IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 19, 2020, accepted May 30, 2020, date of publication June 12, 2020, date of current version June 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3001949

Novel Image Encryption Using a Pseudoset Generated by Chaotic Permutation Multicircular Shrinking With a Gradual Deletion of the Input Set

KALAMULLAH RAMLI[1], (Member, IEEE), YOHAN SURYANTO[1], (Member, IEEE), MAGFIRAWATY[2], (Member, IEEE), AND NUR HAYATI[1,3] (Member, IEEE)

[1]Department of Electrical Engineering, Universitas Indonesia, Depok 16424, Indonesia
[2]Sekolah Tinggi Sandi Negara, Bogor 16120, Indonesia
[3]Faculty of Engineering, Universitas Muhammadiyah Yogyakarta, Bantul 55183, Indonesia

Corresponding author: Kalamullah Ramli (kalamullah.ramli@ui.ac.id)

This research was supported by Universitas Indonesia through Hibah Publikasi Terindeks Internasional (PUTI) Q1 Scheme under contract number NKB-1385/UN2.RST/HKP.05.00/2020.

ABSTRACT High-level security with a large keyspace and a short processing time is needed in digital image encryption. Generally, an encryption method that produces a large keyspace is characterized by a relatively slow encryption process. In this paper, we propose a new image encryption method that uses two chaotic pseudosets. A gradual deletion of the input set (GDIS) is introduced to enhance the process of chaotic permutation multicircular shrinking (CPMCS), herein referred to as GDIS CPMCS, to diffuse the image pixels and control the shift distance of the row and column rotations of an image. The proposed encryption scheme offers some advantages: it has a larger keyspace than the referenced image encryption schemes and a shorter processing time than CPMCS. The processing time of the proposed image encryption method with the GDIS CPMCS algorithm is 16.7 times faster for a gray image and 43 times faster for a color image than that in our previous work. Based on histogram and entropy analyses, the proposed scheme is also robust to statistical analysis. Moreover, the ciphered image has a very high degree of randomness according to the National Institute of Standards and Technology (NIST) randomness test results. In terms of differential analysis, a one-bit change in the original image leads to a substantial change in the ciphered image, as indicated by the unified average change intensity (UACI) and number of pixel change rate (NPCR) scores of 33.45% and 99.61%, respectively. Furthermore, GDIS CPMCS is robust to salt-and-pepper, Poisson, Gaussian, and speckle noise, with peak signal-to-noise ratios (PSNRs) higher than 14. The scheme is also robust to data loss since a reconstructed image with 50% data loss can be recognized, as indicated by a PSNR of 11.4.

INDEX TERMS Cryptography, fast image encryption, very large keyspace, chaotic permutation, robust to noise, multiple circular shrinking.

I. INTRODUCTION

In recent years, the Internet of Things (IoT) and machine to machine (M2M) technologies have been widely used by various groups [1], [2]. As predicted by Ericsson [3], in 2022, 18 billion of 29 billion devices connected to the internet will be devices related to the IoT, while the Statista Research Department [4] predicts that by 2025, the total number of devices connected to the IoT around the world will reach 75.44 billion. The number of interconnected devices has caused the corresponding data to rapidly increase in abundance and diversity, so big data technology plays an important role in each stage of data processing [5]. Other important concerns related to a large amount of data are security and privacy [6]. For example, in terms of security, privacy, and ownership, medical image data must be protected [7], [8].

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

Research on image encryption continues to enhance security in the form of robustness to attacks based on differential analysis, brute force and statistical analysis. A promising image encryption technique is chaotic-based encryption. Chaotic methods are nonlinear and have been extensively developed for a wide range of applications and problems, including applications to solve problems related to Pavlov associative memory [9], parameter synchronization problems in chaotic systems [10], and finite numbers of chaotic attractors, as mentioned in [11].

Wang *et al.* [12] proposed a chaotic algorithm using the perceptron model in a neural network method with the Lorenz system to encrypt images. However, Awad and Saadane [13] concluded that a chaotic map has limitations in discrete domains for image encryption, which is known as the discretization problem.

To improve resistance to brute force attacks, researchers have combined chaotic maps. However, there is a penalty to be considered: due to the increased number of iterations, the processing time tends to also increase.

To create a secure cipher image while maintaining a fast processing time, Tong [14] proposed combining topological conjugation with an Arnold cat map (ACM) block and a Henon chaotic map. Bigdeli *et al.* [15] applied a chaotic neural network (CNN) consisting of three neuron layers. Patidar *et al.* [16] used a pseudorandom scheme consisting of permutation and substitution processes using a chaotic standard map. Seyedzadeh *et al.* [17] proposed three encryption stages: diffusion using a chaotic quantum logistical map, scrambling the pixel arrangement using a two-dimensional chaotic map, and coupling the results of the first two stages with nearest-neighbor coupled-map lattices (CMLs). Wang and Gao [18] proposed a new Boolean network algorithm in image encryption by implementing the semitensor product of a matrix in the diffusion process. Wang *et al.* [19] used DNA operations with bitwise XOR and DNA encoding to produce a DNA matrix and then permute the matrix. However, the proposed methods produce a keyspace that is less than 256 bits, which does not meet the National Security Agency (NSA) criteria [20].

To develop an encryption image that has a high level of security with a large keyspace, Wang and Zhang [21] implemented an expanded XOR operation, heterogeneous permutation bits, and a chaotic WPLCW method. Hsiao and Lee [22] applied a chaotic method based on an amplitude phase frequency model (APFM). Wu *et al.* [23] applied a CML and a fractional-order chaotic system. Kanso and Ghebleh [24] implemented the 3 phases of a 3D chaotic map. Zhou *et al.* [25] used a combination of existing 1D chaotic maps for four-stage row substitution and ciphered image rotation. Wang *et al.* [26] employed a combination of permutation and parallel computing methods to diffuse an image. Zhang and Wang [27] utilized non-neighboring CMLs in the permutation of binary pixels. Wang *et al.* [28] encrypted an image by modifying the cat map through a nonstatic random expansion technique to permute the image and then diffused the result with the combination of one tent map and a logistic map. These encryption methods have a significant keyspace of greater than 256 bits, but the processing speed is relatively slow.

In this research, we seek to add robustness to noise as an image encryption feature. To satisfy this objective, Liu and Wang [29] combined robust chaotic maps and one-time keys. Another study conducted by Liu and Wang [30] proposed a bit-level matrix permutated by scrambling-based mapping followed by the utilization of the Chen system for the diffusion and confusion processes. Liu *et al.* [31] also applied nucleotide transformation using DNA coding to confuse pixels, thereby generating keys based on general keys and a plain image to change the initial state of chaotic maps.

Chaotic permutation multicircular shrinking (CPMCS) is a permutation method based on multicircular shifts with gradually decreasing element sizes [32]. The circular method is chosen because it can be efficiently applied in hardware or software and is directly related to a key that determines the shifting distance. However, traditionally, the CPMCS method uses duals iterations in the implementation of multicircular shrinking.

In this paper, we present an image encryption scheme based on CPMCS with the gradual deletion of the input set (GDIS CPMCS). Deletion is used when processing the circular permutation, as explained in the pseudocode (Section II). Compared to CPMCS [33], the advantages of GDIS CPMCS include a faster encryption process and a larger keyspace while maintaining robustness to noise.

The remainder of the paper is organized as follows. Section II introduces the GDIS CPMCS. Section III explains the proposed encryption scheme. Section IV reports keyspace and speed comparisons. Section V presents the results of statistical and robustness analyses. Section VI summarizes the paper.

II. CHAOTIC PERMUTATION MULTICIRCULAR SHRINKING WITH THE GRADUAL DELETION OF THE INPUT SET (GDIS CPMCS)

In CPMCS, permuting the set X, which consists of n elements, requires $n-1$ rounds of circular shifting. Because a key controls the shifting distance in each round, n elements need $n-1$ key streams. Hence, all rounds will have n factorial unique maps of X to Y [33], [34]. However, the CPMCS process requires a relatively high number of iterations equal to $\frac{n^2+n-2}{2}$; thus, the encryption time for a large-sized image is relatively slow. To overcome this problem, this paper proposes GDIS CPMCS, which involves the gradual deletion of the input set. The GDIS CPMCS process is shown in the following pseudocode.

The number of iterations in the GDIS CPMCS process is n; hence, the number of iterations is reduced to approximately $n/2$. If we write the GDIS CPMCS permutation as $\odot(\mathrm{X_n})$, then the output Y_n corresponds to Eq. (1).

$$\mathrm{Y_n} = \odot(\mathrm{X_n}) \tag{1}$$

Algorithm 1 Gradual deletion of the input set

1: $index = 0$;
2: $fori = 1to\,(elementNumber - 1)$
3: $index = mod\,(index + key\,(i, elementNumber - i))$;
4: $Y\,(i) = X\,(index)$;
5: $RemoveX\,(index)$;
6: *end*
7: $Y\,(elementNumber) = X\,(1)$;

In this paper, we propose a new image encryption method that uses two chaotic pseudosets. A GDIS is introduced to enhance the process of the CPMCS, herein referred to as GDIS CPMCS, to diffuse the image pixels and control the shift distance of the row and column rotations of an image.

III. THE PROPOSED ENCRYPTION SCHEME

A. A NEW IMAGE ENCRYPTION METHOD USING A PSEUDOSET BASED ON THE GDIS CPMCS METHOD

The proposed image encryption method uses two pseudosets generated by the GDIS CPMCS method. The pseudoset is used in the row and column diffusion process and is also used to control the circular rows of an image and column shifting. In the first step, any arbitrary initial key for the sequence is chosen as the input of the key expansion. The initial sequence is the sum of the original image pixels so that the permutation is sensitive to changes in the original image. The output of key expansion is the set key, which controls the CPMCS process.

In the second step, an arbitrary seed of the set row (SR) that consists of n elements and the set column (SC) that consists of m elements is created. The set SR_n is the seed for generating the pseudorow PIR_n with Eq. (2), where $i = 1$ is used for the red color component, $i = 2$ is used for the green color component, and $i = 3$ is used for the blue color component. The set SC_m is the seed that is used to produce the pseudocolumn PIC_m with Eq. (3), where $i = 1$ is used for the red color component, $i = 2$ is used for the green color component, and $i = 3$ is used for the blue color component. SR_n is also employed to generate the set of keys PKC_n, which determine the distance of each image row rotation based on Eq. (4), and SC_m is used to generate the set of keys PKR_m, which determine the distance of image rotation for each column in accordance with Eq. (5).

$$\mathrm{PIR_{n(i-1)}} = \odot^{i}\,(\mathrm{SR_n}) \tag{2}$$

$$\mathrm{PIC_{m(i-1)}} = \odot^{i}\,(\mathrm{SC_m}) \tag{3}$$

$$\mathrm{PKC_m} = \odot^{4}\,(\mathrm{SC_m}) \tag{4}$$

$$\mathrm{PKR_n} = \odot^{4}\,(\mathrm{SR_n}) \tag{5}$$

In the third step, the original image is divided into m sets of columns, where each set consists of n elements referred to as P_n. Each P_n consists of three rows that represent the associated red, green and blue (RGB) components. A bitxor function is used to map P_n with PIR_n, which ranges from the first row to the mth row according to Eq. (6), followed by a row rotation with a shift distance that is determined by PKC_m according to Eq. (7) to obtain m sets of C_n. The combined m sets of C_n encompass phase 1 of the ciphered image.

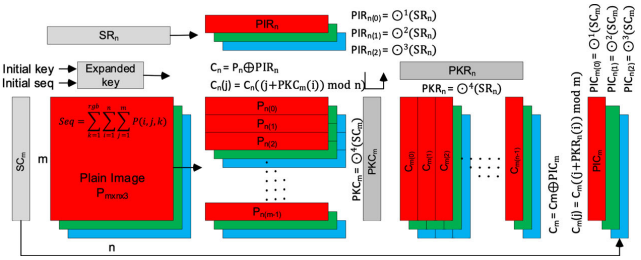

FIGURE 1. The new image encryption algorithm using a pseudoset based on GDIS CPMCS.

In the fourth step, the scrambled image is separated into $n\,x\,C_m$ pieces, where each piece consists of m elements, referred to as C_m. Each C_m consists of three columns representing the associated RGB components. The bitxor function is also used to combine C_m with PIC_m, which ranges from the first column to the last column and corresponds to Eq. (8); this step is followed by a column rotation with a shift distance determined by PKR_n according to Eq. (9). The combined set of C_m is the ciphered image result. The overall encryption process is depicted in Fig. 1.

$$\mathrm{C_n\,(i, j, k)} = \mathrm{P_n\,(i, j, k)} \oplus \mathrm{PIR_n\,(j, k)}\,, \quad 0 \le \mathrm{i} < \mathrm{m},\quad 0 \le \mathrm{j} < \mathrm{n},\ 0 \le \mathrm{k} < 3 \tag{6}$$

$$\mathrm{C_n\,(i, j, k)} = \mathrm{C_n\,(i, (j + PKC_m\,(i))\ mod\ n, k)}\,, \quad 0 \le \mathrm{i} < \mathrm{m},\quad 0 \le \mathrm{j} < \mathrm{n},\ 0 \le \mathrm{k} < 3 \tag{7}$$

$$\mathrm{C_m\,(i, j, k)} = \mathrm{C_m\,(i, j, k)} \oplus \mathrm{PIC_m\,(i, k)}\,, \quad 0 \le \mathrm{i} < \mathrm{m},\quad 0 \le \mathrm{j} < \mathrm{n},\ 0 \le \mathrm{k} < 3 \tag{8}$$

$$\mathrm{C_m\,(j, i, k)} = \mathrm{C_m\,((j + PKR_n\,(i))\ mod\ m, j, k)}\,, \quad 0 \le \mathrm{i} < \mathrm{n},\quad 0 \le \mathrm{j} < \mathrm{m},\ 0 \le \mathrm{k} < 3 \tag{9}$$

B. A NEW IMAGE DECRYPTION METHOD USING A PSEUDOSET GENERATED BY GDIS CPMCS

The image decryption method uses two pseudosets generated by GDIS CPMCS. The pseudoset is used in the row and column diffusion process and to control the circular image row and column shifts. In the first step, the same initial key and initial sequence are used as the inputs of key expansion. The set key, which is the output of the expansion key, is used to control the GDIS CPMCS process.

In the second step, the same row set SR, which consists of n elements, and the column set SC, which consists of m elements, are chosen to form the seed and produce the pseudoset. The set SR_n is the seed used to generate the pseudorow image PIR_n with Eq. (2), where $i = 1$ is the red color component, $i = 2$ is the green color component, and $i = 3$ is the blue color component. The set SC_m is the seed that produces the pseudocolumn image PIC_m in accordance with Eq. (3), where $i = 1$ is the red color component, $i = 2$ is the green color component, and $i = 3$ is the blue color component. SR_n is also used to generate the PKC_n keys, which determine the shift distance of each row rotation based on Eq. (10), and

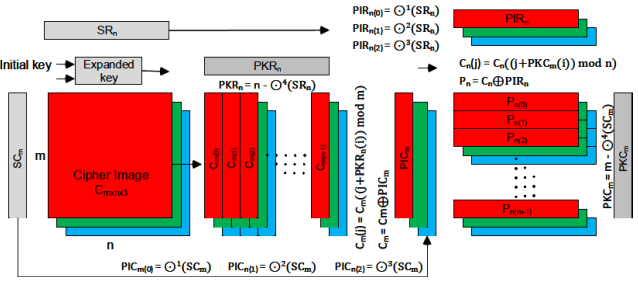

FIGURE 2. The new image decryption algorithm using a pseudoset based on GDIS CPMCS.

SC_m is used to generate the PKR_m keys, which are used to determine the shift distance of each column rotation based on Eq. (11)

$$\mathrm{PKC_m} = \mathrm{m} - \odot^4(\mathrm{SCm}) \tag{10}$$

$$\mathrm{PKR_n} = \mathrm{n} - \odot^4(\mathrm{SRn}) \tag{11}$$

In the third step, the ciphered image is separated into n sets of columns, where each set consists of m elements referred to as C_m. Each C_m consists of 3 sets that represent the associated RGB components. Each C_m is rotated with the shift distance determined by PKR_n from Eq. (12). Next, each column C_m is bitxored with the pseudoset PIC_m in accordance with Eq. (13). The combined set of nxC_m is the output of the first stage of image reconstruction.

The reconstructed image is grouped into m sets of rows referred to as C_n. Each C_n is rotated from the first row to the last row, with a shift distance determined by PKC_m based on Eq. (14). Next, each C_n row is bitxored with the pseudoset PIR_n according to Eq. (15), and the combined n sets of P_n form the reconstructed plain image. The overall proposed decryption scheme is depicted in Fig. 2.

$$\mathrm{C_m\,(i,j,k)} = \mathrm{C_m\,((j + PKR_n\,(i))\,mod\,m, j, k)}\,, \quad 0 \le \mathrm{i} < \mathrm{m},\quad 0 \le \mathrm{j} < \mathrm{n},\ 0 \le \mathrm{k} < 3 \tag{12}$$

$$\mathrm{C_m\,(i,j,k)} = \mathrm{C_m\,(i,j,k) \oplus PIC_m\,(i,k)}\,, \quad 0 \le \mathrm{i} < \mathrm{m},\quad 0 \le \mathrm{j} < \mathrm{n},\ 0 \le \mathrm{k} < 3 \tag{13}$$

$$\mathrm{C_n\,(i,j,k)} = \mathrm{C_n\,(i,\,(j + PKC_m\,(i))\,modn, k)}\,, \quad 0 \le \mathrm{i} < \mathrm{m},\quad 0 \le \mathrm{j} < \mathrm{n},\ 0 \le \mathrm{k} < 3 \tag{14}$$

$$\mathrm{P_n\,(i,j,k)} = \mathrm{C_n\,(i,j,k) \oplus PIR_n\,(j,k)}\,, \quad 0 \le \mathrm{i} < \mathrm{m},\quad 0 \le \mathrm{j} < \mathrm{n},\ 0 \le \mathrm{k} < 3 \tag{15}$$

IV. KEYSPACE AND SPEED COMPARISON

A. CHAOTIC MAP KEYSPACE COMPARISON

When the set X is transformed to the set Y by a chaotic function in a discrete domain, without considering the recurrence period, the number of possible transformations is determined by the number of controlled variables. Because PCMCS uses $n-1$ keys as the controlled variables with a gradually shrinking modulus, the size of the keyspace of PCMCS is n factorial. Moreover, other chaotic functions, such as the ACM [17], as shown in Eq. (16), have two controlled variables. Hence, for the discrete domain modulus N, the keyspace of the ACM is N^2.

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & P \\ Q & PQ+1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \end{bmatrix} modN \tag{16}$$

A similar approach can be applied to other chaotic maps, such as the standard map [35] by using Eq. (17), the Henon map [36] by using Eq. (18), Baker's map [37] in accordance with Eq. (19), the prime modulus multiplicative linear congruential generator (PMMLCG) [38] by using Eq. (20), the logistic map [1] as defined by Eq. (21), the tent map [39], [40] as defined by Eq. (22), the sine map [25] by using Eq. (23), and the 3D ACM [41] by using Eq. (24).

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} x_i + y_i \\ y_i + Ksin\left(\frac{x_{i+1}N}{2\pi}\right) \end{bmatrix} modN \tag{17}$$

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \end{bmatrix} = \begin{bmatrix} y_{i+1} + 1 - \alpha x_i^2 \\ \beta x_i \end{bmatrix} modn \tag{18}$$

$$\begin{bmatrix} \mathrm{x_{i+1}} \\ \mathrm{y_{i+1}} \end{bmatrix} = \begin{bmatrix} \frac{ay_{i+1}}{2}\ for\ 0 < x_i < \frac{1}{2};\ \frac{(ay_{i+1}+1)}{2}\ for\ \frac{1}{2} \le x_i < 1 \end{bmatrix} \mathrm{modn} \tag{19}$$

$$x_{i+1} = (Ax_i)\ modN; \quad \mathrm{A} \in \text{Prime number} \tag{20}$$

$$x_{i+1} = Ax_i\,(1 - x_i)\ modN; \quad \mathrm{A} \in (3; 4] \tag{21}$$

$$x_{i+1} = f\,(x_i, h) \begin{cases} \frac{x_i}{h}; & 0 < x_i \le h \\ \frac{1 - x_{i,}}{1 - h}; & h < x_i \le 1 \end{cases} \tag{22}$$

$$x_{i+1} = f\,(\alpha, x_i) = \frac{\alpha \sin(\pi x_i)}{4}; \quad \alpha \in (0, 4] \tag{23}$$

$$\begin{bmatrix} x_{i+1} \\ y_{i+1} \\ z_{i+1} \end{bmatrix} = \begin{bmatrix} 1 & P & 0 \\ Q & PQ+1 & 0 \\ R & S & 1 \end{bmatrix} \begin{bmatrix} x_i \\ y_i \\ z_i \end{bmatrix} modN \tag{24}$$

A comparison of the discretized keyspace sizes using different chaotic maps can be seen in Table 1. According to the

TABLE 1. Comparison of discretized keyspace sizes using different chaotic maps.

No	Chaotic map	Dimension	Discretized keyspace scaling	Keyspace with 256 elements
1	ACM	2	N^2	6.55E+04
2	Standard map	2	N^2	6.55E+04
3	Hennon map	2	N^3	6.55E+04
4	Baker map	2	$2^{N/4}$	5.79E+76
5	PMMLCG	1	N	2.56E+02
6	Logistic map	1	N^2	6.55E+04
7	Tent map	1	N^2	6.55E+04
8	Sine map	1	N^2	6.55E+04
9	GDIS CPMCS	N	N!	8.60E+506
10	3D ACM	3	N^4	1.68E+07

TABLE 2. Keyspace comparison between the GDIS CPMCS and reference schemes.

Analysis	Keyspace (power of 2)
GDIS CPMCS	3368
Wang [26]	588
Wang [43]	165
Tong [14]	219
Wang [21]	487
Hsiao [22]	651
Patidar [16]	161
Bigdeli [15]	160
Kanso [24]	480
Wu [23]	299
Seyedzadeh [17]	128
Zhou [25]	279

table, the chaotic map used for the proposed image encryption scheme has the largest keyspace, with a size of 8.60×10^{506} for 256 elements.

B. IMAGE ENCRYPTION KEYSPACE COMPARISON

The encryption scheme uses two pseudosets generated by GDIS PCMCS with two difference keys. The size of the keyspace for a 256×256 pixel image using the proposed encryption method is $(256!)^2 = 2^{3368}$. It is clear that this value is much larger than the keyspace that is required for modern cryptography [20], [42]. A comparison of the image encryption keyspaces is presented in Table 2. According to the table, the proposed encryption method has a larger keyspace than the referenced encryption schemes. Thus, in terms of robustness to brute force attacks, the proposed scheme can advance the development of M2M and IoT technology and promote the emergence of quantum computers.

C. ENCRYPTION AND DECRYPTION SPEEDS

An experiment is conducted to evaluate the speed performance of the proposed method using MATLAB 8.5 on a computer with a 64-bit Intel(R) Core (TM) i7-5500U CPU @ 2.4 GHz, 8 GB of RAM, and Windows 10. Experiments were also performed using MATLAB 7.0.4 on an Acer Core 2 Duo with CPUT7100 @ 1.8 GHz, 2.48 GB of RAM, and Windows XP SP3 to observe the speed performance of the proposed method using a less powerful computer.

TABLE 3. Comparison of the processing speeds of reference schemes and the associated platforms.

Scheme	Processing speed (ms)		Platform
	Color image	Gray image	
GDIS CPMCS	27.78	20.99	MATLAB 8.5, Intel (R) core(TM) i7-5500U CPU @2.4 GHz, RAM 8 GB, Windows 10, 64 bit.
GDIS CPMCS	32.29	24.01	MATLAB 7.0.4, Core 2 Duo, CPUT7100, @1.8 GHz, 2.48 GB RAM Windows XP
Wang [26]		2.5	Windows 7 operating system with a 1.8-GHz CPU, 8 GB of memory and MATLAB 2016a.
Wang [43]	354.78		MATLAB 2017, Intel Core i5-7500 CPU, 8 GB memory and Windows 10
Suryanto [32]	1198.00		MATLAB 8.5, Intel (R) core(TM) i7-5500U CPU @2.4 GH, RAM 8 GB Windows 10, 64 bit.
Suryanto [33]		392.00	MATLAB 8.5, Intel (R) core(TM) i7-5500U CPU @2.4 GH, RAM 8 GB Windows 10, 64 bit.
Tong [14]	181.00		Unspecified
Hsiao [22]	550.00		MATLAB 7.0 version on a computer of Dual-Core CPU, 2.3 GHz and 4 GB of RAM
Patidar [16]	160.00		MATLAB 7.2, Intel Core 2 Duo, 2.1 GHz CPU, 2 GB RAM, Windows Vista
Bigdeli [15]	56.00		MATLAB 7.7.0, 1.60 GHz, Pentium IV with 512 MB RAM, Windows XP
Kanso [24]	1,500.00		2.27 GHz Intel Core™ i5 notebook with 4 GB of RAM running Ubuntu Linux 10.04
Wu [23]	448.00		MATLAB 8.0.0.7, Windows 8, Intel(R) Core (TM) i5-4300U CPU @2.49 GHz. 8GB RAM.
Seyedzadeh [17]	36.48		Intel Core 2 Duo, 3 GHz CPU, 3.25 GB RAM, XP Home, Eclipse 3.5 compiler
Zhou [25]		178.90	MATLAB7.1.10, Windows 7, Intel(R) Core(TM) i7-2600 CPU@3.40 GHz and 4 GB RAM

Based on the conducted experiment, the encryption and decryption speeds are balanced; for a color image, the encryption speed is 27.78 *ms*, and the decryption speed is 27.64 *ms*. Table 3 suggests that the speed of the proposed encryption scheme is the fastest among those of all methods considered, even when compared to the speed reported in the reference paper with the smallest keyspace. According to Tables 2 and 3, as the keyspace size increases, the encryption process tends to take longer to complete. However, the proposed method can overcome this problem. Clearly, the keyspace of the proposed scheme is the largest, yet it has the fastest encryption speed.

The speed of the encryption and decryption processes is influenced by the complexity of the cryptographic algorithm used [44]. In general, the lower the complexity of the algorithm is, the faster the encryption and decryption

TABLE 4. Complexity analysis of the GDIS CPMCS method.

Operation	Computational complexity	
	Grayscale image	RGB image
Sum	2M+ 2N+ 4MN	2M+ 2N+12MN
Divide	M +N	M +N
Modulus	2M + 2N + MN	2M + 2N + 3MN
Bitxor	3MN	9MN
Substitution	2MN	6MN
Deletion	M + N + 2MN	M+N +6MN
Total	6M+6N+12MN	6M+6N+36MN

TABLE 5. Comparison of the complexity and order of magnitude among image encryption schemes.

Method	Complexity order	Order of magnitude
[45] Hua	O(40MN)	$\mathbf{2.6x10^6}$
[46] Hua	O(180MN)	$\mathbf{11.8x10^6}$
[47] Belazi	O(124MN)	$\mathbf{8.1x10^6}$
[44] Sun	O(74MN)	$\mathbf{4.8x10^6}$
GDIS CPMCS	O(37MN)	$\mathbf{2.42x10^6}$

processes. The proposed GDIS-CPMS algorithm for RGB images has a complexity level of less than 37 MN, and the complexity level is less than 13 MN for grayscale images. Table 4 shows the computational complexity of the proposed encryption algorithm. For an image size of 256 × 256 pixels, the order of magnitude is shown in Table 5. According to the comparison of the complexity results, the proposed image encryption scheme has the lowest computational complexity.

V. STATISTICAL AND ROBUSTNESS ANALYSES

Statistical and robustness analysis methods were used to assess the visualization performance of the proposed encryption scheme based on histogram analysis, entropy analysis, the National Institute of Standards and Technology (NIST) randomness test, differential analysis (i.e., NPCR and UACI), key sensitivity analysis (i.e., NPCR, UACI, and correlation), resistance to standard noise, and robustness against data loss.

A. VISUALIZATION AND HISTOGRAM ANALYSIS

To test the correlation between adjacent pixels in an encrypted image, an analysis of covariance correlation or Pearson correlation was performed. Encrypted images are compared with the original image and shifted vertically, horizontally, and diagonally. Generally, the data being compared include as many as 1000 to 2500 pairs of pixels chosen randomly. This method is used by Fouda [48], which can be described according to Eq. (25).

$$r_{xy} = \frac{\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{25}$$

where

- r_{xy} is the correlation coefficient
- n is the number of data pairs

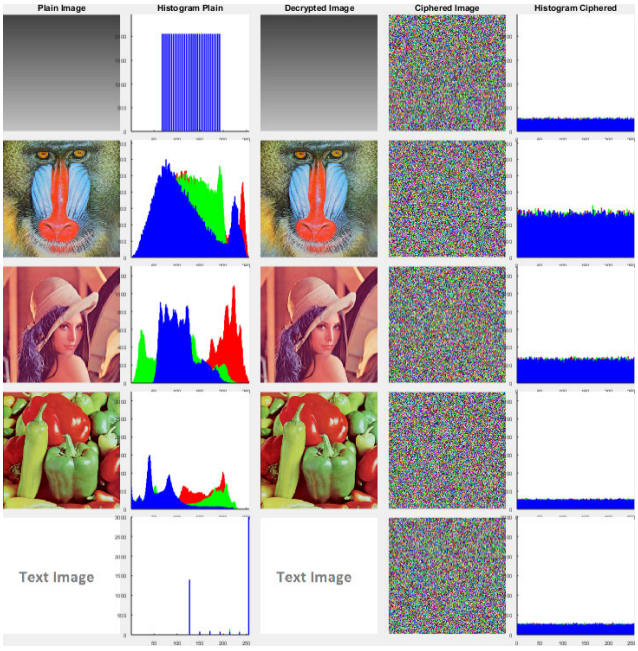

FIGURE 3. Visualization of the original images, deciphered images, ciphered images, and associated histograms.

- x_i is the i^{th} value from data set X
- y_i is the i^{th} value from data set Y
- $\bar{x}$ is the average data set X
- $\bar{y}$ is the average data set Y.

The proposed method generates a ciphered image that is unrecognizable, and the deciphered image is the same as the original, as shown in Fig. 3. According to the figure, the ciphered image has a uniform histogram, which indicates that the proposed method can strongly prevent an attacker from exploiting any useful statistical information.

B. ENTROPY AND THE NIST RANDOMNESS TEST

The Shannon entropy [49] and local Shannon entropy (LSE) [50] tests were performed for the proposed method by using Eq. (26) and Eq. 27. The test results in Table 6 show that the proposed scheme generates a ciphered image that exhibits a very high entropy value near 8. The LSE values for all plain images, which are relatively low after they are encrypted using the GDIS COMS algorithm, have relatively high entropy values. A comparison of the entropy values of the ciphered image 'Lena' based on the methods in the referenced papers can be observed in Table 7. This comparison shows that no local image is perfectly scrambled. The randomness level was further analyzed using the NIST standard.

$$H(X) = -\sum_{i=0}^{2^n-1} P_i log_2(P_i) \tag{26}$$

where

- H (X) is the Shannon entropy equation
- P (i) is the probability associated with pixel i.

$$\overline{H}_{k,T_B}(s) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{27}$$

TABLE 6. Entropy values for the original and ciphered images.

Scheme	gradient	baboon	Lena	peppers	textImage
Entropy, original	5.0000	7.6780	7.7329	7.7036	0.2135
Entropy, ciphered	7.9989	7.9990	7.9991	7.9992	7.9991
LSE original	2.5905	7.3687	7.2685	7.1527	0.1781
LSE ciphered	7.9673	7.9676	7.9683	7.9674	7.9677

TABLE 7. Comparison of the entropies of the ciphered Lena image for the referenced schemes.

Analysis	Entropy
GDIS CPMCS	7.9991
Tong [14]	7.9992
Wang [21]	7.9974
Hsiao [22]	7.9993
Patidar [16]	7.9963
Bigdeli [15]	7.9981
Wu [23]	7.9903
Seyedzadeh [17]	7.9995

TABLE 8. Results from the randomness test using NIST test suite SP22-800 for a ciphered image using the proposed method.

Statistical test	P-value				
	gradient	baboon	Lena	peppers	sailboat
Frequency	0.1223	0.3505	0.0669	0.5341	0.7399
Block frequency	0.3505	0.3505	0.5341	0.7399	0.2133
Cumulative sums (forward)	0.2133	0.2133	0.5341	0.9114	0.7399
Cumulative sums (reverse)	0.7399	0.0669	0.7399	0.9114	0.0179
Runs	0.1223	0.9114	0.2133	0.3505	0.9114
Longest run	0.9915	0.9114	0.2133	0.5341	0.9915
Rank	0.7399	0.9114	0.1223	0.2133	0.3505
FFT	0.5341	0.5341	0.0669	0.9114	0.5341
Nonoverlapping template	0.4847	0.4628	0.4758	0.5237	0.5088
Overlapping template	0.7399	0.1223	0.2133	0.2133	0.5341
Approximate entropy	0.7399	0.9114	0.5341	0.5341	0.1223
Serial (1)	0.7399	0.3505	0.7399	0.7399	0.1223
Serial (2)	0.9114	0.5341	0.1223	0.1223	0.9114
Linear complexity	0.9114	0.2133	0.5341	0.7399	0.5341

where

- $\overline{H_{k,T_B}}$ (s) is the local Shannon entropy (LSE)
- $S_i(i = 1, 2, \ldots, k)$ is a randomly selected and nonoverlapping image block with TB pixels
- H(Si) is the information entropy of image block Si

for $k = 30$ and $TB = 1936$.

The NIST randomness test suite SP800-22 [51] was used to assess the randomness of the ciphered image. The ciphered pixel values for each color component were converted into a binary format and prepared in accordance with the sequence of rows and color components. The test was performed for 13 randomness test criteria. The universal test criteria require a minimum number of bits of $10 \times 387,840$, and the random excursions and random excursion variant require at least 10×1 million bits; however, a $256 \times 256 \times 3$ color image only has 1, 572, 864 bits. The proposed scheme produces a very random ciphered image, as reflected by the high p-values in Table 8.

TABLE 9. NPCR and UACI values for two ciphered images with a one-bit difference in the original image for each color component.

Statistic	RGB	gradient	baboon	Lena	peppers	textImage
NPCR (%)	R	99.62	99.65	99.61	99.61	99.61
	G	99.58	99.59	99.62	99.62	99.65
	B	99.62	99.56	99.60	99.60	99.66
UACI (%)	R	33.44	33.38	33.39	33.38	33.44
	G	33.34	33.70	33.51	33.39	33.46
	B	33.31	33.42	33.44	33.48	33.40

TABLE 10. Comparison of the NPCR and UACI values of the referenced schemes for two ciphered images with a one-bit difference in the original image for each color component.

Scheme	NPCR (%)			UACI (%)		
	r	g	b	r	g	b
GDIS CPMCS	99.61	99.62	99.60	33.39	33.51	33.44
Wang [21]	99.61	99.61	99.62	33.44	33.52	33.50
Hsiao [22]	99.61	99.59	99.60	33.42	33.51	33.45
Patidar [16]	99.61	99.60	99.60	33.39	33.50	33.47
Wu [23]	99.61	99.61	99.61	33.46	33.50	33.48

C. DIFFERENTIAL ANALYSIS (NPCR AND UACI)

Differential analysis is performed for the proposed method using the NPCR [52] and UACI methods. These methods are used to determine the ciphered image difference when the original image changes by only one bit, in accordance with Eqs. (28-30).

$$D_{ij} = \begin{cases} 0, & if\ X_{ij} = Y_{ij} \\ 1, & if\ X_{ij} \neq Y_{ij} \end{cases} \tag{28}$$

$$NPCR = \sum_i \sum_j \frac{D_{ij}}{N} \times 100\% \tag{29}$$

$$UACI = \sum_i \sum_j \frac{|X_{ij} - Y_{ij}|}{F.N} \times 100\% \tag{30}$$

Table 9 shows that with the proposed method, the NPCR and UACI values for the two ciphered images are very high when the original image changes by one bit. Based on the table, although the original image only changes by one bit, the two ciphered images are completely different. Table 10 shows a comparison of the NPCR and UACI values for differential statistical tests with the referenced methods. It can be deduced that the proposed scheme is highly sensitive to changes in the original image.

TABLE 11. NPCR, UACI and correlation values for the two deciphered images with a one-bit difference in the initial key for each color component.

Image	RGB	NPCR (%)	UACI (%)	Correlation Cipher					
				Coefficient			p-value		
				Hor.	Ver.	Diag.	Hor.	Ver.	Diag.
gradient	r	99.62	33.44	0.0031	-0.0012	0.0033	0.3993	0.3570	0.4609
	g	99.58	33.34	0.0073	-0.0007	-0.0039	0.4764	0.3518	0.6752
	b	99.62	33.31	-0.0156	0.0103	0.0065	0.4012	0.3533	0.5789
baboon	r	99.65	33.38	0.0100	0.0063	0.0021	0.3696	0.4330	0.5392
	g	99.59	33.70	-0.0128	0.0038	-0.0012	0.4680	0.5930	0.5276
	b	99.56	33.42	0.0113	-0.0054	-0.0016	0.4364	0.4995	0.3629
Lena	r	99.61	33.39	-0.0070	-0.0014	-0.0029	0.5042	0.4646	0.5164
	g	99.62	33.51	0.0072	-0.0009	0.0149	0.5152	0.4394	0.4561
	b	99.60	33.44	-0.0120	0.0203	0.0118	0.3970	0.2619	0.4985
peppers	r	99.61	33.38	-0.0008	-0.0157	0.0018	0.3871	0.3785	0.3155
	g	99.62	33.39	0.0150	-0.0168	-0.0118	0.4723	0.2981	0.3129
	b	99.60	33.48	0.0150	-0.0040	-0.0033	0.3068	0.5968	0.4010
textImage	r	99.61	33.44	-0.0006	-0.0011	0.0005	0.3985	0.5651	0.5742
	g	99.65	33.46	-0.0019	0.0119	0.0117	0.3581	0.4052	0.4487
	b	99.66	33.40	-0.0112	0.0009	0.0078	0.4752	0.5388	0.3644

D. KEY SENSITIVITY ANALYSIS

A key sensitivity test is conducted for the proposed method to determine its sensitivity to a key change. When a good encryption scheme is used, a one-bit difference in the key will lead to a notable change in both the ciphered image and the deciphered image. Table 11 represents the NPCR, UACI, and correlation coefficient values of two ciphered images encrypted using two similar keys. The first key is 987654321012345, and the second key is 987654321012346. Because the size of the keyspace for each GDIS CPMCS process for set P256 is 2^{1684}, a one-bit difference means that a key only differs by as much as 2^{-1684} of the entire keyspace. Thus, the proposed scheme is very sensitive to key alterations. A comparison of the NPCR and UACI values from the key sensitivity test for images encrypted using the referenced methods can be seen in Table 12.

The proposed encryption method passes the NIST benchmark test, test of sensitivity to differential analysis, and test of sensitivity to keys; hence, attempts to attack utilizing ciphertext only, known plaintext, chosen ciphertext, and chosen plaintext can only be executed when an adversary has the original key in the form of the initial key and sequence key. However, it is difficult to obtain the initial and sequence keys from the used permutation pattern because we apply a one-way function to process key generation. Moreover, the ciphertext key is associated with plaintext so that different plaintexts with the same key will produce different permutation patterns.

TABLE 12. Comparison of the NPCR and UACI key sensitivity values of the referenced schemes.

Scheme	NPCR (%)	UACI (%)
GDIS CPMCS	99.60	33.47
Tong [14]	99.56	34.05
Seyedzadeh [17]	99.61	33.45

Furthermore, a slight shift in the plaintext causes a significant and random shift in the ciphertext. Then, breaking the key is only possible if the pattern used by the key is unchanged. Additionally, the key sequence used in our method continues to change from time to time. Thus, according to the aforementioned analysis, we can conclude that the proposed algorithm is resistant to ciphertext only, known-plaintext, chosen-ciphertext, and chosen-plaintext attacks, as discussed by Wang [53], [54].

E. ANALYSIS OF THE ROBUSTNESS TO NOISE

An analysis of the robustness to noise is conducted for the proposed method when the ciphered image contains Gaussian, Poisson, salt-and-pepper and speckle noise. The peak signal-to-noise ratio (PSNR) [55] is calculated by Eq. (31), where Imax is the maximum intensity of the image (255 for a gray level image) and the mean square error (MSE) is determined using Eq. (32); the MSE is used to measure the robustness to noise. High PSNR values and low MSE values for the original and deciphered images when the ciphered

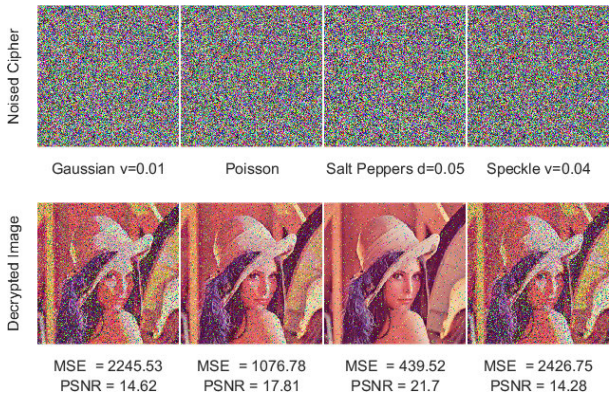

FIGURE 4. The deciphered Lena image when the ciphered image contains Gaussian noise, Poisson noise, salt-and-pepper noise, and speckle noise.

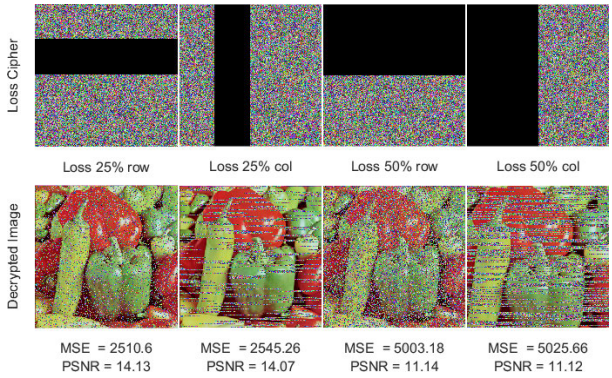

FIGURE 5. The deciphered pepper image shows data loss in the ciphered image at 25% and 50% loss levels for columns and rows, respectively.

image contains noise indicate that the encryption method is robust to noise.

$$PSNR = 20 \times log_{10}\left(\frac{I_{max}}{\sqrt{MSE}}\right) \tag{31}$$

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{n}\sum_{j=1}^{m}\left(X_{ij} - Y_{ij}\right)^2 \tag{32}$$

Fig. 4 shows the deciphered Lena image when the ciphered image contains standard Gaussian noise with v=0.01 and Poisson noise, salt-and-pepper noise, or speckle noise with v=0.04. As shown in Fig. 4, the deciphered image can be recognized with low MSE values and relatively high PSNR values, which suggests that the proposed scheme is robust to noise.

F. ANALYSIS OF THE ROBUSTNESS TO DATA LOSS

An analysis is conducted for the proposed method when the ciphered image experiences some data loss. According to Fig. 5, the decrypted image can be retrieved even when the ciphered image experiences significant data loss (i.e., data loss levels of 25% and 50% for the rows and columns, respectively). The relatively low values of the MSE and high values of the PSNR verify that the proposed scheme is robust to data loss.

VI. CONCLUSION

The proposed image encryption scheme uses two pseudosets generated by GDIS CPMCS to diffuse image pixels and control the shift distance of the row and column rotations. Commonly, encryption methods with a large keyspace are characterized by long processing times. However, the proposed method produces a larger keyspace than the referenced encryption schemes and achieves an encryption processing time that is much shorter than those of the referenced papers. The size of the keyspace reaches 2^{3368} for an image size of 256×256, and the encryption process requires only 27.78 ms running on the test laptop.

The ciphered image has a very high degree of randomness based on the results of the entropy and NIST randomness tests. The proposed method is also very sensitive to key alteration; changing one bit of the 21,684 possible initial keys will produce a notably different ciphered image, as shown for the Lena image, with NPCR and UACI values of 99.61% and 33.44%, respectively, and a correlation of 0.0095. In terms of differential analysis, changing one bit in the original image leads to a significant difference in the ciphered image, as indicated by NPCR and UACI values of 99.61% and 33.45%, respectively. The proposed method is also robust to noise (i.e., Gaussian, Poisson, salt-and-pepper, and speckle noise) and data loss, so it can be used to efficiently transmit information via a nonerror-free communication system.

REFERENCES

[1] K. J. Singh and D. S. Kapoor, "Create your own Internet of things: A survey of IoT platforms.," *IEEE Consum. Electron. Mag.*, vol. 6, no. 2, pp. 57–68, Apr. 2017.

[2] I. Lee, "The Internet of things for enterprises: An ecosystem, architecture, and IoT service business model," *Internet Things*, vol. 7, Sep. 2019, Art. no. 100078.

[3] *Ericson Mobility Report: Internet of Things Forecast*. Accessed: Nov. 18, 2019. [Online]. Available: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

[4] Statista Research Department. (Aug. 9, 2019). *Internet of Things–Number of Connected Devices Worldwide 2015-2025*. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

[5] T. R. Rao, P. Mitra, R. Bhatt, and A. Goswami, "The big data system, components, tools, and technologies: A survey," *Knowl. Inf. Syst.*, vol. 60, no. 3, pp. 1165–1245, Sep. 2019.

[6] C. Stergiou, K. E. Psannis, B. B. Gupta, and Y. Ishibashi, "Security, privacy & efficiency of sustainable cloud computing for big data & IoT," *Sustain. Comput., Inform. Syst.*, vol. 19, pp. 174–184, Sep. 2018.

[7] J. Andreu-Perez, C. C. Y. Poon, R. D. Merrifield, S. T. C. Wong, and G.-Z. Yang, "Big data for health," *IEEE J. Biomed. Health Inform.*, vol. 19, no. 4, pp. 1193–1208, Jul. 2015.

[8] R. Jiang, M. Shi, and W. Zhou, "A privacy security risk analysis method for medical big data in urban computing," *IEEE Access*, vol. 7, pp. 143841–143854, 2019.

[9] J. Sun, G. Han, Z. Zeng, and Y. Wang, "Memristor-based neural network circuit of full-function pavlov associative memory with time delay and variable learning rate," *IEEE Trans. Cybern.*, early access, Nov. 21, 2019, doi: 10.1109/TCYB.2019.2951520.

[10] J. Sun, Y. Wu, G. Cui, and Y. Wang, "Finite-time real combination synchronization of three complex-variable chaotic systems with unknown parameters via sliding mode control," *Nonlinear Dyn.*, vol. 88, no. 3, pp. 1677–1690, May 2017, doi: 10.1007/s11071-017-3338-z.

[11] J. Sun, X. Zhao, J. Fang, and Y. Wang, "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization," *Nonlinear Dyn.*, vol. 94, no. 4, pp. 2879–2887, Dec. 2018, doi: 10.1007/s11071-018-4531-4.

[12] 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, Nov. 2010.

[13] A. Awad and A. Saadane, "New chaotic permutation methods for image encryption," *IAENG Int. J. Comput. Sci.*, vol. 37, no. 4, pp. 402–410, 2010.
[14] X.-J. Tong, "Design of an image encryption scheme based on a multiple chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 7, pp. 1725–1733, Jul. 2013.
[15] N. Bigdeli, Y. Farid, and K. Afshar, "A novel image encryption/decryption scheme based on chaotic neural networks," *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 753–765, Jun. 2012.
[16] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Opt. Commun.*, vol. 284, no. 19, pp. 4331–4339, Sep. 2011.
[17] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi, and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dyn.*, vol. 81, nos. 1–2, pp. 511–529, Jul. 2015.
[18] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.
[19] 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.
[20] *Cryptography Today*, NSA, Maryland, MD, USA, Aug. 2015.
[21] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, May 2015.
[22] H.-I. Hsiao and J. Lee, "Color image encryption using chaotic nonlinear adaptive filter," *Signal Process.*, vol. 117, pp. 281–309, Dec. 2015.
[23] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using CML and a fractional-order chaotic system," *PLoS ONE*, vol. 10, no. 3, Mar. 2015, Art. no. e0119660.
[24] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlinear Sci. Numer. Simulation*, vol. 17, no. 7, pp. 2943–2959, Jul. 2012.
[25] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172–182, Apr. 2014.
[26] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.
[27] 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.
[28] 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.
[29] 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, May 2010.
[30] 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, Aug. 2011.
[31] 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, May 2012.
[32] Y. Suryanto, Suryadi, and K. Ramli, "Chaos properties of the chaotic permutation generated by multi circular shrinking and expanding movement," in *Proc. Int. Conf. Qual. Res. (QiR)*, Aug. 2015, pp. 65–68.
[33] Y. Suryanto, Suryadi, and K. Ramli, "A new image encryption using color scrambling based on chaotic permutation multiple circular shrinking and expanding," *Multimedia Tools Appl.*, vol. 76, no. 15, pp. 16831–16854, Aug. 2017.
[34] Y. Suryanto and K. Ramli, "A secure and robust image encryption based on chaotic permutation multiple circular shrinking and expanding," *J. Inf. Hiding Multimedia Signal Process.*, vol. 7, no. 4, pp. 697–713, 2016.
[35] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *Int. J. Bifurcation Chaos*, vol. 08, no. 06, pp. 1259–1284, Jun. 1998.
[36] A. Soleymani, M. J. Nordin, and E. Sundararajan, "A chaotic cryptosystem for images based on Henon and Arnold cat map," *Sci. World J.*, vol. 2014, Aug. 2014, Art. no. 536930.
[37] A. Jolfaei and A. Mirghadri, "A novel image encryption scheme using pixel shuffler and A5/1," in *Proc. Int. Conf. Artif. Intell. Comput. Intell.*, Oct. 2010, pp. 369–373.
[38] S. G. A., R. Srinivas, and K. Bhoopathy Bagan, "Image encryption using random pixel permutation by chaotic mapping," in *Proc. IEEE Symp. Comput. Informat. (ISCI)*, Mar. 2012, pp. 247–251.
[39] 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, Oct. 2005.
[40] 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, Jan. 2011.
[41] P. N. Khade and M. Narnaware, "3D chaotic functions for image encryption," *J. Comput. Sci. Issues*, vol. 9, no. 3, p. 6, 2012.
[42] E. Barker, "Recommendation for key management part 1: General," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST SP 800-57pt1r4, Jan. 2016.
[43] X. Wang, S. Gao, L. Yu, Y. Sun, and H. Sun, "Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion," *IEEE Access*, vol. 7, pp. 103662–103677, 2019.
[44] S. Sun, Y. Guo, and R. Wu, "A novel plaintext-related image encryption algorithm based on stochastic signal insertion and block swapping," *IEEE Access*, vol. 7, pp. 123049–123060, 2019, doi: 10.1109/ACCESS.2019.2937767.
[45] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018.
[46] Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.
[47] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.
[48] J. S. Fouda, A. Eyebe, 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.
[49] Y. Wu, J. P. Noonan, and S. Agaian, "Shannon entropy based randomness measurement and test for image encryption," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[50] S. Sun, Y. Guo, and R. Wu, "A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping," *IEEE Access*, vol. 7, pp. 28539–28547, 2019, doi: 10.1109/ACCESS.2019.2901870.
[51] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. Boozallen and hamilton inc mclean va. National Institute of Standards Technology (NIST). Special Publication 800-22, Revision 1a. Accessed: Aug. 24, 2019. [Online]. Available: https://www.nist.gov/publications/statistical-test-suite-random-and-pseudorandom-numbergenerators-cryptographic?pub_id=906762
[52] Y. Wu and S. Agaian, "NPCR and UACI randomness tests for image encryption," Tech. Rep., 2011, vol. 8.
[53] 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.
[54] 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.
[55] National Instrument. (Mar. 5, 2019). *Peak Signal-to-Noise Ratio as an Image Quality Metric*. White Paper. Accessed: May 22, 2019. [Online]. Available: https://www.ni.com/en-id/innovations/whitepapers/11/peak-signal-to-noise-ratio-as-an-image-quality-metric.html

KALAMULLAH RAMLI (Member, IEEE) received the master's degree in telecommunication engineering from the University of Wollongong, NSW, Australia, in 1997, and the Ph.D. degree in computer networks at Universitaet Duisburg-Essen (UDE), Germany, in 2003. He has been a Lecturer at Universitas Indonesia (UI), since 1994, where he has also been a Professor of computer engineering, since 2009. He currently teaches advanced communication networks, embedded systems, object-oriented programming, and engineering and entrepreneurship. He is a prolific author, published over 120 journal/conference papers and written four books. His research interests include embedded systems, information and data security, computers and communications, and biomedical engineering. The government of Indonesia has awarded him several competitive research grants and international collaborative grants with UDE and UI.

YOHAN SURYANTO (Member, IEEE) received the B.S. degree in electrotechniques from the Department of Electrical Engineering, Bandung Institute of Technology, Indonesia, in 1997, the M.S. degree in information and multimedia and the Ph.D. degree from the Department of Electrical and Computer Engineering, Universitas Indonesia, in 2014 and 2016, respectively. He worked for an Indonesian national satellite telecommunication company for more than 20 years and has dynamic and challenging work experience in initiating and managing IP network implementation and engaging in a variety of IP-based network development projects. He has gained a broad range of technical expertise in communication systems and network security. He has also been the Owner and Founder of PT Rambinet Digital Network, a consultant and integration IP network partner, since 2006. He is currently a Teacher with the Faculty of Engineering, Universitas Indonesia, where he also taught courses on security risk management, forensic digital, and embedded systems with computer techniques. He holds patents on permutation algorithm, key expansion algorithm, and security token. His research interests include parallel processing for multimedia, broadband networks, applied physics, M2M, the IoT, cryptography, and information security.

MAGFIRAWATY (Member, IEEE) received the B.S. and M.S. degrees in physics from Universitas Indonesia, in 2004 and 2007, respectively, and the Ph.D. degree from the Electrical Engineering Department, Universitas Indonesia, in 2018. She currently works at Sekolah Tinggi Sandi Negara, an Indonesian state school for encoding and cryptography. Her research interests include physics, cryptography, and embedded systems.

NUR HAYATI (Member, IEEE) received the bachelor's degree in applied science (major in telecommunication engineering) from the Politeknik Elektronika Negeri Surabaya, in 2010, and the master's degree in computer engineering from Universitas Indonesia, in 2015, where she is currently pursuing the Ph.D. degree. She is also an Electrical Engineering Lecturer for undergraduate students at the Faculty of Engineering, Universitas Muhammadiyah Yogyakarta. Her research interests include embedded systems, computer networks, and IoT security.