ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR

CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW

Vol.02 No.04 (2024)

PIXEL BIT SWAPPING-BASED IMAGE ENCRYPTION USING A 4D UNIFIED HYPER-CHAOTIC FRAMEWORK

Abdullah Nasir
International School Lahore, Lahore, Pakistan
Email: realabdullahnasir@gmail.com
Talha Irfan
The Crescent College, Lahore, Pakistan
Email: irfantalha703@gmail.com
Muhammad Abdur Rehman Nasir
Aitchison College, Lahore, Pakistan
Email: abdurrehman132109@gmail.com
Muhammad Sheharyar Khan Daym
Punjab University College of Information Technology (PUCIT), Lahore, Pakistan.
Email: sheharyar.daym@gmail.com

Corresponding Authors: realabdullahnasir@gmail.com

Abstract

Digital images have assumed a lot of importance in the current era of time. So, their safety from the unauthorized access is of prime importance. In order to boost the security effects, this research study has made an endeavor to write a novel image encryption algorithm based on the dynamically spawned matrices and the swapping of bits within the pixels' data. First of all, a 2D lattice of random numbers is constructed from the streams of the chaotic map. Two square matrices are dynamically generated within the confines of the 2D lattice. Then, the determinants of these matrices are calculated. Further, these calculated determinants are translated to get the required range of numbers. These values help in selecting one pixel from the given plaintext image. The same operation has been repeated to select the second pixel from the given plaintext image but by flipping the streams of random numbers. Two bits have been chosen randomly from these selected two pixels of the given image. These selected bits are swapped with each other. This operation has been repeated a number of times to embed the required confusion effects in the input image. Diffusion effects have been introduced by carrying out the XoR operation between the mask image and the confused image. To spawn the streams of random numbers, 4D unified hyperchaotic map has been sparked by giving the initial values. Machine experiments and the security evaluation depict that the suggested cipher can defy the multifarious attacks possibly launched by the cryptanalytic savvy. We assert that this image cipher can be installed in some real world setting to reap its inherent benefits.

INDEX TERMS Cyber security, encryption, decryption, chaos, image, matrix, bits

1. Introduction

The twin revolution of the information of communication technologies have changed the entire complexion of the world. Moreover, digital images have assumed a lot of importance in today's high-tech world. These images have become a necessary component of virtually every facet of human endeavor. Be it medicine, commerce, traffic, showbiz, space science, diplomacy and government, these images have penetrated in all walks of life. In normal situation, we store and transmit these images without any potential fear. But sometimes, situations develop in which the storage and transmission of these images may have grave repercussions and implications if they are not dealt with extreme care, the image of some new automobile, the image of some new missile, for

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

instance. So, serious steps must be taken to safeguard these precious and sensitive images from the hackers. Historically, the technique of encryption has been used for the safety and integrity of the precious data. For this purpose, the ciphers like Data Encryption Standard (DES) (Subaselvi et al., 2023), Advanced Encryption Standard (AES) (Santhanalakshmi et al., 2023) and Rivest–Shamir–Adleman (RSA) (Jamaludin & Romindo, 2020) have been developed. But they can't be applied over the digital images since they were developed to safeguard the textual data. Images have diametrically opposite properties like bulky volume, high redundancy and strong inter-pixel correlation (Jasra & Moon, 2020). Confusion and diffusion are two principal operations in order to develop some cryptographic product. In the former operation, the given data or pixels are rearranged. In the later operation, the intensity values of the pixels of the given image are changed. We need chaotic and random numbers in order to carry out these two necessary operations. Fortunately, the theory of chaos and chaotic systems/map has rendered a great job in generating the streams of random numbers (Pourasad et al., 2021).

By employing the different mathematical constructs, many image ciphers have been developed by the image cryptographers. These constructs include DNA (Zhu & Zhu, 2020), cellular automaton (Roy et al., 2021), Latin Square (Hua et al., 2021), Fractals (Ahmad et al., 2022), Sudoku (Deshpande et al., 2023), matrices (Kanwal et al., 2022) etc. In (Zhu & Zhu, 2020), a novel 5D hyperchaotic map has been developed. Besides, DNA dynamic encoding framework has been written. Additionally, scrambling diffusion scheme has been developed to heighten the security effects. Apart from that, rules of DNA encoding (DNA decoding) have been dynamically adapted strictly in accordance with the given pixel values. In this way, the cipher has been made resistant to the chosen-plaintext attack. The evaluation and the computer simulation demonstrated that the algorithm has been furnished with a large key space and is defiant to the varied attacks possibly launched by the hackers' community. In another work (Roy et al., 2021), a novel image encryption algorithm has been developed through the usage of 2D Moore Cellular Automata (MCA). It is to be noted that MCA has the ability to spawn the random numbers more speedily as compared to the chaotic systems. Besides, it utilizes local transformations through the approach of 1-bit state value for its neighbors. The randomness of the encrypted images have been measured through NIST test suite. Many image ciphers have also been successfully cracked due to varied loopholes and defects in their design principles. For instance, the work (Gao et al., 2021) was broken by the (Jiang et al., 2023) through the chosen plaintext attack. Hence, new ciphers must be developed to thwart the potential threats from the hackers and other adversaries.

Inspired by the above discussion, this research study ventures to craft a yet another image encryption scheme in which scrambling has been carried out at the bit level. Apart from that, both the necessary operations of scrambling and diffusion have been conducted in a parallel fashion. To begin, a 2D lattice of random numbers is created using the streams generated by the chaotic map. Within this lattice, two square matrices are dynamically formed. The determinants of these matrices are then computed. Subsequently, the resulting determinants undergo a translation process to obtain a desired range of numbers. These values play a crucial role in the selection of one pixel from the given plaintext image. The same process is iterated to select a second pixel from the plaintext image, with a twist—flipping the streams of random numbers to enhance security measures. To introduce an additional layer of security, two bits are randomly

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

chosen from the aforementioned selected pixels, and these selected bits undergo a swapping operation. This procedure is iterated multiple times to embed the necessary confusion effects into the input image. Diffusion effects are introduced by performing the XoR operation between the mask image and the confused image. The generation of random number streams is facilitated by igniting a 4D unified hyperchaotic map (Wang and Zhao, 2010) with specified initial values.

The rest of the paper has been structured like this. Section 2 discusses the theory of chaos and 4D unified hyperchaotic system. In Section 3, two things have been described, i.e., the way initial values have been spawned for carrying out the diffusion and scrambling operations and the suggested image encryption scheme. Apart from that, the machine experimentation and simulation have been given in the Section 4. Section 5 provides a detailed security analysis by employing the different state of the art benchmarks in the community of cryptographers. Lastly, the Section 6 ends the paper by giving the necessary concluding remarks and the possible future directions.

2. CHAOS THEORY AND ITS INCARNATION IN THE FORM OF CHAOTIC MAPS

According to the classical theory of chaos (Gupta et al., 2020), the faintest alteration in dynamical system initial state ends up with a sweeping change in the output. Strictly in line with this notion, mathematicians have discovered myriads of chaotic maps to spawn the streams of random numbers. This study has chosen a 4D hyper-chaotic system whose mathematical equations are described below.

$$\begin{aligned} \dot{x} &= a_1(y - x) + w \\ \dot{y} &= a_2 x - xz + a_4 y \\ \dot{z} &= xy - a_3 z \\ \dot{w} &= 0.2w + 0.1yz \end{aligned} \qquad (1)$$

In this set of equations, the tuple $(x, y, z, w) \in \mathbb{R}$ refers to state variables of selected chaotic map. Besides, (a_1, a_2, a_3, a_4) constitute the system parameters. The pioneering work (Wang and Zhao, 2010) studied this system in depth in the varied perspectives of Poincare maps, bifurcation diagram, Lyapunov exponents spectrum, etc. This system exhibits the conduct of hyper-chaoticity when the system parameters are set to $a_1 = 45, a_2 = 45, a_3 = 10$ and $10 \leq a_4 \leq 40$.

The above 4D hyper-chaotic system depicts hyper-chaotic behavior in varied regions depending upon the particular values of the system parameter a_4:

- Hyper-chaotic attractor's output resembles to the Lorenz attractor when the value of a_4 is set to 13.
- Hyper-chaotic attractor's output resembles to Lu attractor when the value of a_4 is set to 27.
- Hyper-chaotic attractor's output resembles to the Chen attractor when value of a_4 is set to 36.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

Moreover, fourth-order Runge-Kutta integrator with a fixed step size of 0.001 has been employed. The initial values of the system are$(x, y, z, w) = [1,1,1,1]^T$.

3. SUGGESTED IMAGE ENCRYPTION SCHEME

The suggested scheme to impart security to the digital grayscale images is based on the dynamically generated square matrices of varied lengths from the given $(m \times n)$lattice of random numbers, where(m, n) is the size of the plaintext image. These random numbers have been spawned by igniting the 4D Unified Hyperchaotic System (1). The first two streams out of the four streams decide the top left corner$(pointx,\ point\ y)$ of the dynamically generated matrix within the $(m \times n)$lattice of random numbers. The third stream decides the square length (*length*) of this generated matrix. Moreover, using the outputs of first two streams, one more stream *lattice* has been created. Lastly, the last stream of random numbers has been consumed to come up with the mask image *mask*.

Confusion and diffusion effects have been realized in a parallel fashion in this particular research project. In each iteration, the streams *pointx*, *pointy* and *length* decide the first square matrix *TempMatrix1*. The same streams have been employed by flipping their chaotic data to generate the second square matrix *TempMatrix2*. Moreover, the determinants of these matrices have been calculated to decide the particular row *row* and column *col* of the selected pixels. It is to be noted that the values of the determinants have been translated to the ranges of $[1, m]$and $[1, n]$. Additionally, the address for the second pixel has been calculated by taking a sort of "complements" of these rows and columns $(row' = m - row, col' = n - col)$. Further, the streams *pointx* and *pointy* have been recycled to get the particular bits *bit*1 and *bit*2. Moreover, these bits have been employed to swap the bits of the pixels *I*(*row*, *col*) and *I*(*row', col'*) for the *image I*. After swapping these bits, an XoR operation has been carried out between the scrambled image *I* and the mask image *mask*.

A. ENGINEERING PRIMARY VALUES OF CHAOTIC SYSTEM

The family of chaotic maps requires some starting values so that it may spark it and required numbers of random data may be obtained. In the steps below, we will shed light on the way, the primary values have been obtained.

Step 1: Supply algorithm with grayscale *image I* of dimensions *m* ×*n*. To introduce plaintext sensitivity, determine average value *avg* of intensity values across pixels. Subsequently, apply the following equation to modify the initial key x_0 of Chaotic System (1) currently in use.

$$x_0 = x_0 + \frac{avg}{2^{100}} \qquad (2)$$

Step 2: As the System (1) is iterated$(mn + n_0)$times,$\{x_t\}_{t=1}^{mn+n_0}$, $\{y_t\}_{t=1}^{mn+n_0}$, $\{z_t\}_{t=1}^{mn+n_0}$and $\{w_t\}_{t=1}^{mn+n_0}$ have been obtained. Moreover, value of $n_0 \geq 500$. These initial n_0 values are typically regarded as unripe random data. To prevent any adverse impact, these values are skipped.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

Step 3: In previous Step 2, random numbers deviate from the specific logic envisioned in this study. Consequently, the sequences *x*, *y*, *z*, and *w* undergo set of equations (3). As a result, we obtain modified streams of arbitrary data referred to as $\{pointx_t\}_{t=1}^{mn+n_0}$, $\{pointy_t\}_{t=1}^{mn+n_0}$, $\{length_t\}_{t=1}^{mn+n_0}$, $\{lattice_t\}_{t=1}^{mn+n_0}$ and $\{mask_t\}_{t=1}^{mn+n_0}$.

$$\begin{cases} \text{point } x_t = floor\left(mod\left(abs(x_t) - floor\left(abs(x_t)\right) \times 10^{14}, m\right)\right) + 1 \\ \text{point } y_t = floor\left(mod\left(abs(y_t) - floor\left(abs(y_t)\right) \times 10^{14}, n\right)\right) + 1 \\ length_t = floor\left(mod\left(abs(z_t) - floor\left(abs(z_t)\right) \times 10^{14}, 10\right)\right) + 1 \\ lattice_t = mod\left(\text{point } x_t + \text{ point } y_t, 10\right) + 1 \\ mask_t = floor\left(mod\left(abs(w_t) - floor\left(abs(w_t)\right) \times 10^{14}, 256\right)\right) \end{cases} \quad (3)$$

Here $1 \leq t \leq mn + n_0$. Moreover, ignore the first n_0 random numbers of the stream *lattice* and reshape it to $m \times n$so that the conceived logic of image encryption may be applied.

B.SUGGESTED PROCEDURE FOR IMAGE ENCRYPTION

Provide grayscale *image I* with dimensions $m \times n$ as input. Invoke Algorithm 1 using the parameters *I*, *pointx*, *pointy*, *length*, *lattice*, *mask*, *m*, and *n* to achieve the objectives of scrambling and diffusion for the provided image *I*. In the following, Algorithm 1 will be explained.

Step 1: Line 1 iterates for loop *formn* times. Lines 2 and 3 initialize the temporary matrices $TempMatrix_1$ and $TempMatrix_2$ with the values of zeros and of the lengths of $length_i$ and $flip(length)_i$ in each of the i^{th} iteration of the *for* loop. It is to be noted that we have recycled the stream $length_i$ by invoking the *flip* function over it. This function reverses the given streams of random numbers.

Step 2: The *if* condition (Line 4) checks whether the values of $pointx_i + length_i$and $pointy_i + length_i$ stay within the ranges of *m* and *n* of the generated lattice *lattice* of random numbers? If it does, then the lines 5 and 6 pick the values for the matrices $TempMatrix_1$ and $TempMatrix_2$ from the lattice populated with the random numbers. It is to be noted that *a : a + l, b : b + l* picks the random numbers from the lattice starting at the address (*a*, *b*) and with the length of*l*. Besides, the symbol *&&* denotes the logical and operation.

Step 3: Lines 7 and 8 calculate the particular row *row* and column *col* at each of the i^{th} iteration of the *for* loop (Line 1). These values will, of course, be used to swap the bits of the given image *I* in the coming lines of the algorithm. It is to be noted that the built-in function *det* has been employed to find the determinants of the matrices $TempMatrix_1$ and $TempMatrix_2$. The *mod* operation ensures that the values of both *row* and *col* may stay within the required ranges of [*1, m*] and [*1, n*].

Step 4: In case, the *if* condition of the line 4 happens to be false, the control is being shifted to the start of the loop by executing the statement at the line 10.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

Step 5: Lines 12 and 13 find the address (*row′, col′*) of the second pixel of the given input image *I*. It is to be observed that we have used the already calculated address (*row, col*) of the first pixel by taking a sort of "complement" of the (*row, col*) from the dimensions (*m, n*) of given image *I*.

Step 6: Particular bits' indices *bit1ToAccess* and *bit2ToAccess* have been calculated by using the key streams *pointx* and *pointy* at the i^{th} index (Lines 14 - 15).

Step 7: Lines (16-17) get the particular bits at the positions *bit1ToAccess* and *bit2ToAccess* from the image *I* at the pixel addresses of (*row, col*) and (*row′, col′*) respectively and assign these values to the bit variables *bit1* and *bit2*.

Step 8: Line 18 carries out the real "*manufacturing*" of the algorithm by swapping the bits at the pixel addresses of (*row, col*) and (*row′, col′*) for the given image *I*.

Step 9: Line 19 reshapes the image *I* to the size of $1 \times mn$ so that an XoR operation between the image *I* and the mask at the i^{th} iteration of the loop may be carried out at the line 20. It is to be further observed that the resultant image has been assigned to the image *I′*.

Step 10: The image *I′* has been again reshaped to its originaldimensions of (*m,n*) at the line 21. Further, line 22 assigns the image *I′* to the variable *I* so that it may be processed in the next iteration.

Step 11: Lastly, line 24 assigns the scrambled and diffused image *I* to the image variable I_1 and returns it to the calling program.

Apart from that, Figure 1 details the proposed algorithm through the instrument of flowchart.

C. PROCEDURE FOR IMAGE DECRYPTION

This research project has been carried out by applying the tenets of private/symmetric key cryptography. Just reversing the instructions of the encryption algorithm would yield the corresponding decryption algorithm.

4. SUGGESTED ALGORITHM'S MACHINE SIMULATION

To demonstrate the proposed encryption framework, four grayscale images were selected from the USC-SIPI Image Database, available at http://sipi.usc.edu/database/. The machine simulation was performed in MATLAB version 2016, utilizing double-precision (64-bit) arithmetic in compliance with the IEEE 754 standard for floating-point computations (Ghosh et al., 2013). The chosen grayscale images include Lena, Truck, Butterfly, and Girl, each sized 256 × 256. Apart from that, random data was generated for suggested image security scheme using chaotic map/system of the 4D Unified Hyperchaotic System. System parameters and initial values chosen are$x_0 = 1, y_0 = 1, z_0 = 1, w_0 = 1, a_1 = 45, a_2 = 45, a_3 = 10$ and $a_4 = 20$. Figure 2 showcases the plaintext images (Row 1), their corresponding cipher/encrypted versions (Row 2), and the successfully decrypted images (Row 3). The transformation of the original plaintext images into a visually noisy and indistinct form highlights the effectiveness of the encryption

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

process. Additionally, the ability to recover the original images through the decryption algorithm demonstrates the robustness and reliability of the proposed encryption scheme.

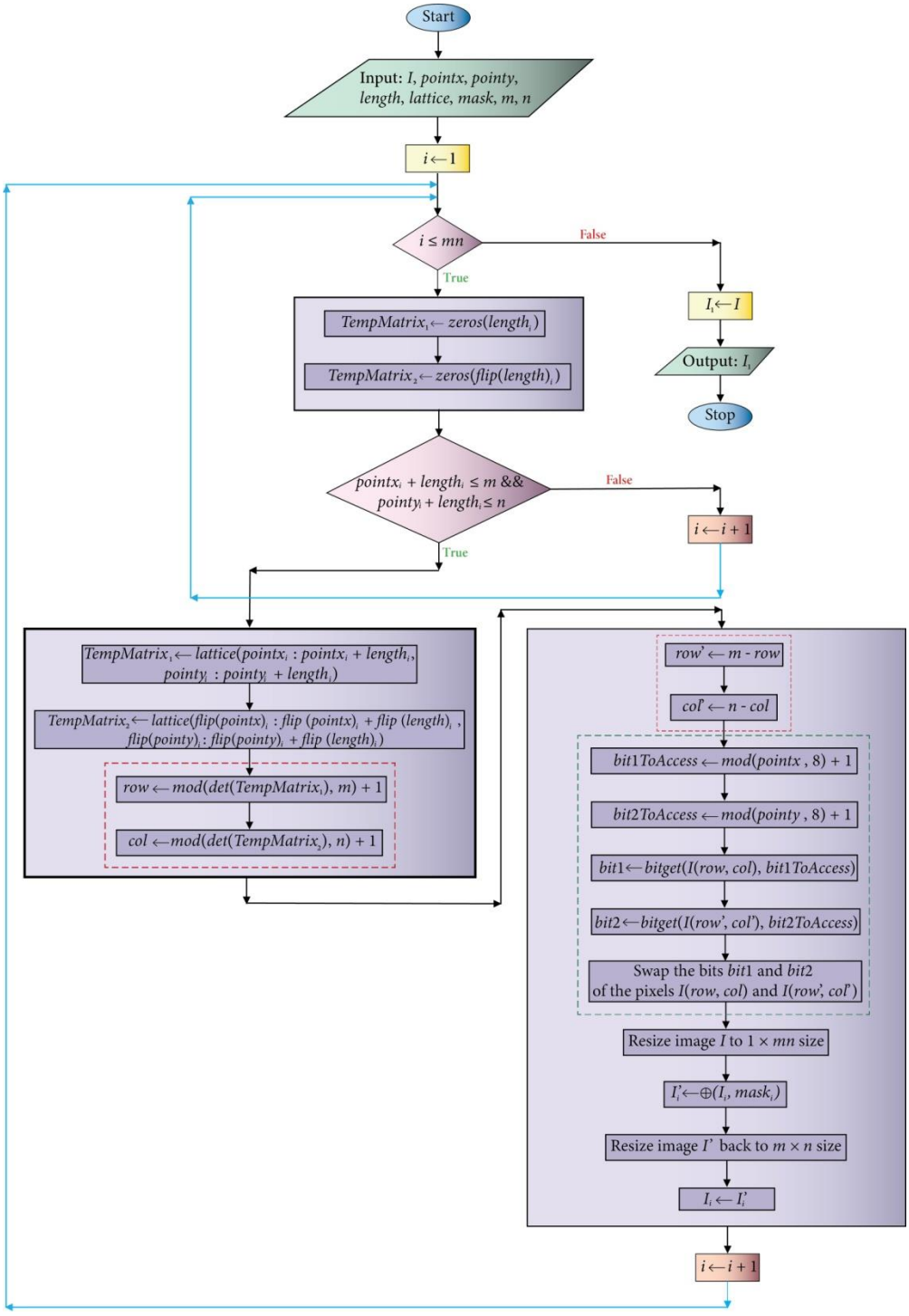


FIGURE 1: Proposed Image Encryption Methodology.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

Algorithm 1: Image Scrambler Based On Dynamically Generated Matrices (ISBDGM)

Input: I, $pointx$, $pointy$, $length$, $lattice$, $mask$, m, n
Output: I_1

for $i \leftarrow 1$ to mn **do**
  $TempMatrix_1 \leftarrow zeros(length_i)$
  $TempMatrix_2 \leftarrow zeros(flip(length)_i)$
  if $pointx_i + length_i \leq m \&\& pointy_i + length_i \leq n$ **then**
    $TempMatrix_1 \leftarrow lattice(pointx_i : pointx_i + length_i, pointy_i : pointy_i + length_i)$
    $TempMatrix_2 \leftarrow lattice(flip(pointx)_i : flip(pointx)_i + flip(length)_i, flip(pointy)_i : flip(pointy)_i + flip(length)_i)$
    $row \leftarrow mod(det(TempMatrix_1), m) + 1$
    $col \leftarrow mod(det(TempMatrix_2), n) + 1$
  else
    Go to *Step*1
  endif
  $row' \leftarrow m - row$
  $col' \leftarrow n - col$
  $bit1ToAccess \leftarrow mod(pointx_i, 8) + 1$
  $bit2ToAccess \leftarrow mod(pointy_i, 8) + 1$
  $bit1 \leftarrow bitget(I(row, col), bit1ToAccess)$
  $bit2 \leftarrow bitget(I(row', col'), bit2ToAccess)$
  Swap the bits $bit1$ and $bit2$ of the pixels $I(row, col)$ and $I(row', col')$
  Resize image I to $1 \times mn$ size
  $I_i' \leftarrow \bigoplus(I_i, mask_i)$
  Resize image I' back to $m \times n$ size
  $I_i \leftarrow I_i'$
end for
$I_1 \leftarrow I$ and return I_1

5. SECURITY/PERFORMANCE ANALYSES

Security analyses provide an essential opportunity for security engineers to validate the effectiveness of their work using various evaluation metrics. In this section, commonly employed metrics are applied to the proposed image cipher to demonstrate its resilience against diverse attacks by the hackers' community. For comparative analysis, we have referenced relevant studies from the literature (Abduljabbar et al., 2022; Gao et al., 2022; Masood et al., 2022; X. Wang and Gao, 2020).

A. KEY SPACE

A strong encryption scheme features a large key space, effectively deterring brute-force attacks. Such attacks involve systematically testing all possible keys, which becomes im practical when the key space is vast, making it infeasible to try all combinations within a

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

reasonable time. The chaotic data in our proposed scheme is generated from the initial values and system parameters of 4D chaotic map utilizedin the encryption process. For the proposed cipher, a key space of 10^{112} has been computed using specific initial values and system parameters, includingx_0, y_0, z_0, w_0, and a_4. It's noteworthy that a computer precision of 10^{-14} has been considered. Unfortunately, the comparison reveals that our scheme could not beat any of the studies given in Table 1,although we have met the minimum threshold 2^{100} of the key space (Khan et al., 2019) to counter any brute force assault.

TABLE 1: Key space of the proposed cipher and comparison with some other algorithms

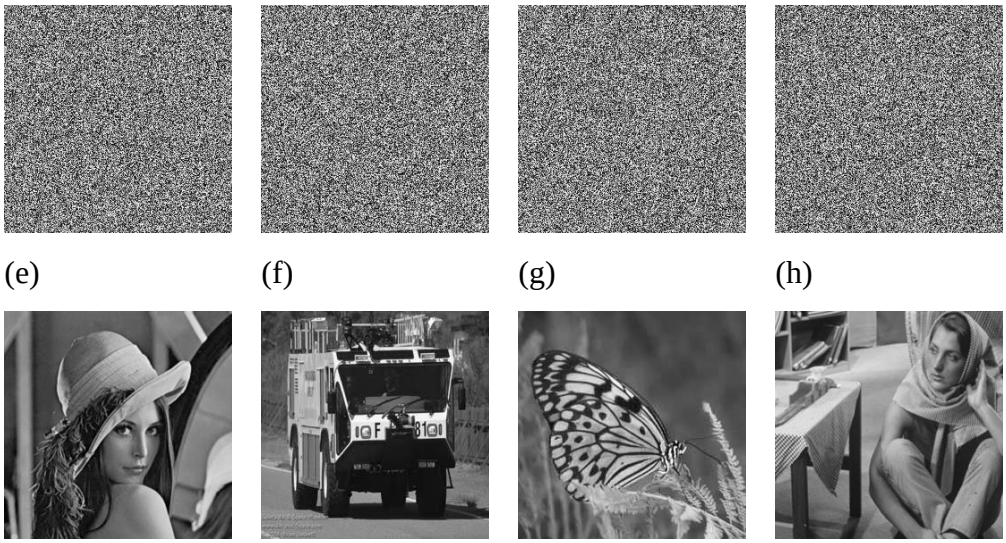
Algorithm	**Key Space**
Ours	$10^{112} \approx 2^{372}$
Ref. (Masood et al., 2022)	-
Ref. (Gao et al., 2022)	10^{144}
Ref. (Abduljabbar et al., 2022)	2^{430}
Ref. (Wang and Gao, 2020)	-

B.COMPUTATIONAL TIME ANALYSIS

A key contribution of this study is the exceptional efficiency of the proposed image cipher, which demonstrates significantly lower encryption time compared to existing studies which have been published in the literature. The implementation of this work was carried out using MATLAB R2024a on a Windows operating system. The hardware specifications include an Intel(R) Core(TM) i5-4210U CPU @ 1.70 GHz (up to 2.40 GHz) and 8 GB of installed memory. As shown in Table 2, the encryption of the Lena image is completed in just 0.3166 seconds, with an average encryption time of 0.3234 seconds for all tested images. Furthermore, a comparison with other published works, such as those by(Masood et al., 2022; Gaoet al., 2022 and Abduljabbar et al., 2022) highlights the superior computational efficiency of the proposed method.

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

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)



(e) (f) (g) (h)

(i) (j) (k) (l)

FIGURE2:Normaltestimages,cipherimagesanddecrypted images:(a) Lena normal image; (b) Truck normal image; (c) Butterfly normal image; (d) Girl normal image; (e) Lena cipher image; (f) Truck cipher image; (g) Butterfly cipher image; (h) Girl cipher image;(i) Lena decrypted image; (j) Truck decrypted image; (k) Butterfly decrypted image; (l) Girl decryptedimage

.

TABLE 2: Speed (Encryption) of proposed algorithm and a comparison		
Algorithm	**Image**	**Speed (sec)**
Proposed	Lena	0.3166
	Truck	0.3439
	Butterfly	0.329
	Girl	0.3044
	Average	**0.3234**
Ref. (Masood et al., 2022)	Baboon	2
Ref. (Gao et al., 2022)	-	0.54
Ref. (Abduljabbar et al., 2022)	Lena	0.3493
Ref. (Wang and Gao, 2020)	Lena	0.16

C. ANALYSIS OF FLOATING FREQUENCY

Chief objective of any image cryptosystem is to achieve effective diffusion and confusion of image pixels, ensuring a uniform distribution across all rows and columns. The concept of floating frequency systematically evaluates this characteristic, as described in (Iqbal et al., 2021). If the diffusion and confusion processes are inadequate, this parameter exposes the deficiencies, allowing cryptographers to refine their algorithms.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

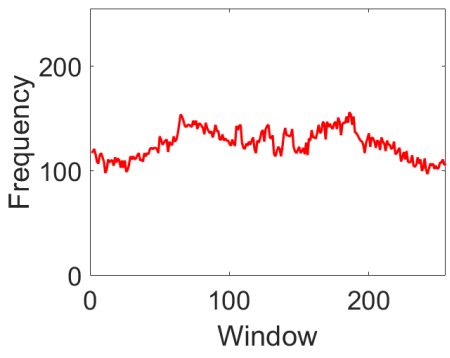
In the evaluation using the construct of floating frequency, 256-pixel windows are taken from both ciphertext and plaintext images for analysis. This process assesses the extent to which pixel intensities differ within these windows, using two measures: column-wise floating frequency (CWFF) and row- wise floating frequency (RWFF). This metric is computed bysteps below:

1) Extract 256-pixel windows from image, forming rows and columns for analysis.
2) Compute CWFF and RWFF for each window.
3) Plot the mean values of CWFF and RWFF in graphical form.

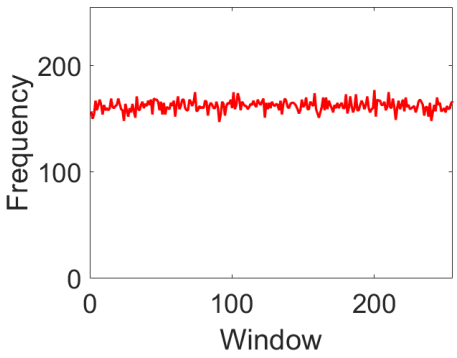
Figure 3 illustrates the *CWFF* and *RWFF* results for both the plain and cipher versions of the Lena image. In Figure 3a, the floating frequency graph for the plain Lena image (columns 1 to 256) reveals relatively more pixels with identical intensity values. Consequently, *CWFF* values are lower for the selected windows. In contrast, Figure 3b demonstrates a reduced number of pixels sharing the same intensity in the cipher image. This indicates a higher number of distinct intensity values across all columns, suggesting enhanced security due to the proposed cryptosystem.

The average *CWFF* values for plain and cipher images of Lena are 163 and 125, respectively. Expressed as percent ages, these values correspond to 49% and 63%. A higher percentage of *CWFF* in the encrypted image reflects stronger security effects.

Similarly, Figures 3c and 3d depict the *RWFF* for the plain and cipher images of Lena, with average values of 106 and 162, respectively. In percentage terms, these values are 42% for the plain image and 63% for the cipher image. A higher *RWFF* percentage in cipher images is indicative of better security performance, validating the effectiveness of the proposed encryption scheme.

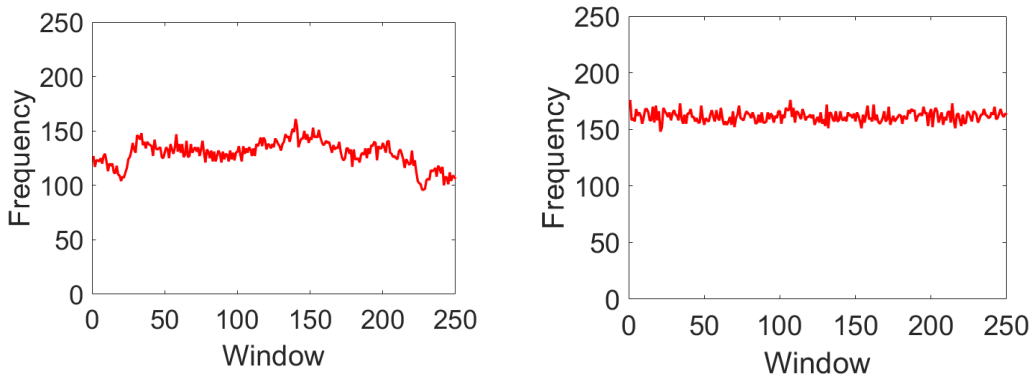


(a)



(b)

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)



(c) (d)

FIGURE3:Floatingfrequency (FF)analysisforTruck imageandmean value: (a) FF (column) of plain image,125; (b) FF (column) of cipher image, 163; (c) FF (row) of plain image, 106; (d) FF (row) of cipher image,162.

TABLE 3: Entropy results			
Algorithm	**Image**	**Plain**	**Cipher**
Ours	Lena	7.5835	7.9976
	Truck	6.7093	7.9974
	Butterfly	6.5148	7.9972
	Girl	6.8449	7.9975
	Average	6.9131	7.9974
Ref. (Masood et al., 2022)	Baboon	-	7.9966
Ref. (Gao et al., 2022)	-	-	7.9999
Ref. (Abduljabbar et al., 2022)	Lena	-	7.99918
Ref. (Wang and Gao, 2020)	Lena	-	7.9992

D. INFORMATION ENTROPY ANALYSIS

Information entropy (IE) or simply entropy, is a widely used security parameter for assessing the utility of ciphers and their resilience against attacks by hackers. This analysis evaluates the degree of scattering in the pixel values of the given image. For a grayscale image with 256 intensity levels, the maximum possible entropy value is 8. If the entropy of a ciphered image approaches the reported ideal value, it signals that cipher has effectively achieved pixel confusion and diffusion, signifying strong security properties. The mathematical formula for entropy, introduced in 1949, is as follows:

$$IE(s) = \sum_{i=0}^{2^n-1} p(s_i) log \frac{1}{p(s_i)} \quad (4)$$

In this context, $IE(s)$ denotes entropy of signal s. The results of entropy for the chosen images are presented in Table 3. The proposed algorithm demonstrates superior performance in terms of this important metric compared to the method described in (Masood et al., 2022).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

The images selected for this research work have the sizes of 256×256. For larger images, this metric tends to yield better results, whereas smaller images generally produce less favorable outcomes.

E.DIFFERENTIAL ATTACK ANAYSIS

Hackers sometimes resort to the differential attack on the ciphers. The peculiar dynamics of this attack works like this. Hacker arranges two samples of the plaintext image. One image has a negligibletempering in intensity value of pixel whereas the second image is straightforward. Now these two plaintext images are encrypted by calling the encryption algorithms. The pixel intensity values of these two images exhibit a secret relationship, which, if analyzed further, could help hackers uncover secret key. To counter this vulnerability, researchers have developed the security metrics *NPCI* (Number of Pixels Change Rate) and *UACI* (Unified Average Changing Intensity). The mathematical expressions for these metrics are as follows:

$$NPCR = \frac{\sum_{s,r} R(s,r)}{m \times n} \times 100\% \qquad (5)$$

TABLE 4: Findings of differential attack analysis		
Image	**NPCR (%)**	**UACI (%)**
Lena	99.6411	33.6016
Truck	99.6200	33.5008
Butterfly	99.6299	33.6187
Girl	99.6074	33.6876
Average	**99.6246**	**33.6022**

.

TABLE 5: A comparative analysis of differential attacks			
Scheme	**Image**	**NPCR (%)**	**UACI (%)**
Suggested	Lena	99.6411	33.6016
Ref. (Masood et al., 2022)	Lena	99.6	36.11
Ref. (Gao et al., 2022)	-	99.62	33.46
Ref. (Abduljabbar et al., 2022)	Lena	99.61937	33.44153
Ref. (Wang and Gao, 2020)	Lena	99.604	33.4736

The values (m, n) indicate the size of the image under consideration. Further, $R(s, r)$ is mathematically expressed as

$$R(s,r) = \begin{cases} 1, if\ \ Encrypted(s,r) \neq Encrypted'(s,r), \\ 0, if\ \ Encrypted(s,r) = Encrypted'(s,r) \end{cases}$$

$$UACI = \sum_{i,j} \frac{|Encrypted(s,r) - Encrypted'(s,r)|}{255 \times m \times n} \times 100\%$$

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

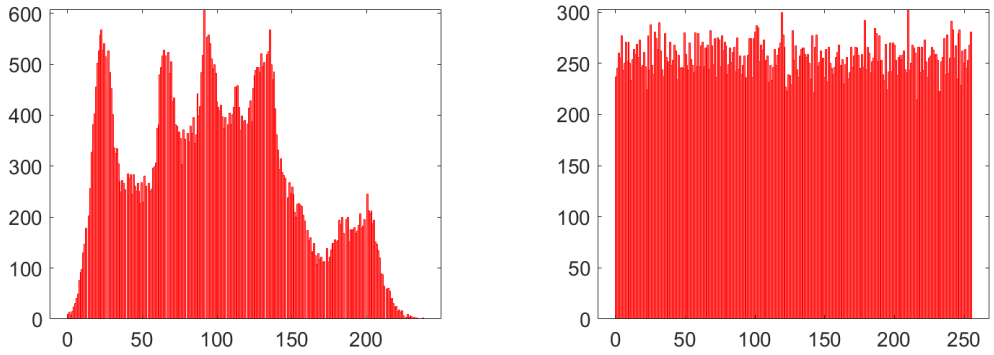
In the above equation, the variables *Encrypted* and *Encrypted′* correspond to the encrypted images with no change in the intensity and with a change in the intensity values in a respective way. Table 4 presents the experimental results of these metrics for the selected test images. Forthe Lena image, the calculated values are 99.6411% and 33.6016%, while the average values across all four test images are 99.6246% and 33.6022%. These results are sufficiently close to the ideal values, indicating that the proposed novel image cipher possesses the necessary capability to effectively resist potential differential attacks. Apart from that, proposed study beats the published studies(Masoodet al., 2022;Gao et al., 2022; Abduljabbar et al., 2022; Wang and Gao, 2020) regarding the security parameters of NPCR and UACI respectively.

F. STATISTICAL ANALYSIS

In this heading, the image cryptographers carry out the histogram and correlation coefficient analyses.

1) Histogram analysis

Hundreds of thousands of tiny pixels make up the plaintext images. These pixels have different intensity values. The tool of histogram provides us the distribution of pixel intensity values in an arranged fashion. The histograms of cipher and plain images are different with each other. For plaintext images, the histograms have a slanting bar over them. Besides, for ciphertext images, their histograms have a rather smooth bar. Of course, such smoothness of the histogram bars plays as a major resistance to the future histogram attacks. Figure 4 shows that the histogram of the plaintext image has a curved bar. In sharp contrast to that, the histogram of the ciphertext has a very smooth looking of its bar. Therefore, we are justified in saying that the proposed image cipher is resistant to the potential threat of histogram attack. Additionally, Figure 5 depicts the drawings of histograms of plain and cipher White and Black images. One can notice vertical lines for histograms of Black (Figure 5b) and White (Figure 5f) images. The reason of this is that the reported two images are furnished with an alone intensity values of 255 and 0 in a respective manner.



(a) (b)

FIGURE 4: Lena image histogram analysis. (a) Plaintext image (b) Ciphertext image.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

2) Correlation coefficient analysis

The pixels of the given plaintext image are tightly correlated with each other. When some image cipher is applied on some plaintext image, its pixels datasuffer an across the board change in both of its locations and the intensity values. Resultantly, powerful interconnectedness among pixels gets dismantled. For measuring the intrinsic correlation among pixels data, the equation below is normally used. (CC) (Kamal et al., 2021):

$$CC = \frac{N\sum_{j=1}^{N}(x_j \times y_j) - \sum_{j=1}^{N} x_j \times \sum_{j=1}^{N} y_j}{\sqrt{(N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_j)^2)(N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \quad (5)$$

In the described formula, the symbol *N*denotes total number of pixels in the image, while variables *x* and *y*stand for the pixels' intensity values. The correlation distribution between the pixels of the plain and cipher images is illustrated in Figure 6, considering three orientations: diagonal, horizontal, and vertical.

Table 6 presents the correlation coefficient between two adjacent pixels in the plain and cipher versions of the Lena image. As shown, this metric is nearly equal to one for the plain image and close to zero for the cipher image. Additionally, Table 7 provides a comparison of results, demonstrating that outcomes are comparable. Apart from that, 6,000 pairs for pixels data were arbitrarily selected from images, and the relevant formula was applied to these pairs. Findings exhibit significant variability due to the randomness of the selection process, as some pairs may yield better outcomes while others may not.

TABLE 6: Findings of correlation coefficient parameter.

Image	Corre. direc.		
	H	V	D
Lena plain image	0.9287	0.9098	0.9177
Lena cipher image	0.0043	0.0081	0.0034

G. PEAK SIGNAL TO NOISE RATIO ANALYSIS

The Peak Signal-to-Noise Ratio (PSNR) provides an objective evaluation of the extent of difference in pixel values be- tween the plain and cipher images. Its mathematical formula is given as:

$$\begin{cases} PSNR = 20\, log_{10}\left(255/\sqrt{MSE}\right) dB \\ MSE = \frac{1}{m \times n}\sum_{f=1}^{m}\sum_{g=1}^{n}(Plain(s,r) - Cipher(s,r))^2 \end{cases} \quad (6)$$

In theabove equation, *m* and *n* represent the dimensions (length and width) of the images under consideration, while *Plain*(*s*, *r*) and *Cipher*(*s*, *r*) correspond to the intensity values of the plain and cipher images at pixel location (*s*, *r*). Additionally, *MSE* denotes the mean squared error. A higher *MSE* indicates stronger security effects, whereas a lower *PSNR* value is preferred, as these two parameters are inversely related.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

Table 8 presents the *PSNR* results obtained by suggested method alongside other studies available in the open literature. As per thereported table, the *PSNR*findings are infinite (*Inf*) when calculated for plain and cipher images, implying that the plain and cipher images are identical due to the factor of*MSE = 0*. This also indicates that there both the restored and plain images suffered no loss. In the table, the abbreviation 'O-C' denotesplaintext and ciphertext images, while 'O-D' denotes the plaintext and restored images.

Furthermore, the PSNR findings for the Lena image achieved by proposed method are superior when compared to other works such as (Ihsan and Do˘gan, 2023; Mansoor and Parah, 2023). This demonstrates that the current study outperforms the others.

H. ANALYSIS OF IMAGE ROTATION ASSAULT

Occasionally, cryptanalytic savvy attempt image rotation assault/attack on image cryptosystems to gain unauthorized access to plaintext image. This attack dynamics proceeds like this. Given ciphertext image gets rotated by a certain degree, denoted as r^o. Ciphertext image is then rotated in other direction using relevant pixels lying on horizontal and vertical directions. In horizontal direction, from the rightmost margin, first non-zeropixel value is identified, and from the leftmost margin, distance of this non-zero pixel value is found. Similar processes are conducted in vertical direction.

Formulas below are utilized for finding r'^o—degree of rotation.

$$r'^0 = tan^{-1}\left(\frac{p}{q}\right) \tag{7}$$

$$rr^0 = \begin{cases} -r'^0 & if\ 0^0 < r^0 < 90^0 \\ -(180 - r')^0 & if\ 90^0 < r^0 < 180^0 \\ -(270 - r')^0 & if\ 180^0 < r^0 < 270^0 \\ -(360 - r')^0 & if\ 270^0 < r^0 < 360^0 \end{cases} \tag{8}$$

The symbolsr^o andrr^o present in the above equations, representhacker's degree of rotation and reverse rotation degree in a respective way. Additionally, the symbols of *p* and *q* refer to vertical & horizontal distances of two corners of image under consideration from the corner of top-left. Moreover, Figures 7a and 7c display ciphertextimages Butterfly and Girl after rotation degrees of 30^o and 45^o, respectively. Furthermore, Figures 7b and 7d illustrate restored images. It is evident that recovered images are easily recognizable, highlighting efficacy and effectiveness of suggested image cipher in resisting future rotation attacks.

To assess the integrity of decrypted images in a dispassionate fashion, image cryptographers commonly use the security parameter of *PSNR*. Table 9 presents the *PSNR* values for the Butterfly and Girl images. A relatively larger *PSNR* value indicates that the decrypted image closely resembles the original images. Additionally, a comparison has been conducted with (El- Khamy and Mohamed, 2021; Elsadany et al., 2023). The results of the proposed work surpass that of (Elsadany et al., 2023).

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

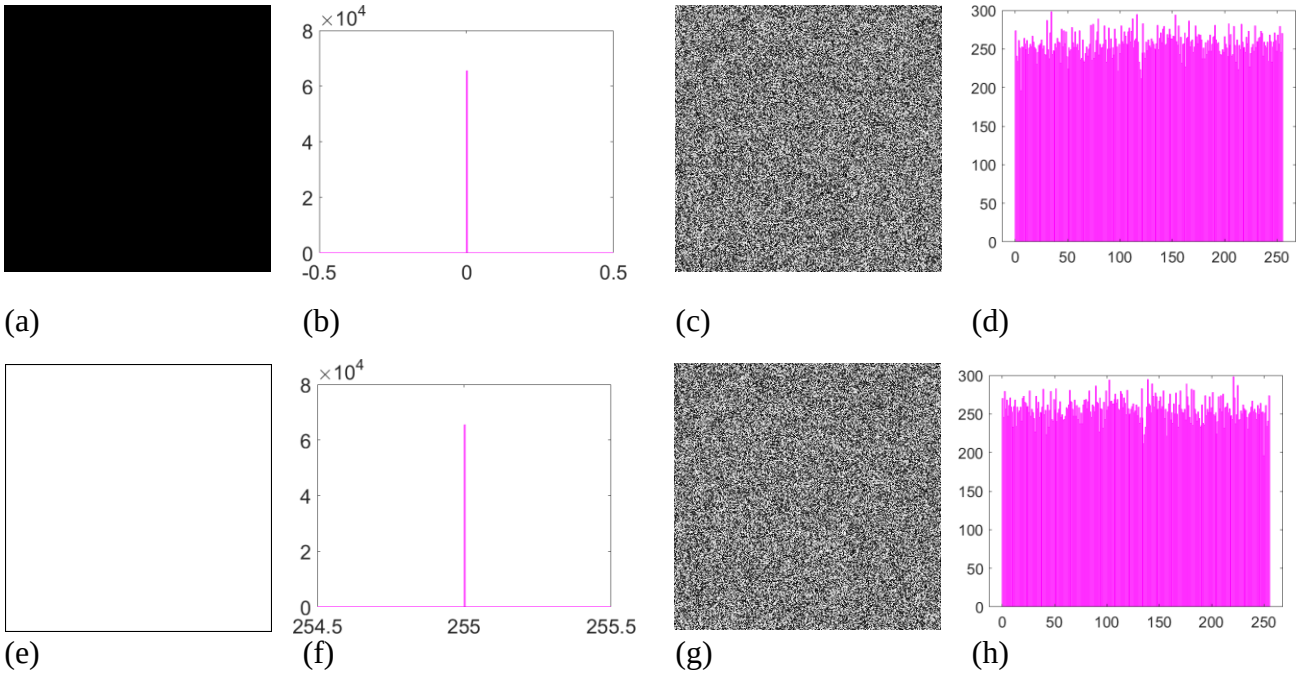


FIGURE5:BlackandWhiteimagesandtheirhistograms:(a)TotalBlackimage;(b)Histogramoft otalBlackimage;(c)Cipher image of total Black image; (d) Histogram of total Black cipher image; (e) Total White image; (f) Histogram of total White image; (g) Cipher image of total White image; (h) Histogram of total White cipherimage.

TABLE 7: Correlation coefficients analysis results and its comparison with published literature.				
Types of image	**Encryption scheme**	**Correlation direction**		
		Horizontal	**Vertical**	**Diagonal**
Lena plaintext image		0.9287	0.9098	0.9177
Lena ciphertextimage	Suggested	0.0043	0.0081	0.0034
	Ref. (Masood et al., 2022)	0.0005	0.1313	-0.0047
	Ref. (Gao et al., 2022)	0.0013	-0.0009	-0.0023
	Ref. (Abduljabbar et al., 2022)	0.0033	0.007	0.0027
	Ref. (Wang and Gao, 2020)	0.0002	0.0022	-0.0015

.

TABLE 8: PSNR results						
Algorithm		**Lena**	**Truck**	**Butterfly**	**Girl**	**Average**

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

Proposed	PSNR (O-D)	*Inf*	*Inf*	*Inf*	*Inf*	*Inf*
	PSNR (O-C)	8.5177	9.2981	8.7872	8.6532	8.8140
Ref. (Ihsan and Do˘gan, 2023)	PSNR (O-C)	19.8469	-	-	-	-
Ref. (Mansoor and Parah, 2023)	PSNR (O-C)	9.2736	-	-	-	-

TABLE 9: Analysis of image rotation attack.

Study	**Image**	**PSNR**
Suggested	Butterfly	14.8854
	Girl	13.3654
Ref. (Elsadany et al., 2023)	Lena	9.739
Ref. (El-Khamy and Mohamed, 2021)	Lena	26.5053

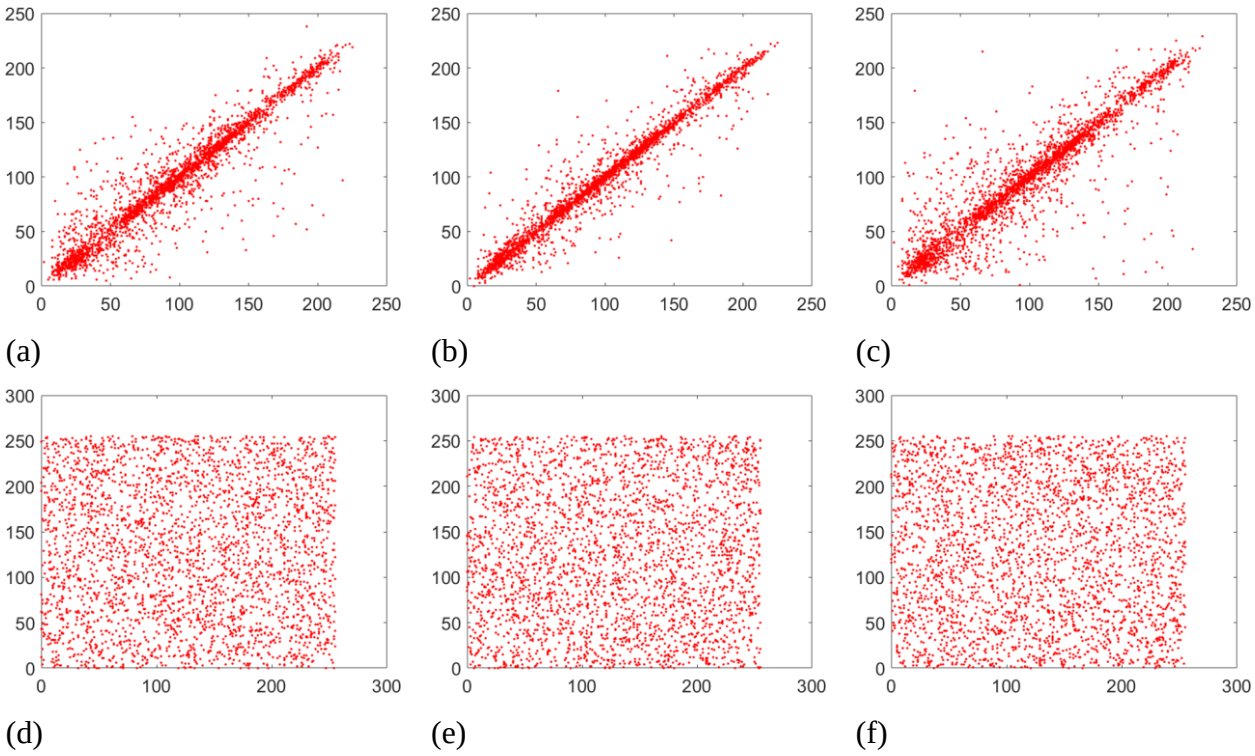


FIGURE 6: Distributions of correlation for Lena image: (a) Horizontal direction for plain image; (b) Vertical direction for plain image; (c) Diagonal direction for plain image; (d) Horizontal direction for cipher image; (e) Vertical direction for cipher image; (f) Diagonal direction for cipher image.

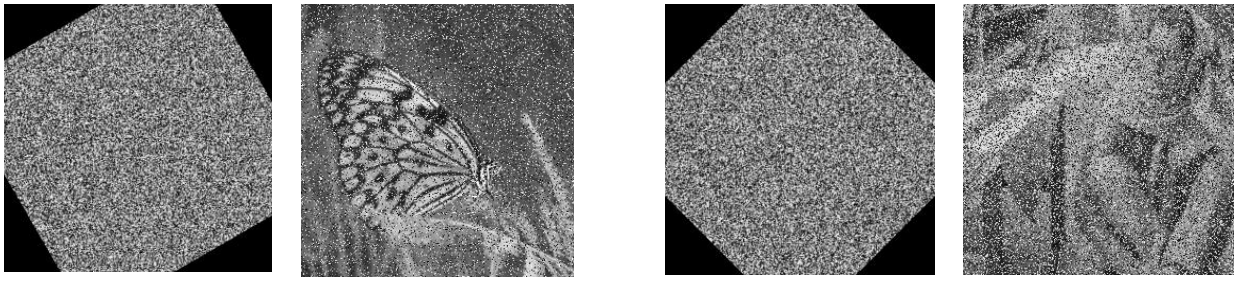
I. COMPUTATIONAL COMPLEXITY ANALYSIS

The speed analysis in Section 5-B highlights certain performance aspects but has limitations. Factors such as software, hardware, platform, and input images significantly

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

influence speed metrics, complicating an exact assessment of the algorithm's performance. To achieve a more intrinsic evaluation, theoretical methods like asymptotic analysis, a mathematical approach discussed in (Ramesh and Gowtham, 2017), are often employed to provide deeper insights into speed and efficiency.

Section 3-A calculates the five streams ofrandom numbers, i.e.,$\{pointx_t\}_{t=1}^{mn+n_0}$, $\{point\ y_t\}_{t=1}^{mn+n_0}$, $\{length_t\}_{t=1}^{mn+n_0}$, $\{lattice_t\}_{t=1}^{mn+n_0}$, $\{mask_t\}_{t=1}^{mn+n_0}$ and $\Theta(5mn)$ steps. Now, we analyze the time complexity of the Algorithm 1. Lines 2 and 3 initialize the matrices $TempMatix1$ and $TempMatix2$ and takes $\Theta(2mn)$ steps. The *if* condition at the line 4 and following lines (5 - 8) takes $\Theta(5mn)$steps. The remaining lines (12 - 22) of the algorithm take $\Theta(11mn)$steps. Lastly, the final line 24 takes the $\Theta(1mn)$step. By adding all these individual time complexities, the total time complexity comes out to be $\Theta(24mn)$ which is equal to (Chai et al., 2019; Wu et al., 2018).



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

FIGURE7:Depiction of resilience of rotation attack for cipher images:(a)Rotation of 30^0 (Butterfly image);(b)Restored image from (a) ;(c)Rotation of 45^0 (Girl image); (d)Restored image from (c).

6. CONCLUSION

By swapping the randomly selected bits of arbitrarily selected pixels from given plaintext image, new scrambling procedure has been introduced in this research project. In particular, square matrices from the 2D lattice have been dynamically generated. Further, their determinants have been calculated. These calculated determinants have been further customized to make them fall within the given range of numbers. The same operation has been carried by reversing the streams of random numbers. These steps make an address of first pixel. The address of the second pixel has been calculated by subtracting these values from the dimensions of the given input image. Now, from the addresses of these two pixels, two bits (one bit from each pixel) have been selected arbitrarily. These selected bits are swapped with each other. Moreover, the diffusion operation has been carried out ina parallel fashion to introduce more complications to the potential hackers. These steps have been looped for numerous times to add both the confusion and diffusion effects. Simulation and security evaluation procedures indicate that the suggested image encryption scheme bears the potential to avert the potential threats of hacking and has the ample promise for some real world application. As far as the future work is concerned, we intend to apply the proposed idea for multiple images and in a 3D setting.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

References

Abduljabbar, Z. A., Abduljaleel, I. Q., Ma, J., Al Sibahee, M. A., Nyangaresi, V. O., Honi, D. G., ... & Jiao, X. (2022). Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. *IEEE Access*, *10*, 26257-26270.

Ahmad, M., Agarwal, S., Alkhayyat, A., Alhudhaif, A., Alenezi, F., Zahid, A. H., & Aljehane, N. O. (2022). An image encryption algorithm based on new generalized fusion fractal structure. *Information Sciences*, *592*, 1-20.

Chai, X., Fu, X., Gan, Z., Lu, Y., & Chen, Y. (2019). A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Processing*, *155*, 44-62.

Deshpande, K., Girkar, J., & Mangrulkar, R. (2023). Security enhancement and analysis of images using a novel Sudoku-based encryption algorithm. *Journal of Information and Telecommunication*, *7*(3), 270-303.

El-Khamy, S. E., & Mohamed, A. G. (2021). An efficient DNA-inspired image encryption algorithm based on hyper-chaotic maps and wavelet fusion. *Multimedia Tools and Applications*, *80*(15), 23319-23335.

Elsadany, A. A., Elsonbaty, A., & Hagras, E. A. (2023). Image encryption and watermarking in ACO-OFDM-VLC system employing novel memristive hyperchaotic map. *Soft Computing*, *27*(8), 4521-4542.

Gao, X. (2021). Image encryption algorithm based on 2D hyperchaotic map. *Optics & Laser Technology*, *142*, 107252.

Gao, X., Mou, J., Banerjee, S., Cao, Y., Xiong, L., & Chen, X. (2022). An effective multiple-image encryption algorithm based on 3D cube and hyperchaotic map. *Journal of King Saud University-Computer and Information Sciences*, *34*(4), 1535-1551.

Ghosh, S., Bhattacharyya, P., & Dutta, A. (2013, January). FPGA based implementation of a double precision IEEE floating-point adder. In *2013 7th International Conference on Intelligent Systems and Control (ISCO)* (pp. 271-275). IEEE.

Gupta, V., Mittal, M., & Mittal, V. (2020). Chaos theory: an emerging tool for arrhythmia detection. *Sensing and Imaging*, *21*(1), 10.

Hua, Z., Zhu, Z., Chen, Y., & Li, Y. (2021). Color image encryption using orthogonal Latin squares and a new 2D chaotic system. *Nonlinear Dynamics*, *104*(4), 4505-4522.

Ihsan, A., & Doğan, N. (2023). Improved affine encryption algorithm for color images using LFSR and XOR encryption. *Multimedia Tools and Applications*, *82*(5), 7621-7637.

Iqbal, N., Hanif, M., Abbas, S., Khan, M. A., & Rehman, Z. U. (2021). Dynamic 3D scrambled image based RGB image encryption scheme using hyperchaotic system and DNA encoding. *Journal of Information Security and Applications*, *58*, 102809.

Jamaludin, J., & Romindo, R. (2020). Implementation of Combination Vigenere Cipher and RSA in Hybrid Cryptosystem for Text Security. *IJISTECH (International Journal of Information System and Technology)*, *4*(1), 471-481.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.02 No.04 (2024)

Jasra, B., & Moon, A. H. (2020, January). Image encryption techniques: A review. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 221-226). IEEE.

Jiang, Q., Yu, S., & Wang, Q. (2023). Cryptanalysis of an image encryption algorithm based on two-dimensional hyperchaotic map. *Entropy*, *25*(3), 395.

Kamal, S. T., Hosny, K. M., Elgindy, T. M., Darwish, M. M., & Fouda, M. M. (2021). A new image encryption algorithm for grey and color medical images. *Ieee Access*, *9*, 37855-37865.

Kanwal, S., Inam, S., Othman, M. T. B., Waqar, A., Ibrahim, M., Nawaz, F., ... & Hamam, H. (2022). An effective color image encryption based on Henon map, tent chaotic map, and orthogonal matrices. *Sensors*, *22*(12), 4359.

Khan, J. S., Ahmad, J., Ahmed, S. S., Siddiqa, H. A., Abbasi, S. F., & Kayhan, S. K. (2019). DNA key based visual chaotic image encryption. *Journal of Intelligent & Fuzzy Systems*, *37*(2), 2549-2561.

Mansoor, S., & Parah, S. A. (2023). HAIE: a hybrid adaptive image encryption algorithm using Chaos and DNA computing. *Multimedia Tools and Applications*, *82*(19), 28769-28796.

Masood, F., Boulila, W., Alsaeedi, A., Khan, J. S., Ahmad, J., Khan, M. A., & Rehman, S. U. (2022). A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map. *Multimedia Tools and Applications*, *81*(21), 30931-30959.

Pourasad, Y., Ranjbarzadeh, R., & Mardani, A. (2021). A new algorithm for digital image encryption based on chaos theory. *Entropy*, *23*(3), 341.

Ramesh, V. P., & Gowtham, R. (2017). Asymptotic notations and its applications. *Ramanujan Math Soc Math Newsl*, *28*(4), 10-16.

Roy, S., Shrivastava, M., Rawat, U., Pandey, C. V., & Nayak, S. K. (2021). IESCA: An efficient image encryption scheme using 2-D cellular automata. *Journal of Information Security and Applications*, *61*, 102919.

Santhanalakshmi, M., Lakshana, M., & GM, M. S. (2023). Enhanced AES-256 cipher round algorithm for IoT applications. *The Scientific Temper*, *14*(01), 184-190.

Subaselvi, S., Mytheesh, C., Sanjay, R., & Ragunath, S. D. (2023, February). VLSI Implementation of Triple-DES Block Cipher. In *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 1162-1166). IEEE.

Wang, X., & Gao, S. (2020). Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. *Information sciences*, *539*, 195-214.

Wang, X. Y., & Zhao, G. B. (2010). Hyperchaos generated from the unified chaotic system and its control. *International Journal of Modern Physics B*, *24*(23), 4619-4637.

Wu, X., Wang, K., Wang, X., Kan, H., & Kurths, J. (2018). Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Processing*, *148*, 272-287.

Zhu, S., & Zhu, C. (2020). Secure image encryption algorithm based on hyperchaos and dynamic DNA coding. *Entropy*, *22*(7), 772.