IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 19 July 2024, accepted 18 August 2024, date of publication 22 August 2024, date of current version 3 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3447889

RESEARCH ARTICLE

A Novel 1-Dimensional Cosine Chaotic Equation and Digital Image Encryption Technique

FARMAN ULLAH[1,2], ZIAUDDIN[1], MUHAMMAD FAHEEM[3], (Member, IEEE), MUNTAZIM ABBAS HASHMI[4], AQEEL-UR-REHMAN[5], RAB NAWAZ BASHIR[5,6], AND AMJAD REHMAN KHAN[6], (Senior Member, IEEE)

[1]Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan 22044, Pakistan
[2]Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus, Abboottabad 22060, Pakistan
[3]School of Computing Technology and Innovations, University of Vaasa, 65200 Vaasa, Finland
[4]Institute of Mathematics, Khwaja Fareed University of Engineering and Information Technology (KFUEIT), Rahim Yar Khan 64200, Pakistan
[5]Department of Computer Science, COMSATS University Islamabad, Vehari Campus, Vehari 61100, Pakistan
[6]Artificial Intelligence and Data Analytics Laboratory(AIDA), College of Computer and Information Sciences (CCIS), Prince Sultan University, Riyadh 12435, Saudi Arabia

Corresponding author: Muhammad Faheem (muhammad.faheem@uwasa.fi)

This work was supported in part by the University of Vaasa, and in part by the Academy of Finland.

ABSTRACT In the 21st century, the digital era, chaotic systems become the backbone in designing the secure ciphers for image cryptography because of their intrinsic features like dynamical behavior and sensitivity to initial conditions. In this regard, 1-dimensional (1D) non-linear dynamical systems are one of the most studied in chaos theory. Besides the advantages of 1D chaotic systems, these systems have short periods and a short range of control parameters. A new 1D chaotic system called as Cosine Chaotic Equation (CCE) was developed to address this issue. The new and simple chaotic system has a larger range of control parameters α which increases the key space to make brute force attacks infeasible. The system is rigorously tested using the randomness evaluation metrics SP800-22 test suite recommended by the National Institute of Standards and Technology (NIST). It proved itself as an excellent addition in the pool of 1D chaotic systems to use safely in designing new ciphers. The new dynamical system is applied in an image encryption technique to prove its efficacy.

INDEX TERMS Cryptography, pseudo-random number generator (PRNG), CCE, chaos theory, non-linear dynamical system, image encryption.

I. INTRODUCTION

The rapid and continuous growth of the computer network is indispensable for every individual and organization concerned with communication technologies. It preserves their privacy in terms of their data security. Every transmission of sensitive data through ordinary networks is not reckless. Most existing algorithms commonly applied for securing transmitted information are more likely suitable for textual data. On the other hand, in today's digital era, images conceal more informative dimensions of the corresponding data than textual data and, thereby, are more significant than textual data. Network users are becoming increasingly conscious of the threats posed by privacy breaches. The constant streams of information leakage that occur throughout the process of network transmission and storage is due to the rapid growth of computer networks. As a result, network information security becomes challenging, which makes the data encryption crucial. From this perspective, effectively securing the transmission of sensitive images over the communicative network is a major challenge [1]. Currently, information protection is indispensable for every individual and organization that persists their privacy in terms of their data security. Every communication needs and deserves the ability to send and receive data in a secure and timely manner – the key ideology of the information cryptography [2].

Conventional text encryption algorithms like DES, IDEA, and RSA can be used to encrypt the data securely and

The associate editor coordinating the review of this manuscript and approving it for publication was Lo'ai A. Tawalbeh.

are not appropriate for the encryption of images due to the vast data volume and data correlation properties of images. Therefore, images' special characteristic and chaotic cryptography has become a workable solution for their encryption. Currently, the researchers [3], [4] are interested in discrete chaotic systems in 1D array encryption because it's easy to understand and implement. The chaotic systems are extremely sensitive to their initial condition and control parameters [5]. For such dynamic systems, even a slight variation in the seed produces significantly different results. However, the degree of sensitivity will be quite greater if the change in seed is higher/larger, hence suitable to encrypt large amount of data like digital images. Many image encryption algorithms that have recently been introduced use varieties of chaotic maps and inventive techniques like tri-partite graphs [6], optical transformations [7], sequence procedures in DNA [8], S-BOX [9], [10], [11] and improved chaotic map [12] for encryption.

A complex system that utilizes deterministic thinking is a chaotic map. Extreme randomness and non-linear behavior can be seen in these chaotic systems [13], [14]. The image encryption algorithms employ two primary methods, i.e., scrambling [15] and diffusion [16]. In Particular, scrambling involves altering pixel positions to reduce pixel correlation and accomplish encryption, while diffusion is a highly secure image encryption technique that disperses pixel information across the image. To apply the above techniques, there are two approaches in common. Some researchers utilize pixels as units, while others employ matrices as units, permuting or shuffling the image either by pixels or matrices. The matrices can be in the form of row matrices or column matrices [17], [18], [19].

Researchers are perpetually developing encryption algorithms to achieve secure communication on public networks. In order to create the effective image encryption systems with good features in terms of speed, cost, processing power, complexity, and vulnerability, the chaos-based cryptographic models are used [20]. There are two general categories of cryptography, i.e., symmetric key cryptography and asymmetric key cryptography. In ours case, symmetric key cryptography is related to the proposed model, therefore, we only discuss it in the context of this paper. In particular, a single key is used for both encryption and decryption in symmetric key cryptography, which is commonly referred to as private key or secret key encryption [21]. There are two categories of symmetric encryption in the literature, i.e., block ciphers and stream ciphers [22]. The stream ciphers encrypt the data one bit at a time, and block ciphers encrypt the data in chunks. Block ciphers use an initialization vector as an additional layer of protection against brute force assaults [20]. Symmetric key cryptography is much simple to use and is ideal for encrypting data files of huge size [23]. Compared to asymmetric algorithms, symmetric algorithms have shorter key length and are faster [24].

In the current research of digital cryptography, various dimensions-enhanced chaotic systems remain commonly practiced. In past few years, several new algorithms are proposed in the area of image encryption for example with hyperchaotic maps along with usage of memristive techniques and neural networks in [25], [26], [27], and [28]. The researches prove that the future of secure and efficient image encryption will be in the hands of chaos-based approaches Moreover, many researchers have used 1D and 2D chaotic techniques for encryption. For instance, the bifurcation analysis and encryption application of dual logistic mapping is proposed by Elsadany et al. [29]. Similarly, logistic mapping based on the complex dynamic conduct of dual-period impulse force was introduced by Jiang et al. [30]. Moreover, the association between the initial-value and the parameters of the fractal controls is exploited to improve the performance of logistic mapping [31]. Caraballo described the comprehensive analysis of the dynamic features of their proposed model based on the 2D Henon continuous model [32]. A review of the features of numerous chaotic systems illustrate the benefits of simplicity and speed of 1D discreteness of those systems.

However, a prevalent drawback is the existence of a minimal key space of that system, which quickly leads to cracking and exploitation [33]. The key space of higher dimension systems (i.e., 3D and 4D) is higher, but their implementation is more complex and less efficient. By implementing 3D and 4D based systems, hyper-chaotic systems can be achieved by aggregating trial-and-error techniques with state-based feedback control [32], [34]. Although the performance of higher dimensionality is better, they suffer from error sensitivity, predictability, implementation complexity and limited efficiency. Compared to the hyper-chaotic systems, 1D non-linear systems boast computational efficiency, simple structure and ease of implementation. Despite these properties, they behave dynamically in complexity, enhancing their suitability for practical applications.

As we discussed, the limited key size of classical 1D chaotic systems creates a small pool of key space, which in turns opens a loophole for brute-force attacks. Therefore, to effectively address the aforementioned research challenges, **A novel Cosine Chaotic Equation named CCE** is proposed, which will generate pseudo-random numbers with enhanced randomness and will be a candidate for use in digital image cryptography. The effectiveness of CCE will be validated by employing state-of-the-art evaluation metrics and NIST tests. A newly designed image encryption algorithm will use the proposed CCE in coordination with the SHA-2 hash function to strengthen the argument. The SHA-2 is a popular cryptographic hash function that generates 256, 384 and 512 bit lengthy hash strings. This mechanism makes it more difficult for the attackers to tamper or forge the underlying or transmitting data in the system. The SHA-2 family of hash functions is specified by NIST[1] as part of the Secure Hash Standard. Comparatively, one of the members of the SHA-2 family is more reliable than SHA-1 and MD5 in

[1]National Institute of Standards and Technology.

diverse application scenarios [35]. It is deemed better than its version because of it's larger output size [36], [37].

The key contributions of this work are described as follows:

- We introduce a novel chaotic system called Cosine Chaotic Equation (CCE) to generate the pseudo-random numbers.
- The new system CCE will be analyzed using the Lyapunov Exponent, Bifurcation diagram, Phase Space, information entropy, uniform distribution etc.
- The new system CCE will be pushed in the NIST test to verify its applicability in cryptography.
- We propose a novel image encryption algorithm enhanced through the SHA-384 hash function. The algorithm is designed to be secure, efficient, and easy to implement. The algorithm's security is based on the difficulty of breaking the SHA-384 generated stream.

II. PERFORMANCE ANALYSIS

Before proceeding to the performance analysis, we will introduce the proposed system's mathematical representation and its characteristics.

A. PROPOSED COSINE CHAOTIC EQUATION (CCE)

High-dimensional chaotic systems are more complex than 1D chaotic systems regarding understanding and implementation. The 1D systems are widely accepted due to their ease and simplicity of implementation, but most lack larger key spaces. So, the proposed approach exploits a 1D chaotic system with comparatively a larger key space to generate random numbers. The objective function of the proposed model to generate the required random numbers is defined as:

$$x_n = \cos\left(x_{n-1}\right)^{1-\alpha} + \frac{1}{x_{n-1}} \bmod 1 \tag{1}$$

where x is the initial seed in the range of [0,1], and α is the control parameter in the range of $1.47096 > \alpha \geq -6.00000$. The proposed system is called Cosine Chaotic Equation or CCE. The α is the controlling parameter, and the modulus operator **mod** is used to enforce the output between 0 and 1. The applied parameters α control the spreading behavior of the Equation and possesses values in the range $1.47097 \leq \alpha \geq -6.00000$ with a floating point precision of 10^{-5} and initial seeds x_i with a floating point precision equal to 10^{-14}. The output of the above equation lies in the range of 0 and 1. In this study, we will conduct a thorough analysis of CCE to confirm the working functionality of the proposed chaotic system.

B. LYAPUNOV EXPONENT ANALYSIS

The Novel Cosine Chaotic Equation (CCE) and the Logistic map are 1D dynamical system that exhibit chaos, which their positive Lyapunov exponents represent. The part of blue and red lines are positive Lyapunov and negative Lyapunov scores. One can observe the blue lines for Logistic map is very short while CCE has longer blue line. However, the maximum

TABLE 1. Lyapunov comparison.

Statistic	Logistic Map	Proposed CCE
Min	-9.2106	-6.6219
Max	0.6829	4.9990
Mean	-7.7756	2.1864
Variance	0.9805	0.0001

Lyapunov exponent is 4.999 for proposed CCE and Logistic system has 0.6829 and similarly, the average magnitude of the Lyapunov exponent for the proposed CCE (i.e., 2.186 as shown in Figure 1) is much larger than that of the logistic map (i.e., -7.7756). This indicates that the novel CCE has a stronger chaotic approach with trajectories diverging at a faster rate than those of the Logistic map.

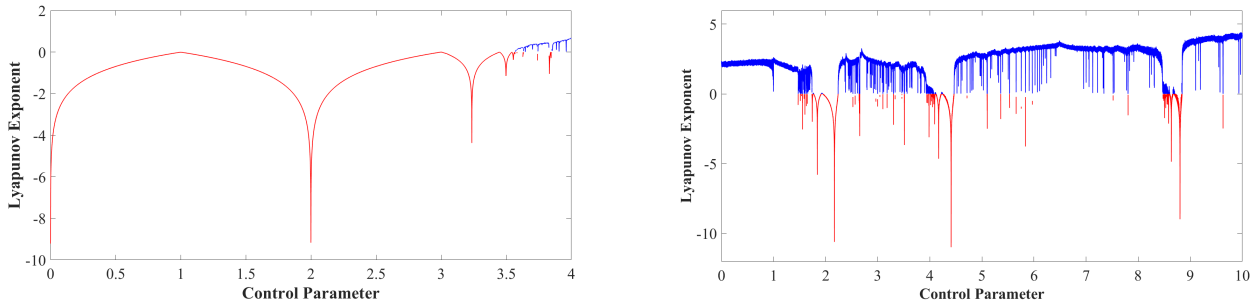
The Lyapunov exponent is computed for 1 million different control parameters α plotted in Figure 1(b) and for Logistic map, the Lyapunov Exponent plotted in Figure 1(a). The performance of the CCE is better than the Logistic map as it has higher positive value than the Logistic map.

C. BIFURCATION ANALYSIS

The bifurcation analysis studies the qualitative changes in a system's behavior as described by the parameter variations. We compare the proposed CCE with a well known 1D classical chaotic system called Logistic map. Experimentally, the working mechanisms of the proposed CCE and the Logistic map are in our consideration, as shown in Figure 2. The chaotic zones that are used to generate pseudo-random numbers are represented in the diagram by the shaded areas. Particularly, the Logistic map's behavior turns periodic to a-periodic since the value of μ increases from 0 to 4, where μ is a control parameter. The range of the control parameter of the proposed Equation is greater than that of the Logistic map, which effectively increases the proposed system's key space. The Logistic map is periodic from 0 to 3.54 while becomes chaotic in the range from 3.541 to 3.828. Then has a periodic window in the range of 3.829 to 3.857, respectively, as illustrated by Figure 2(a). These periodic windows reduce the range of control parameters μ or short key space compared to the proposed CCE, which has a more extended range for chaotic windows shown in Figure 2(b).

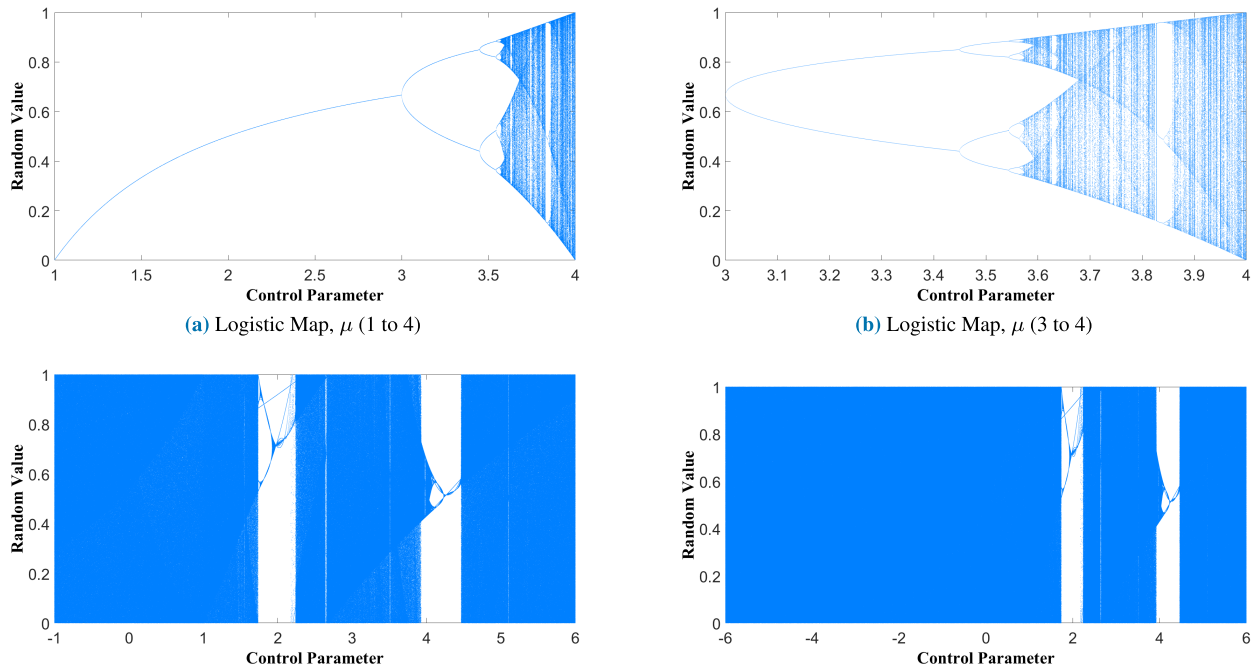
D. ANALYSIS OF PHASE SPACE STRUCTURE

All of the possible states of a system are presented in the phase space, and exploring more potential points illustrates the non-predictability of the particular dynamical system better [38]. The phase space is a mathematical function used to model the population growth and creates a curve to show how the population size changes over time. The proposed system uses discrete points instead of the curve to model the population growth, as shown in Figure 3. In summary, the phase space diagram of the logistic map is a 1D curve while the CCE generated a complex higher dimensional spread of points in its phase space diagram Figure 3(b).



(a) Logistic Map (b) Proposed CCE

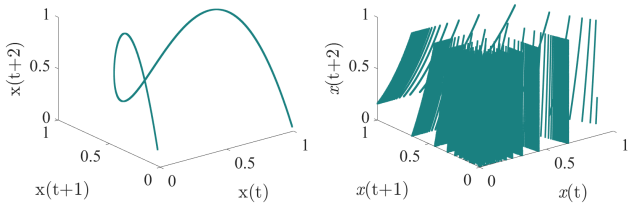
FIGURE 1. Analysis of Lyapunov exponent.



(a) Logistic Map, μ (1 to 4) (b) Logistic Map, μ (3 to 4)

(c) Proposed CCE, α (-1 to 6) (d) Proposed CCE, α (-6 to 6)

FIGURE 2. Bifurcation analysis.



(a) Logistic Map (b) Proposed CCE

FIGURE 3. 3D phase space analysis.

According to Bryla et al. [39], the discrete nature of the phase space algorithm is better than the line curve generated in the baseline method.

E. STATISTICAL ANALYSIS

For the measurements of statistical scores under different tests such as Correlation, Key sensitivity, Information entropy, Uniform Distribution and Frequency, seeds $x_0 = 0.0001$, $x_0' = 0.0002$ are used for both systems to generate random numbers while the control parameters are, $\mu = 3.865$ and $\alpha = -1.9865$, are fixed for Logistic and CCE, respectively.

1) AUTO CORRELATION ANALYSIS

Auto correlation is a statistical measure describing the degree of similarity between the given time series and a lagged version. It can be positive, negative, or zero, depending on the degree of similarity between the current and lagged values.

TABLE 2. Auto-correlation scores of logistic map and proposed CCE.

Statistic	Logistic Map	Proposed CCE
Min	-0.46931987	-0.132787060
Max	0.60729704	0.075920264
Mean	-0.00049988	-0.000499549

The system is predictable if the correlation coefficient is near to 1, and complete chaos is guaranteed if the correlation coefficient is near to 0 [40]. Auto-correlation is used in time series analysis and provides valuable insights into the patterns and trends in the concerned data. The auto correlation can be computed using the following Equation,

$$ac = \frac{\sum_{i=1}^{N-k} (Y_i - \bar{Y})(Y_{i+k} - \bar{Y})}{\sum_{i=1}^{N-k} (Y_i - \bar{Y})^2} \tag{2}$$

The auto correlation scores for different lagged values are graphically represented in Figure 4. It can be observed that auto correlation score varies from -0.6 to 0.6 for Logistic map in Figure 4(a) while auto correlation score varies from -0.14 to 0.08 for proposed system as shown in Figure 4(b). The statistical information is given in Table 2. Experimentally, the proposed system outperforms the classical Logistic map in most cases. The maximum value of auto-correlation for proposed CCE is 0.0759, which is far lower than 0.6073, and the mean values of both systems are equal. The proposed CCE is better in the overall range, close to zero, hence, the proposed system is less predictable.

2) CROSS CORRELATION ANALYSIS

Another statistical method is the cross correlation, which measures how similar or correlated two time series are to one another. It is an effective tool for comprehending the interactions between various elements or variables in a chaotic system. The cross correlation score can be measured using the following Equation

$$cc = \frac{\sum_{i=1}^{N-k} (X_i - \bar{X})(Y_{i+k} - \bar{Y})}{N} \tag{3}$$

TABLE 3. Cross-Correlation scores of logistic map and proposed CCE.

Statistic	Logistic Map	Proposed CCE
Min	-0.01382178	-0.006507421
Max	0.01345258	0.005878665
Mean	0.00000157	0.000014040

Pragmatically, the cross-correlation analysis of two different logistic map-sequences has higher value, as can be observed from Figure 5(a), which varies from -0.014 to 0.014. In contrast, the proposed CCE has cross correlation score that varies in the range of -0.007 to 0.006 depicted in Figure 5(b). The statistical information is computed and represented in Table 3, where the proposed approach performs better as compared to the Logistic map.

3) UNIFORMITY ANALYSIS

Uniformity analysis determines whether or not the random number generator covers the desired range. A system with uniform distribution is the least predictable dynamical system. The degree of uniformity can be analyzed visually by analyzing the graphical representation of the random numbers. Figure 6 represents an iterative distribution graph generated from the two chaotic systems. Figure 6(a) illustrates the distribution of the Logistic map, which is not evenly distributed and has the highest frequencies for the bin [0.1-0.2] and [0.9-1.0], while the frequency is close to zero for the bin [0 -0.1]. Figure 6(b) shows that the random numbers generated with the proposed CCE are uniformly distributed across the range [0, 1] without any cluster, patterns or vacations. So, it proved that the proposed CCE has better chaotic behavior than the classic logistic map.

4) INFORMATION ENTROPY ANALYSIS

The information entropy method finds the complexity of pseudo-random number generator. A well-known method is Shannon's entropy [41] that can be computed as:

$$H = -\sum_{i} \rho_i \log(\rho_i) \tag{4}$$

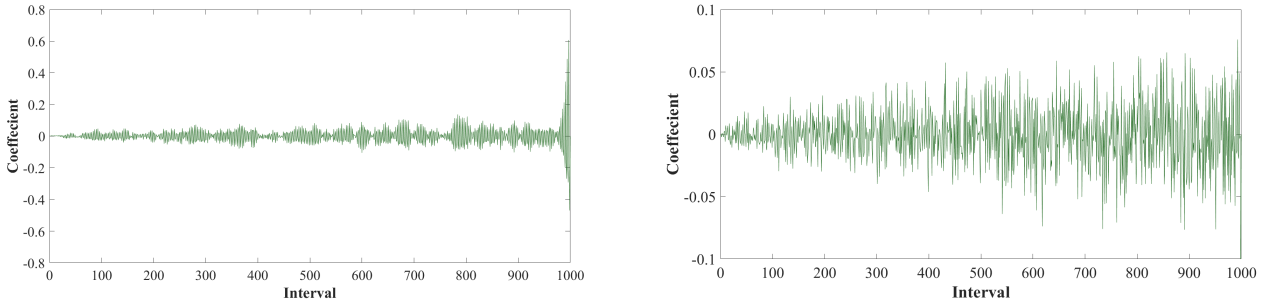
where ρ_i is the probability of a number being in a specific category denoted via i, the numbers generated with the chaotic map are divided into ten different categories. The probability of each category is calculated.

Entropy is used to judge the nonlinearity of a dynamical system. An increase in entropy defines an increase in the nonlinearity of the chaotic system. In comparison, a dynamical system with lower entropy has linear behavior. Table 4 represents the entropy of the logistic map and the proposed PRNG, measured for control parameters $\mu = 3.865$ and $\alpha = -1.9865$, respectively. Random sequences of length 1000 are generated with the Logistic map and the CCE to compute the information entropy. These numbers are divided into ten different categories in the interval [0, 1], and the probability of each class is calculated. The entropy of Logistic map is 0.8793 that is lower than the entropy of the proposed CCE is 0.9943 which proved the better randomness of CCE and have more uniform distribution.

5) KEY SENSITIVITY ANALYSIS

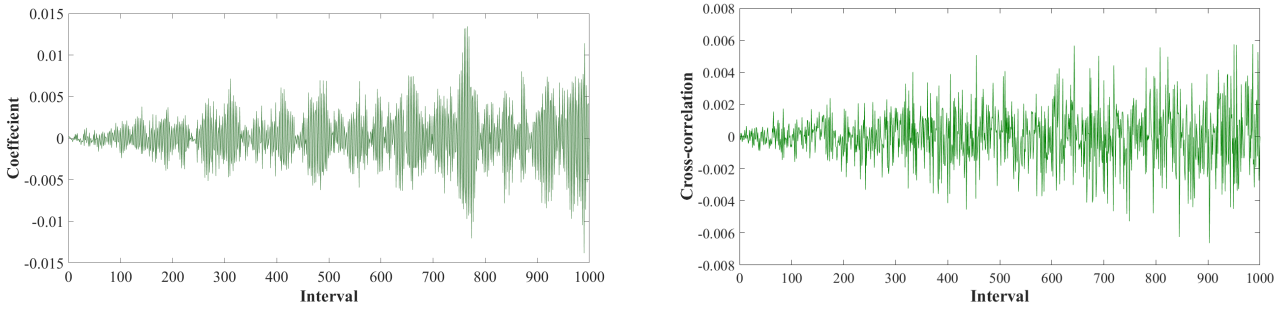
Another pivot statistical analysis of chaotic systems is the measure of key sensitivity to whether a non linear dynamical system can generate entirely different sequences of random numbers on minute change in seed x_0 or control parameter $\mu = 3.865$ or $\alpha = -1.9865$.

For this purpose, three sequences S_1, S_2 and S_3 of size 1000 have been generated from each system and first 900 are discarded. The pair of seed and control parameters for



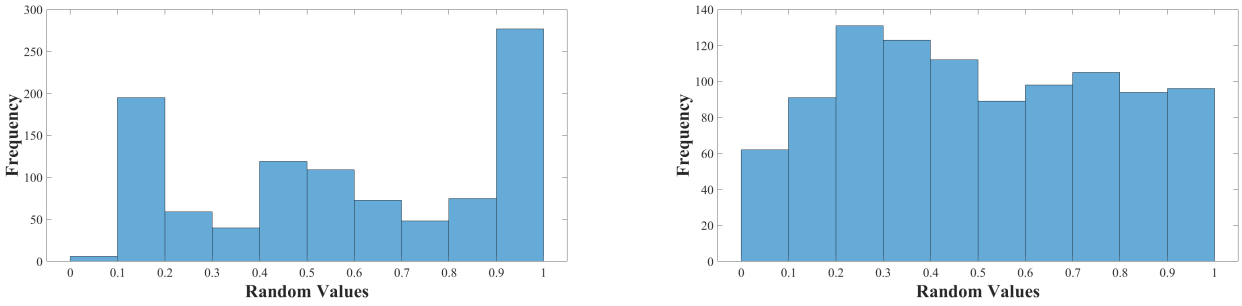
(a) Logistic Map (b) Proposed CCE

FIGURE 4. Auto-Correlation analysis.



(a) Logistic Map (b) Proposed CCE

FIGURE 5. Cross correlation analysis.



(a) Logistic Map (b) Proposed CCE

FIGURE 6. Uniformity analysis.

Logistic are ($x_0 = 0.0001$, $\mu = 3.865$), ($x_0 = 0.0002$, $\mu = 3.865$) and ($x_0 = 0.0001$, $\mu = 3.866$) while pair ($x_0 = 0.0001$, $\alpha = -1.9865$), ($x_0 = 0.0002$, $\alpha = -1.9865$) and ($x_0 = 0.0001$, $\alpha = -1.9875$) for CCE are employed. We then plot the absolute differences of $(S_1 - S_2)$, $(S_1 - S_3)$ in Figure 7.

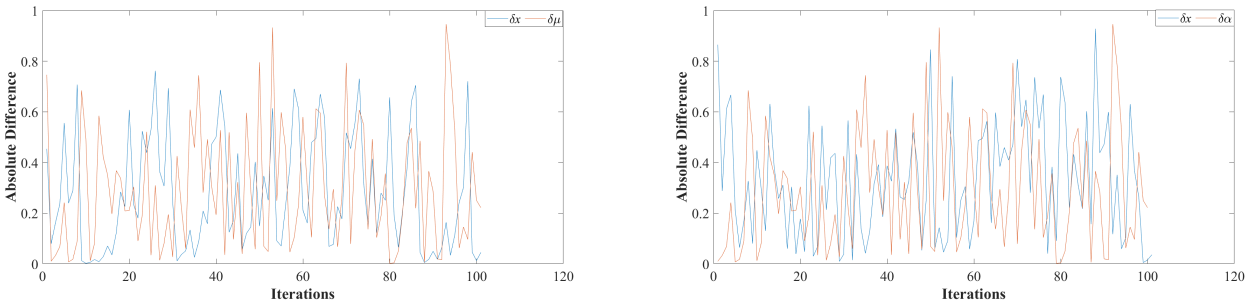
The standard deviation of absolute difference of $abs(S_1 - S_2)$, $abs(S_1 - S_3)$ are computed which are 0.2336 and 0.2400 for the CCE, while variances are 0.05457 and 0.05761. The standard deviation $abs(S_1 - S_2)$, $abs(S_1 - S_3)$ are computed, which are 0.2268 and 0.2529 for the Logistic system, while variances are 0.05145, and 0.06398. The statistical scores are almost equal; hence, both have excellent seed and control parameters sensitivity.

F. NIST ANALYSIS

The NIST Suite is a set of 15 statistical tests that are used to assess cryptography's reliability and randomness and other PRNGs. These tests are designed to find different patterns, biases, and regularities in PRNG's outputs that attackers might exploit against them. Eventually, such PRNG is deemed statistically random and acceptable for use in cryptographic applications if all applied NIST tests validate it. In this work, we have examined about 500 sets of sequences to determine the randomness of the given chaotic map, and the experimental results are presented in Table 5. In particular, the achieved experimental results evaluate four different systems (i.e., the proposed system

TABLE 4. Entropy analysis of logistic map and CCE.

Interval	Logistic Map				CCE			
	f	ρ_i	$Log10\,(\rho_i)$	$\rho_i \times Log10\,(\rho_i)$	f	ρ_i	$Log10\,(\rho_i)$	$\rho_i \times Log10\,(\rho_i)$
(0-0.1)	6	0.006	-2.2218	-0.0133	77	0.077	-1.1135	-0.0857
(0.1 -0.2)	195	0.195	-0.7100	-0.1384	109	0.109	-0.9626	-0.1049
(0.2 -0.3)	59	0.059	-1.2291	-0.0725	120	0.12	-0.9208	-0.1105
(0.3 -0.4)	40	0.04	-1.3979	-0.0559	107	0.107	-0.9706	-0.1039
(0.4 -0.5)	119	0.119	-0.9245	-0.1100	86	0.086	-1.0655	-0.0916
(0.5 -0.6)	109	0.109	-0.9626	-0.1049	132	0.132	-0.8794	-0.1161
(0.6 -0.7)	73	0.073	-1.1367	-0.0830	98	0.098	-1.0088	-0.0989
(0.7 -0.8)	47	0.047	-1.3279	-0.0624	86	0.086	-1.0655	-0.0916
(0.8 -0.9)	75	0.075	-1.1249	-0.0844	86	0.086	-1.0655	-0.0916
(0.9 -1.0)	277	0.277	-0.5575	-0.1544	99	0.099	-1.0044	-0.0994
Sum	**1000**	**1**	**-11.5930**	**-0.8793**	**1000**	**1**	**-10.1080**	**-0.9943**



(a) Logistic Map (b) Proposed CCE

FIGURE 7. Key sensitivity analysis.

and three baseline methods, such as OHenon, NHenon, and Logistic).

III. SUMMARY

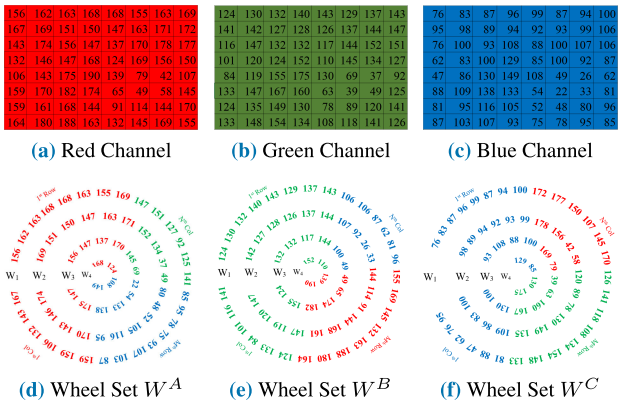
In the previous section, we did compare the CCE with the logistic map across various critical parameters. It is evident that the system boasts an extensive chaotic range, with ongoing testing aimed at expanding its scope. The analysis including correlation, Lyapunov exponent and information entropy confirm the non-linearity of the proposed system with exceptional efficiency and robustness. The equation's resilience and broadened key space make it invaluable for cryptographic applications, emphasizing its critical role in protecting sensitive information.

IV. COLOR IMAGE ENCRYPTION USING CONCEPT OF WHEELS

This section includes the concept of wheels, encryption and decryption using proposed Cosine Chaotic Equation.

A. CONCEPT OF WHEELS

A wheel is a circular object which can roll or rotate around its center. This theme is used to encrypt squared digital images in an innovative way. The wheels are shaped from 24 bit color image of size $M \times M$. For simplicity, the three channels, red, green, and blue of a color images of size $3 \times M$ are



(a) Red Channel (b) Green Channel (c) Blue Channel

(d) Wheel Set W^A (e) Wheel Set W^B (f) Wheel Set W^C

FIGURE 8. Square image and wheels: (a), (b) and (c) RGB Channels of an image; (d), (e) and (f) Generated wheels.

shown in Figure 8. The system will generate wheels using layers of rows and columns of different channels in a cycling manner. The first wheel w_1 of wheels Set A called W^A will form by combining Row 1 of red channel, M^{th} column of green channel, M^{th} row of blue channel and 1st column of red channel as shown in Figure 8(a). The first wheel w_1 of wheels Set B is created by combining Row 1 of green channel, M^{th} column of blue channel, M^{th} row of red channel and 1st column of green channel as shown in Figure 1(e). In this

TABLE 5. NIST test.

S. No.	Test Name	Proposed System	OHenon system	NHenon system	Ref. [42]	Logistic Map	Result
1	Frequency	0.65272	0.527	0.709	0.87645	0.12376	Passed
2	Block Frequency	0.86244	0.838	0.983	0.84266	0.24782	Passed
3	Cumulative Sums	0.77109	0.618	0.803	0.69878	0.13158	Passed
4	Runs	0.77969	0.794	0.935	0.34711	0.10289	Passed
5	Longest Run of Ones	0.49562	0.049	0.504	0.56182	0.24680	Passed
6	Rank	0.53638	0.821	0.915	0.38733	0.40944	Passed
7	Discrete Fourier Transform	0.67101	0.793	0.816	0.37987	0.34625	Passed
8	Nonperiodic Template Matchings	0.88359	0.816	0.995	0.15475	0.45972	Passed
9	Overlapping Template Matchings	0.89723	0.317	0.379	0.71974	0.43992	Passed
10	Universal Statistical	0.30012	0.346	0.541	0.88993	0.00958	Passed
11	Approximate Entropy	0.51860	0.615	0.922	0.32134	0.01093	Passed
12	Random Excursions	0.49908	0.605	0.699	0.01388	0.49246	Passed
13	Random Excurisions Variant	0.22092	0.586	0.708	0.01356	0.002	Passed
14	Serial	0.50670	0.002	0.427	0.00820	0.002	Passed
15	Linear Complexity	0.77451	0.861	0.963	0.68955	0	Passed

way, the rows and columns of each channel are used in a cyclic fashion. This process is repeated $M/2$ times and yields $M/2$ numbers of wheels in each set. An example image of size $3\times8\times8$ with each color channel is shown in Figure 8(a) - 8(c), used as input to form wheels shown in Figure 8(d) to 8(f). As $M/2$ yields 4, so 4 possible wheels can be formed in each of the *WheelsSet* or $W^A = \{w_1, w_2, \cdots, w_{M/2}\}$. In this case, the first wheel consists of 28 pixels, second consists of 20, third consists of 12 and the last wheel comprises of four pixels. The size of each next wheel will be reduced by 8 pixels. The permutation process by rotating of wheel w_1 around $-287$and $+97$ degree angle are shown in Figure 9.

$$w(i) = 4n_i - 4 \tag{5}$$

and n_i can be computed ass

$$n_i = N - 2 \times (i - 1) \tag{6}$$

while $i = 1, 2, \cdots, TW$. The TW is used to denote the Total wheels in a Set $TW = M/2$. The n_1,n_2, n_3 and n_4 can be computed as

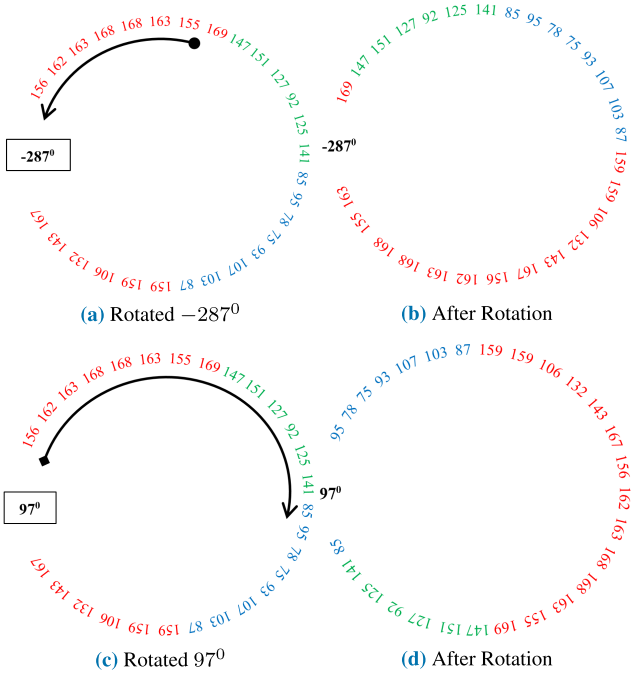
$$\begin{cases} n_1 = 8 - 2 \times (1 - 1) = 8 \\ n_2 = 8 - 2 \times (2 - 1) = 6 \\ n_3 = 8 - 2 \times (3 - 1) = 4 \\ n_4 = 8 - 2 \times (4 - 1) = 2 \end{cases} \tag{7}$$

So the wheels are formed as follows,

$$\begin{cases} w_1 = 4 \times 8 - 4 = 28 \\ w_2 = 4 \times 6 - 4 = 20 \\ w_3 = 4 \times 4 - 4 = 12 \\ w_4 = 4 \times 2 - 4 = 8 \end{cases} \tag{8}$$

The Generalized form of wheels generation is as follows

$$\left[W^A, W^B, W^C\right] = gen\_wheels\,(I, M) \tag{9}$$



(a) Rotated -287^0 (b) After Rotation (c) Rotated 97^0 (d) After Rotation

FIGURE 9. Rotation of wheels: (a) Wheel $W^A(1)$ (b) Wheel $W^B(1)$ (c) Rotation of $-287°$ (d) Rotation of $97°$.

B. KEY GENERATION PROCESS

The concept of the seed or key generation process is taken from the established research [43], [44], [45]. A hash digest H of 384 bits is obtained by inputting the plain image to the SHA-2 hash function. The message digest H consists of 96 hexadecimal digits and is split into eight equal sized blocks, each block is composed of twelve hexadecimal digits and is later transformed into a number by following the Equation,

$$h_i = \frac{hex2dec\,(h_1, h_2, h_3, h_4)}{2^{41}} \tag{10}$$

$$h_i = \frac{hex2dec\,(h_5, \cdots, h_{10})}{2^{46}} \tag{11}$$

$$\begin{cases} a'_1 = a_1 + h_1 + ck \\ a'_2 = a_2 + h_2 + ck \\ a'_3 = a_3 + h_3 + ck \\ a'_4 = a_4 + h_4 + ck \end{cases} \quad \text{mod } 1 \tag{12}$$

$$\begin{cases} ep'_0 = ep_0 + h_5 + ck \\ v'_0 = v_o + h_6 + ck \\ r'_0 = r_0 + h_7 + ck \\ ea'_0 = ea_0 + h_8 + ck \\ eb'_0 = eb_0 + h_9 + ck \\ ec'_0 = ec_0 + h_{10} + ck \end{cases} \quad \text{mod } 1 \tag{13}$$

C. GENERATION OF RANDOM SEQUENCES AND PRE-PROCESSING

The proposed image cipher requires ten vectors of pseudo random numbers to accomplish the encryption task. All of these vectors are generated by newly proposed CCE using different initial conditions or seeds while α is fixed for all these vectors which is -1.9865.

1. First of all, four vectors $Angles^A$, $Angles^B$, $Angles^C$ and $Angles_{pw}$ are generated using a'_1, a'_2, a'_3 and a'_4 seeds computed in Equation 12.

$$\begin{aligned} Angles^A &= \{a_1, a_2, \cdots, a_{TW}\} \\ Angles^B &= \{a_1, a_2, \cdots, a_{TW}\} \\ Angles^C &= \{a_1, a_2, \cdots, a_{TW}\} \\ Angles_{pw} &= \{a_1, a_2, \cdots, a_{(TW-1)\times 3}\} \end{aligned} \tag{14}$$

These vectors can not be used in raw form as these vectors are in the range of [0-1]. Following pre-processing is applied to make them useful for rotations of wheels,

Algorithm 1 Generation of Rotational Angles

```
procedure Angle Generation(Angles^X)
    if Angles^X(i) > 0.5
    Angles^X(i) ⟵ round(Angles^X(i) × 10^16) mod 360
    else
    Angles^X(i) ⟵ round(Angles^X(i) × 10^16) mod −360
    end if
end procedure
```

Algorihm#1 transforms the pseudo random numbers into angles θ between -360 to 360 degree which rotates the image wheels[2] W^X, and the pseudo wheels pw^X in a clockwise or the anti clockwise direction. The $Angles_{pw}$ is further divided into three sub vectors, one vector for each set of the wheel as follows,

$$\begin{aligned} Angles^A_{pw} &= Angles_{pw}\{1, 2, \cdots, TW\} \\ Angles^B_{pw} &= Angles_{pw}\{TW + 1, \cdots, TW \times 2\} \\ Angles^C_{pw} &= Angles_{pw}\{TW \times 2 + 1, \cdots, end\} \end{aligned} \tag{15}$$

[2]X stands A, B, C.

2. In the next step of key generation and pre-processing, three more vectors EP, V and R are generated using the modified seeds ep'_0, v'_0 and r'_0 respectively shown as follows;

$$\begin{aligned} EP &= \{ep_1, ep_2, \cdots, ep_{TW-1\times 3}\} \\ V &= \{v_1, v_2, \cdots, v_{TW-1\times 3}\} \\ R &= \{r_1, r_2, \cdots, r_{TW-1\times 3}\} \end{aligned} \tag{16}$$

The vectors V and R are pre processed as follows.

$$\begin{aligned} V(i) &= round\left(V(i) \times 10^{16}\right) \bmod 256 \\ R(i) &= round\left(R(i) \times 10^{16}\right) \bmod 256 \end{aligned} \tag{17}$$

The processed Vector V and R as well as EP are slpit into three sub vectors: V into IV^A, IV^B, IV^C, R into pw^A, pw^B and pw^C and Vector E is split into epw^A, epw^B, and epw^C.

$$[vaLepw^A, idXepw^A] = sort(epw^A) \tag{18}$$

$$[vaLepw^B, idXepw^B] = sort(epw^B) \tag{19}$$

$$[vaLepw^C, idXepw^C] = sort(epw^C) \tag{20}$$

3. At last, three more vectors of pseudo random numbers are required in order to follow the design of the image cipher. These three vectors are named e^A,e^B,e^C which are generated using Equation (CCE) and seeds ea'_0, eb'_0 and ec'_0. These vectors are used to discard some random elements from each of the image wheels W^A, W^B, W^C during the substitution process. For the sake of the selection of random elements, these vectors are sorted as follows;

$$[vaLe^A, idXe^A] = sort(e^A) \tag{21}$$

$$[vaLe^B, idXe^B] = sort(e^B) \tag{22}$$

$$[vaLe^C, idXe^C] = sort(e^C) \tag{23}$$

D. PERMUTATION

The $Angles^A$, $Angles^B$, $Angles^C$ are generated by iterating Equation (1) up to TW a to permute wheel set W^A, W^B and W^C. The permutation of a wheel is performed by using Algorithm#1.

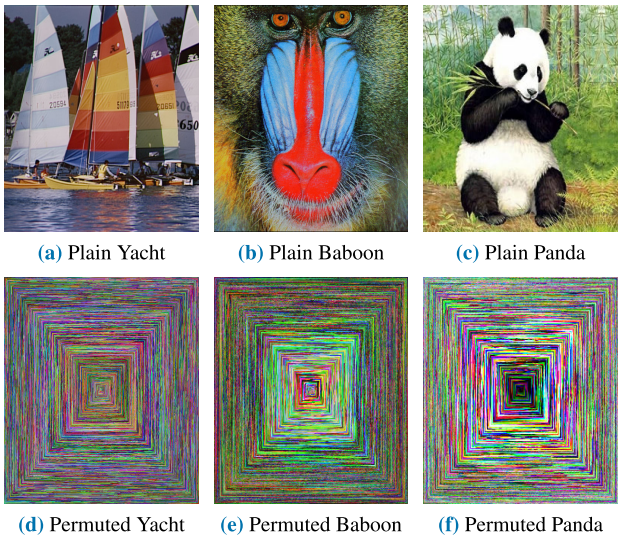
Algorithm 2 Permutation of Wheels

```
procedure Permutation(Angles^X, W^X)
    size ⟵ size(w^X(i))
    pixels_per_Degree ⟵ ceil(size/360)
    θ_i ⟵ round((Pixels_per_Degree × Angles^X(i))
    ẇ^X(i) ⟵ rotate(w^X(i), θ_i)
end procedure
```

while $i = 1, 2, \cdots, TW$ and TW represents the total wheels in Set W^A and similar steps applied on W^B and W^C using $Angles^B$ and $Angles^C$.

E. SUBSTITUTION

The permutation phase of any encryption process alone is not sufficient to achieve standard of data security as the statistical information remains intact and can be used to cryptanalyzed.



(a) Plain Yacht (b) Plain Baboon (c) Plain Panda

(d) Permuted Yacht (e) Permuted Baboon (f) Permuted Panda

FIGURE 10. Output of permutation phase.

So the substitution phase is required to make it harder to cryptanalyzed. In the proposed system, the set of permuted color wheels $\bar{W}^A$, $\bar{W}^B$ and $\bar{W}^C$ are fed into the substitution algorithm. The substitution of each wheel is accomplished in Cipher Block Chaining (CBC) mode in which each wheel is encrypted using the previous encrypted wheel and a pseudo wheel[3] pw^X under bit-wise exclusive operation. The encryption process of $W^X(1)$ is slightly different from the rest of the wheels as there is no ciphered wheel before it so Initial Vector IV and pw^X are used in encryption.

As each of the subsequent wheel is smaller in radius or by 8 pixels. So, to make a successful substitution for each of $W^X(i)$, where $i = 2, 3, \ldots, TW$, the original pw^X is rotated clockwise or anti clockwise around angle θ, then reduced by 1 to k pixels which are selected at random location using pseudo random number generated from CCE. The value of k is incremented by 8 for each next wheel. The encryption process for wheel set W^A is presented as Algorithm 3. Both of these, IV^X and pw^X are created from R after transforming each value into $(0 - 255)$ described in section IV-B.

1) SUMMARY OF PROPOSED CIPHER

Input: A 24-bit color image square image I of size N^2, a_1 to a_4, v_0, r_o, ep_0, ea_0, eb_0 and ec_0, $\alpha = -1.9865$ are the seeds for CCE to generate pseudo random numbers to accomplish the encryption process.

Output: A ciphered image i.e., E

1) Create one-time key by using 512-bits hash value of I and then process the divided hash value to modify common keys to get new common keys as described in section IV-B.
2) The three sets of wheels W^A, W^B and W^C are created from 24-bit image I as described in section IV-A by using Equation (9).
3) Iterate proposed CCE by employing modified a_1', a_2' and a_3' to produce vectors $Angles^A$, $Angles^B$, $Angles^C$ having size equal to total wheels TW while a_4' is used to produced vector $Angles_{pw}$ of size $(TW - 1) \times 3$. These vectors are processed using Algorithm #1 and then split vector $Angles_{pw}$ into three sub vectors called $Angles^A_{pw}$, $Angles^B_{pw}$, $Angles^C_{pw}$.
4) Iterate CCE using v_0', r_0' and ep_0' and processed vector V and R under Equation (17) and then split V and R into three sub vectors while EP is split into three and sorted to record indexes of sroted shown in Equations (18) to (20).
5) Generate vectors e^A, e^B and e^C using modified keys ea_0', eb_0' and ec_0' and sort to record indexes of sorted vectors as shown in Equations (21) to (23).
6) Permute the set of wheels by applying Algorithm # 2.
7) Substitution of the wheel set is achieved by applying the encryption Algorithm # 3.

[3]X stands for A, B or C.

V. DECRYPTION

The decryption process is a straightforward process in which the modified keys are used to generate the pseudo random vectors as generated and sorted as presented in sections IV-C to perform the reverse operations of substitution and permutation, respectively. The difference is only in the decryption of the smallest wheel to the largest wheel, or we can say that the innermost wheel is decrypted first and then the outer wheels in a sequence. The CBC mode of the decryption requires saving the value of $vaLe^A$ as $vaLe^A(mod\_val)$ in a separate vector called $Initial_Seed$. Before processing the decryption of encrypted image, the CCE is iterated TW times and saves the last value after sorting $vaLe^A$, $vaLe^B$, and $vaLe^C$ on each iteration in $Initial_Seed$. Then, the decryption procedure is accomplished as the steps are presented in Algorithm 4.

VI. SIMULATION AND RESULTS

The proposed image encryption is simulated using MATLAB R2021a and standard images of Yacht, Panda, and Baboon with a size of 512 × 512. The plain image is passed to the hash function and the output is used to manipulate the initial values. The set of initial seeds $a_1 = 0.287654321711$, $a_2 = 0.465891234090$, $a_3 = 0.035467896782$, $a_4 = 0.219833543872$, $ep_0 = 0.34567870987643$, $v_0 = 0.65432098712343$, $r_0 = 0.09876543456784$, $ea_0 = 0.13441357476514$, $eb_0 = 0.87654345678105$ and $ec_0 = 0.62345098721075$ are provided as keyboard inputs. For the further assessment of the algorithm, it is analyzed for various factors like key space, information entropy, key sensitivity, statistical analysis, correlation analysis, and differential analysis. The encryption and decryption of Yacht, Baboon and Panda images are given in Figure 11.

Algorithm 3 Encryption Algorithm

procedure Substitution($\dot{W}^A$, TW, IV^A, pw^A, $Angles^A_{pw}$, $idXepw^A$,$vaLe^A$,$idXe^A$, $k = 0$, $mod\_val = size(w^A(1))$)

$\bar{w}^A(1) = \left(\dot{w}^A(1) \oplus IV^A\right) \oplus pw^A$ ▷ The 1^{st} wheel of w^A is encrypted

for $i \leftarrow 2$ to TW **do**

$size_{pw^A} \longleftarrow \textbf{\textit{size}}\left(pw^A\right)$ ▷ compute the size of previous encrypted wheel

$pixels\_per\_Degree \longleftarrow \textbf{\textit{ceil}}(size_{pw^A}/360)$ ▷ compute the number of pixels used in rotation for 1 degree

$\theta \longleftarrow \textbf{\textit{round}}\left(Pixels\_per\_Degree \times Angles^A_{pw}(i-1)\right)$ ▷ Convert angle into No. of pixels

$\dot{p}w^A \longleftarrow \textbf{\textit{rotate}}\left(pw^A, \theta\right)$ ▷ Rotate pseudo Wheel at angle θ

$p'w^A \longleftarrow \textbf{\textit{eliminate}}\left(\dot{p}w^A\left(idXepw^A(1:k+8)\right)\right)$ ▷ Discard 1 to k elements from pseudo wheels

$w'^A(i-1) \longleftarrow \textbf{\textit{eliminate}}\left(\bar{w}^A(i-1), idXe^A(1:8)\right)$ ▷ Discard 8 random values from wheel $\bar{w}^A(i-1)$

$\bar{w}^A(i) \longleftarrow \left(\dot{w}^A(i) \oplus w'^A(i-1)\right) \oplus p'w^A$ ▷ bitXOR pseudo wheel, current wheel and encrypted wheel.

$e^A \longleftarrow \textbf{\textit{CCE}}\left(vaLe^A(mod\_val), mod\_val - 8\right)$ ▷ iterate CCE = (seed, no. of iterations)

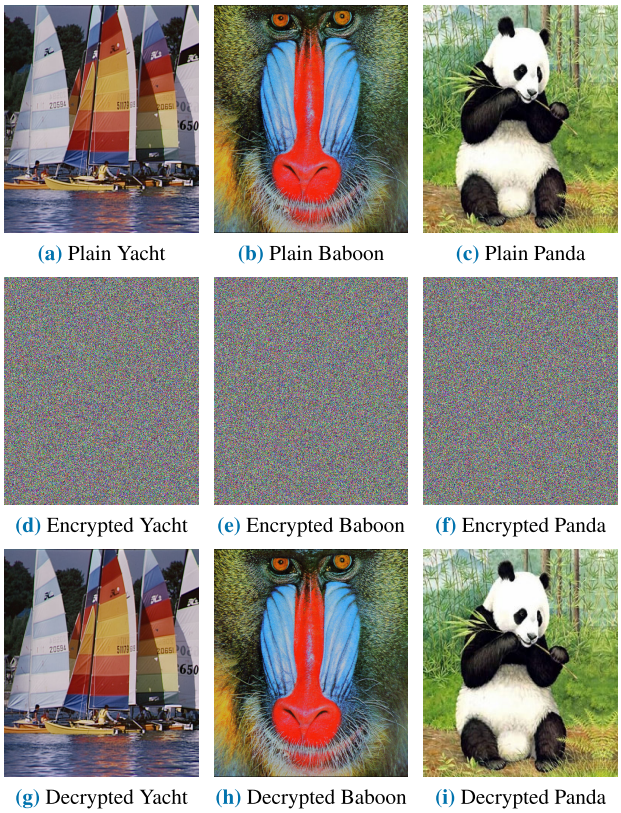
$[vaLe^A, idXe^A] \longleftarrow \textbf{\textit{sort}}(e^A)$ ▷ Sort New vector e^A

$k \longleftarrow k + 8$

$mod\_val \longleftarrow mod\_val - 8$

end for

end procedure



(a) Plain Yacht (b) Plain Baboon (c) Plain Panda

(d) Encrypted Yacht (e) Encrypted Baboon (f) Encrypted Panda

(g) Decrypted Yacht (h) Decrypted Baboon (i) Decrypted Panda

FIGURE 11. Encrypted and decrypted images using proposed cipher.

A. STATISTICAL ANALYSIS

1) KEY SPACE ANALYSIS

The sensitivity of the chaotic equation to the initial conditions decides the complexity of the non-linear system [46]. Our proposed random number generator is extremely sensitive to the initial seeds that makes the crypto-system secure against different attacks. The proposed algorithm requires three pseudo-random sequences generated through the chaotic system for which three pairs of initial seeds are passed. The initial values and the control parameter have a precision of 10^{14} and 10^5 respectively. The output of the SHA-1 hash function is also added to the key space. Hence, the total key space is 10^{238} that is ultra large enough to make differential and statistical attacks infeasible.

2) 3D HISTOGRAM ANALYSIS

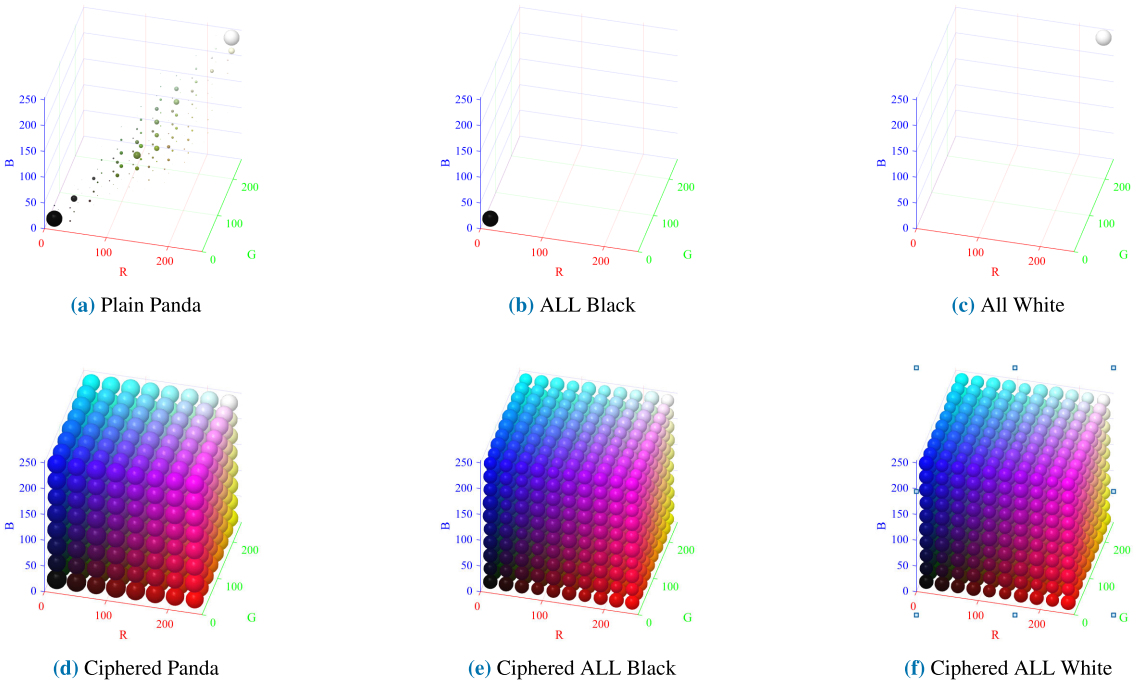
Histogram analysis is a qualitative way of measuring the encryption quality by visualizing the distribution of image pixels. Figure 12 represents the 3D histogram of the plain and encrypted images of Panda, All Black and All White. In 3D histograms, the location of spheres represents the gray values and the size of spheres represent the amplitude of frequencies; the higher the amplitude, the larger the size of spheres. We can see that the distribution of frequencies in the original images has a high concentration of gray values at few points depicted with large spheres while the encrypted images has uniform distribution of gray values presented by equal sized spheres which spread uniformly in the histograms. The uniform distribution of the information shows that the image is resistant against the statistical attacks and it has no information leakage. This is why the uniformity in the histogram of the images is an important factor to analyze the image encryption algorithm.

3) CORRELATION COEFFICIENT

Digital color images exhibit inherent correlations between adjacent pixels. However, these correlations extend beyond spatial proximity and also exist within the individual color channels themselves (RGB). Furthermore, natural images are comprised of distinct regions characterized by homogeneous gray-scale intensity. Effective image cryptography aims to

Algorithm 4 Decryption Algorithm

procedure Substitution($\bar{W}^A, TW, IV^A, pw^A, Angles^A_{pw}, idXepw^A, vaLe^A, idXe^A, k = (TW-1)\times 3, mod\_val = size(\bar{w}^A(1))$)
  $Saved\_InitialSeed(1) \longleftarrow vaLe^A(mod\_val)$
  for $i \leftarrow 2$ to TW **do**
    $e^A \longleftarrow$ ***CCE*** $\left(vaLe^A(mod\_val), mod\_val - 8\right)$ ▷ iterate CCE = (seed, no. of iterations)
    $[vaLe^A, idXe^A] \longleftarrow$ ***sort***(e^A) ▷ Sort New vector e^A
    $Saved\_InitialSeed(i) \longleftarrow vaLe^A(mod\_val)$ ▷ To save last value of $vaLe^A$ on each itearation
    $mod\_val = mod\_val - 8$
  end for
  for $i \leftarrow TW$ to 2 **do**
    $size_{pw^A} \longleftarrow$ ***size*** $\left(pw^A\right)$ ▷ compute the size of previous encrypted wheel
    $pixels\_per\_Degree \longleftarrow$ ***ceil***$(size_{pw^A}/360)$ ▷ compute the number of pixels used in rotation for 1 degree
    $\theta \longleftarrow$ ***round*** $\left(Pixels\_per\_Degree \times Angles^A_{pw}(i)\right)$ ▷ Convert angle into No. of pixels
    $\dot{p}w^A \longleftarrow$ ***rotate*** $\left(pw^A, -\theta\right)$ ▷ Rotate pseudo Wheel at angle θ
    $p'w^A \longleftarrow$ ***eliminate*** $\left(\dot{p}w^A\left(idXepw^A(1:k-8)\right)\right)$ ▷ Discard 1 to K elements from pseudo wheels
    $e^A \longleftarrow$ ***CCE***$(Saved\_InitialSeed(i), mod\_val)$ ▷ iterate CCE = (seed, no. of iterations)
    $[vaLe^A, idXe^A] \longleftarrow$ ***sort***(e^A) ▷ Sort New vector e^A
    $w'^A(i-1) \longleftarrow$ ***eliminate*** $\left(\bar{w}^A(i-1), idXe^A(1:8)\right)$ ▷ Discard 8 random values from wheel $\bar{w}^A(i-1)$
    $\dot{w}^A(i) \longleftarrow \left(\bar{w}^A(i) \oplus w'^A(i-1)\right) \oplus p'w^A$ ▷ bitXOR pseudo wheel, current wheel and encrypted wheel.
    $k \longleftarrow k - 8$
  end for
  $\dot{w}^A(1) = \left(\bar{w}^A(1) \oplus IV^A\right) \oplus pw^A$ ▷ The 1^{st} wheel of w^A is decrypted
end procedure



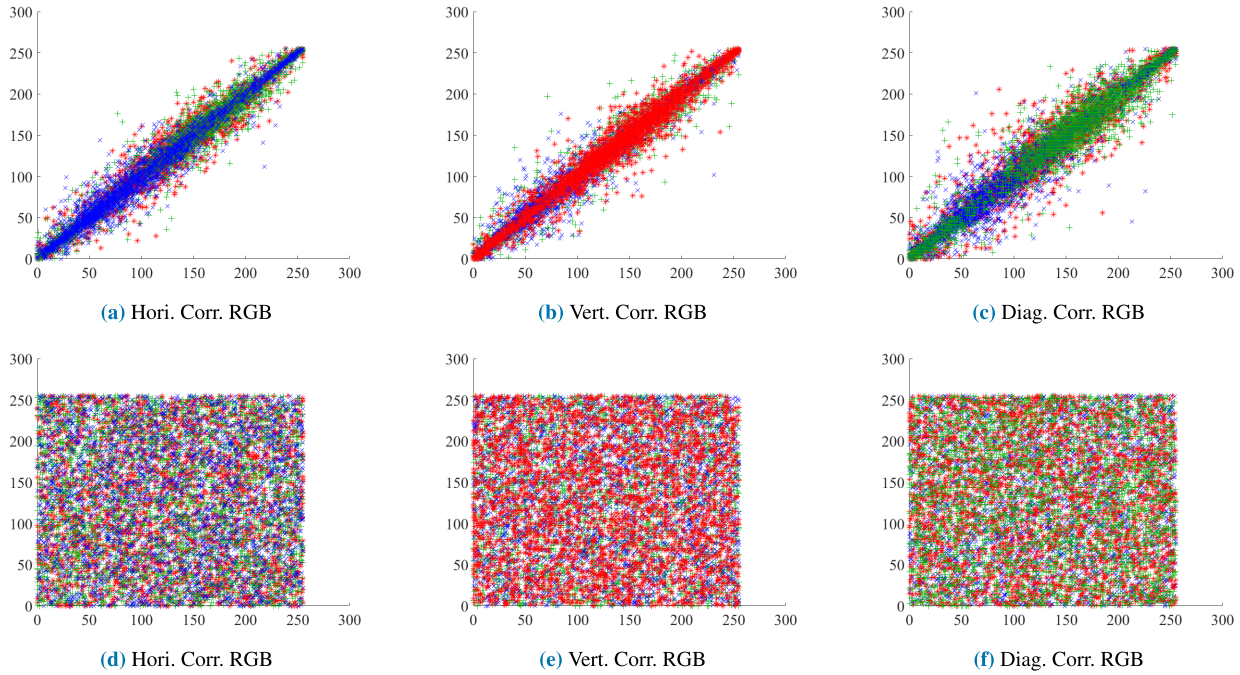
(a) Plain Panda (b) ALL Black (c) All White

(d) Ciphered Panda (e) Ciphered ALL Black (f) Ciphered ALL White

FIGURE 12. 3D histogram analysis.

disrupt these inherent correlations, thereby dismantling the underlying regional structure of the image.

The correlation between adjacent pixels is quantified using Equation (24), where ρ_{xy} denotes the correlation coefficient, x and y represent the gray intensity values of two adjacent pixels, while $D(x)$ and $cov(x, y)$ denote the mean and covariance, respectively. The coefficient ρ_{xy} ranges from $+1$ to -1, with values closer to $+1$ indicating a strong



(a) Hori. Corr. RGB (b) Vert. Corr. RGB (c) Diag. Corr. RGB

(d) Hori. Corr. RGB (e) Vert. Corr. RGB (f) Diag. Corr. RGB

FIGURE 13. Correlation analysis: (a), (b), (c) Plain image panda; (d), (e), (f) Ciphered image panda.

positive correlation and values closer to -1 signifying a strong negative correlation.

The correlation results are assessed by randomly choosing 3,000 pairs in each of the three directions (horizontal, vertical, and diagonal). These random pairs are then plotted on the x-axis and y-axis, as seen in Figure 13. Each sub-figure in 13 represents 3000 pairs in each direction from all channels. To measure the correlation coefficient score for plain and encrypted images, 3000 pairs selected randomly and this process is repeated 500 times. After the completion of said process 500 times, the mean, minimum, maximum, standard deviation and variance of correlation scores are given in Table 6 and histograms of correlation coefficient are plotted in Figures 14.

$$\begin{cases} \rho_{xy} = \dfrac{|Cov(x,y)|}{\sqrt{D(x) \times D(y)}} \\ Cov(x,y) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} (x_i - E(x))\,(y_i - E(y)) \\ D(x) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} (x_i - E(x))^2 \\ E(x) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} (x_i \times D(x)) \end{cases} \tag{24}$$

4) INFORMATION ENTROPY ANALYSIS

The information entropy is another measure of randomness of the distribution of gray scale image. The higher value of the entropy indicates that the pixel values are more uniformly distributed. The following Equation represents the famous Shannon's theory of the information entropy [41]:

$$H = \sum_{i=1}^{n} p_i log_2 \frac{1}{p_i} \tag{25}$$

where N represents the values and $P(S)$ is the probability of values in the information provided. For an 8-bit image, the ideal value of information entropy should be 8. The table 7 represents the information entropy of the cipher-text image Baboon and also comparison to some recent techniques.

TABLE 6. Statistical information derived from Figure 14.

Channel	Direction	Mean	Min	max	Std	Var
Red	H	0.0031	-0.0540	0.0594	0.0191	0.00036
	V	0.0004	-0.0593	0.0598	0.0184	0.00034
	D	-0.0005	-0.0520	0.0550	0.0184	0.00034
Green	H	-0.0004	-0.0465	0.0624	0.0183	0.00034
	V	-0.0033	-0.0535	0.0425	0.0183	0.00030
	D	0.0021	-0.0522	0.0529	0.0176	0.00031
Blue	H	-0.0010	-0.0610	0.06565	0.0175	0.00031
	V	-0.0016	-0.0499	0.0473	0.0183	0.00034
	D	-0.0002	-0.0510	0.0496	0.0182	0.00033

TABLE 7. Information entropy analysis of baboon image.

Proposed	Ref. [47]	Ref. [48]	Ref. [49]	Ref. [50]	Ref. [51]
7.99989	7.9972	7.9999	7.9998	7.9991	7.9993

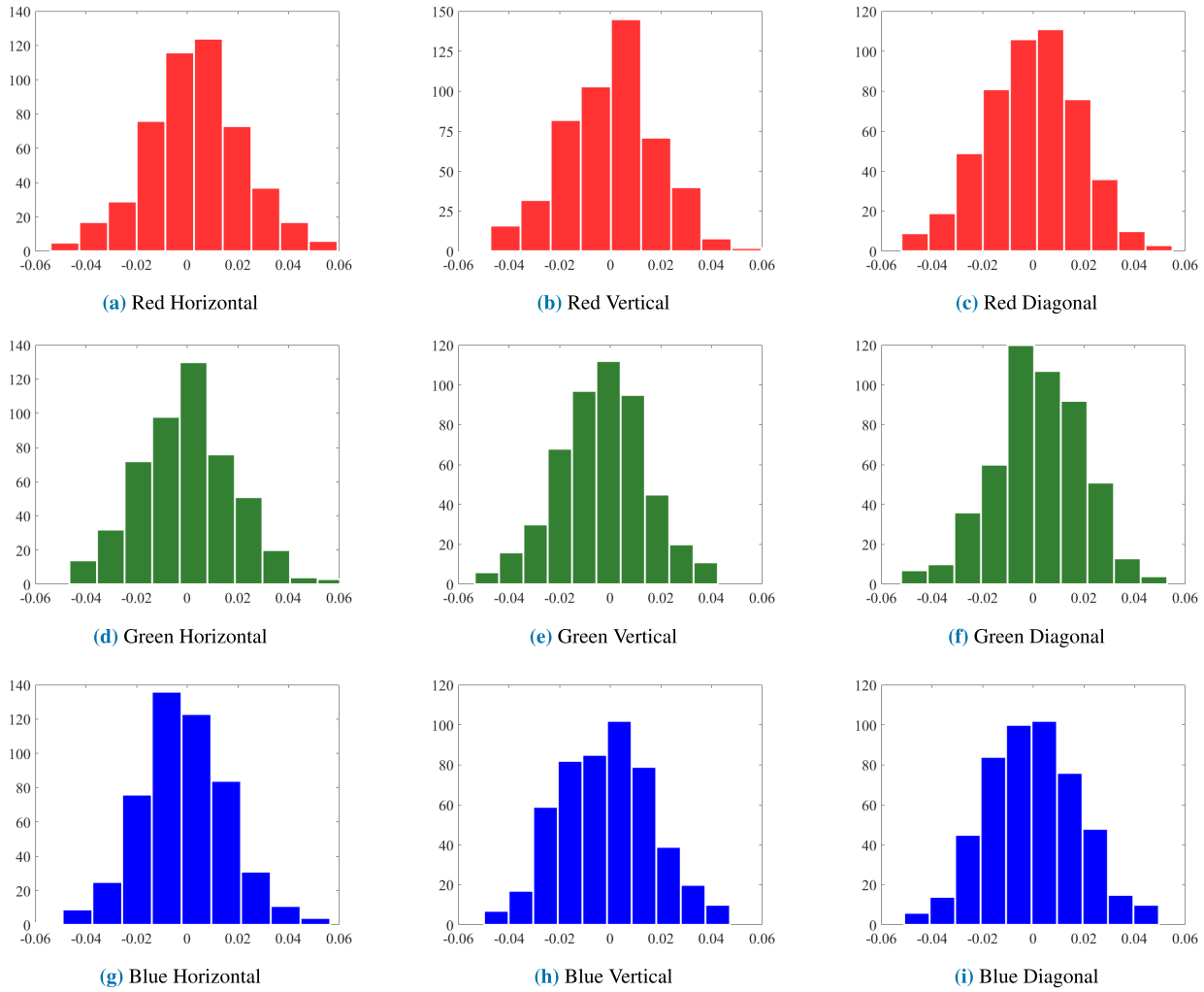


FIGURE 14. Correlation analysis of red, green and blue channels of encrypted baboon.

5) PEARSON'S CHI-SQUARE TEST

The chi-square test is crucial for determining the unpredictability of cipher images. It quantitatively measures encryption quality by studying histograms. This test, also known as the g̈oodness-of-fitẗest, is used to assess the relationship between data and a specific distribution. The test is only suitable for univariate datasets. Since image pixels are discrete values and part of a univariate dataset, statistical tests can be used for analyzing the χ^2. It is described as:

$$\chi^2 = \sum_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i} \tag{26}$$

In the context of 24-bit color images, where each color pixel can hold intensity values from 0 to 255 ($k = 255$), the chi-square (x^2) test serves as a valuable tool for evaluating the randomness of encrypted images. As shown in Equation 26, the chi-square statistic (x^2) is calculated based on the observed frequency O_i of each intensity value i in the image histogram compared to its expected frequency (E_i) under a hypothesized distribution (typically, a uniform distribution).

Experimentally, an encrypted image must pass the χ^2 square test with the value less than the critical value χ^2_α where α is known as the significance level and the degree of freedom of the χ distribution. With $\alpha = 0.05$, critical χ value is computed as $\chi_{0.05}(255) = 293.247$ [52]. The table 8 shows the result that proposed system has successfully passed the test and a comparison have also been made there to some recent image techniques.

B. DIFFERENTIAL ANALYSIS

The Net Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are established metrics employed to assess the resistance of an encryption algorithm against differential attacks. The NPCR specifically quantifies the percentage of pixels that differ in value between two cipher images generated using 1-bit different images. The C^0 represents the encrypted image of the baboon and C^1,

TABLE 8. Chi square analysis of baboon image.

Image	Red	Green	Blue	Mean	conclusion
Plain Baboon	91191.12	141811.64	146302.26	126435.10	Passed
Encrypted Baboon	239.77	254.85	227.90	240.80	Pass
Encrypted Baboon [53]	279.84	283.54	252.15	271.84	Passed
Encrypted Baboon [54]	274.38	254.71	272.74	267.28	Passed
Encrypted Baboon [51]	237.27	254.15	247.32	246.25	Passed

C^2 and C^3 are produced by changing the pixel value at position (1,1) of red, green and blue channels, respectively. One can observe that the proposed system passed the test with confidence level $\alpha = 0.05$ successfully and compared with the [47], [49], [51], [53], [55], and [56]. A higher NPCR value, ideally close to 100%, signifies a greater sensitivity of the encryption scheme to minute changes in the plaintext, making it more resistant to differential attacks. The equation (27) is utilized for conducting the NPCR test.

$$N(C^1, C^2) = \sum_{i=1}^{N}\sum_{j=1}^{N}\frac{D(i,j)}{N \times N} \times 100\% \tag{27}$$

Considering an image with dimensions $N \times N$ pixels, where N represents the width and height, the pixel locations within the encrypted images C^1 and C^2 are denoted by (i, j). In this context, the NPCR (Net Pixel Change Rate) is defined as:

$$\delta(i,j) = \begin{cases} 0. & if\, C^1(i,j) = C^2(i,j) \\ 1, & if\, C^1(i,j) \neq C^2(i,j). \end{cases} \tag{28}$$

The Unified Average Changing Intensity (UACI) measures the average absolute difference in intensity between comparable pixels in two cipher pictures created with slightly different plain-text, as opposed to NPCR which looks at the percentage of changed pixel values. A UACI value closer to 33.33% suggests a notable change in pixel intensity levels in encrypted images, indicating the encryption's efficiency against differential assaults. The UACI is described as:

$$U(C^1, C^2) = \sum_{i=1}^{N}\sum_{j=1}^{N}\frac{|C^1(i,j) - C^2(i,j)|}{L \bullet N \times N}100\% \tag{29}$$

The image's dimensions are represented by $N \times N$, and the cipher images C^1 and C^2 pixel locations are denoted by (i, j). The results of NPCR and UACI are given in Table 9 and compared to Refs. [47], [49], [51], [53], [55], and [56].

C. NOISE ROBUSTNESS

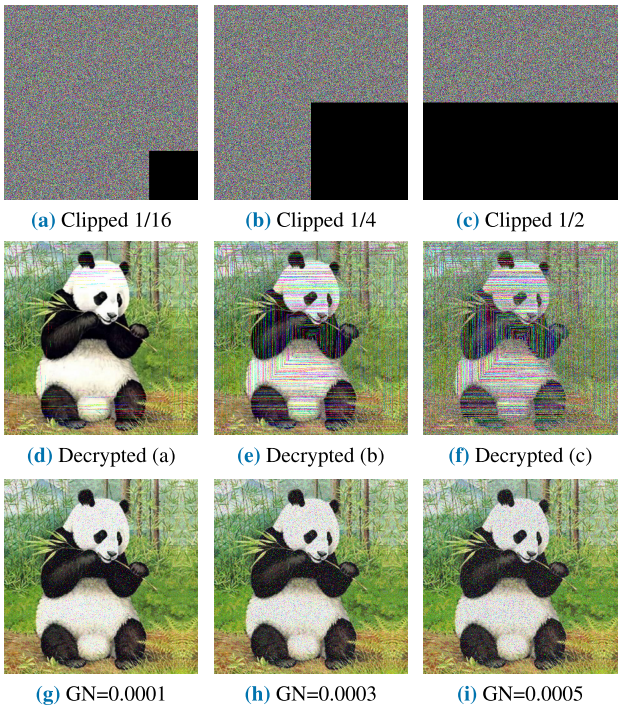
Many noises can be heard in the encrypted data as it passes through the communication channels. This noise could make it difficult to retrieve the original image. For this reason, the encryption technique needs to be powerful enough to enable the image to be decrypted. The image quality following an attack is evaluated using the Peak Signal to Noise Ratio. This formula is utilized to determine the PSNR value [4], [57]:

$$PSNR = 10 \times \log_{10}\left[\frac{255^2}{MSE}\right] \tag{30}$$

Mean Squared Error (MSE) serves as a quantitative measure of the difference between two images. It is calculated as

TABLE 9. NPCR and UACI scores of baboon.

Images	NPCR	p-Value	UACI	p-Value	Test
C^0, C^1	99.6001	0.2736	33.4718	0.7572	Passed
C^0, C^2	99.6067	0.3521	33.4743	0.6854	Passed
C^0, C^3	99.6153	0.8022	33.4363	0.5461	Passed
C^1, C^2	99.6240	0.9811	33.5120	0.0692	Passed
C^1, C^3	99.6068	0.3521	33.4814	0.5019	Passed
C^2, C^3	99.6110	0.5929	33.4721	0.7459	Passed
Ref. [53]	99.6266	–	33.4700	–	Passed
Ref. [47]	99.6100	–	33.3800	–	Passed
Ref. [49]	99.5800	–	29.4000	–	Failed
Ref. [51]	99.6100	–	33.4700	–	Passed
Ref. [55]	99.6100	–	33.4865	–	Passed
Ref. [56]	99.6100	–	33.4600	–	Passed



(a) Clipped 1/16 (b) Clipped 1/4 (c) Clipped 1/2

(d) Decrypted (a) (e) Decrypted (b) (f) Decrypted (c)

(g) GN=0.0001 (h) GN=0.0003 (i) GN=0.0005

FIGURE 15. Noise robustness against gaussian noise.

TABLE 10. PSNR, MSE, NPCR and UACI scores of panda image for noise attack.

Noise	Ratio	PSNR	MSE	NPCR	UACI
Clipping	1/16	20.53	575.31	6.3	1.94
	1/4	13.73	2725.90	24.97	8.41
	1/2	10.77	5447.75	49.89	16.72
Gaussian Noise	0.0001	19.94	658.54	90.98	4.23
	0.0003	17.64	1118.96	94.76	6.36
	0.0005	16.96	1392.36	95.89	7.55

the average squared difference between corresponding pixel intensities in the two images.

$$MSE = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} \left| C^1(i,j) - C^2(i,j) \right|^2 \tag{31}$$

In $N \times N$ images, PSNR measures the quality of the reconstructed image after decryption compared to the original image. A greater PSNR suggests better image fidelity and quality. Clipping and decrypting encrypted images tests the suggested encryption algorithm's noise durability [58]. The encrypted Baboon image is used to test for noise robustness, as shown in 10(b). The encrypted image is clipped by 1/16, 1/4 and 1/2 are shown in Figure 15(a) to 15(c) and corresponding decrypted images are shown in 15(d) to 15(e) while 15(g) to 15(h) are decrypted results images which Gaussian Noise poisons. The PSNR, MSE, NPCR and UACI quantities are given in Table 10.

VII. CONCLUSION

This research introduces a new non-linear equation named Cosine Chaotic Equation (CCE) for random number generation. The dynamical properties of chaos are used to analyze the efficiency of the proposed Equation. The system has large key space, uniform distribution, and randomness, and it is more efficient for practical applications as it is highly sensitive to initial conditions. The system shows better pseudo-random properties than the logistic map. A color image encryption method, with the concept of rotating wheels, is introduced to prove the efficacy of the proposed CCE. The permutation is performed by rotating the wheels created by combining the pixels from all three color channels. The substitution is performed by rotating and discarding some elements randomly from pseudo wheel in cipher block chaining mode to hinder the differential attack. The algorithm is analyzed for the statistical and differential analysis. The experimental results and security analysis proved that the algorithm is strong enough to resist the statistical and differential attacks and has excellent resistance against everyday noises.

ACKNOWLEDGMENT

The authors would like to thank the University of Vaasa, Finland; the Institute of Mathematics, Khwaja Fareed University of Engineering, Science and Technology, Rahim Yar Khan, Pakistan; and the Artificial Intelligence and Data Analytics Laboratory (AIDA), College of Computer and Information Science (CCIS), Prince Sultan University, Riyadh, Saudi Arabia, for supporting this study.

REFERENCES

[1] N. N. Hurrah, S. A. Parah, J. A. Sheikh, F. Al-Turjman, and K. Muhammad, "Secure data transmission framework for confidentiality in IoTs," *Ad Hoc Netw.*, vol. 95, Dec. 2019, Art. no. 101989.
[2] R. B. Saglam, J. R. C. Nurse, and D. Hodges, "Personal information: Perceptions, types and evolution," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103163.
[3] H. Tang, Q. T. Sun, X. Yang, and K. Long, "A network coding and des based dynamic encryption scheme for moving target defense," *IEEE Access*, vol. 6, pp. 26059–26068, 2018.
[4] A. U. Rehman, A. Firdous, S. Iqbal, Z. Abbas, M. M. A. Shahid, H. Wang, and F. Ullah, "A color image encryption algorithm based on one time key, chaos theory, and concept of rotor machine," *IEEE Access*, vol. 8, pp. 172275–172295, 2020.
[5] A. Ghaffari, "Image compression-encryption method based on two-dimensional sparse recovery and chaotic system," *Sci. Rep.*, vol. 11, no. 1, p. 369, Jan. 2021.
[6] A. Ur Rehman, X. Liao, and H. Wang, "An innovative technique for image encryption using tri-partite graph and chaotic maps," *Multimedia Tools Appl.*, vol. 80, no. 14, pp. 21979–22005, Jun. 2021.
[7] W. Zamrani, E. Ahouzi, A. Lizana, J. Campos, and M. J. Yzuel, "Optical image encryption technique based on deterministic phase masks," *Opt. Eng.*, vol. 55, no. 10, Oct. 2016, Art. no. 103108.
[8] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.
[9] Ü. Çavusoglu, S. Kaçar, I. Pehlivan, and A. Zengin, "Secure image encryption algorithm design using a novel chaos based S-box," *Chaos, Solitons Fractals*, vol. 95, pp. 92–101, Feb. 2017.
[10] V. M. Silva-García, R. Flores-Carapia, C. Rentería-Márquez, B. Luna-Benoso, and M. Aldape-Pérez, "Substitution box generation using chaos: An image encryption application," *Appl. Math. Comput.*, vol. 332, pp. 123–135, Sep. 2018.
[11] Y. Zhang, "The unified image encryption algorithm based on chaos and cubic S-box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.
[12] D. S. Laiphrakpam, R. Thingbaijam, K. M. Singh, and M. Al Awida, "Encrypting multiple images with an enhanced chaotic map," *IEEE Access*, vol. 10, pp. 87844–87859, 2022.
[13] A. Firdous, A. U. Rehman, and M. M. S. Missen, "A gray image encryption technique using the concept of water waves, chaos and hash function," *IEEE Access*, vol. 9, pp. 11675–11693, 2021.
[14] A. G. Radwan, S. H. AbdElHaleem, and S. K. Abd-El-Hafiz, "Symmetric encryption algorithms using chaotic and non-chaotic generators: A review," *J. Adv. Res.*, vol. 7, no. 2, pp. 193–208, Mar. 2016.
[15] C. Fu, J.-J. Chen, H. Zou, W.-H. Meng, Y.-F. Zhan, and Y.-W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Opt. Exp.*, vol. 20, no. 3, pp. 2363–2378, 2012.
[16] K.-W. Wong, B. S.-H. Kwok, and C.-H. Yuen, "An efficient diffusion approach for chaos-based image encryption," *Chaos, Solitons Fractals*, vol. 41, no. 5, pp. 2652–2663, Sep. 2009.
[17] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu, and J.-J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption," *Opt. Commun.*, vol. 284, no. 23, pp. 5415–5423, Nov. 2011.
[18] G. A. Sathishkumar, R. Srinivas, and K. B. Bagan, "Image encryption using random pixel permutation by chaotic mapping," in *Proc. IEEE Symp. Comput. Informat. (ISCI)*, Mar. 2012, pp. 247–251.
[19] A. Firdous, A. Ur Rehman, and M. M. S. Missen, "A highly efficient color image encryption based on linear transformation using chaos theory and SHA-2," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24809–24835, Sep. 2019.
[20] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, Aug. 2022.
[21] R. Scholar and S. Kumari, "A research paper on cryptography encryption and compression techniques," *Int. J. Eng. Comput. Sci.*, vol. 6, no. 4, pp. 20915–20919, 2017.

[22] J. Zhang, "An image encryption scheme based on cat map and hyperchaotic Lorenz system," in *Proc. IEEE Int. Conf. Comput. Intell. Commun. Technol.*, Feb. 2015, pp. 78–82.

[23] N. A. Abbas, "Image encryption based on independent component analysis and Arnold's cat map," *Egyptian Informat. J.*, vol. 17, no. 1, pp. 139–146, Mar. 2016.

[24] X. Liao, M. A. Hahsmi, and R. Haider, "An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos," *Optik-Int. J. Light Electron Opt.*, vol. 153, pp. 117–134, Jan. 2018.

[25] Q. Lai, H. Hua, X.-W. Zhao, U. Erkan, and A. Toktas, "Image encryption using fission diffusion process and a new hyperchaotic map," *Chaos, Solitons Fractals*, vol. 175, Oct. 2023, Art. no. 114022.

[26] Q. Lai, L. Yang, G. Hu, Z.-H. Guan, and H. H.-C. Iu, "Constructing multiscroll memristive neural network with local activity memristor and application in image encryption," *IEEE Trans. Cybern.*, vol. 54, no. 7, pp. 4039–4048, Jul. 2024.

[27] Q. Lai, Z. Wan, H. Zhang, and G. Chen, "Design and analysis of multiscroll memristive Hopfield neural network with adjustable memductance and application to image encryption," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 34, no. 10, pp. 7824–7837, Oct. 2023.

[28] Q. Lai, L. Yang, and G. Chen, "Design and performance analysis of discrete memristive hyperchaotic systems with stuffed cube attractors and ultraboosting behaviors," *IEEE Trans. Ind. Electron.*, vol. 71, no. 7, pp. 7819–7828, Jul. 2024.

[29] A. A. Elsadany, A. M. Yousef, and A. Elsonbaty, "Further analytical bifurcation analysis and applications of coupled logistic maps," *Appl. Math. Comput.*, vol. 338, pp. 314–336, Dec. 2018.

[30] H.-B. Jiang, T. Li, X.-L. Zeng, and L.-P. Zhang, "Bifurcation analysis of the logistic map via two periodic impulsive forces," *Chin. Phys. B*, vol. 23, no. 1, 2013, Art. no. 010501.

[31] Z. Chen, D. Liang, X. Deng, and Y. Zhang, "Performance analysis and improvement of logistic chaotic mapping," *J. Electron. Inf. Technol.*, vol. 38, no. 6, pp. 1547–1551, 2016.

[32] T. Caraballo, R. Colucci, and L. Guerrini, "Dynamics of a continuous Henon model," *Math. Methods Appl. Sci.*, vol. 41, no. 10, pp. 3934–3954, 2018.

[33] M. Ubaidullah and Q. Makki, "A review on symmetric key encryption techniques in cryptography," *Int. J. Comput. Appl.*, vol. 147, no. 10, pp. 43–48, Aug. 2016.

[34] D. M. Huang, X. Geng, L. F. Wei, and C. Su, "A secure query scheme on encrypted remote sensing images based on Henon mapping," *J. Softw.*, vol. 27, no. 7, pp. 1729–1740, 2016.

[35] M. Sumagita, I. Riadi, J. Sh, and U. Warungboto, "Analysis of secure hash algorithm (SHA) 512 for encryption process on web based application," *Int. J. Cyber-Secur. Digit. Forensics (IJCSDF)*, vol. 7, no. 4, pp. 373–381, 2018.

[36] F. Pub, "Secure hash standard (SHS)," *Fips Pub*, vol. 180, no. 4, pp. 183–194, 2012.

[37] M. Wang, X. Wang, Y. Zhang, and Z. Gao, "A novel chaotic encryption scheme based on image segmentation and multiple diffusion models," *Opt. Laser Technol.*, vol. 108, pp. 558–573, Dec. 2018.

[38] L. Merah, P. Lorenz, and A.-P. Adda, "A new and efficient scheme for improving the digitized chaotic systems from dynamical degradation," *IEEE Access*, vol. 9, pp. 88997–89008, 2021.

[39] J. Bryła, T. Buchner, and J. J. Żebrowski, "Analysis of phase space structure of a 1-D discrete system using global and local symbolic dynamics," *Acta Phys. Polonica B*, vol. 36, no. 5, pp. 1457–1471, 2005.

[40] R. B. Naik and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," *Ann. Data Sci.*, vol. 11, no. 1, pp. 25–50, Feb. 2024.

[41] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[42] X. Ye, X. Wang, S. Gao, J. Mou, Z. Wang, and F. Yang, "A new chaotic circuit with multiple memristors and its application in image encryption," *Nonlinear Dyn.*, vol. 99, no. 2, pp. 1489–1506, Jan. 2020.

[43] R. Blom, "An optimal class of symmetric key generation systems," in *Proc. Workshop Theory Appl. Cryptograph. Techn.*, Paris, France. Berlin, Germany: Springer, Apr. 1985, pp. 335–338.

[44] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, "Image encryption techniques: A comprehensive review," *Multimedia Tools Appl.*, vol. 22, pp. 1–36, Jan. 2024.

[45] D. Kumar, V. K. Sudha, and R. Ranjithkumar, "A one-round medical image encryption algorithm based on a combined chaotic key generator," *Med. Biol. Eng. Comput.*, vol. 61, no. 1, pp. 205–227, Jan. 2023.

[46] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 1671–1675, 2014.

[47] B. Ge, X. Chen, G. Chen, and Z. Shen, "Secure and fast image encryption algorithm using hyper-chaos-based key generator and vector operation," *IEEE Access*, vol. 9, pp. 137635–137654, 2021.

[48] H.-M. Yuan, Y. Liu, T. Lin, T. Hu, and L.-H. Gong, "A new parallel image cryptosystem based on 5D hyper-chaotic system," *Signal Process., Image Commun.*, vol. 52, pp. 87–96, Mar. 2017.

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

[50] S. Beg, F. Baig, Y. Hameed, A. Anjum, and A. Khan, "Thermal image encryption based on laser diode feedback and 2D logistic chaotic map," *Multimedia Tools Appl.*, vol. 81, no. 18, pp. 26403–26423, Jul. 2022.

[51] D. Mou and Y. Dong, "Color image encryption algorithm based on Mackey–Glass time-delay chaotic system and quantum random walk," *New J. Phys.*, vol. 26, no. 3, Mar. 2024, Art. no. 033010.

[52] Y. Zhang, W. Dong, J. Zhang, and Q. Ding, "An image encryption transmission scheme based on a polynomial chaotic map," *Entropy*, vol. 25, no. 7, p. 1005, 2023.

[53] X. Chen, M. Gong, Z. Gan, Y. Lu, X. Chai, and X. He, "CIE-LSCP: Color image encryption scheme based on the lifting scheme and cross-component permutation," *Complex Intell. Syst.*, vol. 9, no. 1, pp. 927–950, Feb. 2023.

[54] E. Güvenoğlu, "An image encryption algorithm based on multi-layered chaotic maps and its security analysis," *Connection Sci.*, vol. 36, no. 1, Dec. 2024, Art. no. 2312108.

[55] J. Wen, X. Xu, K. Sun, Z. Jiang, and X. Wang, "Triple-image bit-level encryption algorithm based on double cross 2D hyperchaotic map," *Nonlinear Dyn.*, vol. 111, no. 7, pp. 6813–6838, Apr. 2023.

[56] Q. Zhang and J. Han, "A novel color image encryption algorithm based on image hashing, 6D hyperchaotic and DNA coding," *Multimedia Tools Appl.*, vol. 80, no. 9, pp. 13841–13864, Apr. 2021.

[57] R. Premkumar, M. Mahdal, and M. Elangovan, "An efficient chaos-based image encryption technique using bitplane decay and genetic operators," *Sensors*, vol. 22, no. 20, p. 8044, Oct. 2022.

[58] H. Shen, X. Shan, M. Xu, and Z. Tian, "A new chaotic image encryption algorithm based on transversals in a Latin square," *Entropy*, vol. 24, no. 11, p. 1574, Oct. 2022.

FARMAN ULLAH received the bachelor's degree in computer science from the Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan, Pakistan, in 2012, and the M.Phil. degree in computer science from the National College of Business Administration and Economics, Lahore, in 2016. He is currently a Lecturer with the Department of Computer Science, COMSATS University Islamabad. His research interests include cryptography, image processing, computer graphics, and programming languages.

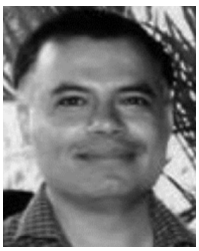
ZIAUDDIN received the master's (Hons.) and Ph.D. degrees in computer science, in 1990 and 2010, respectively. He is currently an Associate Professor with the Institute of Computing and Information Technology, Gomal University, Dera Ismail Khan, Pakistan. He has been teaching there for the last 33 years. He has experience in many areas of computer science with an emphasis on software process improvement and machine learning. He has supervised many Ph.D. and master's students. Besides teaching, he is also a Painter and Poet.

MUHAMMAD FAHEEM (Member, IEEE) received the B.Sc. degree in computer engineering from Bahauddin Zakariya University, Pakistan, in 2010, the M.S. and Ph.D. degrees in computer science from Universiti Teknologi Malaysia in 2012 and 2021, respectively, and the Postdoctoral degree from the School of Technology and Innovations, University of Vaasa, Finland, in 2024. He has held academic positions as a Lecturer at the Comsats Institute of Information and Technology, Pakistan, from 2012 to 2014, and an Assistant Professor at the Department of Computer Engineering, Abdullah Gul University, Turkey, from 2014 to 2022. Currently, he is an Assistant Professor with the Department of Computer Science at the University of Vaasa (2024-Conti.). He has published high-quality research articles in peer-reviewed journals and conferences, and serves as referee for several prestigious journals of IEEE, IET, Elsevier, Springer, Wiley, and MDPI. His research focuses on cybersecurity, blockchain, artificial intelligence, smart grids, and smart cities, and the Internet of Things. He serves as the editorial boards of several esteemed journals, including IEEE IoT Sensors, Sustainable Futures, *PLOS ONE*, Frontiers in the Internet of Things, Frontiers in Artificial Intelligence, Computers, Materials and Continua, and others.

MUNTAZIM ABBAS HASHMI has a long academic, research, and administrative profile from his profession. He is currently the Head of Mathematics at the Khwaja Fareed University of Engineering and Information Technology (KFUEIT), Rahim Yar Khan. He is the pioneer and the first Head of this department. His efficient working, dedication toward his job, and experience are making the department in a process of continuous growth. Under his supervision, he manages and motivates all departmental staff and increases and enables pupils to receive an education in the subject, in a positive, encouraging, and effective working environment. Manage income and expenditure in order to promote financial stainability.

AQEEL-UR-REHMAN received the M.Sc. degree in computer science from The Islamia University of Bahawalpur, Pakistan, the second master's degree in computer engineering from UET Taxilla (CASE Campus), Islamabad, Pakistan, and the Ph.D. degree in computer science and technology from Chongqing University, Chongqing, China. He was a Senior Research Fellow at Southwest University, Chongqing, from 2018 to 2020. He is currently an Associate Professor with the Department Computer Sciences, COMSATS University Islamabad, Vehari Campus. He has published more than 22 research articles in Impact Factor journals. His primary research interests include non-linear dynamics and cryptography. He is a Reviewer of *Optics and Laser Technology*, *Optics and Lasers in Engineering*, and *Engineering Science and Technology, an International Journal*.

RAB NAWAZ BASHIR received the M.S. and Ph.D. degrees in computer science from The Islamia University of Bahawalpur, Bahawalpur, Pakistan, in 2015 and 2021, respectively. He is currently an Assistant Professor at COMSATS University Islamabad, Vehari, Pakistan. His research interests include the Internet of Things (IoT) and machine learning applications in agriculture.



AMJAD REHMAN KHAN (Senior Member, IEEE) received the Ph.D. and Postdoctoral degrees (Hons.) from the Faculty of Computing, University Teknologi Malaysia, with a specialization in forensic documents analysis and security, in 2010 and 2011, respectively. He is currently a Senior Researcher with the Artificial Intelligence and Data Analytics Laboratory, College of Computer and Information Sciences (CCIS), Prince Sultan University, Riyadh, Saudi Arabia. He is the author of more than 200 ISI journal articles and conferences. He is also a PI in several funded projects and also completed projects funded from MOHE Malaysia and Saudi Arabia. His research interests include data mining, health informatics, and pattern recognition. He received the Rector Award for the 2010 Best Student from Universiti Teknologi Malaysia.