IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received June 7, 2018, accepted July 12, 2018, date of publication July 23, 2018, date of current version August 20, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2858839

An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations

HOSSAM DIAB
Computer Science Department, College of Computer Science and Engineering, Taibah University, Medina 41411, Saudi Arabia
Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
e-mail: dr.hosamdiab@gmail.com

This work was supported by the Deanship of Scientific Research, Taibah University, Al-Madinah Al-Munawwarah, Saudi Arabia.

ABSTRACT Recently, several multimedia encryption techniques with permutation–diffusion architecture have been developed. The traditional architecture applies the diffusion and permutation functions as two separate phases. This separable design enables the attacker to launch several forms of attacks in addition to the degradation of the encryption speed. Furthermore, during the diffusion phase, the image pixels are masked in a static order, which may expose significant information about the encryption technique to the attacker. Accordingly, to remedy these problems, this paper suggests an efficient image cryptosystem based on simultaneous permutation and diffusion functions that process the image pixels in a dynamic order fashion. Specifically, the proposed method employs the Chebyshev-Chebyshev map to horizontally and vertically mix the plain-image information. Then, it utilizes the modified Logistic map to mask the image pixels and shuffle the masked values simultaneously. Meanwhile, the control parameters of the employed chaos systems are directly correlated to the plain-image to assure that different key-streams are created for distinct plain-images. Simulation results and security scrutiny confirm that the suggested cipher has several brilliant characteristics, including the robustness against various types of attacks.

INDEX TERMS Chaos system, cryptography, image encryption, security analysis, simultaneous permutation–diffusion.

I. INTRODUCTION

With the evolution of communication technologies, a variety of sensitive media are processed, stored and delivered in digital format. Unauthorized adversaries can easily intercept and eavesdrop on the transmitted media over public communications channels, such as Internet, mobile phone, and satellite. In most cases, this media is critical and must be maintained from any unauthorized party. Particularly, the security of digital images represents a bottleneck for many multimedia applications including military images applications, medical images systems, and secure exchange of multimedia information through different wireless networks and portable devices [1]–[4]. Accordingly, to preserve the confidentiality of the transmitted images, different encryption techniques are employed. Specifically, the chaotic-based ciphers have shown brilliant performance in this direction, this is due to their good features which mimic the required attributes of good cryptosystems. These features include noise like behavior, ergodicity, extreme sensitivity to initial control parameters. Taking into account these features, several image ciphers based on chaos systems have been extensively presented. Indeed, most of the employed approaches adopted the classical permutation-diffusion structure in which two iterative stages of permutation and diffusion are alternately used. The general permutation–diffusion architecture for image cipher is illustrated in Figure 1 as depicted in [4]. This structure is composed of two main building blocks which are permutation and diffusion operations. The former one only shuffles the positions of the plain-image, usually using 2D chaotic map such as Cat map, Standard map and Baker map, to break the correlation between neighbouring pixels. While the latter operation sequentially changes the pixels values of the permuted image by a quantized chaotic key stream to spread out any slight change of any pixel to almost all image pixels. Further, the whole architecture is iterated to enhance the encryption effect of algorithm.

A. RELATED WORK

In what follows, several related image ciphers are investigated. Chen *et al.* [5] extended the 2D Cat map to 3D for

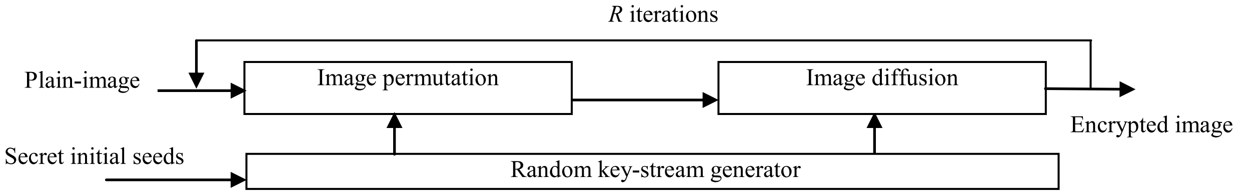


FIGURE 1. Classical permutation–diffusion based architecture for image ciphering.

constructing a secure cryptosystem in which the generalized map is utilized in the permutation phase to scramble the pixels and then the Logistic map is employed in the diffusion phase to mask the shuffled image. Lian *et al.* [6] investigated the sensitivity properties of the Standard chaotic map and also examined the key space associated to this map compared to the Baker map and Cat map. Then an amended Standard map is presented to consummate pixel scrambling while the diffusion phase employed the Logistic map to modify the values of pixels. In [7], the Baker map was generalized to 3D and then utilized in permuting the positions of pixels, whereas the Logistic map is employed to alter the values of the shuffled image. In [8], a cryptosystem that also adopts the permutation-diffusion architecture was presented. The trait of this cipher is employing several simple operations (add-and-shift) along with the permutation to achieve a certain diffusion effect in the permutation phase. In [9], an image cipher employing the permutation and diffusion structure was presented. First, the original image is divided into several blocks of pixels. After that, a spatiotemporal chaotic system is applied to permute these blocks, and concurrently modify the image pixels. A hyper-chaotic image cipher with a large key space was presented in [10] to encrypt the plain-image using pixel-level permutation. Afterward, Rhouma and Belghith [11] demonstrated that this algorithm could not thwart chosen attacks including both chosen plaintext/ciphertext attacks, further, they improved the algorithm. Jeng *et al.* [12] proved that both the original algorithm and its improvement [10], [11] have many security flaws. Patidar *et al.* [13] presented an image cryptosystem utilizing the confusion–diffusion architecture by combining the Logistic and Standard chaotic maps. The cryptosystem is intended for encrypting the color images. It involves three main stages of confusion, diffusion, and confusion, respectively. Wang *et al.* [14] presented an efficient image cryptosystem using Lorenz chaos system and simple perceptron model. The proposed method can repair the periodicity and the cycle state issues related to discrete chaotic system by dynamically adjusting its chaotic parameters. A one-time key-based encryption scheme for image cipher was presented in [15]. Liu and Wang [16] developed an encryption scheme for color images based on the piecewise linear chaotic map and Chen chaotic system. Specifically, the proposed approach permuted the original image at bit-level and simultaneously masked the color components using Chen system. Ye [17] presented an efficient image cipher using two chaotic maps. In [18], a new color image-ciphering scheme using a Logistic map was suggested. The method implemented the permutation and substitution approaches to diminish the relations between the color channels of the original image. After that, Li *et al.* [19] developed an attack model to break the permutation-diffusion mechanism in [18] with two chosen plain-images. Further, Tu *et al.* [20] studied the cipher presented in [18], and identified the main flaws of the scheme. Their analysis firstly demonstrated that the cipher uses fixed encryption parameters for the first image pixel and the generated key stream is independent of the image. Secondly, they developed a chosen plain-image attack model to crack the scheme. Finally, an improved cryptosystem is designed to fix these weaknesses. Zhu [21] designed a new image cryptosystem with only two rounds of diffusion in which an enhanced hyper-chaos system is employed for key-stream generation. Ozkaynak *et al.* [22] and Li *et al.* [23] independently broke the Zhu scheme [21] by employing chosen-plaintext and known-plaintext attacks, respectively. Zhou *et al.* [24] presented a novel switching chaotic map in which the Logistic, Sine and Tent maps are combined to build a single chaotic system. The chaotic sequence resulted from the Logistic map is employed as a control parameter to govern a switch that selects between the Sine and Tent maps generator to yield the chaotic sequence for the new system. Wang and Luan [25] employed the intertwining Logistic map and reversible cellular automata to design a new image cipher. This cipher adopts the permutation-substitution architecture at bit level which considers the higher four bits of each image pixel. Further, an image cryptosystem with one round of diffusion was presented in [26] in which a hyper chaotic system is utilized as a random key-stream generator. The core idea of this method lays in employing the summation of all pixel located after the processed pixel in the encryption process. Zhang *et al.* [27] presented a cryptanalytic model based on known plain-image attack to divulge the key-stream of the cryptosystem presented in [26] and they also indicated that this cryptosystem can be broken by a chosen plain-image attack. Moreover, Diab and El-semary [28] analyzed the image encryption technique presented in [26] and proposed a chosen-plaintext attack strategy to break the scheme. Further, they suggested an efficient cryptosystem that utilizes the fingerprint of the image to generate a unique encryption key stream to resist all types of attacks. A new pixel swapping strategy for image scrambling that can achieve a satisfactory diffusion effect in the permutation phase was proposed in [29]. Fouda *et al.* [30]

presented a fast chaos-based technique for image ciphering. Zhang and Wang [31] proposed a novel image cipher by employing the spatiotemporal dynamics of non-adjacent coupled map lattices. They developed a novel bit-level scrambling strategy by which the bit groups of one plain-image bit plane can be shuffled into any other bit plane. Consequently, the permutation process changes the statistical traits of bit-planes and masks the intrinsic features of the original image. Wang *et al.* [32] developed a chaotic based image cryptosystem by employing the primitive operations of pixels scrambling, cycle shift and image diffusion. Moreover, the scheme generates the initial values of the employed chaotic map based on the scrambled image information, so, it can resist different types of attacks. Yuan *et al.* [33] introduced a cryptosystem employing 2D hyper-chaotic system in which the confusion and diffusion functions are related to obtain a secure image cipher. A new chaotic based cipher for encrypting gray level images using a dynamic random growth method was presented in [34]. However, the scheme was cryptanalyzed in [35] using chosen-type attacks. Liu *et al.* [36] suggested an efficient image cryptosystem in which only one stage of confusion and diffusion is applied. Wang *et al.* [37] proposed a novel hybrid cipher to encrypt color channels of the plain-image by employing two complex chaotic systems. Zhou *et al.* [38] coupled the Sine and Tent maps together to produce a new 1D chaotic map which is exploited to mask the plain-image pixels. Dhall *et al.* [39] demonstrated the insecurity of the encryption scheme proposed in [38] and identified the weakness of this cipher. Specifically, the original scheme suffered from several vulnerabilities including the static permutation mapping, inadequate specification of encryption key stream and weak substitution-permutation architecture. Murillo-Escobar *et al.* [40] exploited the plain-image features and chaotic system in designing a new cipher for encrypting color images. Chen *et al.* [41] presented an image-ciphering approach in which the permutation sequence of the permutation stage is reused in the diffusion stage to obtain a dynamic key-stream for different images with no extra chaotic iterations and quantization. Diab and El-semary [42] cryptographically investigated the cryptosystem presented in [41] and designed a chosen plaintext attack model to crack that scheme. In addition, they repaired the defects of the cipher by revising its structure based on the plain-image features. Accordingly, the encryption parameters of the proposed scheme are dynamically changed to yield a secure image cipher. A new image cryptosystem with permutation-substitution network was presented in [43]. Pak and Huang [44] presented a total shuffling cryptosystem by utilizing their novel proposed chaos systems: the Sine-Sine system, the Logistic-Logistic system, and the Chebyshev-Chebyshev system. The new combined maps can repair the flaws associated with simple 1D maps. Wang *et al.* [45] broke the cryptosystem suggested in [44] by mounting chosen plain-image attacks. The vulnerability of the scheme arises from the independence of the generated chaotic sequence for permutation and diffusion from the plain-image. Namely, the permutation matrix and the diffusion matrix are fixed regardless of the image being encrypted. Further, they enhanced the scheme by relating the encryption parameters with the plain-image. Zhang *et al.* [46] proposed an image encryption scheme that decomposes the input image into three-color components and then employs a chaotic scrambling mapping to shuffle each image unit of 8×8 pixels. In [47], a modified version of Logistic map with large key space was proposed to remedy the main problems of the original Logistic map. Moreover, this map is employed to design an efficient image cryptosystem in [48] and [49]. Ponnaian and Chandranbabu [48] studied the security aspects of the cipher presented in [46] and reported that it is vulnerable to known/chosen plain-image attacks. The scheme is permutation only cipher and hence it cannot hide the statistical traits of the plain-image. In addition, they developed a revised version of the underlying scheme using a modified Logistic chaotic map [47]. Parvaz and Zarebnia [50] defined a novel chaotic system by combining primitive maps of Logistic and Tent systems. They also analyzed the chaotic properties of the suggested system and exploited it to design a novel image cryptosystem. Liu *et al.* [51] presented a new image cipher mechanism based on DNA encoding rules by employing the permutation–diffusion architecture. Their cipher exploits the MD5 hashing to generate an encryption key stream related to the input plain-image. Wang *et al.* [52] suggested a new DNA based image cipher in which the DNA operations and a coupled map lattice are employed. The encryption scheme firstly mixed the plain-image information with a chaotic sequence and secondly applied DNA operations to encode the masked image. Finally, it employed DNA-level shuffling, DNA-level confusion, and DNA decoding operations to obtain the final encrypted image.

B. LIMITATIONS OF TRADITIONAL PERMUTATION-DIFFUSION STRUCTURE

Based on the study and security analysis of several chaotic image cryptosystems with a permutation-diffusion structure [3], [9], [11]–[13], [17], [22], [23], [26], [28], [41], [42], [48], [49], it is found that most of them carry out the permutation and the diffusion processes as two separate stages. From cryptography perspective, this separation causes several defects for such architecture. Specifically, the common defects of these ciphers are: Firstly, the initial parameters for the permutation phase are fixed which in turn returns the same permutation sequence in all permutation-diffusion iterations. Secondly, for the diffusion phase, the generated key-stream is only dependent on the secret initial parameters of the employed chaos system. Additionally, the values of image pixels are altered during the diffusion stage in a static fashion from left upper corner to right bottom corner which exposes significant information about the encryption technique to the attackers. Accordingly, an adversary could simply split the architecture into two unrelated phases by feeding the encryption algorithm with a flat plain-image of identical values. Therefore, the shuffling process has no effect on this specific chosen image and the attacker can easily compute the key-stream used in the diffusion stage which is only dependent on the initial parameters and not related to the information of plain-images. Thus, in most cases, the attacker can break such schemes by lunching known/chosen plaintext attacks. Further, the chaotic orbit of most simple chaotic maps tends to be periodic under the finite precision computation, which degrades their dynamical features and weakens the security level. Accordingly, this motivates us to develop an encryption scheme that can solve these flaws.

C. CONTRIBUTION AND ORGANIZATION OF THE PAPER

To remedy the aforementioned problems, an efficient image encryption technique that combines the two basic operations (permutation and diffusion) together in one stage is proposed. Namely, the permutation and diffusion are simultaneously applied. Further, a dynamical pixel order mechanism for diffusion is suggested. The proposed image cryptosystem firstly mixes the image pixels in horizontal and then in vertical directions with a key-stream generated in advance from Chebyshev-Chebyshev chaotic map. After that, the modified Logistic map is employed to create both a dynamic pixel order and diffusion key that are used to simultaneously change and permute the image pixels. The initial parameters for the employed chaotic map, at each pixel, are dynamically adapted based on the cipher-image information, which in turn guarantees a distinct key-stream is generated for distinct plain-images. Accordingly, the suggested cipher can successfully thwart different attacks including the most powerful chosen plaintext/ciphertext attack. In addition, the suggested scheme takes into account the dynamic degradation problems [53] associated with chaotic systems. Simulation results and security study attest that the suggested cipher is efficient and has several brilliant cryptographic characteristics. Additionally, the numerical computations also prove that the proposed cryptosystem outperforms several related image ciphers in terms of encryption quality and performance.

The rest of this paper is organized as follows: Section 2 briefly describes the employed chaotic maps. Section 3 depicts the suggested image cipher. Simulations results and security analysis for the suggested cipher are discussed in Section 4. Finally, conclusions are drawn in Section 5.

II. PRELIMINARIES

This section presents a brief overview of the chaotic systems employed in the proposed image cipher. According to its sensitivity to initial values and control parameters, simple structure and ease of implementation, the classical chaotic maps such as Logistic map, Sine map, Chebyshev map and Tent map are commonly employed in designing image cryptosystems [5], [6], [7], [13], [14]. However, these maps have several flaws including small key space, non-uniform distribution of their output, the limited chaotic range of their control parameters, and blank windows. Accordingly, several mechanisms have been presented to repair these weaknesses and improve chaotic performance, for example see [38], [44], [47], [50]. Therefore, the proposed scheme employs the Chebyshev-Chebyshev chaotic map presented in [44] and the modified Logistic map presented in [47].

The Chebyshev-Chebyshev chaotic map is defined as:

$$x_i = \cos((u_1+1)\times \arccos(x_{i-1}))\times 2^{k_1} \\ -floor(\cos((u_1+1)\times \arccos(x_{i-1}))\times 2^{k_1}) \quad (1)$$

where $u_1 \epsilon (0, 10]$ and $8 \leq k_1 \leq 20$ are the control parameters of the map and $x_0 \epsilon (0, 1]$ is an initial parameter.

While the modified Logistic map is defined as:

$$y_n = (u_2 \times k_2 \times y_{n-1} \times (1 - y_{n-1})) \bmod 1 \quad (2)$$

where $u_2 \epsilon (0, 4]$ and $k_2 > 1$ are the control parameters of the map and $y_0 \epsilon (0, 1]$ is an initial parameter.

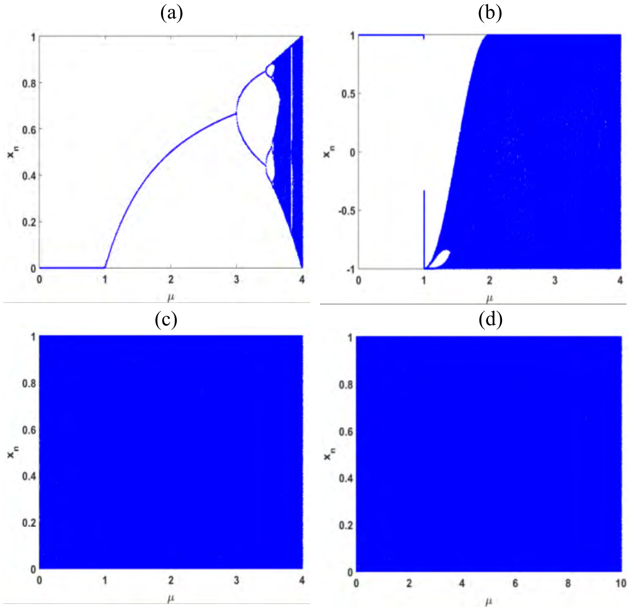


FIGURE 2. The Bifurcation diagrams of the (a) Logistic map; (b) Chebyshev map; (c) Modified Logistic map; (d) Chebyshev-Chebyshev map.

Pak and Huang [44] and Jianquan *et al.* [47] analyzed the chaotic behavior of the Chebyshev-Chebyshev map and the modified Logistic map, respectively. They independently showed that these maps could overcome several flaws of Logistic map and Chebyshev map such as small key space, stable windows, blank windows and uneven distribution of generated sequences. Further, for the modified Logistic map, the term $u_2 \times k_2$ can be treated as a single parameter with any positive real value which in turn expands the key space of the map. Actually, the Chebyshev-Chebyshev map and the modified Logistic map used in our scheme have several advantages compared with simple maps such as Logistic map and Chebyshev map based on their chaotic performance. Firstly, the distribution of the generated sequence from the employed maps is more uniform than its corresponding simple maps. From the bifurcation diagram shown in Figure 2, the Logistic map and Chebyshev map have a limited data range within

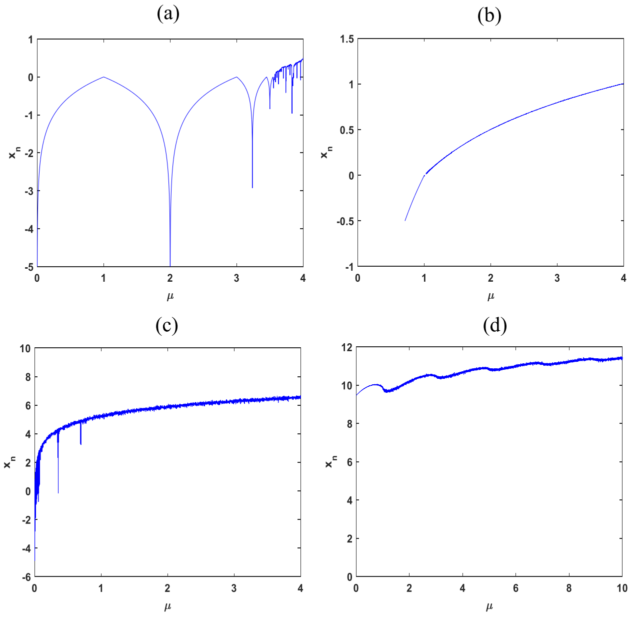


FIGURE 3. **The Lyapunov Exponent of the (a) Logistic map; (b) Chebyshev map; (c) Modified Logistic map; (d) Chebyshev-Chebyshev map.**

the interval [0, 1]. On the other hand, the produced sequences from the Chebyshev-Chebyshev chaotic map and the modified Logistic map spread out in the entire data range of the interval [0, 1]. This feature attests that the employed chaotic systems are more appropriate for designing new chaotic based ciphers. Secondly, the utilized chaotic maps have a broader chaotic range than the corresponding seed maps. This property can be demonstrated by the Lyapunov exponent as shown in Figure 3. The Lyapunov exponent of the Chebyshev-Chebyshev chaotic map and the modified Logistic map are always positive in the entire range of the control parameter. On the other hand, the Lyapunov exponents of the seed maps are positive within a limited data range. The wide chaotic range of the control parameters also expands the key space of the cipher. Thirdly, both chaotic maps have better chaotic behavior, as illustrated in Figure 3, the Lyapunov exponents of them are greater than the corresponding seed maps which indicates the better chaotic traits. In addition to the good chaotic features of both maps, the employing of multiple chaotic systems together extends the key space of the scheme, which improves the security level of the suggested cipher compared with those approaches based on single chaotic map. Therefore, we adopt the Chebyshev-Chebyshev chaotic map and the modified Logistic map to build our cryptosystem. Note that in Figure 2 and Figure 3, the value μ indicates the control parameter of each map.

III. THE SUGGESTED IMAGE CIPHER

In this section, the details of the suggested image cipher are thoroughly depicted and then in the following section its feasibility for image security application is demonstrated. The proposed cipher uses ten parameters (x_0, u_1, k_1, N_0, y_0, $u_2 \times k_2$, t_0, V_0, V'_0, and c_0) as a secret key. The proposed scheme consists of three main steps: generation of intermediate keys, horizontal and vertical mixing, and simultaneous permutation and diffusion operations as shown in Figure 4. Accordingly, the details of the suggested cipher can be represented as follows:

Step 1: Generate the intermediate keys for horizontal and vertical pixel mixing

1.1 Iterate the Chebyshev-Chebyshev chaotic map [44] depicted in *Eq.*1 for $N_0 + 2MN$ times to get a chaotic sequence $\{x_i: 1 \leq i \leq N_0 + 2MN\}$.
For Eq.1, the control parameters ($u_1 \epsilon (0,\ 10]$ and $8 \leq k_1 \leq 20$) and the initial value $x_0 \epsilon (0,\ 1]$ are parts of the secret key. In addition, N_0, M, and N indicate some secret integer, the width and the height of the plain-image, respectively. It is worth to note that, with the given ranges of u_1 and k_1 the chaotic map in *Eq.*1 reveals a good chaotic performance as shown in Section 2.

1.2 Compute the intermediate keys (key_1 and key_2) according to

$$key_L(i,j) = (x_W \times 10^{14}) \bmod 256 \tag{3}$$

where

$$W = \begin{cases} N_0 + 2r_1 - 1 & \text{if } L = 1 \\ N_0 + 2r_2 & \text{if } L = 2 \end{cases} \tag{4}$$

where r_1 and $r_2 = 1, 2, \ldots, MN$.

*Eq.*4 states that the first N_0 values of the generated chaotic sequence are discarded to hinder the transient effect and to promote the initial parameters sensitivity of the map. Further, it denotes that the first key-stream key_1 is obtained from the values indexed by the odd position in the sequence x while key_2 is acquired by the even indices.

Step 2: Horizontal and vertical mixing of image pixels

2.1 Mix the pixels information of the plain-image P by sequentially chaining them through *XOR* operation. The horizontal pixel mixing (*HPM*) operation is accomplished as follows:

```
For $r = 1 : M$
    For $s = 1 : N$
        If $r = 1\&s = 1$
        $P(r,s) = P(r,s) \oplus V_0 \oplus Key_1(r,s)$
        Elseif $r \geq 2\&s = 1$
        $P(r,s) = P(r,s) \oplus P(r-1,N) \oplus Key_1(r,s)$
        Else
        $P(r,s) = P(r,s) \oplus P(r,s-1) \oplus Key_1(r,s)$
        End If
    End For
End For
```

where V_0 is an initial secret seed maintained by the sender and receiver.

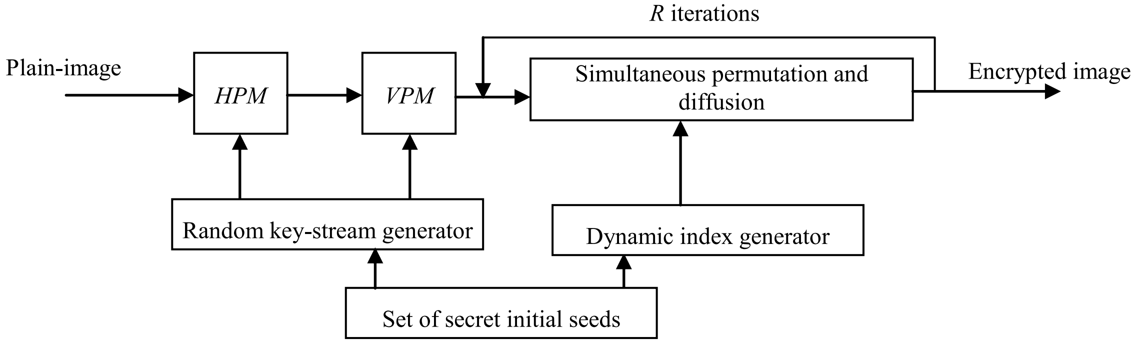

R iterations
Plain-image
HPM
VPM
Simultaneous permutation and diffusion
Encrypted image
Random key-stream generator
Dynamic index generator
Set of secret initial seeds

FIGURE 4. Proposed architecture for image ciphering.

2.2 Apply the mixing operation in vertical direction. The vertical pixel mixing (*VPM*) operation is performed as follows:

```
For $s = N : -1 : 1$
    For $r = M : -1 : 1$
        If $r = M \,\&\, s = N$
        $P(r,s) = P(r,s) \oplus V'_0 \oplus Key_2(r,s)$
        Elseif $r = M \& s < N$
        $P(r,s) = P(r,s) \oplus P(1,s+1) \oplus Key_2(r,s)$
        Else
        $P(r,s) = P(r,s) \oplus P(r+1,s) \oplus Key_2(r,s)$
        End If
    End For
End For
```

where V'_0 is also an initial secret seed.

It is obvious that *HPM* is applied row-wise from the first pixel to the last one to make each pixel of the plain-image influenced by all preceding pixels [13]. Similarly, the *VPM* is implemented column-wise in a reverse order from the last pixel to the first one to relate each pixel with all pixels located after it. Accordingly, the high sensitivity of the suggested cipher for tiny variations occurred in a plaintext is guaranteed. Further, the intermediate keys, key_1 and key_2, are involved in *HPM* and *VPM* to ensure the key sensitivity of the proposed cipher and to preserve its confidentiality.

Step 3: The simultaneous permutation and diffusion operation

3.1 Set $j = 1$

3.2 Iterate the modified Logistic map [47], given in *Eq.*2, t_j times using the initial parameter y_j. These parameters are calculated according to *Eq.*5 and *Eq.*6, respectively.

$$y_j = (y_0 + \frac{cs_j}{255}) \bmod 1 \tag{5}$$

$$t_j = t_0 + cs_j \tag{6}$$

where y_0, t_0 and cs_1 are initial seeds and they are part of the secret key while the value of S_j is determined at each step according to *Eq.*7

$$S_j = \begin{cases} 0 & if\ j = 1 \\ MN & if\ j = 2 \\ S_{j-1} - 1 & otherwise \end{cases} \tag{7}$$

Alternatively, S_j can be calculated according to Eq.8

$$S_j = (MN - j + 2) \bmod (MN + 1) \tag{8}$$

*Eq.*5 and *Eq.*6 state that both the initial value and the number of iterations of the employed map at each step of the encryption are not fixed and severely correlated to the previous cipher pixel along with the secret parameters. In particular, employing the traits of the cipher-image generates a distinct key-stream and can be exploited to produce a dynamical pixel order for each different image while the utilization of secret parameters maintains the secrecy.

3.3 Calculate the parameter n_j to determine the index of the processed pixel (the processed pixel is the selected pixel at each step to be substituted and then scrambled with another pixel of the image) according to *Eq.*9

$$n_j = \left\lceil y_{t_j} \times 10^{14} \right\rceil \bmod S_{j+1} + 1 \tag{9}$$

*Eq.*9 chaotically generates a dynamical order model by which the pixels are encrypted and permuted. Specifically, *Eq.*9 generates a random value n_j ranging from 1 to MN to randomly select a pixel from the plain-image.

3.4 Compute the key-stream item associated to the processed pixel according to *Eq.*10

$$\phi_j = \left\lceil y_{t_j} \times 10^{14} \right\rceil \bmod 256 \tag{10}$$

3.5 Encrypt the n_j^{th} pixel of the image according to *Eq.*11

$$c_{n_j} = (c_{n_j} + \phi_j) \bmod 256 \oplus cs_j \tag{11}$$

where cs_j is the previous swapped-encrypted pixel.

3.6 Swap the encrypted pixel c_{n_j} and cs_{j+1} pixel according to *Eq.*12

$$\text{Temp} = c_{n_j}, \quad c_{n_j} = cs_{j+1} \text{and } cs_{j+1} = \text{Temp} \tag{12}$$

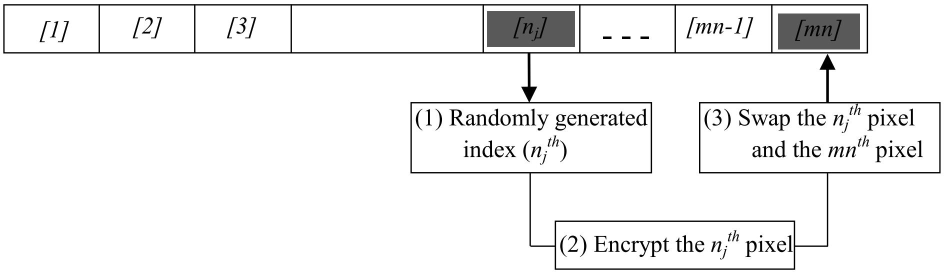

[1]
[2]
[3]
[n_j]
- - -
[mn-1]
[mn]
(1) Randomly generated index (n_j^{th})
(3) Swap the n_j^{th} pixel and the mn^{th} pixel
(2) Encrypt the n_j^{th} pixel

FIGURE 5. The depiction of the proposed simultaneous permutation and diffusion.

It is noted that the *steps* 3.5 and 3.6 simultaneously perform diffusion and permutation on the current processed pixel. In addition, *Eq.*7/*Eq.*8 and *Eq.*9 enable the cipher to randomly choose one of the non-encrypted pixels of the image at each step of the algorithm. The core idea of the proposed scheme is illustrated in Figure 5.

3.7 Set $j = j + 1$ and repeat the steps from 3.2 to 3.6 until all image pixels are treated.

On the other hand, according to the symmetric nature of the proposed cipher, the decryption procedure can correctly restore the plain-image by reversing the order of the steps of the encryption operation using the same secret key.

Further, from the cryptography point of view, the proposed cryptosystem exhibits several desirable properties, which include the following:

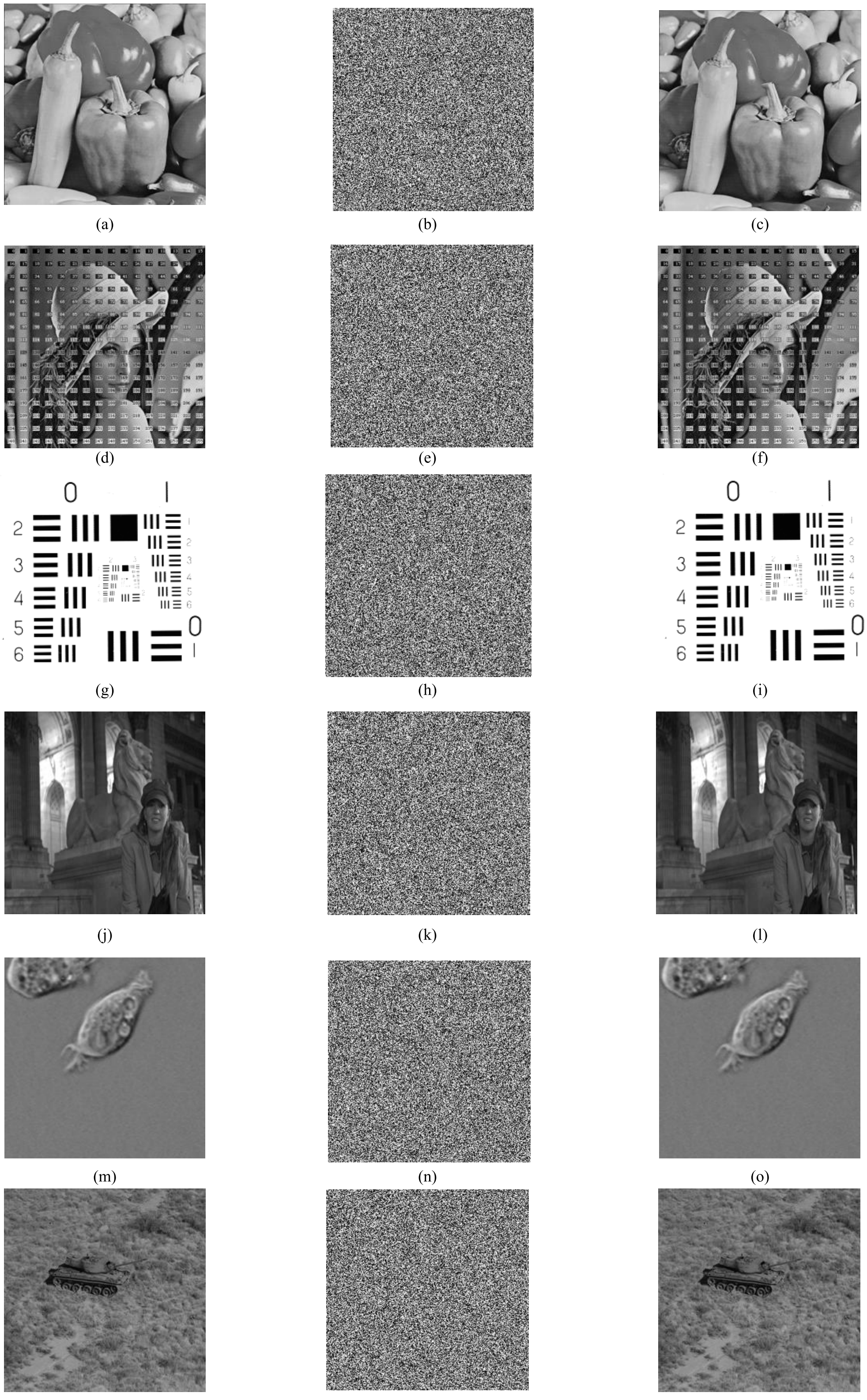
1. The substitution and permutation on image pixels are executed in a dynamic order fashion which is chaotically generated based on image information and secret key. Specifically, with only two iterations, the proposed scheme can generate two totally random indices, at each step, that invoke a dynamic order mechanism to the simultaneous permutation and diffusion operation. Accordingly, an adversary cannot mount any type of attacks.
2. For each pixel encryption, the parameter S_j (defined in Eq. 7) is always changed and decreased by one to control the swapping (permutation) process. Thus, there is a guarantee that each pixel will be swapped to location that cannot be assigned to another different pixel. In other words, a different pixel will be transmitted at each step even if the same index value is generated, namely, the permutation mapping is reversible.
3. The substitution and permutation are related and simultaneously applied, thus, the divide and conquer technique to attack the proposed scheme cannot be applied and the scheme is strongly secure.
4. The horizontal and vertical diffusion make each pixel strongly affected by all pixels preceding and following it, respectively. Accordingly, the suggested cipher is highly sensitive to tiny changes of the plain-image. Moreover, both *HPM* and *VPM* are key dependent which ensures the strong sensibility of the proposed cryptosystem to small variance in the secret key.
5. In addition, the suggested scheme takes into account the dynamic degradation problems [53] associated with chaotic systems. In general, the solutions of these problems include the use of high precision implementation of parameters, time–varied chaos systems, and cascade several chaos systems [53], [54]. Specifically, the developed scheme employs the following strategies: The high precision is represented by applying 10^{-15} decimal precision (64 bits) for chaos parameters. The time–varied chaos systems are accomplished through generating distinct initial values for the employed map, at each step of the encryption, based on the plain–image pixels. Indeed, the utilization of plain-image information by the modified Logistic map enforces the system to be of a time–varied behavior at each pixel which in turn results in cascading the map $N \times M$ times. Further, the adaptable parameters of the map can extend the cycle length of the generated sequences.
6. The initial parameters of the employed chaotic map, for each pixel encryption, are dynamically adapted based on the cipher-image information, which in turn guarantees that a distinct key-stream and a different permutation sequence are generated for each distinct image.

IV. EXPERIMENTAL RESULTS

This section displays the simulation results and security analysis for the suggested cipher to demonstrate its validity and effectiveness. Several standard images are tested and as expected, we found that the simulation results over each tested image reflect the same conclusion; therefore, the results and analysis of only six gray-scale plain-images (Pepper, TestPat, Res-chart, Mandi, Cell, and Tank shown in the first column of Figure 6) are depicted below. Also, the conducted experiments numerically compare the proposed cipher with a group of related schemes presented in Zhu [21], Norouzi *et al.* [26], Zhang and Wang [31], Wang *et al.* [32], Yuan *et al.* [33], Chen *et al.* [41] and Wang *et al.* [52].

A. EVALUATION OF SCHEME EFFECTIVENESS

To validate the encryption capability of the suggested cipher, each test image of the set of images shown in the first column



(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

(j) (k) (l)

(m) (n) (o)

(p) (q) (r)

FIGURE 6. Encryption and decryption of the proposed image cipher. a) Pepper plain-image. b) Pepper cipher-image. c) Pepper recovered image. d) TestPat plain-image. e) TestPat cipher-image. f) TestPat recovered image. g) Res-chart plain-image. h) Res-chart cipher-image. i) Res-chart recovered image. j) Mandi plain-image. k) Mandi cipher-image. l) Mandi recovered image. m) Cell plain-image. n) Cell cipher-image. o) Cell recovered image. p) Tank plain-image. q) Tank cipher-image. r) Tank recovered image.

TABLE 1. Numerical results based on *MSE* criterion.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	8099	8077.8	8088.8	8113.7	8098.0	8041.4	8085.9	8157.1
TestPat	8917.8	8888.3	8957.5	8945	8878.4	8892.6	8958.7	8976.4
Res-chart	20878	20857	20853	20937	20773	20884	20959	21021
Mandi	10263	10252	10275	10304	10315	10240	10226	10330
Cell	5723	5736.3	5767.8	5696.3	5726.9	5747.2	5754.6	5776.2
Tank	6380.6	6421	6352.6	6391.5	6371.9	6367.6	6406.4	6397.5
Average	10043.6	10038.7	10049.1	10064.5	10027.2	10028.8	10065.1	10109.7

TABLE 2. Numerical results based on *PSNR* criterion.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	9.0465	9.0579	9.0520	9.0386	9.047	9.0775	9.0535	9.0155
TestPat	8.6282	8.6426	8.6089	8.6150	8.6475	8.6405	8.6084	8.5998
Res-chart	4.9339	4.9382	4.9391	4.9216	4.9558	4.9327	4.9171	4.9042
Mandi	8.0183	8.0227	8.0129	8.0007	7.996	8.0278	8.0336	7.9899
Cell	10.5545	10.5445	10.5207	10.5749	10.5516	10.5362	10.5307	10.5144
Tank	10.0822	10.0548	10.1013	10.0748	10.0881	10.091	10.0647	10.0707
Average	8.5439	8.5435	8.5392	8.5376	8.5477	8.5510	8.5347	8.5158

of Figure 6 is enciphered using the suggested scheme and the results are displayed in the second column of Figure 6. These results point out that the cipher-images have a noise-like appearance and visually cannot leak any information about the corresponding plain-images. Thus, the proposed scheme has a robust encryption effect in hiding all details of the original images. Further, the recovered images by decrypting the encrypted images using the correct secret key are shown in the third column of Figure 6, which are entirely identical to the corresponding related plain-images. Accordingly, the obtained results confirm the effectiveness and feasibility of the suggested cryptosystem.

Furthermore, to measure the encryption degree of the proposed cipher, the mean square error (*MSE*), peak signal-to-noise ratio (*PSNR*), structural similarity index metric (*SSIM*), and correlation coefficient (*CC*) between the plain-images and the corresponding cipher-images are evaluated. Mathematically, the *MSE*, *PSNR*, *SSIM* and *CC* are respectively defined by *Eq.*13, *Eq.*14, *Eq.*15 and *Eq.*16 as depicted in [42], [44], [55], and [56].

$$MSE = \frac{1}{mn}\sum_{r=1}^{m}\sum_{s=1}^{n}(P(r,s)-C(r,s))^2 \tag{13}$$

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{14}$$

$$SSIM = \frac{(2\mu_P\mu_C+\varepsilon_1)(2\sigma_{PC}+\varepsilon_2)}{(\mu_P^2+\mu_C^2+\varepsilon_1)(\sigma_P^2+\sigma_C^2+\varepsilon_2)} \tag{15}$$

where μ_P and μ_C are the mean for the images P and C, respectively. σ_P^2, σ_C^2 and σ_{PC} represent the variance of P, the variance of C, and the covariance between P and C, respectively. While ε_1 and ε_2 denote two predefined quantities.

$$CC = \frac{E(z-E(z))(w-E(w))}{\sqrt{D(z)}\sqrt{D(w)}} \tag{16}$$

where

$$E(z) = \frac{1}{N}\sum_{i=1}^{N} z_i, \quad D(z) = \frac{1}{N}\sum_{i=1}^{N}(z_i - E(z))^2 \tag{17}$$

Accordingly, the values of *MSE, PSNR, SSIM* and *CC* are calculated and compared for the proposed scheme, Zhu [21], Norouzi *et al.* [26], Zhang and Wang [31], Wang *et al.* [32], Yuan *et al.* [33], Chen *et al.* [41] and Wang *et al.* [52] ciphers. The underlying results related to each criterion are displayed in Table 1, Table 2, Table 3, and Table 4, respectively. It is noted that the proposed cipher produces the largest average value of *MSE* and the smallest average value of *PSNR*, *SSIM*, and *CC*, which demonstrate its superior quality compared to the related ciphers presented in [21], [26], [31]–[33], [41], and [52].

B. SECURITY ANALYSIS

To assess the performance and security of the suggested cipher, numerous experiments are conducted on the set of plain-images shown in Figure 6. These tests include a differential attack analysis, statistical analysis tests (by performing a histogram analysis and adjacent pixels correlation analysis), and sensibility tests regarding slight changes of secret key.

TABLE 3. Numerical results based on *SSIM* criterion.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	0.00900	0.00980	0.0075	0.0071	0.00930	0.01460	0.0075	0.00370
TestPat	0.01140	0.00960	0.0082	0.0077	0.01160	0.01220	0.0018	0.00670
Res-chart	0.00320	0.000540	0.0026	0.0012	0.00061	0.00120	0.0063	0.00051
Mandi	0.00710	0.00730	0.0022	0.0035	0.00240	0.00470	0.0050	0.00100
Cell	0.01140	0.01160	0.0093	0.0114	0.01070	0.00860	0.0093	0.00910
Tank	0.00770	0.00740	0.0121	0.0109	0.00850	0.00910	0.0072	0.00920
Average	0.0083	0.007707	0.007	0.0070	0.00719	0.0084	0.0062	0.00504

TABLE 4. Numerical results based on *CC* criterion.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	0.00190	0.00280	0.0035	0.0010	0.00230	0.00800	0.0038	0.00170
TestPat	0.0050	0.00300	0.0015	0.0096	0.00510	0.00580	0.0053	0.00046
Res-chart	0.00150	0.00460	0.0021	0.0054	0.00190	0.00380	0.0045	0.00180
Mandi	0.00750	0.00770	0.0082	0.0040	0.00540	0.00260	0.0021	0.00720
Cell	0.0038	0.00390	0.0026	0.0031	0.00120	0.00440	0.0026	0.00310
Tank	0.0033	0.00380	0.0046	0.0025	0.00190	0.00087	0.0042	0.00050
Average	0.00383	0.00430	0.00380	0.00430	0.00297	0.00425	0.00380	0.00246

TABLE 5. The *NPCR, UACI* and *CC* for plain-image sensitivity of the proposed scheme.

Image	Plain-image sensitivity criteria		
	NPCR (%)	UACI (%)	CC
Pepper	99.6429	33.5182	0.00092
TestPat	99.6201	33.5112	0.00050
Res-chart	99.6094	33.5017	0.00070
Mandi	99.6109	33.5204	0.0026
Cell	99.6567	33.5785	0.00085
Tank	99.6658	33.5342	0.00082
Average	99.6343	33.5274	0.00106

1) DIFFERENTIAL ATTACK ANALYSIS

To prevent the differential attacks, any trivial amendment in the original image (even one bit) must yield a substantial difference in the enciphered images. Three measures can be utilized for quantitatively evaluating this capability: Number of Pixel Change Ratio *(NPCR)*, Unified Average Change in Intensity *(UACI)*, and correlation coefficient (*CC*) [26], [41], [42]. Mathematically, *NPCR*, and *UACI* are defined in *Eq.*18 and *Eq.*20. The experiment in this test starts by encrypting a plain-image P_1 by the proposed cipher to obtain the corresponding cipher-image C_1. Then, another cipher-image C_2 is obtained by encrypting a trivially modified plain-image P_2 which differs in only one bit from P_1. After that, the *NPCR, UACI*, and *CC* criteria are applied to evaluate the difference between C_1 and C_2. The underlying results are depicted in Table 5. It is obvious that the *NPCR* and *UACI* values gained from the proposed scheme fall within the optimal bounds (99.60 and 33.46 for *NPCR* and *UACI*, respectively, as indicated in [57]). Accordingly, these values verify that the suggested cipher is intensely sensitive to such slight changes of the plain-image.

$$NPCR = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\% \tag{18}$$

$$D(i,j) = \begin{cases} 0 & if\ C_1(i,j) = C_2(i,j) \\ 1 & otherwise \end{cases} \tag{19}$$

$$UACI = \frac{1}{m \times n}\left(\sum_{i=1}^{m}\sum_{j=1}^{n}\left(\frac{|C_1(i,j) - C_2(i,j)|}{255}\right)\right) \times 100\% \tag{20}$$

2) KEY SPACE ANALYSIS

To hinder the exhaustive search attack, the key space of the ciphering approach must be reasonably large. The suggested cipher employs two chaos mappings for simultaneously permuting and masking the plain-image pixels. The secret key of the proposed cipher encompasses a set of ten secret parameters, namely, x_0, u_1, k_1, N_0, y_0, $u_2 \times k_2$, t_0, V_0, V'_0, *and* c_0. The proposed cipher employs a double-precision implementation that contains 10^{15} different combinations for each parameter. Thus, the key space of the suggested cipher can be reached to $2.2 \times 10^{73} > 2^{243}$, which is suitably large to thwart the exhaustive search with the current available technologies.

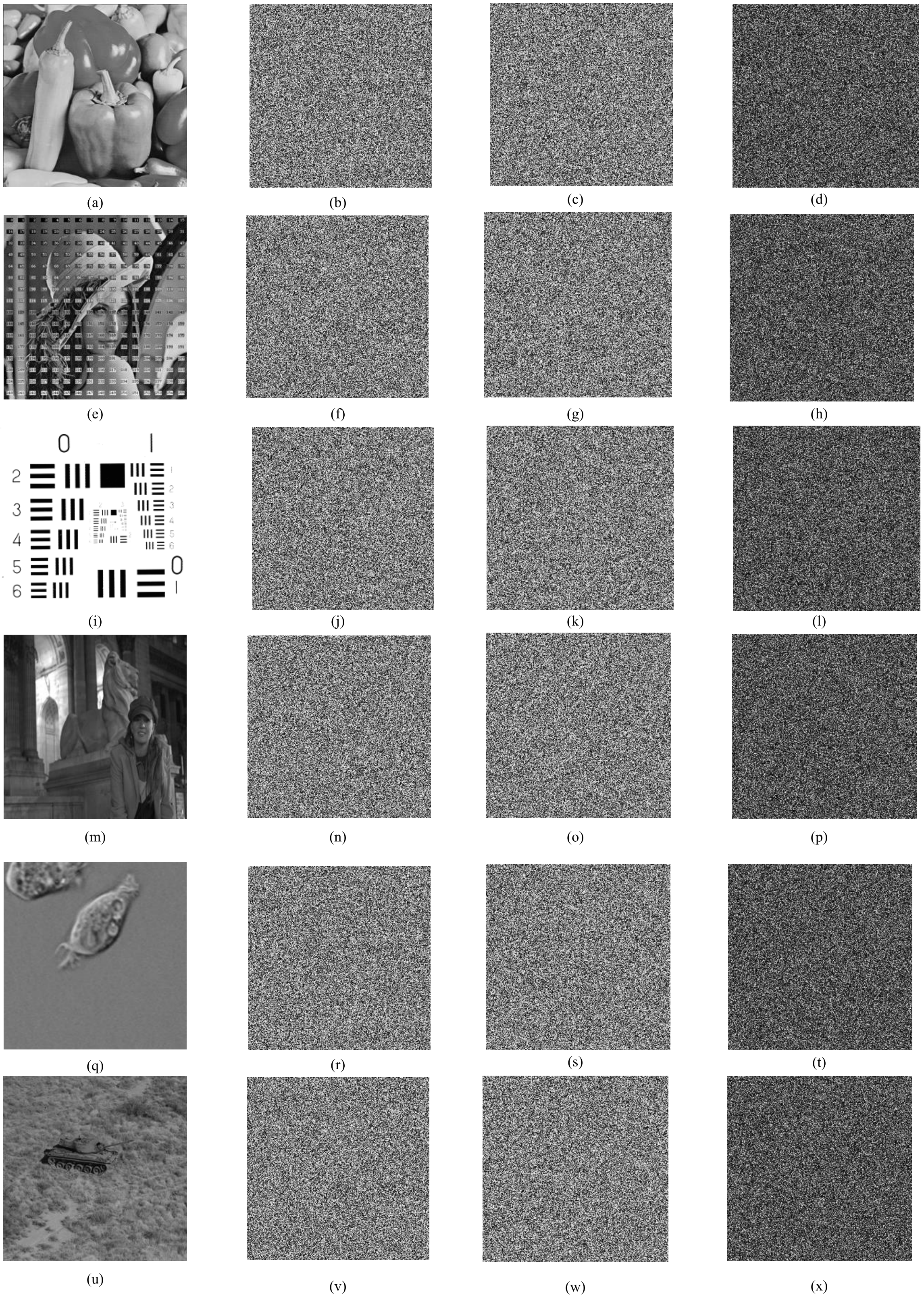


FIGURE 7. The results of key sensitivity for the proposed cryptosystem. a) Pepper plain-image. b) Pepper cipher-image: C_1. c) Pepper cipher-image: C_2. d) Difference of (b) and (c). e) TestPat plain-image. f) TestPat cipher-image: C_1. g) TestPat cipher-image: C_2. h) Difference of (f) and (g). i) Res-chart plain-image. j) Res-chart cipher-image: C_1. k) Res-chart cipher-image: C_2. l) Difference of (j) and (k). m) Mandi plain-image. n) Mandi cipher-image: C_1. o) Mandi cipher-image: C_2. p) Difference of (n) and (o). q) Cell plain-image. r) Cell cipher-image: C_1. s) Cell cipher-image: C_2. t) Difference of (r) and (s). u) Tank plain-image. v) Tank cipher-image: C_1. w) Tank cipher-image: C_2. x) Difference of (v) and (w).

TABLE 6. The key sensitivity results of the proposed method for parameters x_0 and u_1.

Image	x_0			u_1		
	NPCR	CC	UACI	NPCR	CC	UACI
Pepper	99.6384	0.00029	33.4707	99.6246	0.0012	33.5208
TestPat	99.6109	0.0029	33.497	99.6292	0.0065	33.651
Res-chart	99.6521	0.0014	33.5573	99.6353	0.0019	33.5193
Mandi	99.617	0.0035	33.6046	99.6201	0.0051	33.5704
Cell	99.617	0.0022	33.447	99.6216	0.0053	33.5774
Tank	99.6277	0.0042	33.5668	99.6155	0.00087	33.5323
Average	99.6272	0.00242	33.5239	99.6244	0.00348	33.5619

TABLE 7. The key sensitivity results of the proposed method for parameters y_0, K_2 and u_2.

Image	y_0			K_2			u_2		
	NPCR	CC	UACI	NPCR	CC	UACI	NPCR	CC	UACI
Pepper	99.6399	0.00031	33.4531	99.6033	0.0067	33.5957	99.6368	0.0019	33.5492
TestPat	99.6017	0.0028	33.5666	99.6475	0.0047	33.6467	99.6124	0.0013	33.525
Res-chart	99.6201	0.0025	33.5718	99.6307	0.0021	33.4935	99.6017	0.0012	33.5761
Mandi	99.6094	0.006	33.6569	99.6674	0.0062	33.5594	99.6185	0.0034	33.6032
Cell	99.646	0.0042	33.5896	99.6094	0.0053	33.5808	99.6002	0.00019	33.4681
Tank	99.6094	0.0089	33.5893	99.6109	0.0023	33.4519	99.6262	0.006	33.6154
Average	99.6211	0.00412	33.5712	99.6282	0.0046	33.5547	99.6160	0.00233	33.5562

3) KEY SENSITIVITY TEST

A robust image cipher must be substantially sensitive to slight changes in the encryption keys. Any secure encryption algorithm must produce completely different cipher-images for a single bit variation in the encryption keys. To estimate the key sensibility, a set of initial seeds and control parameters of the used chaos maps are chosen. After this, the plain-image P is encrypted using these values to get the enciphered image C_1. Then, a tiny change (Δ) is made to any of the secret key parameters and the image P is enciphered again to obtain another cipher-image C_2. Now, to analytically demonstrate the key sensitivity of the proposed cipher, the *NPCR, CC,* and*UACI* criteria are employed to calculate the difference between the two encrypted images C_1 and C_2. The sensitivity results of key parameters are shown in Figure 7 and the numerical computations are listed in Table 6 and Table 7, which demonstrate the strong key sensitivity of the suggested cipher.

4) STATISTICAL ANALYSIS

To reveal the robustness of the suggested cipher against statistical attack, adjacent pixels correlation analysis and histogram analysis are executed.

a: ADJACENT PIXELS CORRELATION ANALYSIS

An effective encryption scheme must eliminate/reduce the strong relation between adjacent pixels in the enciphered image. The correlations between two horizontally, vertically, and diagonally adjacent pixels in the enciphered images shown in Figure 6 have been examined and compared with the schemes presented in [21], [26], [31]–[33], [41], and [52].

The results illustrated in Tables 8, 9 and 10 reveal that all obtained values of correlation tend to zero. In addition, the distributions of two horizontally adjacent pixels for the plain-images and the cipher-images related to our scheme are plotted in Figure 8. From these computational results, we found that the proposed cipher yields the smallest average correlation value between the neighboring pixels of the encrypted images, which is a good indicator for the superior performance of the suggested cipher against statistical attack compared with all related cipher schemes.

b: HISTOGRAM ANALYSIS

An image histogram shows the values distribution of an image. The histogram for the plain-images and the associated ciphered ones are illustrated in Figure 9.

TABLE 8. Correlation coefficients of two horizontally adjacent pixels in encrypted images.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	0.0147	0.0227	0.0119	0.0077	0.0281	0.0013	0.0221	0.0076
TestPat	0.0033	0.0216	0.0120	0.0011	0.0094	0.0052	0.0015	0.0062
Res-chart	0.0086	0.015	0.0165	0.0020	0.0277	0.0151	0.0119	0.0025
Mandi	0.0012	0.0197	0.0116	0.0017	0.0029	0.0062	0.0089	0.0047
Cell	0.0258	0.0093	0.0154	0.0187	0.0382	0.0039	0.0147	0.0099
Tank	0.0098	0.0315	0.0090	0.0023	0.0176	0.0041	0.0095	0.0017
Average	0.0106	0.0200	0.0127	0.0056	0.0207	0.0060	0.0114	0.0054

TABLE 9. Correlation coefficients of two vertically adjacent pixels in encrypted images.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	0.0049	0.0166	0.0083	0.0139	0.0077	0.0242	0.0067	0.0117
TestPat	0.0221	0.0208	0.0197	0.0035	0.0297	0.0066	0.0115	0.0095
Res-chart	0.0099	0.0039	0.0122	0.0092	0.0020	0.0226	0.0075	0.0054
Mandi	0.0137	0.0167	0.0055	0.0083	0.0048	0.0084	0.0097	0.0228
Cell	0.0031	0.0123	0.0031	0.0062	0.0046	0.0051	0.0087	0.0069
Tank	0.0031	0.013	0.0088	0.0077	0.0225	0.0086	0.0178	0.00027
Average	0.0095	0.0139	0.0096	0.0081	0.0119	0.0126	0.0103	0.00943

TABLE 10. Correlation coefficients of two diagonally adjacent pixels in encrypted images.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	0.0057	0.0343	0.0039	0.0179	0.0158	0.0123	0.0028	0.0035
TestPat	0.0229	0.0144	0.0210	0.0076	0.0212	0.0019	0.0174	0.0066
Res-chart	0.0048	0.0107	0.0082	0.0290	0.0132	0.0148	0.0091	0.0016
Mandi	0.0060	0.0291	0.0132	0.0033	0.0166	0.0149	0.0387	0.0211
Cell	0.0208	0.0048	0.0015	0.0105	0.0097	0.0119	0.0063	0.0124
Tank	0.0069	0.0028	0.0092	0.0067	0.0025	0.0026	0.0165	0.006
Average	0.0112	0.0160	0.0095	0.0125	0.0132	0.0097	0.0151	0.0085

Obviously, the histogram for the enciphered images is closely uniform distributed and remarkably varies from that of the plain-images. Accordingly, no information about the plain-images can be extracted from their encryption, which in turn, makes the statistical attack entirely infeasible.

Further, to numerically confirm the uniformity of the cipher-image histogram, the histogram variance (*HV*) [58] is mathematically evaluated according to *Eq.* 21. Table 11 summaries the results associated to each cipher-image produced by the suggested cipher, Zhu [21], Norouzi *et al.* [26], Zhang and Wang [31], Wang *et al.* [32], Yuan *et al.* [33], Chen *et al.* [41] and Wang *et al.* [52] ciphers. The evaluated values of *HV* demonstrate the uniformity of the enciphered images obtained by the suggested cryptosystem.

Moreover, the *HV* analysis indicates that our approach is more secure than the underlying ciphers presented in [21], [26], [31]–[33], [41], and [52] because it yields the smallest average variance value.

$$HV(R) = \frac{1}{H^2}\sum_{s=0}^{H-1}\sum_{t=0}^{H-1}\frac{1}{2}(r_s - r_t)^2 \qquad (21)$$

where $R = r_s$, $s = 0, 1, \ldots, H-1$, and r_s is the number of image pixels with value s.

5) RESISTANCE AGAINST CHOSEN PLAINTEXT/CIPHERTEXT ATTACK

The suggested cipher concurrently employs the permutation and diffusion operations. Further, the values of image pixels are processed in a dynamic order. That is, the proposed cipher generates a random sequence of indices that indicates the order in which the pixels are simultaneously diffused and permuted. By this way, the attacker cannot split the proposed architecture into two separate phases. Moreover, the diffusion and permutation parameters are chaotically generated based

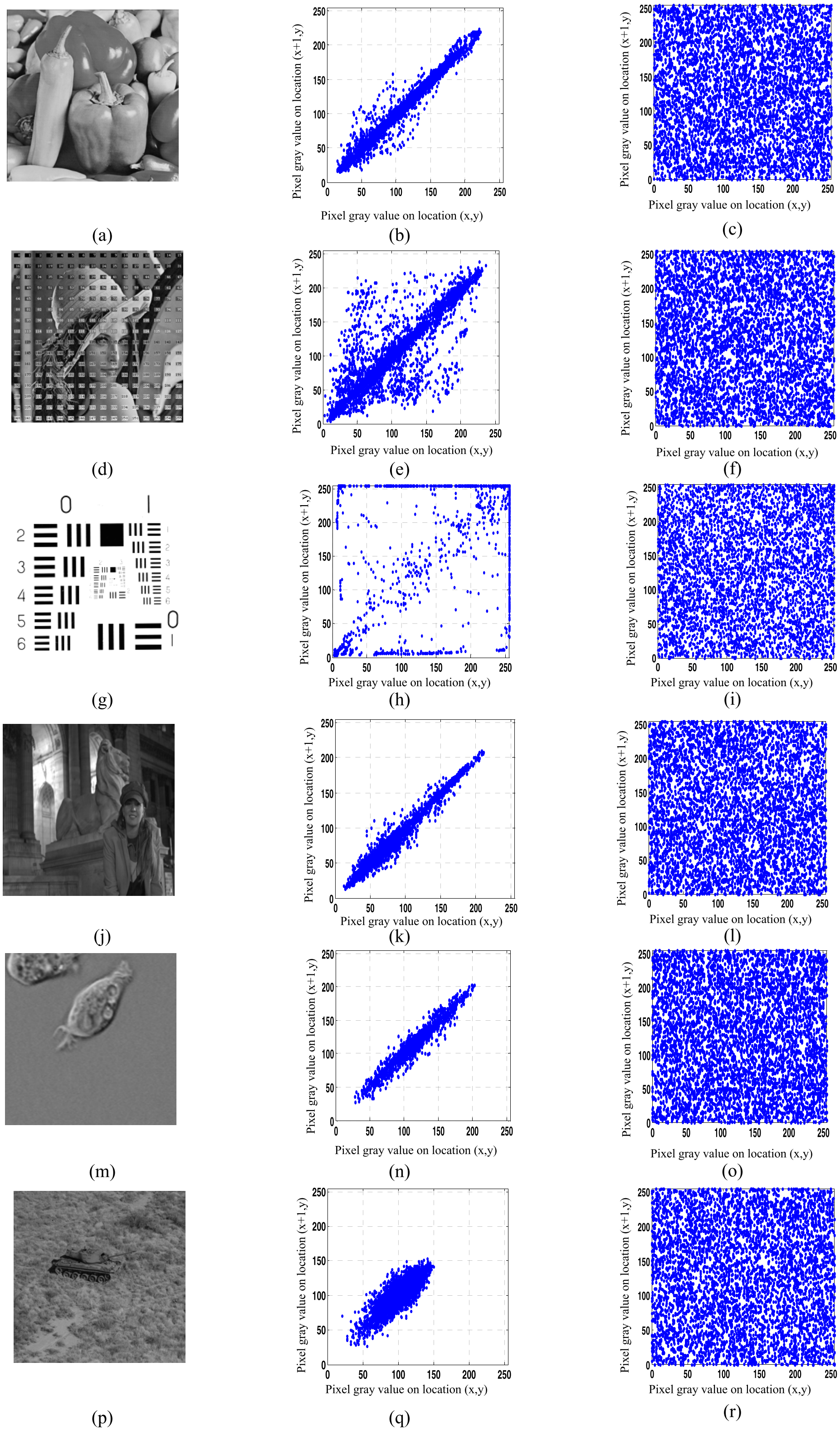


FIGURE 8. Adjacent pixels correlation analysis of the proposed image cipher. a) Pepper plain-image. b) Distribution of Pepper plain-image. c) Distribution of Pepper cipher-image. d) TestPat plain-image. e) Distribution of TestPat plain-image. f) Distribution of TestPat cipher-image. g) Res-chart plain-image. h) Distribution of Res-chart plain-image. i) Distribution of Res-chart cipher-image. j) Mandi plain-image. k) Distribution of Mandi plain-image. l) Distribution of Mandi cipher-image. m) Cell plain-image. n) Distribution of Cell plain-image. o) Distribution of Cell cipher-image. p) Tank plain-image. q) Distribution of Tank plain-image. r) Distribution of Tank cipher-image.

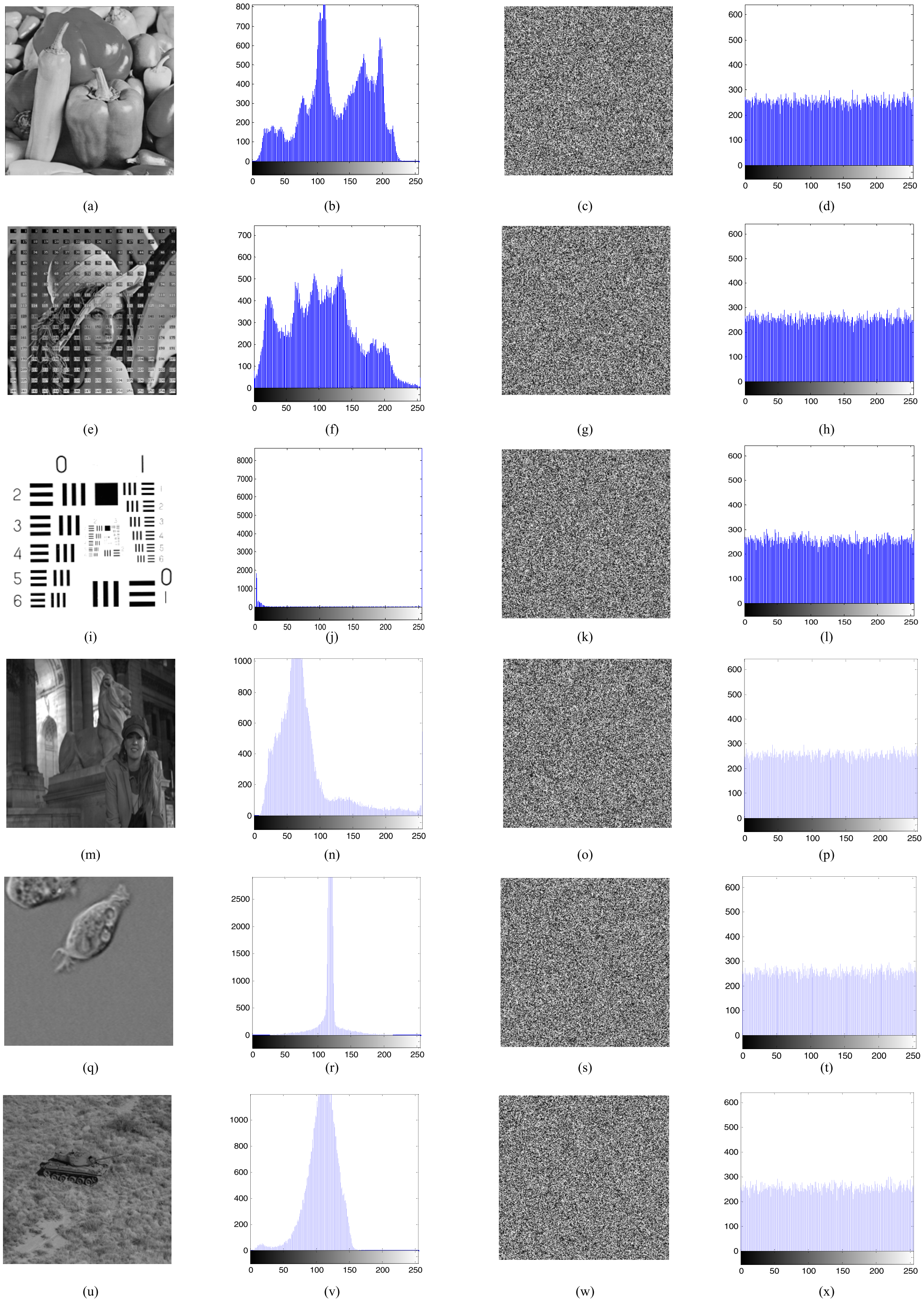


FIGURE 9. Histogram analysis of the proposed image cipher. a) Pepper plain-image. b) Pepper plain-image histogram. c) Pepper cipher-image. d) Pepper cipher-image histogram. e) TestPat plain-image. f) TestPat plain-image histogram. g) TestPat cipher-image. h) TestPat cipher-image histogram. i) Res-chart plain-image. j) Res-chart plain-image histogram. k) Res-chart cipher-image. l) Res-chart cipher-image histogram. m) Mandi plain-image. n) Mandi plain-image histogram. o) Mandi cipher-image. p) Mandi cipher-image histogram. q) Cell plain-image. r) Cell plain-image histogram. s) Cell cipher-image. t) Cell cipher-image histogram. u) Tank plain-image. v) Tank plain-image histogram. w) Tank cipher-image. x) Tank cipher-image histogram.

TABLE 11. Results related to HV of the cipher-images.

Image	Ref.[21]	Ref.[26]	Ref.[31]	Ref.[32]	Ref.[33]	Ref.[41]	Ref.[52]	Proposed cipher
Pepper	225	267	240	242	268	295	210	198
TestPat	249	261	261	268	276	242	254	241
Res-chart	237	250	271	278	245	265	348	242
Mandi	229	251	221	252	246	266	301	204
Cell	277	234	245	253	291	235	247	207
Tank	247	240	209	243	281	231	271	245
Average	244	250.50	241.17	256	267.83	255.67	271.83	222.83

on plain-image information, which in turn guarantees that slightly different plain-images will have distinct diffusion and permutation sequences. In other words, even if the attacker selects some specific images and computes the diffusion and permutation sequences, he cannot break the proposed scheme since the obtained sequence is related only to those chosen images and be totally different from that associated to other different images. Accordingly, even if the suggested cipher employs simple primitive operations (Xor and addition) it can successfully thwart different attacks including the most powerful chosen plaintext/ciphertext attack.

TABLE 12. The difference between the generated key streams DK_1 and DK_2.

Image	Generated key difference		
	NPCR (%)	UACI (%)	CC
Pepper	99.2843	33.9564	0.00061
TestPat	99.2505	33.9850	0.00044
Res-chart	99.2271	33.8242	0.00260
Mandi	99.2150	33.9835	0.00770
Cell	99.2427	33.9262	0.00380
Tank	99.2261	33.8809	0.00030
Average	99.2410	33.9260	0.00258

To demonstrate this feature, an experiment is conducted to estimate the difference between the two diffusion key streams associated with two plain-images that are varied in only one bit. Specifically, each plain-image P in Figure 6 is firstly encrypted by the suggested cipher and the related diffusion key-stream DK_1 is recorded. Secondly, a tiny modified image p' is obtained by changing only one bit of the image P and then encrypted by the same secret key. The key-stream DK_2 associated to the image P' is stored. Finally, the difference between the two key-streams DK_1 and DK_2 is evaluated in terms of *NPCR, UACI* and *CC* as presented in Table 12. Accordingly, the obtained results ensure that the key-streams generated for two slightly different images are completely distinct and be dependent on the input plain-image. Further, another experiment with the same methodology is performed to measure the difference between two permutation sequences (PS_1 and PS_2) generated for the same images P and P'. The values obtained from this experiment presented in Table 13 draw the same conclusion about the permutation sequences.

TABLE 13. The difference between the generated permutation sequences PS_1 and PS_2.

Image	Generated key difference		
	NPCR (%)	UACI (%)	CC
Pepper	99.9928	33.3781	0.0017
TestPat	99.9919	33.4840	0.0069
Res-chart	99.9909	33.4352	0.0048
Mandi	99.9911	33.4150	0.0044
Cell	99.9975	33.4263	0.0038
Tank	99.9936	33.4504	0.0042
Average	99.9930	33.4315	0.0043

V. CONCLUSION

This paper suggested an effective image cipher based on simultaneous permutation and diffusion operations. These operations handled the pixels in a dynamic order, which is chaotically produced based on image information. The proposed technique employed the Chebyshev-Chebyshev chaotic map and the modified Logistic chaotic map with dynamic control parameters to implement this structure. Simulation results and security analysis proved that the suggested cipher has several brilliant features and good performance against different types of attacks. Thus, the proposed cryptosystem is strongly appropriate for practical image security applications.

REFERENCES

[1] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Process., Image Commun.*, vol. 41, pp. 144–157, Feb. 2016.

[2] B. Wang, Y. Xie, C. Zhou, S. Zhou, and X. Zheng, "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps," *Opt.-Int. J. Light Electron Opt.*, vol. 127, no. 7, pp. 3541–3545, 2016.

[3] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.

[4] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 8, no. 6, pp. 1259–1284, 1998.

[5] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[6] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos, Solitons Fractals*, vol. 26, no. 1, pp. 117–129, 2005.

[7] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcation Chaos*, vol. 14, no. 10, pp. 3613–3624, Oct. 2004.

[8] K.-W. Wong, B. S.-H. Kwok, and W.-S. Law, "A fast image encryption scheme based on chaotic standard map," *Phys. Lett. A*, vol. 372, no. 15, pp. 2645–2652, 2008.

[9] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," *Appl. Soft Comput.*, vol. 11, no. 1, pp. 514–522, 2011.

[10] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394–400, 2008.

[11] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 38, pp. 5973–5978, 2008.

[12] F.-G. Jeng, W.-L. Huang, and T.-H. Chen, "Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes," *Signal Process., Image Commun.*, vol. 34, pp. 45–51, May 2015.

[13] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 7, pp. 3056–3075, 2009.

[14] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.

[15] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, 2010.

[16] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, 2011.

[17] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism," *Opt. Commun.*, vol. 284, no. 22, pp. 5290–5298, 2011.

[18] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.

[19] C. Li, L. Y. Zhang, R. Ou, K.-W. Wong, and S. Shu, "Breaking a novel colour image encryption algorithm based on chaos," *Nonlinear Dyn.*, vol. 70, no. 4, pp. 2383–2388, 2012.

[20] G. Tu, X. Liao, and T. Xiang, "Cryptanalysis of a color image encryption algorithm based on chaos," *Opt.-Int. J. Light Electron Opt.*, vol. 124, no. 22, pp. 5411–5415, 2013.

[21] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, 2012.

[22] F. Özkaynak, A. B. Özer, and S. Yavuz, "Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 24, pp. 4946–4948, 2012.

[23] C. Li, Y. Liu, T. Xie, and M. Z. Q. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," *Nonlinear Dyn.*, vol. 73, no. 3, pp. 2083–2089, 2013.

[24] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Process.*, vol. 93, no. 11, pp. 3039–3052, 2013.

[25] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 11, pp. 3075–3085, 2013.

[26] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools Appl.*, vol. 71, no. 3, pp. 1469–1497, 2014.

[27] Y. Zhang, D. Xiao, W. Wen, and M. Li, "Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Nonlinear Dyn.*, vol. 76, no. 3, pp. 1645–1650, 2014.

[28] H. Diab and A. M. El-Semary, "Secure image cryptosystem with unique key streams via hyper-chaotic system," *Signal Process.*, vol. 142, pp. 53–68, Jan. 2018.

[29] J.-X. Chen, Z.-L. Zhu, C. Fu, and H. Yu, "A fast image encryption scheme with a novel pixel swapping-based confusion approach," *Nonlinear Dyn.*, vol. 77, no. 4, pp. 1191–1207, 2014.

[30] J. S. A. E. Fouda, J. Y. Effa, S. L. Sabat, and M. Ali, "A fast chaotic block cipher for image encryption," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 3, pp. 578–588, 2014.

[31] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft. Comput.*, vol. 26, pp. 10–20, Jan. 2015.

[32] X.-Y. Wang, S.-X. Gu, and Y.-Q. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Opt. Lasers Eng.*, vol. 68, pp. 126–134, May 2015.

[33] H.-M. Yuan, Y. Liu, L.-H. Gong, and J. Wang, "A new image cryptosystem based on 2D hyper-chaotic system," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8087–8108, 2017.

[34] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.

[35] X.-Y. Wang, Y.-Q. Zhang, and L.-T. Liu, "An enhanced sub-image encryption method," *Opt. Lasers Eng.*, vol. 86, pp. 248–254, Nov. 2016.

[36] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

[37] L. Wang, H. Song, and P. Liu, "A novel hybrid color image encryption algorithm using two complex chaotic systems," *Opt. Lasers Eng.*, vol. 77, pp. 118–125, Feb. 2016.

[38] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, 2014.

[39] S. Dhall, S. K. Pal, and K. Sharma, "Cryptanalysis of image encryption scheme based on a new 1D chaotic system," *Signal Process.*, vol. 146, pp. 22–32, May 2018.

[40] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. A. Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Process.*, vol. 109, pp. 119–131, Apr. 2015.

[41] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, and Y. Zhang, "Reusing the permutation matrix dynamically for efficient image cryptographic algorithm," *Signal Process.*, vol. 111, pp. 294–307, Jun. 2015.

[42] H. Diab and A. M. El-Semary, "Cryptanalysis and improvement of the image cryptosystem reusing permutation matrix dynamically," *Signal Process.*, vol. 148, pp. 172–192, Jul. 2018.

[43] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[44] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 138, pp. 129–137, Sep. 2017.

[45] H. Wang, D. Xiao, X. Chen, and H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Process.*, vol. 144, pp. 444–452, Mar. 2018.

[46] D. Zhang and F. Zhang, "Chaotic encryption and decryption of JPEG image," *Opt.-Int. J. Light Electron Opt.*, vol. 125, no. 2, pp. 717–720, 2014.

[47] J. Xie, C. Yang, Q. Xie, and L. Tian, "An encryption algorithm based on transformed logistic map," in *Proc. Int. Conf. Netw. Secur., Wireless Commun. Trusted Comput.*, Apr. 2009, pp. 111–114.

[48] D. Ponnaian and K. Chandranbabu, "Crypt analysis of an image encryption algorithm and an enhanced scheme," *Opt.-Int. J. Light Electron Opt.*, vol. 127, no. 1, pp. 192–199, 2016.

[49] D. Ponnaian and K. Chandranbabu, "Security analysis of an image encryption algorithm based on paired interpermuting planes and a modified scheme," *Opt.-Int. J. Light Electron Opt.*, vol. 127, no. 19, pp. 8111–8123, 2016.

[50] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.

[51] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft. Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.

[52] 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.

[53] H. Hu, Y. Deng, and L. Liu, "Counteracting the dynamical degradation of digital chaos via hybrid control," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 6, pp. 1970–1984, 2014.

[54] L. Liu and S. Miao, "An image encryption algorithm based on Baker map with varying parameter," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16511–16527, 2017.

[55] Z. Wang and A. Bovik, *Modern Image Quality Assessment: Synthesis Lectures on Image, Video & Multimedia Processing*, 1st ed. San Rafael, CA, USA: Morgan & Claypool, 2006.

[56] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on dna sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput.*, vol. 37, pp. 24–39, Dec. 2015.

[57] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[58] Y.-Q. Zhang and X.-Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.

HOSSAM DIAB received the B.S., M.Sc., and Ph.D. degrees in computer science from the Faculty of Science, Menoufia University, Egypt, in 1999, 2004, and 2010, respectively. He is currently with the Computer Science and Engineering College, Taibah University, Saudi Arabia, as a Visitor. He is also an Assistant Professor with the Department of Mathematics and Computer Science, Faculty of Science, Menoufia University. His research interests are in the areas of cryptography, application of chaotic systems in multimedia content encryption, digital image processing, image compression, and image watermarking.