729	0.9393	– 0.0042	0.0079	– 0.0361
4.1.02	Color	0.9582	0.9450	0.9184	– 0.0140	– 0.0277	– 0.0068
4.1.03	Color	0.9278	0.9391	0.8982	0.0036	– 0.0207	– 0.0101
4.1.04	Color	0.9878	0.9776	0.9669	– 0.0004	– 0.0244	– 0.0064
4.1.05	Color	0.9289	0.9667	0.9131	– 0.0024	– 0.0377	– 0.0229
4.1.08	Color	0.9396	0.9640	0.9015	– 0.0315	– 0.0072	– 0.0213
4.2.07	Color	0.9670	0.9649	0.9512	– 0.0234	– 0.0238	– 0.0014
5.1.09	Gray	0.9417	0.9009	0.8560	– 0.0071	– 0.0023	– 0.0379
5.1.10	Gray	0.8553	0.9028	0.7063	– 0.0069	– 0.0094	– 0.0039
5.1.11	Gray	0.9356	0.9526	0.9042	– 0.0274	– 0.0506	– 0.0118
5.1.12	Gray	0.9783	0.9544	0.9331	– 0.0111	– 0.0072	– 0.0306
5.2.08	Gray	0.8918	0.9194	0.8456	– 0.0129	– 0.0184	– 0.0019
5.2.09	Gray	0.8644	0.8576	0.8071	– 0.0222	– 0.0195	0.0064
7.1.01	Gray	0.9229	0.9602	0.9045	– 0.003	– 0.0100	– 0.0009
5.3.01	Gray	0.9822	0.9776	0.9652	– 0.0085	– 0.0442	– 0.0155
5.3.02	Gray	0.9022	0.9062	0.8649	– 0.0112	– 0.0251	– 0.0188
7.2.01	Gray	0.9423	0.9593	0.9448	– 0.0064	– 0.0232	– 0.0110

where t_i is the pixel value and $p(t_i)$ is its probability of occurrence in the image.

Table 5 contains the entropy values of color and grayscale images. It has been delineated that the entropy values of the encrypted images procured using the proposed model lies between 7.9970 and 7.9999 which is near to 8. Hence, in the proposed model there are very less chances of information leakage. This implies that the proposed model is less prone to statistical and entropy attacks.

The comparison of the proposed model with the erstwhile models for the entropy values is shown in Table 6. The bold values indicate the better score obtained by the proposed model which proves that the proposed model is more secure to the entropy and statistical attacks as compared to the existing models.

5.8 Differential attack

The information transmitted through open network in the form of images is prone to the differential attacks. The performance of the model against differential attack is ensured by using the two widely used parameters: NPCR and UACI. The extent of percentage of distinct pixels in the two encrypted images is measured by using NPCR (number of pixels change rate). On the other hand, UACI metric (unified averaged changed intensity) depicts the average dissimilarity between the two encrypted images. The formulas used for finding the NPCR and UACI values are as follows:

$$\mathrm{NPCR}(C_1, C_2) = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} c(i, j)}{w \times h} \tag{29}$$

$$\mathrm{UACI}(C_1, C_2) = \frac{1}{w \times h} \left(\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i, j) - C_2(i, j)|}{255} \right) \tag{30}$$

where M and N represent the width and height of the plain image, C_1 and C_2 are two encrypted images encrypted before and after one pixel change, c is the difference between the corresponding pixel values of the encrypted images C_1 and C_2, and $w \times h$ is the number of pixels in the plain image.

The NPCR and UACI values of the encrypted images using the proposed model are shown in Table 7. The values of NPCR and UACI have been analyzed for signif-

Table 5 Entropy values of color and grayscale test images

Image name	Type	Plain image	Encrypted image
4.1.01	Color	6.4155	7.9973
4.1.02	Color	6.2945	7.9990
4.1.03	Color	5.9709	7.9991
4.1.04	Color	7.4270	7.9992
4.1.05	Color	7.0686	7.9990
4.1.08	Color	6.8527	7.9990
4.2.07	Color	7.6698	7.9998
5.1.09	Gray	6.7093	7.9972
5.1.10	Gray	7.3118	7.9971
5.1.11	Gray	6.4523	7.9970
5.1.12	Gray	6.7057	7.9973
5.2.08	Gray	7.2010	7.9994
5.2.09	Gray	6.9940	7.9993
7.1.01	Gray	6.0274	7.9992
5.3.01	Gray	7.5237	7.9998
5.3.02	Gray	6.8303	7.9998
7.2.01	Gray	5.6415	7.9999

Table 6 A comparison of entropy values

Image name →	5.1.09	5.1.10	5.1.11	5.1.12	5.2.08	5.2.09	7.1.01	5.3.01	5.3.02	7.2.01
Plain entropy →	6.7093	7.3118	6.4523	6.7057	7.2010	6.9940	6.0274	7.5237	6.8303	5.6415
Encrypted entropy										
Hu and Li [15]	**7.9974**	**7.9975**	7.9971	**7.9975**	7.9993	7.9992	7.9992	7.9998	7.9998	7.9998
Alawida et al. [1]	7.9965	7.9972	7.9973	7.9954	7.9992	7.9990	7.9980	7.9993	7.9992	7.9988
Lan et al. [27]	7.9971	7.9971	7.9973	7.9968	7.9993	7.9993	7.9992	7.9998	7.9998	7.9998
Hua and Zhou [18]	7.9971	7.9971	7.9972	7.9970	7.9993	7.9993	7.9992	7.9998	7.9998	7.9998
Hua et al. [19]	7.9973	7.9972	**7.9975**	7.9968	7.9993	7.9993	7.9993	7.9998	7.9998	7.9992
Zhou et al. [71]	7.9966	7.9971	**7.9975**	7.9972	7.9991	7.9992	7.9990	7.9998	7.9996	7.9996
Wu et al. [61]	7.9972	7.9970	7.9974	7.9974	7.9993	7.9993	7.9992	7.9998	7.9998	7.9992
Proposed model	7.9972	7.9971	7.9970	7.9973	**7.9994**	**7.9993**	**7.9993**	**7.9998**	**7.9998**	**7.9999**

icance value at $\alpha = 0.05$. The proposed model pass the test results for all the images corresponding to the theoretical NPCR and UACI critical values which shows the resistance against the differential attacks.

In Table 8, juxtaposition of the proposed model with existing models is presented. The bold values of NPCR and UACI indicates the failure of the encryption models. It has been observed that the proposed model pass all the NPCR and UACI test results for the significant level at $\alpha = 0.05$. However, the existing encryption models proposed by [2], [27] and [18] do not give a test result of 100% which implies that these models can be prone to the differential attack than the rest of the models. However, the proposed scheme exhibits excellent performance by comparison, which proves the progress of this work.

Table 7 The NPCR and UACI results of color and grayscale images (significance level $\alpha = 0.05$)

Theoretical NPCR and UACI critical values [63]
256×256 $\mathrm{NPCR}^{*}_{0.05} = 0.995693$ $\mathrm{UACI}^{*-}_{0.05} = 0.332824$, $\mathrm{UACI}^{*+}_{0.05} = 0.336447$
512×512 $\mathrm{NPCR}^{*}_{0.05} = 0.995893$ $\mathrm{UACI}^{*-}_{0.05} = 0.333730$, $\mathrm{UACI}^{*+}_{0.05} = 0.335541$
1024×1024 $\mathrm{NPCR}^{*}_{0.05} = 0.995994$ $\mathrm{UACI}^{*-}_{0.05} = 0.334183$, $\mathrm{UACI}^{*+}_{0.05} = 0.335088$
Experimental NPCR and UACI values using proposed model

Image name	Type	Image size	NPCR	UACI	Pass rate (%)
4.1.01	Color	256 × 256	0.9961	0.3352	100
4.1.02	Color	256 × 256	0.9961	0.3339	100
4.1.03	Color	256 × 256	0.9961	0.3335	100
4.1.04	Color	256 × 256	0.9962	0.3346	100
4.1.05	Color	256 × 256	0.9961	0.3340	100
4.1.08	Color	256 × 256	0.9962	0.3355	100
4.2.07	Color	512 × 512	0.9961	0.3346	100
5.1.09	Gray	256 × 256	0.9961	0.3353	100
5.1.10	Gray	256 × 256	0.9958	0.3338	100
5.1.11	Gray	256 × 256	0.9961	0.3351	100
5.1.12	Gray	256 × 256	0.9960	0.3335	100
5.2.08	Gray	512 × 512	0.9961	0.3342	100
5.2.09	Gray	512 × 512	0.9960	0.3344	100
7.1.01	Gray	512 × 512	0.9960	0.3342	100
5.3.01	Gray	1024 × 1024	0.9961	0.3348	100
5.3.02	Gray	1024 × 1024	0.9961	0.3345	100
7.2.01	Gray	1024 × 1024	0.9960	0.3347	100

Table 8 A comparison of NPCR and UACI values

Image name →	5.1.09	5.1.10	5.1.11	5.1.12	5.2.08	5.2.09	7.1.01	5.3.01	5.3.02	7.2.01	Test results (%)
Hu and Li [15]											
NPCR	0.99629	0.99576	0.99622	0.99611	0.99603	0.99635	0.99598	0.99623	0.99613	0.99616	100
UACI	0.33365	0.33422	0.33518	0.33487	0.33481	0.33474	0.33398	0.33468	0.33455	0.33484	100
Hua et al. [20]											
NPCR	0.99628	0.99629	0.99706	0.99706	0.99625	0.99629	0.99621	0.99606	0.99619	0.99608	100
UACI	0.33505	0.33524	0.33511	0.33417	0.33497	0.33478	0.33415	0.33468	0.33443	0.33469	100
Alawida et al. [2]											
NPCR	0.99603	0.99636	0.99942	0.99792	0.99960	0.99876	0.99957	0.99950	0.99982	0.99980	100
UACI	0.33552	0.33453	0.33586	0.33453	**0.33692**	0.33548	**0.33648**	**0.33508**	**0.33514**	0.33487	**60**
Lan et al. [27]											
NPCR	0.99600	0.99640	0.99600	0.99610	0.99620	0.99630	0.99590	0.99610	0.99610	0.99610	100
UACI	0.33420	0.33450	0.33410	0.33400	0.33450	**0.33570**	0.33470	0.33470	0.33490	0.33500	**90**
Hua and Zhou [18]											
NPCR	0.99607	0.99615	0.99624	0.99570	**0.99587**	0.99626	0.99599	0.99593	0.99613	0.99616	**90**
UACI	0.33446	0.33494	0.33554	0.33430	0.334008	0.33480	0.33504	0.33459	0.33461	0.33456	100
Proposed model											
NPCR	0.99613	0.99584	0.99610	0.99599	0.99610	0.99597	0.99600	0.99606	0.99609	0.99602	100
UACI	0.33534	0.33380	0.33508	0.33345	0.33424	0.33441	0.33425	0.33480	0.33452	0.33474	100

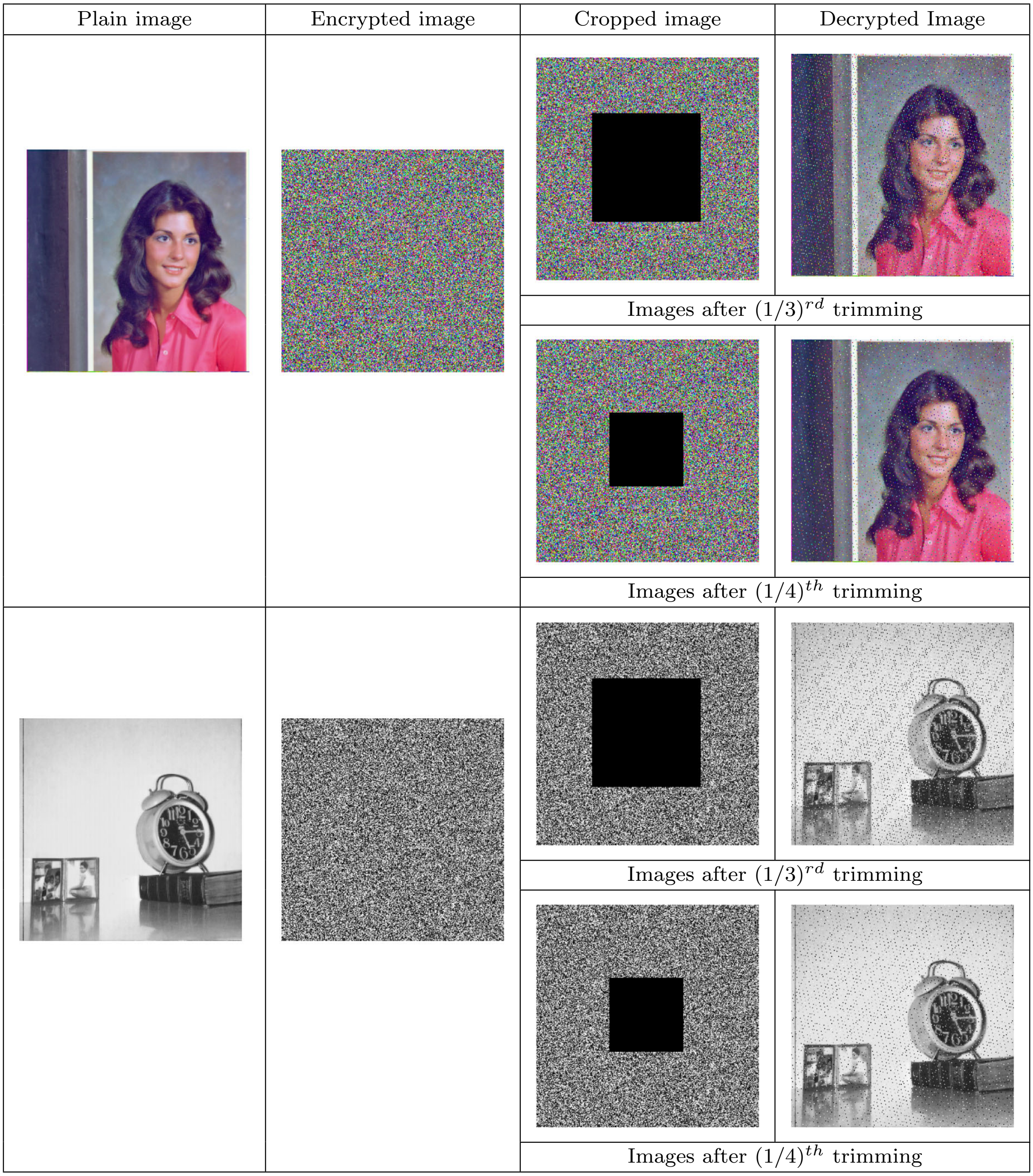

Plain image
Encrypted image
Cropped image
Decrypted Image
Images after $(1/3)^{rd}$ trimming
Images after $(1/4)^{th}$ trimming
Images after $(1/3)^{rd}$ trimming
Images after $(1/4)^{th}$ trimming

Fig. 11 Cropping attack analysis results for (1/3)rd and (1/4)th data loss

5.9 Cropping attack

The anti-shearing aptness of the encryption model is verified by trimming some portions of the encrypted image. The trimming can spread the subtle changes in the plain image to the whole encrypted image in the encryption process. It also, tells about the effect of data

Table 9 SSIM values of color and grayscale test images

Image name	Type	Plain versus encrypted	Plain versus decrypted
4.1.01	Color	0.0079	1.0000
4.1.02	Color	0.0043	1.0000
4.1.03	Color	0.0095	1.0000
4.1.04	Color	0.0096	1.0000
4.1.05	Color	0.0089	1.0000
4.1.08	Color	0.0089	1.0000
4.2.07	Color	0.0074	1.0000
5.1.09	Gray	0.0103	1.0000
5.1.10	Gray	0.0106	1.0000
5.1.11	Gray	0.0106	1.0000
5.1.12	Gray	0.0088	1.0000
5.2.08	Gray	0.0106	1.0000
5.2.09	Gray	0.0082	1.0000
7.1.01	Gray	0.0107	1.0000
5.3.01	Gray	0.0080	1.0000
5.3.02	Gray	0.0094	1.0000
7.2.01	Gray	0.0049	1.0000

loss in an encrypted image before decryption process [19].

The cropping attack has been applied on all the test images, but the results of only one grayscale and one color image are represented in Fig. 11. It has been observed that decryption process of the proposed model can still recover the plain image even after the loss of (1/3)rd and (1/4)th amount of data in the encrypted image [17]. The most of the information of the recovered images are easily recognizable even with addition of some noise. Therefore, when the encrypted image encounters cropping attack in the transmission, the proposed model has better security and can effectively resist the cropping attack.

5.10 SSIM

Structural Similarity Index Metric (SSIM) qualifies the degree of structural invariance between the two images [7]. It ranges from 0 to 1. The SSIM value 1 instigates that the images are completely indistinguishable, while its 0 value represents the characteristic dissimilarity between two images [14].

From Table 9 it has been analyzed that the plain versus decrypted images got the SSIM value equal to 1 which depicts the complete structural similarity between the plain and decrypted images. The SSIM values of the plain versus encrypted images ranges from 0.0043 to 0.0107 which means that the two images are completely distinct with respect to the image pixel values. Hence, the proposed image encryption model is effective and feasible against statistical attacks which implies that there are very few chances of information loss.

The experimental and statistical analysis conveys that the proposed image encryption and decryption model has better performance as compared to the existing models. The experimental results show that the proposed model resist statistical, entropy, differential, and cropping attacks in an efficient way.

6 Conclusion

This work propounds an image encryption and decryption model based on the scrambling algorithm, a novel magic square and differential encoding technique along with chaotic maps to enhance the level of security and privacy. The propounded model comprises two phases: confusion and diffusion. In the proposed model, the coordinate positions of the image pixels have been randomized by employing the scrambling algorithm which intensifies the degree of intricacy in the encrypted image before altering the pixel values. The elements of the magic square are utilized to change the image pixel values which reduce the plain image information hidden in the encrypted image. Further, the bit-level security of the proposed model has been improved by virtue of the implementation of the differential encoding technique on the magic square values. The XOR operation has been performed on the encoded and chaotic map values before applying the circular shift. Next, the complexity of the magic square values has been increased by using differential encoding and chaotic map. The in-depth security, structural, visual, and robustness anatomization of the propounded model have been performed to check the validity of the model against entropy, statistical, cropping, and differential attacks. The comparative inspection of the proposed model with the existing models reveals that the proposed model is more secure against different types of attacks. Henceforth, the proposed model is feasible and efficient for cryptographic application areas. In future, the researchers may work on the combination of algebraic properties of the magic square propounded in this paper along with wavelet transformations, numerical methods, DNA encoding technique, etc. These combinations might be able to generate the image encryption model with more enhanced level of security and complexity. Also, the proposed model will be tested for video and audio data encryption.

Data availability The data that support the findings of the study are available in USC-SIPI [http://sipi.usc.edu/database].

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Alawida, M., Samsudin, A., Teh, J.S., Alkhawaldeh, R.S.: A new hybrid digital chaotic system with applications in image encryption. Signal Process. **160**, 45–58 (2019). https://doi.org/10.1016/j.sigpro.2019.02.016
2. Alawida, M., Teh, J.S., Samsudin, A., et al.: An image encryption scheme based on hybridizing digital chaos and finite state machine. Signal Process. **164**, 249–266 (2019). https://doi.org/10.1016/j.sigpro.2019.06.013
3. Ayoup, A.M., Hussein, A.H., Attia, M.A.: Efficient selective image encryption. Multimed. Tools Appl. **75**(24), 17171–17186 (2016). https://doi.org/10.1007/s11042-015-2985-7
4. Bao, L., Tang, J., Ding, H., He, M., Zhao, L.: The n-level ($n \geq 4$) logistic cascade homogenized mapping for image encryption. Nonlinear Dyn. **105**, 1911–1935 (2021). https://doi.org/10.1007/s11071-021-06688-6
5. Chai, X., Gan, Z., Yuan, K., Chen, Y., Liu, X.: A novel image encryption scheme based on DNA sequence operations and chaotic systems. Neural Comput. Appl. **31**(1), 219–237 (2019). https://doi.org/10.1007/s00521-017-2993-9
6. Chan, C.Y.J., Mainkar, M.G., Narayan, S.K., Webster, J.D.: A construction of regular magic squares of odd order. Linear Algebra Appl. **457**, 293–302 (2014). https://doi.org/10.1016/j.laa.2014.05.032
7. Deb, S., Biswas, B., Bhuyan, B.: Secure image encryption scheme using high efficiency word-oriented feedback shift register over finite field. Multimed. Tools Appl. **78**(24), 34901–34925 (2019). https://doi.org/10.1007/s11042-019-08086-y
8. Faragallah, O.S., Afifi, A., El-Shafai, W., El-Sayed, H.S., Alzain, M.A., Al-Amri, J.F., Abd El-Samie, F.E.: Efficiently encrypting color images with few details based on rc6 and different operation modes for cybersecurity applications. IEEE Access **8**, 103200–103218 (2020). https://doi.org/10.1109/ACCESS.2020.2994583
9. Farhan, A.S., Abed, S.H., Awad, F.H.: Color image encryption with a key generated by using magic square. J. Eng. Appl. Sci. **13**(8), 2038–2041 (2018). https://doi.org/10.36478/jeasci.2018.2038.2041
10. Gaffar, A.F.O., Malani, R., Putra, A.B.W.: Magic cube puzzle approach for image encryption. Int. J. Adv. Intell. Inform. **6**(3), 290–302 (2020). https://doi.org/10.26555/ijain.v6i3.422
11. Ghadirli, H.M., Nodehi, A., Enayatifar, R.: An overview of encryption algorithms in color images. Signal Process. **164**, 163–185 (2019). https://doi.org/10.1016/j.sigpro.2019.06.010
12. Gupta, A., Singh, D., Kaur, M.: An efficient image encryption using non-dominated sorting genetic algorithm-iii based 4-d chaotic maps. J. Ambient. Intell. Humaniz. Comput. **11**(3), 1309–1324 (2020). https://doi.org/10.1007/s12652-019-01493-x
13. Herzog, A., Shahmehri, N., Duma, C.: An ontology of information security. Int. J. Inf. Secur. Priv. (IJISP) **1**(4), 1–23 (2007). https://doi.org/10.4018/jisp.2007100101
14. Hore, A., Ziou, D.: Image quality metrics: PSNR versus SSIM. In: 2010 20th International Conference on Pattern Recognition, pp. 2366–2369. IEEE (2010). https://doi.org/10.1109/ICPR.2010.579
15. Hu, G., Li, B.: A uniform chaotic system with extended parameter range for image encryption. Nonlinear Dyn. **103**(3), 2819–2840 (2021). https://doi.org/10.1007/s11071-021-06228-2
16. Hu, T., Liu, Y., Gong, L.H., Ouyang, C.J.: An image encryption scheme combining chaos with cycle operation for DNA sequences. Nonlinear Dyn. **87**(1), 51–66 (2017). https://doi.org/10.1007/s11071-016-3024-6

17. Hu, X., Wei, L., Chen, W., Chen, Q., Guo, Y.: Color image encryption algorithm based on dynamic chaos and matrix convolution. IEEE Access **8**, 12452–12466 (2020). https://doi.org/10.1109/ACCESS.2020.2965740
18. Hua, Z., Zhou, Y.: Image encryption using 2D logistic-adjusted-sine map. Inf. Sci. **339**, 237–253 (2016). https://doi.org/10.1016/j.ins.2016.01.017
19. Hua, Z., Zhou, Y., Pun, C.M., Chen, C.P.: 2D sine logistic modulation map for image encryption. Inf. Sci. **297**, 80–94 (2015). https://doi.org/10.1016/j.ins.2014.11.018
20. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. **480**, 403–419 (2019). https://doi.org/10.1016/j.ins.2018.12.048
21. Hua, Z., Zhu, Z., Chen, Y., Li, Y.: Color image encryption using orthogonal Latin squares and a new 2D chaotic system. Nonlinear Dyn. **104**, 4505–4522 (2021). https://doi.org/10.1007/s11071-021-06472-6
22. Ibrahim, D.R., Abdullah, R., Teh, J.S.: An enhanced color visual cryptography scheme based on the binary dragonfly algorithm. Int. J. Comput. Appl. **44**(7), 623–632 (2022). https://doi.org/10.1080/1206212X.2020.1859244
23. Khedr, W.I.: A new efficient and configurable image encryption structure for secure transmission. Multimed. Tools Appl. **79**(23), 16797–16821 (2020). https://doi.org/10.1007/s11042-019-7235-y
24. Kumar, C.M., Vidhya, R., Brindha, M.: An efficient chaos based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function. Appl. Intell. **52**(3), 2556–2585 (2022). https://doi.org/10.1007/s10489-021-02508-x
25. Kumar, S., Srivastava, P.K., Srivastava, G.K., Singhal, P., Singh, D., Goyal, D.: Chaos based image encryption security in cloud computing. J. Discrete Math. Sci. Cryptogr. **25**(4), 1041–1051 (2022). https://doi.org/10.1080/09720529.2022.2075085
26. Lai, Q., Zhang, H., Kuate, P.D.K., Xu, G., Zhao, X.W.: Analysis and implementation of no-equilibrium chaotic system with application in image encryption. Appl. Intell. 1–24 (2022). https://doi.org/10.1007/s10489-021-03071-1
27. Lan, R., He, J., Wang, S., Gu, T., Luo, X.: Integrated chaotic systems for image encryption. Signal Process. **147**, 133–145 (2018). https://doi.org/10.1016/j.sigpro.2018.01.026
28. Lee, M.Z., Love, E., Narayan, S.K., Wascher, E., Webster, J.D.: On nonsingular regular magic squares of odd order. Linear Algebra Appl. **437**(6), 1346–1355 (2012). https://doi.org/10.1016/j.laa.2012.04.004
29. Li, W., Wu, D., Pan, F.: A construction for doubly pandiagonal magic squares. Discret. Math. **312**(2), 479–485 (2012). https://doi.org/10.1016/j.disc.2011.09.031
30. Liao, X., Yin, J., Chen, M., Qin, Z.: Adaptive payload distribution in multiple images steganography based on image texture features. IEEE Trans. Depend. Secure Comput. (2020). https://doi.org/10.1109/TDSC.2020.3004708
31. Liu, L., Gao, Z., Zhao, W.: On an open problem concerning regular magic squares of odd order. Linear Algebra Appl. **459**, 1–12 (2014). https://doi.org/10.1016/j.laa.2014.06.046
32. Liu, Y., Zhang, J., Han, D., Wu, P., Sun, Y., Moon, Y.S.: A multidimensional chaotic image encryption algorithm based on the region of interest. Multimed. Tools Appl. **79**, 17669–17705 (2020). https://doi.org/10.1007/s11042-020-08645-8
33. Miranda, D.O., Miranda, L., Bacelar, L.B.: Generalization of Dürer's magic square and new methods for doubly even magic squares. J. Nepal Math. Soc. **3**(2), 13–15 (2020). https://doi.org/10.3126/jnms.v3i2.33955
34. Nordgren, R.P.: On properties of special magic square matrices. Linear Algebra Appl. **437**(8), 2009–2025 (2012). https://doi.org/10.1016/j.laa.2012.05.031
35. Norouzi, B., Seyedzadeh, S.M., Mirzakuchaki, S., Mosavi, M.R.: A novel image encryption based on hash function with only two-round diffusion process. Multimed. Syst. **20**(1), 45–64 (2014). https://doi.org/10.1007/s00530-013-0314-4
36. Pappachan, J., Baby, J.: Tinkerbell maps based image encryption using magic square. Int. J. Adv. Res. Electric. Electron. Instrum. Eng. (IJAREEIE) **4**, 6226–6232 (2015). https://doi.org/10.15662/ijareeie.2015.0407034
37. Patro, K.A.K., Acharya, B.: A novel multi-dimensional multiple image encryption technique. Multimed. Tools Appl. **79**(19), 12959–12994 (2020). https://doi.org/10.1007/s11042-019-08470-8
38. Peng, F., Zhang, X., Lin, Z.X., Long, M.: A tunable selective encryption scheme for H. 265/HEVC based on chroma IPM and coefficient scrambling. IEEE Trans. Circuits Syst. Video Technol. **30**(8), 2765–2780 (2019). https://doi.org/10.1109/TCSVT.2019.2924910
39. Rageed, H.A.H., Sadiq, A.M.: A new algorithm based on magic square and a novel chaotic system for image encryption. J. Intell. Syst. **29**(1), 1202–1215 (2020). https://doi.org/10.1515/jisys-2018-0404
40. Raju, D., Eleswarapu, L., Pranav, M.S., Sinha, R.K.: Multilevel image security using elliptic curve and magic matrix with advanced encryption standard. Multimed. Tools Appl. 1–21 (2022). https://doi.org/10.1007/s11042-022-12993-y
41. Rani, N., Mishra, V.: Application of magic squares in cryptography. In: International Conference on Intelligent Vision and Computing, pp. 321–329. Springer (2021). https://doi.org/10.1007/978-3-030-97196-0_26
42. Rani, N., Mishra, V.: Behavior of powers of odd ordered special circulant magic squares. Int. J. Math. Educ. Sci. Technol. **53**, 1044–1062 (2022). https://doi.org/10.1080/0020739X.2021.1890846
43. Rani, N., Sharma, S.R., Mishra, V.: Grayscale and colored image encryption model using a novel fused magic cube. Nonlinear Dyn. **108**(2), 1773–1796 (2022). https://doi.org/10.1007/s11071-022-07276-y
44. Sadhukhan, D., Ray, S., Biswas, G., Khan, M.K., Dasgupta, M.: A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. J. Supercomput. **77**(2), 1114–1151 (2021). https://doi.org/10.1007/s11227-020-03318-7
45. Sahila, K., Thomas, B.: Secure digital image watermarking by using SVD and AES. In: Intelligent Data Communication Technologies and Internet of Things, pp. 805–818. Springer (2021). https://doi.org/10.1007/978-981-15-9509-7_65
46. Sasikaladevi, N., Geetha, K., Sriharshini, K., Aruna, M.D.: Radiant-hybrid multilayered chaotic image encryption system for color images. Multimed. Tools Appl. **78**(9), 11675–11700 (2019). https://doi.org/10.1007/s11042-018-6711-0
47. Senthilnayaki, B., Venkatalakshami, K., Dharanyadevi, P., Nivetha, G., Devi, A. An efficient medical image encryption using magic square and PSO. In: 2022 International

Conference on Smart Technologies and Systems for Next Generation Computing (ICSTSN), pp. 1–5. IEEE (2022)

48. Shuangyuan, Y., Zhengding, L., Shuihua, H.: An asymmetric image encryption based on matrix transformation. In: IEEE International Symposium on Communications and Information Technology, 2004. ISCIT 2004, vol. 1, pp. 66–69. IEEE, Sapporo, Japan (2004). https://doi.org/10.1109/ISCIT.2004.1412451
49. Singh, K.N., Singh, O.P., Baranwal, N., Singh, A.K.: An efficient chaos-based image encryption algorithm using real-time object detection for smart city applications. Sustain. Energy Technol. Assess. **53**, 102566 (2022). https://doi.org/10.1016/j.seta.2022.102566
50. Sneha, P., Sankar, S., Kumar, A.S.: A chaotic colour image encryption scheme combining Walsh–Hadamard transform and Arnold–Tent maps. J. Ambient. Intell. Humaniz. Comput. **11**(3), 1289–1308 (2020). https://doi.org/10.1007/s12652-019-01385-0
51. Sowmiya, S., Tresa, I.M., Chakkaravarthy, A.P.: Pixel based image encryption using magic square. In: 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), pp. 1–4. IEEE, Chennai, India (2017). https://doi.org/10.1109/ICAMMAET.2017.8186634
52. Tedmori, S., Al-Najdawi, N.: Image cryptographic algorithm based on the Haar wavelet transform. Inf. Sci. **269**, 21–34 (2014). https://doi.org/10.1016/j.ins.2014.02.004
53. Telem, A.N.K., Fotsin, H.B., Kengne, J.: Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems. Multimed. Tools Appl. **80**(12), 19011–19041 (2021). https://doi.org/10.1007/s11042-021-10549-0
54. Vidhya, R., Brindha, M., Gounden, N.A.: Analysis of zig–zag scan based modified feedback convolution algorithm against differential attacks and its application to image encryption. Appl. Intell. **50**(10), 3101–3124 (2020). https://doi.org/10.1007/s10489-020-01697-1
55. Wang, J., Liu, L.: A novel chaos-based image encryption using magic square scrambling and octree diffusing. Mathematics **10**(3), 457 (2022). https://doi.org/10.3390/math10030457
56. Wang, M., Yang, W.F., Xiong, X.W.: Application of information hiding technology based on matlab in military information security. In: Advanced Materials Research, vol. **546**, 395–400. Trans Tech Publications Ltd (2012). https://doi.org/10.4028/www.scientific.net/AMR.546-547.395
57. Wang, S., Wang, C., Xu, C.: An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm. Opt. Lasers Eng. **128**, 105995 (2020). https://doi.org/10.1016/j.optlaseng.2019.105995
58. Wang, X., Liu, C.: A novel and effective image encryption algorithm based on chaos and DNA encoding. Multimed. Tools Appl. **76**(5), 6229–6245 (2017). https://doi.org/10.1007/s11042-016-3311-8
59. Weber, G.: USC-SIPI image database: Version 4. dept elect eng-syst, univ southern california, los angeles, ca. Technical reports, USA, Tech Rep 244 (1993). http://sipi.usc.edu/database
60. Wootton, R.: Assessing telemedicine: a systematic review of the literature. BMJ **323**(7312), 557–560 (2001). https://doi.org/10.1136/bmj.323.7312.557
61. Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J.P., Natarajan, P.: Local Shannon entropy measure with statistical tests for image randomness. Inf. Sci. **222**, 323–342 (2013). https://doi.org/10.1016/j.ins.2012.07.049
62. Yan X, Wang X, Xian Y (2021). Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation. Multimedia Tools Appl **80**(7), 10949–10983. https://doi.org/10.1007/s11042-020-10218-8
63. Yavuz, E.: A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme. Opt. Laser Technol. **114**, 224–239 (2019). https://doi.org/10.1016/j.optlastec.2019.01.043
64. Ye, G., Liu, M., Wu, M.: Double image encryption algorithm based on compressive sensing and elliptic curve. Alex. Eng. J. **61**(9), 6785–6795 (2022). https://doi.org/10.1016/j.aej.2021.12.023
65. Yu, W., Liu, Y., Gong, L., Tian, M., Tu, L.: Double-image encryption based on spatiotemporal chaos and DNA operations. Multimed. Tools Appl. **78**(14), 20037–20064 (2019). https://doi.org/10.1007/s11042-018-7110-2
66. Zhan, K., Wei, D., Shi, J., Yu, J.: Cross-utilizing hyperchaotic and DNA sequences for image encryption. J. Electron. Imaging **26**(1), 013021 (2017). https://doi.org/10.1117/1.JEI.26.1.013021
67. Zhang, Y., Xiao, D., Shu, Y., Li, J.: A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations. Signal Process. Image Commun. **28**(3), 292–300 (2013). https://doi.org/10.1016/j.image.2012.12.009
68. Zheng, F., Chen, C., Zheng, X., Zhu, M.: Towards secure and practical machine learning via secret sharing and random permutation. Knowl. Based Syst. **245**, 108609 (2022). https://doi.org/10.1016/j.knosys.2022.108609
69. Zhong, W., Deng, Y.H., Fang, K.T.: Image encryption by using magic squares. In: 2016 9th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), pp. 771–775. IEEE (2016). https://doi.org/10.1109/CISP-BMEI.2016.7852813
70. Zhou, M., Wang, C.: A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. Signal Process. **171**, 107484 (2020). https://doi.org/10.1016/j.sigpro.2020.107484
71. Zhou, Y., Bao, L., Chen, C.P.: Image encryption using a new parametric switching chaotic system. Signal Process. **93**(11), 3039–3052 (2013). https://doi.org/10.1016/j.sigpro.2013.04.021
72. Zhou, Y., Li, C., Li, W., Li, H., Feng, W., Qian, K.: Image encryption algorithm with circle index table scrambling and partition diffusion. Nonlinear Dyn. **103**(2), 2043–2061 (2021). https://doi.org/10.1007/s11071-021-06206-8
73. Ziemer, R.: Modulation. In: Meyers, R.A. (ed.) Encyclopedia of Physical Science and Technology, 3rd edn., pp. 97–112. Academic Press, New York (2002). https://doi.org/10.1016/B0-12-227410-5/00456-7