Hindawi
Security and Communication Networks
Volume 2021, Article ID 6615708, 17 pages
https://doi.org/10.1155/2021/6615708

Research Article

A Robust and Fast Image Encryption Scheme Based on a Mixing Technique

Lee Mariel Heucheun Yepdia,[1] **Alain Tiedeu**,[1,2] **and Guillaume Kom**[3]

[1]*Signal Image and Systems Laboratory, HTTTC of EBOLOWA, University of Yaounde 1, P.O. BOX 886, Ebolowa, Cameroon*
[2]*Centre for Research, Experimentation and Production, HTTTC of Ebolowa, University of Yaoundé 1, P.O. Box 886, Ebolowa, Cameroon*
[3]*Automation and Signal Processing Laboratory, Department of Electrical Engineering, IUT-FV Bandjoun, University of Dschang, Dschang, Cameroon*

Correspondence should be addressed to Alain Tiedeu; alain_tiedeu@yahoo.fr

Received 5 October 2020; Revised 28 December 2020; Accepted 10 February 2021; Published 24 February 2021

Academic Editor: Fulvio Valenza

This paper introduces a new image encryption scheme using a mixing technique as a way to encrypt one or multiple images of different types and sizes. The mixing model follows a nonlinear mathematical expression based on Cramer's rule. Two 1D systems already developed in the literature, namely, the May-Gompertz map and the piecewise linear chaotic map, were used in the mixing process as pseudo-random number generators for their good chaotic properties. The image to be encrypted was first of all partitioned into N subimages of the same size. The subimages underwent a block permutation using the May-Gompertz map. This was followed by a pixel-based permutation using the piecewise linear chaotic map. The result of the two previous permutations was divided into 4 subimages, which were then mixed using pseudo-random matrices generated from the two maps mentioned above. Tests carried out on the cryptosystem designed proved that it was fast due to the 1D maps used, robust in terms of noise and data loss, exhibited a large key space, and resisted all common attacks. A very interesting feature of the proposed cryptosystem is that it works well for simultaneous multiple-image encryption.

1. Introduction

Volumes of images are produced daily in numerous fields and usually carry confidential information. Cryptography is one of the effective techniques used to protect these images. With the rapid expansion of the internet, new technologies, and sophisticated cryptanalysis, it becomes necessary to design advanced, robust, and efficient image encryption algorithms suitable to secure image transmission. Researchers have then developed a variety of image encryption algorithms in symmetric or asymmetric ways. The most types of modern algorithms developed are based on chaotic systems [1–4], transform domain [5, 6], evolutionary algorithm [7], deoxyribonucleic acid (DNA) sequence [8, 9], and others [10–12].

Chaos-based systems have experienced considerable growth as they allow a good level of security. Chaos properties such as ergodicity, randomness and extreme sensitivity to initial conditions, and control parameters make them suitable for carrying out the confusion and diffusion operations required to build robust cryptosystems [13]. In order to design robust encryption algorithms, authors generally combine confusion and diffusion operations that help strengthen the ciphered image by modifying the position and value of the pixels in the target image to make it more confused. It should be noted that some of these cryptosystems require several rounds of permutation and/or diffusion to obtain a robust encrypted image [14–17].

In recent years, the patterns of image mixing or fusion-based encryption algorithms have been developed to improve on cryptosystem efficiency. In fact, so far, the majority of image fusion schemes was used as tools for better decision-making in various applications such as location and

identification of abnormalities in medical images, location of natural phenomena, and pattern recognition. Image fusion or mixing has been proven to have potential for encryption. Several algorithms in this category combine various target images either through operations in the transform domain or by using chaotic maps in a confusion-diffusion process. For example, Alfalou [13] proposed a fusion and encryption scheme in which an approximated form of discrete cosine transform (DCT) was used at the first stage to combine the secret images into one. In the encryption stage, Henon and skew tent maps were used, respectively, to achieve the confusion and diffusion effects on the pixels of the mixed image. Another encryption scheme has been suggested in [4], where the concepts of pure image element and mixed images are introduced. In this approach, the plain images are combined into a big image which is concatenated into blocks of small sizes named pure image elements, and then the mixed image is obtained after the shuffling and diffusion operations implemented by the piecewise linear chaotic map (PWLCM). This proposed cryptosystem offers good performances against the main attacks (brute-force attack, chosen plain image attack, and chosen cipher attack) but can be improved in terms of time spent when the number of plain images becomes greater in size. In [18], Xianye Li et al. devised a multiple-image encryption method based on a modified logistic map algorithm, compressive ghost imaging, and coordinate sampling. In the encryption process, multiple target images were transformed through the discrete cosine transform and then scrambled by different random sequences from the modified logistic map (MLM). Thereafter, scrambled images were fused into one image with the help of the coordinate sampling matrices. Finally, the ciphered image was obtained from the buck detector of the plane object of the compressive ghost imaging system. While this cryptosystem yielded good results, the key space was not large enough to resist some cryptanalysis attacks as chosen plaintext attack. Isha Mehra and Nishchal [19] worked out an image fusion encryption using wavelets in order to secure multiple images. In this asymmetric algorithm, the image sources were coded in two-phase masks using the principle of interference. They were then merged into a big image by the discrete wavelet transformation. It offered a large key space, which enhanced the system's security. Another optical image encryption scheme [20] based on the theory of diffraction was developed by Yi Qin et al. This algorithm proceeded in two levels of encryption; the first level consisted of realising the spectral fusion of input images through discrete cosine transformation and the nonlinear operations using the sign matrix. Then, the resultant image was ciphered at the second level by a multiple random-phase encoding process. The proposal offered a large key space and a high quality of decrypted images, but the encrypted images were affected by noise effects. The authors in [21] proposed a multiple-image encryption scheme via the mixed image elements and two-dimensional chaotic economic map (CEM). In this scheme, a set of input images were first grouped into a single image, which was then concatenated into blocks of small size named pure image elements (PIEs). Secondly, logistic map and the chaotic economic map were used to scramble the PIE and diffuse the pixels of the resultant image, respectively. The merit of this algorithm is the fact that, after decryption, the plain images were recovered without significant losses, and the computation time was low.

Despite the fact that a number of image mixing-based encryption algorithms were suggested as seen above, some flaws still have to be addressed, of whom many have been detailed in the work by Teh et al. in [22]. For instance, some schemes exhibited reduced key space [11, 23] which in turns affected the encryption robustness. Other setbacks such as a poor mean square error during decryption [19, 24], a high computational time [25, 26], and a lack of sensitivity to the plaintext [20, 27, 28], amongst others, are found. In the same vein, operational problems in cryptosystems can be noticed. For example, after analysing several developed cryptosystems, it appears that, in those which do not perform several rounds of permutation-diffusion, the NPCR value of most encrypted images is evaluated on the first pixel and decreases in value as one moves to the last pixel. Therefore, in order to improve the sensitivity to the plaintext, several authors [29–32] developed cryptosystems operating the chaining modes, such as the cipher block chaining (CBC), cipher feedback (CFB), electronic codebook (ECB), output feedback (OFB), and counter (CTR). These methods must therefore perform several rounds to propagate the values and positions of the pixels of the image to be encrypted, making the encryption time longer. Moreover, they have the disadvantage of propagating error in the encryption process.

In order to address some of the above setbacks, a two-stage image encryption algorithm using a mixing technique at the second encryption stage was designed in this study. First, the plain image was subdivided into blocks of small sizes (4×4). These blocks were permutated using data sequences from the May-Gompertz map. This block permutation was followed by pixel permutation using coefficients from the PWLCM. The two permutations (at block and pixel levels) represented the first stage. The second stage consisted of a nonlinear relationship based on Cramer's rule and was performed after one or more iterations to get the encrypted image. Initial conditions and control parameters of the three maps used as pseudo-random number generators (PRNGs) served as the keys for the cryptosystem, while some were made dependent on the plain image through the SHA-256 function. The main advantages of the proposed cryptosystem are listed as follows:

(1) Simple and fast encryption scheme, thanks to the use of 1D maps: the chaotic maps used in this paper are the piecewise linear chaotic map, the May map, and the Gompertz map. All these are one dimensional and have a simple structure. These properties speed up the encryption procedure.

(2) Enhanced security through the use of a combination of 1D maps (May and Gompertz maps): the robustness of chaos-based image encryption (CIE) algorithms depends on how suitable the chaotic map is to build a cryptosystem. This suitability depends on the "level of chaocity" of the map. In this paper,

we used two simple and fast maps of lower chaocity that we combined in order to improve the chaotic properties of the resulting map. The combined map leads to a more robust and secure cryptosystem.

(3) Featuring high security against classical attacks: cryptanalyses are based on the extraction of subkeys either from an all-null or all-one image or a significant image and their corresponding encrypted image. These classical attacks (chosen plain image attack and chosen cipher attack) on the proposed cryptosystem do not work because all-null or all-one image will not produce a subkey, but a nonusable linear combination of these subkeys. The attempt to extract the subkeys will give each time more unknown than equations.

(4) Possibility of multiple-image encryption: the proposed cryptosystem permits the encryption of many images at the same time.

(5) The cryptosystem does not allow the error to propagate: the proposed scheme supports noise well as it allows to encrypt an image without error propagation, compared to cryptosystems using chaining modes (CBC, CFB, ECB, OFB, and CTR). For instance, for two image pixels intervening in a two-dimensional Cramer system, an error on one pixel of the input image will affect only one pixel on the output image. So, the error will not be wrapped in a diffusion process.

The method is therefore suitable for images that do not tolerate noise propagation, such as medical and military images.

The assessment of our cryptosystem was carried out. Included in this paper also is the comparison of the performance of our system versus those of recent publications. The rest of the paper is structured as follows. Section 2 presents the chaotic maps used in this work. The key generation process is explained in Section 3, while the proposed encryption algorithm is described in Section 4. Experimental results and algorithm analyses are shown in Section 5.

2. Chaotic Maps Used

As indicated above, the level of chaocity of the map used in CIE is critical as far as the security of the scheme is concerned. Generally, when 1D chaotic maps are used in cryptosystems, they are simple and have a fast encryption time, which is an advantage. These cryptosystems are however not robust enough as they can easily be cryptanalyzed due to poor chaocity level of the map. To address this dilemma, some authors have developed new 1D maps with better properties based on some metrics such as Lyapunov exponent, range of the control parameter, and entropy [33–36]. In the same vein, others have suggested to combine a number of 1D maps in order to both improve on the chaocity level and keep the advantage of simplicity and speed [37, 38]. This second approach is what we are going to do in the next section, using May and Gompertz maps.

2.1. May-Gompertz System. The May-Gompertz system is obtained by combining May and Gompertz maps. This is done in order to obtain better chaotic properties as compared to the one generated by each map alone. The combination is carried out through the following equation [24]:

$$x_{n+1} = \left(x_n \exp\left((r+10)\left(1-x_n\right)\right) - (r+10)x_n \log\, x_n\right) \bmod 1, \tag{1}$$

where $x_n \in [0,1]$ and $r \in [0,5]$.

The plot of Lyapunov exponents and bifurcation diagram for May and Gompertz maps are presented in Figures 1(a)–1(d), while those of the May-Gompertz system are shown in Figures 2(a) and 2(b). By comparison, we can observe that, for May-Gompertz, the output sequence is uniformly distributed within [0, 1] (for Gompertz and May, there are some white strips that indicate chaos discontinuity), while the Lyapunov exponents are all positive with a maximum value of 8.7 (respectively, 0.4 and 0.5 for May and Gompertz).The improvement in chaotic properties as compared to those of the seed maps is therefore obvious. Assets exhibited by this combination which are 1D map (simplicity and speed), a large chaotic range, and a uniform distribution of discrete values are very suitable to build a robust, secure, and fast cryptosystem.

We can also notice from Table 1 that the May-Gompertz system passed the National Institute of Standards and Technology (NIST) tests (SP 800-22rev1a test).

2.2. Piecewise Linear Chaotic Map (PWLCM). The PWLCM is a 1D system widely used in cryptosystems, thanks to its simplicity and good dynamics. Its density function exhibits a uniform distribution for different values of the control parameter. The PWLM system is described by the following equation [4]:

$$u_{i+1} = \begin{cases} \dfrac{u_i}{p}, & 0 \le u_i < p, \\ \dfrac{(u_i - p)}{(0.5 - p)}, & p \le u_i < 0.5, \\ (1 - u_i) & u_i \ge 0.5, \end{cases} \tag{2}$$

where $u_i \in [0, 1]$ and $p \in [0, 0.5]$ is the control parameter.

Figure 3 illustrates the distribution of u_i as a function of p for 5000 iterations. As can be seen, the values are uniformly distributed within [0, 1].

According to Za [39], the National Institute of Standards and Technology (NIST) tests were applied to the PWLCM sequences. Results revealed that, for 100 binary sequences of length 10^6 each, the success rate of the test was 94%. The PWLCM can therefore be considered a good pseudo-random number generator. The set of values $u_1 = \{0.13, 0.15, 0.17, 0.5, 0.87, 1\}$ which failed the frequency test must not be used as initial conditions.

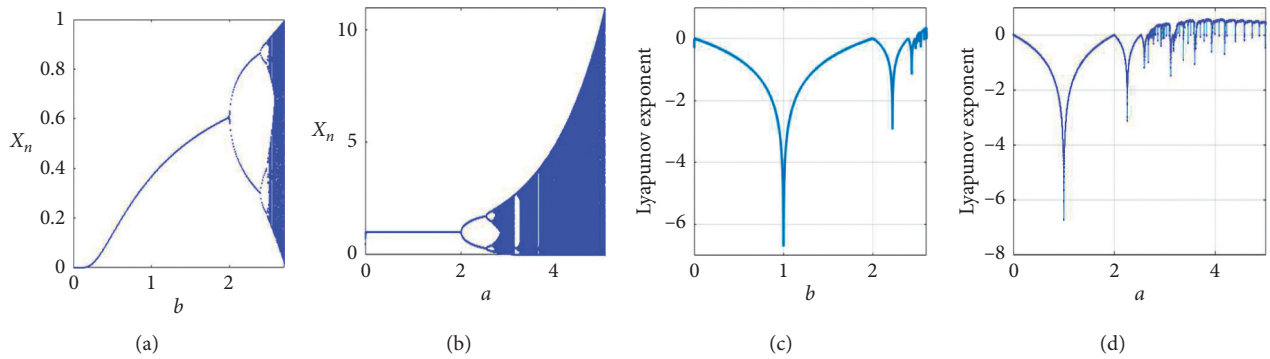


Figure 1: (a), (b) Bifurcation diagram and (c), (d) plot of Lyapunov exponents of Gompertz and May maps.

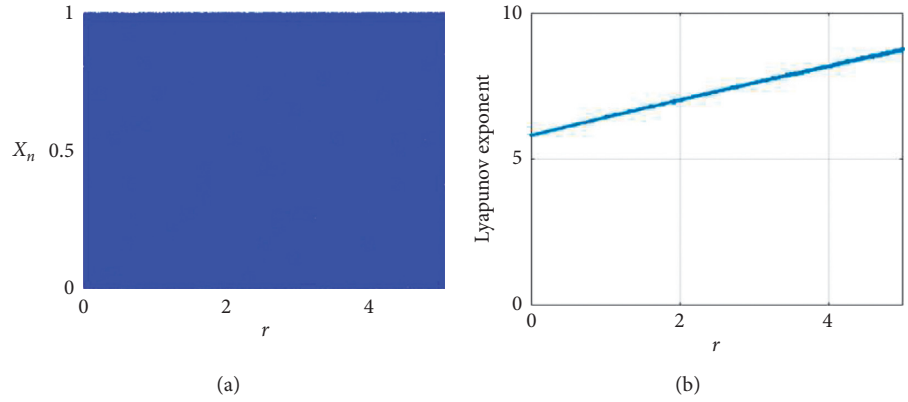


Figure 2: Bifurcation diagram (a) and Lyapunov exponent (b) of May-Gompertz maps.

Table 1: NIST SP800-22 test for results of the May-Gompertz system in SC and CDC modes.

Mode	SC		CDC	
Test index	P value	Decision	P value	Decision
Approximate entropy	0.0907	Success	0.4705	Success
Block frequency	0.9972	Success	0.7320	Success
Cumulative sums	0.5263	Success	0.5462	Success
Fast Fourier transform	0.1554	Success	0.2743	Success
Frequency	0.0409	Success	0.9519	Success
Random excursions	0.9896	Success	0.0905	Success
Random excursions variable	0.7604	Success	0.6228	Success
Longest runs of ones	0.2417	Success	0.2735	Success
Rank	0.0528	Success	0.9754	Success
Runs	0.1551	Success	0.2780	Success
Serial	0.5869	Success	0.4908	Success
Universal statistical	0.9792	Success	0.8975	Success

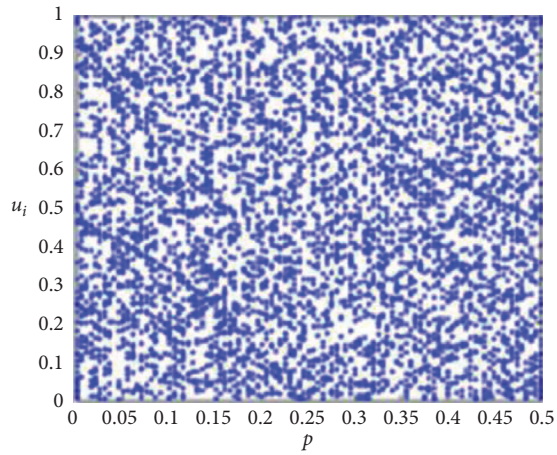


Figure 3: Distribution of u_i with different values of the control parameter p.

3. Key Generation Procedure

The importance of the key and its confidential nature cannot be overemphasized, knowing that the key is mandatory for decryption. The goal is to design such that the key cannot be computed by an attacker. In the following lines, we describe the key generation technique we devised for the proposed cryptosystem. Initial conditions of May-Gompertz were determined by the SHA-256 function. The key generation process was designed so as to be dependent on hash of the plain image. In fact, the one-time pad scheme guarantees high sensitivity to even the slightest bit change in the image: two images encrypted with a different bit will have different NPCR values [39].Thus, the slightest change of a bit of the image modifies the value of the key, therefore of the random

sequence, which is not the case when the key is chosen randomly from a secure pseudo-random number function. This precaution was taken in order to protect the final cryptosystem from attacks. The procedure is as follows. The hash value of the plain image I of size $M \times N$ was computed by the SHA-256 function. The 64-hexadecimal digit obtained was divided into 8 sequences of 8 hexadecimal digits each. Let d_i $(i = 1, \ldots, 8)$ be these parts. Using equation (3), the values of each part were converted into decimal:

$$h_i = \text{hex2dec}(d_i), \quad (i = 1, \ldots, 8). \tag{3}$$

To generate three different sequences of the May-Gompertz system described in equation (1), the initial conditionsx_{01}, x_{02}, and x_{03} and the control parameter r for the three sequences were derived from equation (4). The first sequence was used in the block's permutation process and the two others in the mixing procedure of the proposed scheme.

$$\begin{aligned} x_{01} &= \left(\frac{h_1}{2^{32}}\right), \\ x_{02} &= \left(\frac{h_2}{2^{32}}\right), \\ x_{03} &= \frac{\left(\left(h_3/2^{32}\right)/\left(h_4/2^{32}\right)\right)}{2}. \end{aligned} \tag{4}$$

The control parameter r of the May-Gompertz system was obtained using the following equation:

$$r = 4.9 + \frac{\text{mean}\,(I)}{\max\,(I) + 1}, \tag{5}$$

where $\text{mean}\,(I)$ and $\max\,(I)$ are, respectively, the average and maximum values of the pixel's intensities of image I.

Similarly, the parameters of PWLCM, i.e., the initial conditions x_0, x_1 and the control parameters p_0, p_1, which were used at the second stage of permutation on the pixel level are computed by the following relation:

$$\begin{aligned} x_0 &= \left(\frac{h_5}{2^{32}}\right), \\ x_1 &= \left(\frac{h_6}{2^{32}}\right), \\ p_0 &= \left(\frac{h_7}{2^{33}}\right), \\ p_1 &= \left(\frac{h_8}{2^{33}}\right). \end{aligned} \tag{6}$$

4. Proposed Encryption Algorithm

The flowchart of the proposed algorithm comprises three main stages which are two permutation steps and the mixing step, illustrated in Figure 4. The proposed scheme is designed

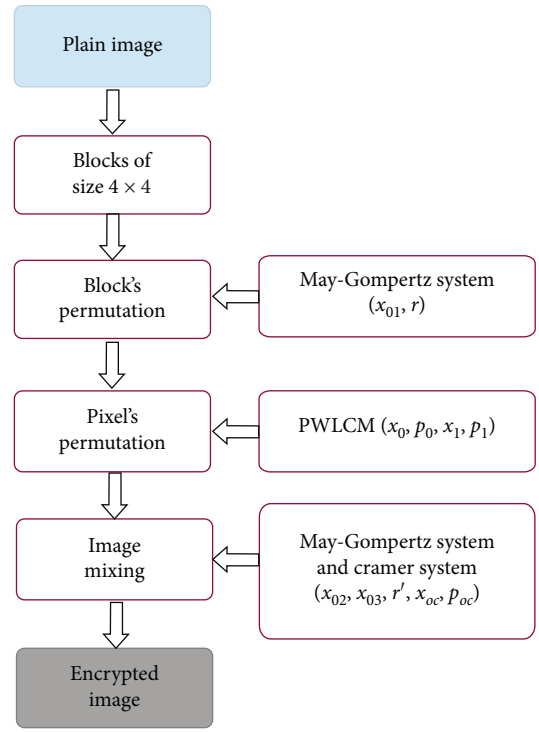


Figure 4: Flowchart of the encryption algorithm.

to encrypt one or several images of different types. In the case where the plain image consists of a single source of information, the permutation at the pixel level is sufficient to perform the confusion operation. On the contrary, when the input image is rather made up of several sources of information (different juxtaposed images), it is necessary to carry out a first level of permutation at the block level in order to reduce the coherence between different source images by generating a noncoherent synthesis image. For this purpose, we have chosen the block permutation of the plain images because it is less time consuming [40–42], increases the disorder in the processed image, and brings the pixels of images that have nothing in common closer to them. In other words, block permutations allow building from several images, a new image that is poorly correlated and visually unusable. On the contrary, this first level of permutation, which yields a composite image, prepares the second phase of permutation which is done at the pixel level. The latter is done to reinforce the visual incoherence of the preprocessed image, i.e., by further increasing the clutter in the image. The third encryption step carried out by the mixing operation contributes to modify the value of the pixels of the swapped image, thus contributing to raise the level of security while preserving the good quality of the source images.

In this section, each of the three steps of the proposed scheme is presented and summarized by an algorithm. In order to avoid the transient effect, in each algorithm, the first 300 iterations are discarded for each map used.

4.1. Blocks' Permutation of the Plain Image. The first encryption level is operated by interchanging different sub-block's positions of the plain image with the aim to degrade

the visual quality of the image and shuffle different blocks of the image. In a specific way, when the input image is made of various source images combined into one, the block's permutation performs a mixing process of different components and contributes to make the output image more confused. The block's permutation process is described in Algorithm 1.

An example of the subdivided image (Step 1) and its permuted blocks (Step 4) of Algorithm 1 are shown in Figure 5. We realized that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy, and therefore reduction of intelligible information present in the image.

4.2. Pixels' Permutation of the Plain Image. This permutation was carried out along rows and columns, as described in Algorithm 2.

4.3. Image Fusion or Mixing

4.3.1. Illustration of the Fusion Procedure. The mixing step consisted in subdividing the image into many subblocks and combining them with random matrices according to a predefined transformation. This transformation was able to modify the values of pixels in the image. In this contribution, the image I was first of all divided into two subblocks I_1 and I_2 of same size. The two image blocks were then fused in a process as described in Algorithm 3.

During our experiments, we realized that equation (8) had to be performed twice in order to obtain the best results. Furthermore, this equation (8) can be generalized into a Kramer system of order n by subdividing the permuted image I and the random matrices r and Winto n blocks of equal size as shown by the following relation:

$$\begin{pmatrix} C_1' \\ \vdots \\ C_n' \end{pmatrix} = \begin{pmatrix} I_{11} & \cdots & I_{1k} \\ \vdots & \ddots & \vdots \\ I_{l1} & \cdots & I_{lk} \end{pmatrix} \times \left[r_{i,j}\right] \oplus \left[\text{floor}\left(W_i \times W_j\right) \times 10^{15}\right], \tag{7}$$

where $[c] = [C_1', C_2', \ldots, C_n']$ and l and k are, respectively, equal to $(N/4)$ and $(M/4)$, with $[N, M]$ being the size of image I. The elements $\{I_{lk}\}$ are the subblocks of image I, $n = l * k$, i and j are taken arbitrarily in between the sets $\{1, 2, \ldots, l\}$ and $\{1, 2, \ldots, k\}$.

4.3.2. Encryption of Multiple Images. A very interesting feature of the proposed cryptosystem is that many images of different types and sizes can be encrypted in one go. It is what we call multiple-image encryption (MIE). So, instead of encrypting images one after another, a number of them can be encrypted simultaneously, resulting in huge time saving.

In order to carry out MIE, all the plain images B_j to be encrypted are fitted into a unique image C (by concatenation) before proper encryption. After the block permutation step, the result is a composite image with subblocks coming from $k$sources: $\{C_i\} = \{B_{1i}\} \cup \{B_{2i}\} \cup \cdots \cup \{B_{ki}\}$. The rest of the procedure is the same. Figure 7 presents an example of the proposed cryptosystem for multiple images. The final encrypted image in this case will be a hybrid image, which contains all relevant information of the image sources. Then, without knowledge of the key, it will be difficult to break the cryptosystem.

4.4. Decryption Steps. The decryption procedure is the reverse of encryption, and the knowledge of the keys is mandatory for decryption.

Let us start from an encrypted image C:

(1) The permuted image can be recovered by solving equation (10) using Kramer's rule, whose unknowns are I_1 and I_2:

$$\begin{cases} \left(I_1 \times r_1 + I_2 \times r_3\right)_{\text{mod}256} = C_1' \oplus \left(\text{floor}\left(W_1 \times W_2\right) \times 10^{15}\right) \\ \left(I_1 \times r_2 + I_2 \times r_4\right)_{\text{mod}256} = C_2' \oplus \left(\text{floor}\left(W_3 \times W_4\right) \times 10^{15}\right), \end{cases} \tag{8}$$

where $I_1 = I(i, j)$ and $I_2 = I(i, j + (M/2))$. Then, the permuted image $I = [I_1, I_2]$. The same approach is used if we subdivide I into n subblocks.

(2) The plain image can be recovered after applying the reverse byte permutation and reverse block permutation successively on the image obtained in Step 1.

5. Experimental Result Analysis

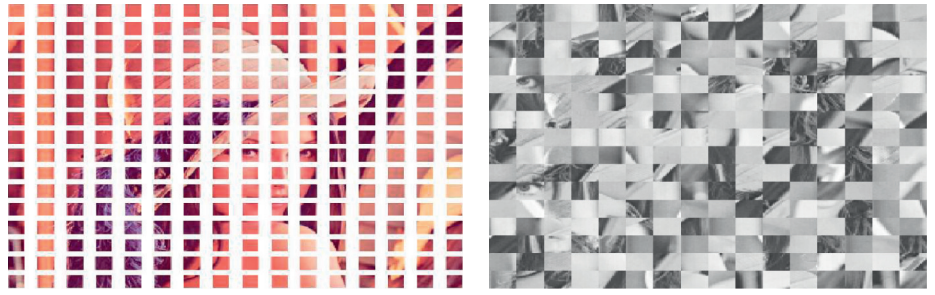
The proposed cryptosystem analysis is presented in this section. Grey and colour images (cameraman, peppers, plane, Lena, and mixture) were used in our database. They were of size $n \times m$ with $n = m$ for some and $n \neq m$ for others in order to treat all possible cases. These images are displayed in Figure 8. Simulations were carried out using the MATLAB 2016b platform, with a core processor (TM) i7-353U, 2.5 GHz, and a 4.0 GB memory. In order to appreciate the efficiency and robustness of the proposed cryptosystem against the main attacks, many tests (key test, spatial complexity, and encryption time evaluation) and analyses (statistical analysis, differential attack analysis, and security and noise analyses) were performed. The parameters that constitute the key of this cryptosystem were made of the initial conditions and control parameters of the two pseudo-random generators used. The colour Lena (512×512) image was used to compute the hash values with the SHA-256 function.

The values of elements of the key used for simulation were $x_{01} = 0.351482953177765$; $x_{02} = 0.972970074275508$; $x_{03} = 0.144375115865841$; $r = 4.934980827591863$; $x_0 = 0.788$; $x_1 = 0.209$; $p_0 = 0.391$; $p_1 = 0.363$; $x_{0c} = 0.041$; $p_{0c} = 0.397$; and $r' = 4.728$.

5.1. Statistical Analysis. Three metrics, namely, histogram, entropy of information, and correlation between adjacent pixels, are used in this section to assess the robustness of the system.

(1) Divide the plain image $\mathbf{I}$ of size $\mathbf{N} \times \mathbf{M}$ into $\mathbf{k}$ blocks of size (4×4), with $\mathbf{k} = (\mathbf{N}/4) \times (\mathbf{M}/4)$.
(2) Use initial condition $\mathbf{x}_{01}$ and control parameter $\mathbf{r}$ of the May-Gompertz system to generate a chaotic sequence by iterating equation (1) k times. The values obtained are stored in the row vector $\mathbf{P}$ of size $(1\mathbf{k})$.
(3) Sort the chaotic sequence $\mathbf{P}$ in the ascending order and get a new sequence $\mathbf{P}' = \{\mathbf{P}'_{\mathbf{i}}\}_{\mathbf{k}} = \{\mathbf{P}'_{\mathbf{t1}}, \mathbf{P}'_{\mathbf{t2}}, \ldots, \mathbf{P}'_{\mathbf{tk}}\}$. Therefore, the sequence $\mathbf{t}_1$, $\mathbf{t}_2$,. . ., $\mathbf{t}_{\mathbf{k}}$ is the permutation of the sequence 1, 2, . . ., $\mathbf{k}$.
(4) Number all the blocks of the plain image obtained at Step 1, and adjust their positions following the permutations of Step 3. Then, the image obtained is a block permuted image (less correlated).

Algorithm 1: Pseudo-code of block's permutation.



(a) (b)

Figure 5: Example of the concatenated image and block permutation. (a)256×256 Lena-subdivided $(16 \times 16$ blocks). (b) Lena-permuted blocks.

(1) Use initial condition and control parameter of the PWLCM, $\mathbf{x}_0$,$\mathbf{p}_0$ and $\mathbf{x}_1$, $\mathbf{p}_1$, respectively, in horizontal (row) and vertical (column) directions for pixels' permutation
(2) Iterate the PWLCM system of equation (2) N times for rows and M times for columns
(3) Take out the values and sort them in the ascending order
(4) For each couple row-column of a pixel's position, find the previous position of the corresponding row-column of the pseudo-random number-sorted value and substitute
(5) Permute the position of the last pixel of the permuted matrix with the real one

Algorithm 2: Pseudocode of pixels' permutation.

(1) Divide the image $\mathbf{I}$ (permuted image) of size $[\mathbf{N}, \mathbf{M}]$ into two parts $\mathbf{I}_1$ and $\mathbf{I}_2$ of the same size. $I_1 = I\,(i, j)$ and $I_2 = I\,(i, j + M/2)$, with $i = 1, \ldots, N$ and $j = 1, \ldots, (M/2)$.
(2) Choose initial conditions $\mathbf{x}_{02}$, $\mathbf{x}_{03}$ and control parameter $\mathbf{r}\prime$ to generate two chaotic sequences $\mathbf{X}$ and $\mathbf{Y}$ by iterating equation (1) of the May-Gompertz system $\mathbf{N} \times \mathbf{M}$ times.
(3) Also, divide $\mathbf{X}$ and $\mathbf{Y}$, respectively, into two subblocks of the same size (see Figure 6).$X = [r_1, r_2]$, where $r_1 = X\,(i, j)$ and $r_2 = X\,(i, j + M/2)$, with $i = 1, \ldots, N$; $j = 1, \ldots, M/2$, $Y = [r_3, r_4]$, where $r_3 = X\,(i, j)$ and $r_4 = X\,(i, j + M/2)$, with $i = 1, \ldots, N$; $j = 1, \ldots, M/2$.
The values of X and Y must be integer values in order to recover all the information during the decryption phase. For the simulations, we have chosen $r_i = r_i \times 10^{12}\,(i = 1, \ldots, 4)$.
(4) Choose initial conditions and control parameters, $\mathbf{x}_{0\mathbf{c}}$ and $\mathbf{p}_{0\mathbf{c}}$, to generate a chaotic sequence $\mathbf{W}$ by iterating equation (2) of the PWLCM system $2\mathbf{N} \times 2\mathbf{M}$ times. The values obtained are stored in an array of size $[2\mathbf{N}, 2\mathbf{M}]$.
(5) Subdivide the array $\mathbf{W}$ into 4 parts, each having the same size of the image I.
(6) Combine the two blocks $\mathbf{I}_1$ and $\mathbf{I}_2$ of the permuted image using the nonlinear relationship defined by equation (8) to get the ciphered image. $\{C'_1 = (I_1 \times r_1 + I_2 \times r_3)_{\mathrm{mod}\,256} \oplus (\mathrm{floor}\,(W_1 \times W_2) \times 10^{15}), C'_2 = (I_1 \times r_2 + I_2 \times r_4)_{\mathrm{mod}\,256} \oplus (\mathrm{floor}\,(W_3 \times W_4) \times 10^{15})$,
where $C\prime = [C'_1, C'_2]$ represents the fused image (encrypted), with $C'_1 = C\prime\,(i, j)$ and $C'_2 = C\prime\ \ (i, j + (M/2))$, $i = 1, \ldots, N$; $j = 1, \ldots, (M/2)$, and floor(X) rounds the elements of X to the nearest integers.

Algorithm 3: Pseudo-code of the mixing process.

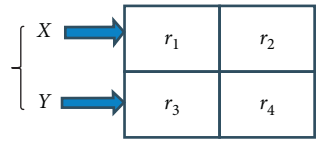
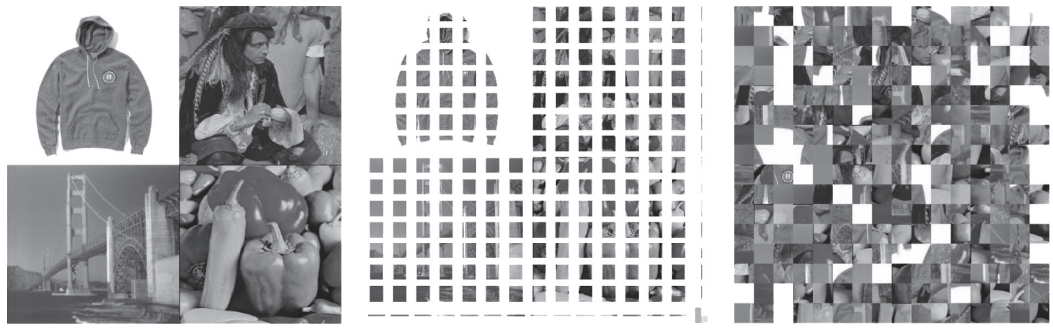


Figure 6: Pseudo-random matrices X and Y of the May-Gompertz system segmented in subblocks.



(a) (b) (c)

Figure 7: Example of the block's permutation process for MIE. (a) Composite image of size 512×512. (b) Image subdivided into blocks of size 32×32. (c) Image after permutation of blocks.

5.1.1. Histogram and Variance of the Histogram. The histogram of an image is a metric, which indicates the frequency of each grey level in the image. For a well-ciphered image, all the frequencies must be uniformly distributed. As one can see in Figure 8, the grey levels of the ciphered images (cameraman, peppers, plane, and mixture) look flat as expected. The same result can be confirmed by computing the variance of the histogram as follows [38]:

$$\mathrm{Var}(y) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}\left(y_i - y_j\right)^2, \tag{9}$$

where Y is a one-dimensional array of the histogram values, $\{i, j\} \in \{1, 2, \ldots, 256\}$, and y_i and y_j denote the numbers of pixel's values, respectively, equal to i and j. For a sample of images, the values of variance of the histogram of plain and ciphered images are displayed in Table 2, and those of ciphered images differ totally from their corresponding plain images. It is therefore obvious that our cryptosystem is safe from statistical attacks.

5.1.2. Correlation Analysis. The correlation coefficient (C_c) measures the strength of the relationship between two adjacent pixels in an image. C_c tends to either 1 or −1 for strong correlation and towards zero for poor correlation. The mean value of the correlation coefficient of a ciphered image for a good cryptosystem should be nearly equal to zero. Equation (12) is used to compute the correlation coefficients in horizontal, vertical, and diagonal directions, respectively [13]:

$$C_c = \frac{N \times \sum_{i=1}^{N} X_i Y_i - \sum_{i=1}^{N} X_i^2 \times \sum_{i=1}^{N} Y_i^2}{\sqrt{\left(N \times \sum_{i=1}^{N} \sum_{N}^{(X_i)^2} - \left(\sum_{i=1}^{N} X_i\right)^2\right) \times \left(N \times \sum_{i=1}^{N} (Y_i)^2 - \left(\sum_{i=1}^{N} Y_i\right)^2\right)}}, \tag{10}$$

where X and Y represent the values of two adjacent pixels in the image, C_c belongs to the range [−1, 1], and N denotes the number of pairs of pixels randomly selected. The computed values of correlation coefficient of some plain images in three different directions are shown in Table 3. From this table, we observe that the average value of the correlation coefficients for the plain images is 0.97, which indicates a strong correlation between the adjacent pixels. Conversely, the mean value of correlation coefficients of ciphered images is 0.008, which is an indication of a poor correlation between adjacent pixels as expected. This result can be confirmed by observing Figures 9(a)–9(c) which show strong correlation between the pixels of the cameraman plain image in each direction. On the contrary, Figures 9(d)–9(f) show that the cipher cameraman image is poorly correlated in all directions. Therefore, we can conclude that correlation attacks cannot succeed with the proposed cryptosystem.

5.1.3. Entropy Analysis. In information theory, the information entropy quantifies the degree of randomness in a set of data. Let y be a sequence of data; the entropy is computed by the following equation [45]:

$$S(y) = \sum_{i=0}^{2^M-1} P(y_i)\log_2\left(\frac{1}{P(y_i)}\right), \tag{11}$$

where $P(y_i)$ is the probability of the recurrence of the pixel value y_i and M denotes the maximum number of bits used to represent the information y. The expected entropy value of an encrypted image coded on 8 bits with the same probability is 8 [46]. Different values of entropy of some encrypted images are shown in Table 4. As can be seen, they are very close to 8 as expected. Comparing with values from recent good standing papers [4, 28], our metrics are either better or in the same range.

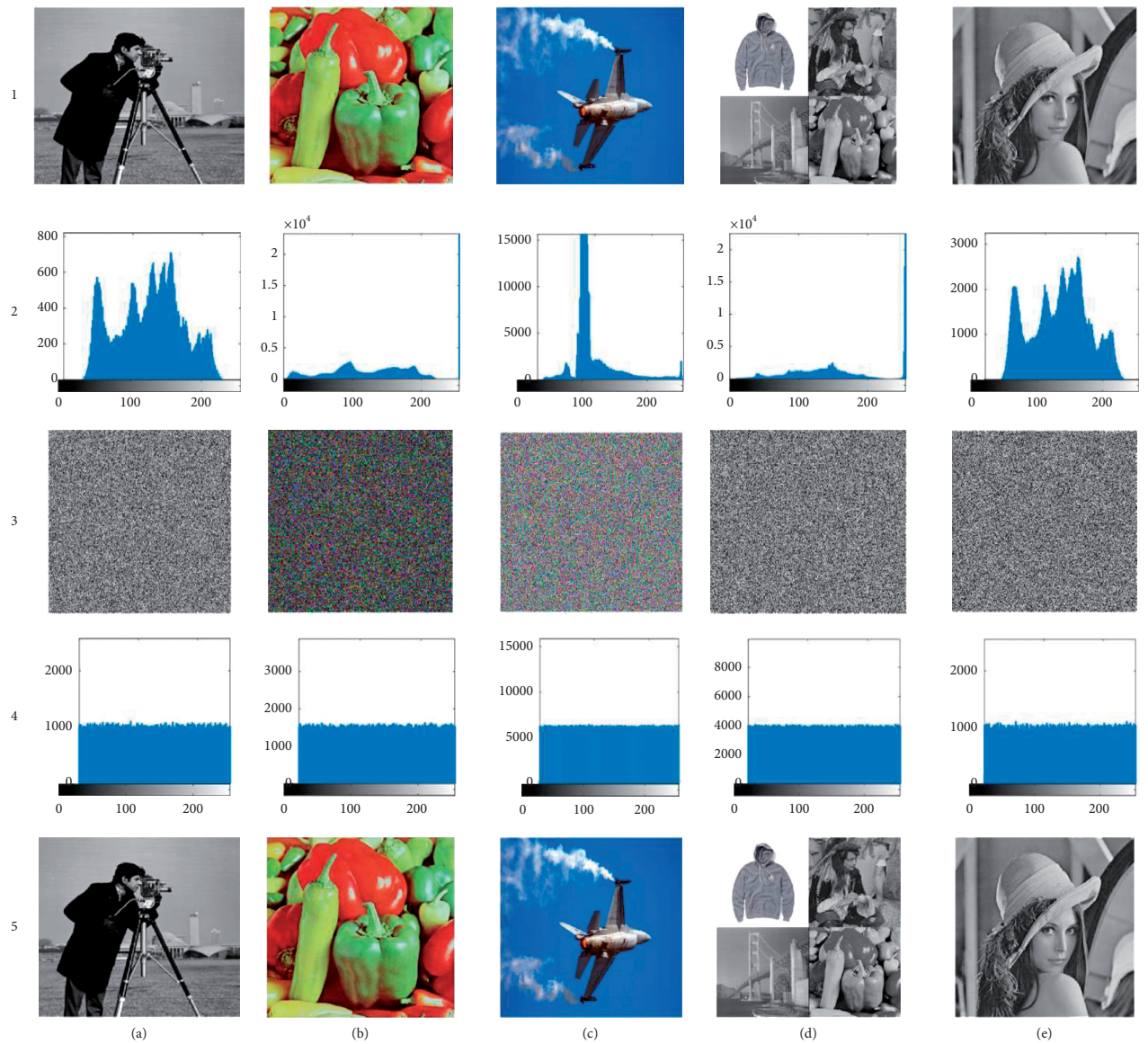


Figure 8: Encryption and decryption results for some plain images: (a) cameraman, (b) peppers, (c) plane, (d) mixture, and (e) Lena. From top to bottom: the input image and its histogram, the encrypted image and its histogram, and the decrypted image.

Table 2: Variance of histograms for plain and ciphered images from the proposed scheme.

Image	Ciphered image		Ciphered image		
	Proposed scheme		[38]	[37]	[43]
Cameraman (256 × 256)	5.129×10^{6}	5347.24	5482.6	—	—
Mixture (512 × 512)	6.255×10^{5}	4278.6	—	—	—
Peppers (512 × 512)	6.892×10^{6}	5263.5	—	—	—
Plane (900 × 600)	7.451×10^{5}	4763.28	—	—	—
Lena (512 × 512)	6.255×10^{6}	4148.5	5450.8	1050.87	1077

5.2. Key Test

5.2.1. Key Space Analysis. A way to prevent a cryptosystem from the brute-force attack is to design a large key space. In a chaotic system, the high sensitivity to initial conditions improves on the security of the cryptosystem [48]. In the literature, a key space of at least 10^{30} is required for the system to be robust [49]. The key's parameters used in the proposed cryptosystem are $(x_{01}, x_{02}, x_{03}, x_0, x_{0c}, x_1)$, i.e., initial conditions and control parameters $(p_0, p_1, p_{0c}, r, \text{and } r\prime)$ of chaotic maps. Assume that the computer accuracy is 10^{-15}, and the key space is $10^{15\times11}$ =

Table 3: Correlation coefficient of images before and after encryption.

Plain image	Size	Cor. coef.	Original image		Ciphered image	
			Proposed scheme		[38]	[44]
Cameraman	(256 × 256)	HC	0.9314	−0.009	−0.009	—
		VC	0.9400	0.014	0.010	
		DC	0.8931	−0.006	−0.006	
Lena	(512 × 512)	HC	0.9849	0.001	0.001	0.008
		VC	0.9928	−0.011	−0.014	0.001
		DC	0.9734	−0.006	−0.006	−0.004
Plane	(900 × 600)	HC	0.9956	0.002	—	0.013
		VC	0.9942	−0.012		0.012
		DC	0.9951	0.017		−0.003

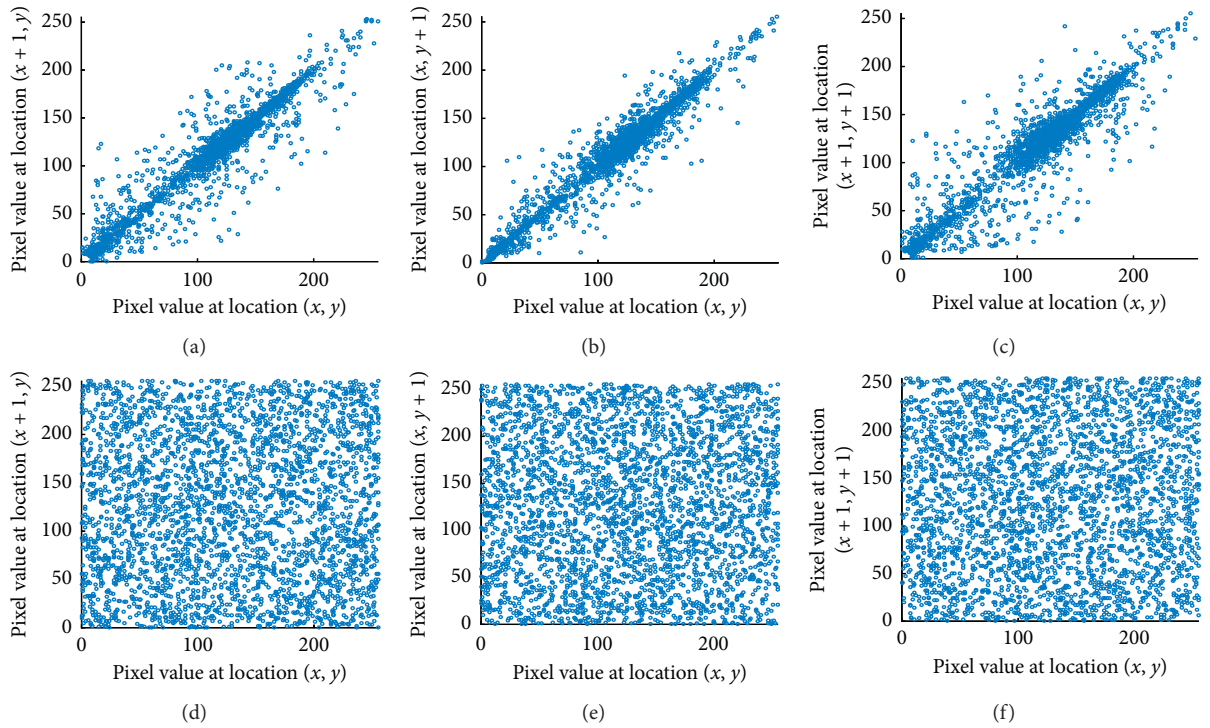


Figure 9: Pixel value distribution of plain and cipher cameraman (256 × 256).

Table 4: Information entropy of different encrypted images.

Image	Proposed scheme	[38]	[47]	[28]
Cameraman (256 × 256)	7.9992	7.9971	—	—
Lena (512 × 512)	7.9993	7.9994	7.9993	7.9975
Peppers (512 × 512)	7.9993	—	7.9992	7.9991
Plane (900 × 600)	7.9996	—	—	—
Mixture (512 × 512)	7.9993	—	—	—

10^{165}, sufficient to resist any brute-force attack. Moreover, the problem of weak key encountered in several encryption algorithms, as mentioned by Teh et al. in [22], does not arise in the proposed cryptosystem. Indeed, the bifurcation diagram of the May-Gompertz map does not show periodic zones; thus, the values chosen as initial conditions and control parameter for this map cannot lead to nonchaotic behaviour. Similarly, parameters of the PWLCM used as initial conditions were chosen out of the problematic ones as stated by the National Institute of Standards and Technology (NIST) [39].

5.2.2. Key Sensitivity. Key sensitivity is a necessary feature for a cryptosystem. It implies that any slightest change in the original key used to encrypt the plain image will lead to an

incorrect decrypted image [50]. To test this feature for the proposed cryptosystem, we modified the original key (K_1) (by changing the value of the last digit) from value x_{02} = 0.972970074275508 to 0.972970074275509, while the rest of the parameters remained unchanged to obtain key K_2. The last digit of $p_0$was modified to obtain key K_3, while that of r' was changed and yielded key K_4. The plain image (Figure 8(c)) was decrypted using the keys of this set, one after the other, and the outcome was compared to what was obtained using K_1. Table 5 recapitulates the percentage of difference of different deciphered images as compared to that obtained using K_1. The average difference percentage was 99.62%. The example of the plane image decrypted with slightly modified keys (Figures 10(a) and 10(b)) shows that a slight change to keys leads to decrypted images totally different from the original ones. Therefore, the proposed cryptosystem is sensitive to the key.

Table 5 also reveals that our cryptosystem is more sensitive to key change than the one proposed by Zhang and Wang [47], Zhenjun and Sun [28], and Nkandeu et al. [38].

5.3. Differential Attack Analysis. In a good encryption algorithm, the influence of an infinitesimal pixel change of a plain image in the corresponding cipher image should be high. To quantify the effect of any slight change on the plain image over the ciphered one, two metrics are generally used, namely, the number of pixel change rate (NPCR) and the unified average change intensity (UACI). These quantities are defined by equations (14) and (15), respectively [28]:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%, \tag{12}$$

$$\text{UACI} = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C(i,j) - C\prime(i,j)|}{255}\right] \times 100\%, \tag{13}$$

where C and C' are the encrypted images before and after a slight change, respectively. When $C(i,j) \neq C\prime(i,j)$, $D(i,j) = 1$; else, $D(i,j) = 0$.

Table 6 presents the NPCR and UACI values of different plain images when one bit is changed. We can notice that mean values for NPCR and UACI are, respectively, 99.61 and 33.49. These average values are illustrated in Figure 11, where NPCR (a) and UACI (b) are represented as a function of different values of the key. Then, these results are in the range of accepted values in the literature [50]. This proves that the proposed algorithm is not vulnerable to differential attacks.

5.4. Security Analysis. In order to assess the resistance of encryption algorithms against the main attacks, two tests are generally used, namely, the chosen plain image attack and the chosen cipher image attack [52].

5.4.1. Chosen Plain Image Attack. This attack stems from the idea that two different images encrypted with the key must produce two different ciphered images. Let us assume that an attacker does not possess the encryption key, but has the encrypted image C. He will try to recover the plain images I by applying equations (16) and (17):

$$k_0^{i,j} = C_0^{i,j} \oplus I_0^{i,j}, \tag{14}$$

where $I_0^{i,j}$ is a null image (all the pixels are equal to zero), while $C_0^{i,j}$ is its corresponding cipher image, and (i, j) denotes the 2D position of the pixel.

$$I^{i,j} = C^{i,j} \oplus k_0^{i,j}, \tag{15}$$

where $I^{i,j}$ is an image with the same size as $C_0^{i,j}$ and $C^{i,j}$ is its corresponding encrypted image [38].

As illustrated in Figures 12(a) and 12(c), it appears that the chosen plain image attack on the cameraman encrypted image did not succeed. Therefore, the proposed algorithm has a good ability to resist against the chosen plain image attack.

Table 5: Information entropy of different encrypted images.

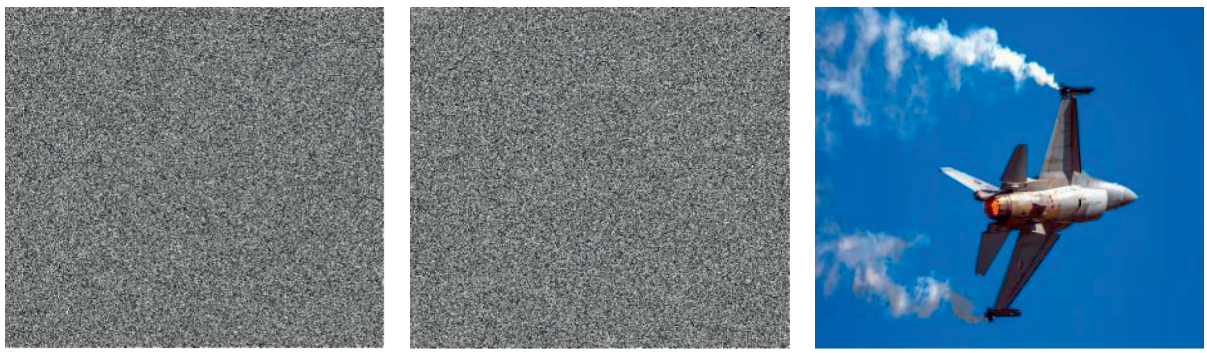
Key	Proposed scheme	[38] (2018)	[48] (2017)	[28] (2016)
Key 1 vs. key 2	99.729	99.61	99.727	99.651
Key 1 vs. key 3	99.803	99.62	99.678	99.605
Key 1 vs. key 4	99.727	99.65	99.769	99.592

5.4.2. Chosen Cipher Attack. The attacker still does not have the key. He uses equation (16) to try to decrypt and obtain the plain image. To achieve its goal, he possesses the null image P_0 and its corresponding encrypted image C_0 and knows the decryption steps [53]. In Figures 12(b) and 12(d), the outcome of this attack using the plane image is displayed. These figures show that the attack was not successful.

5.5. Encryption Time Analysis

5.5.1. Encryption Speed. The encryption time of the proposed algorithm using a colour Lena image of size 512×512 is 0. 2880 s. Table 7 recapitulates the encryption time obtained for different images using our cryptosystem as compared to those of recent algorithms using the same images. The experimental results showed that averagely, the suggested cryptosystem exhibited the best encryption time.

5.5.2. Complexity of the Proposed Scheme. The proposed cryptosystem is based on three main steps including two permutation phases and a mixing phase. Thus, the evaluation of the complexity of the cryptosystem depends on these three encryption steps. Since the permutation process does not require any calculation, but only iterations [37], the whole spatial complexity of the proposed scheme will mainly come from the mixing step. This value can be estimated at $\Theta(1 \cdot M \cdot N)$ on a PC with a multiple-core processor platform, where M and N are the number of rows and columns

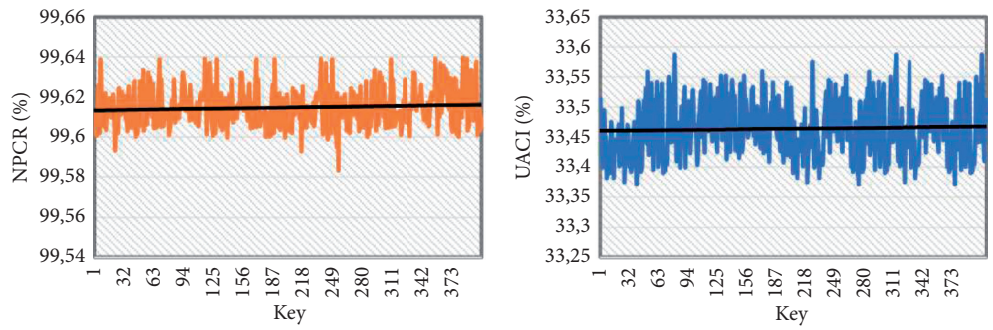


(a) (b) (c)

Figure 10: Key sensitivity tests applied on the plane image: (a) $K2$, (b) $K3$, and (c) $K1$.

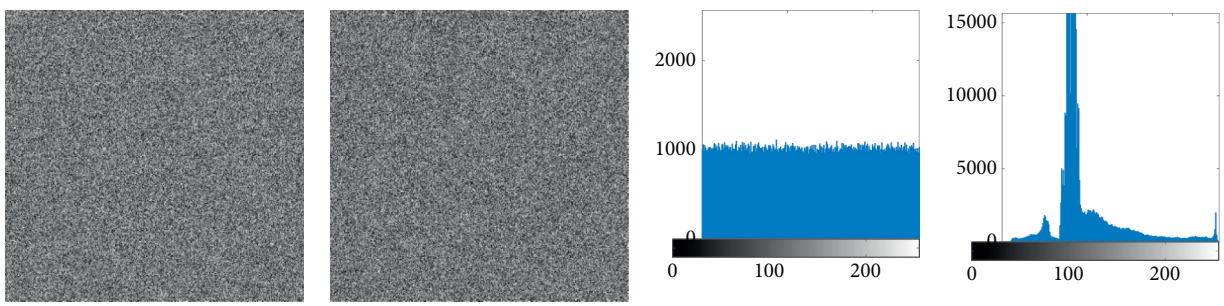
Table 6: UACI and NPCR values of encrypted images.

Plain image	Changed pixel position Metric	First pixel	Middle pixel	[44] (2018)	[37] (2020)	[51] (2020)	Last pixel
Cameraman (256 × 256)	NPCR	99.62	99.61	99.62	—	99.62	99.63
	UACI	33.54	33.55	33.53	—	33.42	33.63
Lena (512 × 512)	NPCR	99.62	99.62	99.61	99.61	99.63	99.62
	UACI	33.46	33.47	33.46	30.47	33.52	33.28
Plane (900 × 600)	NPCR	99.63	99.62	99.62	99.60	—	99.60
	UACI	33.47	33.48	33.47	32.60	—	33.42
Mixture (512 × 512)	NPCR	99.61	99.61	99.61	—	—	—
	UACI	33.42	33.41	33.42	—	—	—



(a) (b)

Figure 11: Average values of NPCR (a) and UACI (b) as a function of different values of the key.



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

Figure 12: Result of cryptanalysis tests on the cameraman image: (a) chosen plain image attack, (b) chosen cipher image attack, (c) histogram of image (a), and (d) histogram of image (b).

Table 7: Encryption time in seconds.

Image	Size	Proposed algorithm	[54] 2019	[55] (2018)	[4] (2017)	[28] (2016)
Cameraman	(256×256)	0.2672	0.0949	0.102	—	—
Lena	(512×512)	0.2880	0.4010	0.281	0.7103	0.665
Plane	(900×600)	0.3505	—	—	—	—

(a) (b) (c)

Figure 13: Decrypted image with Gaussian noise: (a) var = 0.4, (b) var = 0.7, and (c) var = 0.9.

of the image. The obtained value is equal or better compared with other schemes developed in [37] ($\Theta(1 \cdot M \cdot N)$), [56] ($\Theta(4 \cdot M \cdot N)$), [57] ($\Theta(24 \cdot M \cdot N)$), and [58]($\Theta(100 \cdot M \cdot N)$).

5.6. Noise Interference Analysis. During image transmission, it may be contaminated by noise. In this section, we assess the stability of the proposed cryptosystem under the influence of noise.

5.6.1. Gaussian Noise Analysis. The Gaussian noise with zero mean defined by equation (18) [59] was used to assess the influence of noise on an encrypted image obtained by the proposed cryptosystem. The test consisted in adding in a plain image some quantity of noise before encryption and then getting the decrypted image affected by the noise to check if it was still recognizable.

$$I = \text{imnoise}(\text{img}, \prime\text{gaussian}\prime, 0, \text{var}), \tag{16}$$

where img and I are, respectively, encrypted image data before and after Gaussian noise was added and var is the noise variance with values ranging from 0.01 to 1.

In Figure 13, the decrypted cameraman image (512×512) affected by the Gaussian noise was presented for three different values of the variance. From this figure, we observed that even for a high value of the variance (var = 0.9), the decrypted image was still recognizable.

5.6.2. Occlusion Noise Analysis. In order to simulate the influence of noise on the encrypted image during transmission, percentages of noise, respectively, 25% and 50%, were added to the pixels of Lena encrypted image as shown in Figures 14(a) and 14(b). The black pixels represented the percentage of data lost during the transmission process.

Although the input encrypted image had been affected by the occlusion noise, it could still be perceptible as seen in Figures 14(c) and 14(d). Finally, based on the above last two sections' tests, we concluded that the proposed algorithm presented a high stability and robustness against noise.

5.6.3. Peak Signal-to-Noise Ratio (PSNR). The PSNR is a tool used to evaluate the difference between the plain image and the corresponding encrypted image. This measure informs about the level of degradation of the plain image after the encryption process. For a good cryptosystem, the PSNR value must be below dB [60]. The PSNR is defined by the following relation:

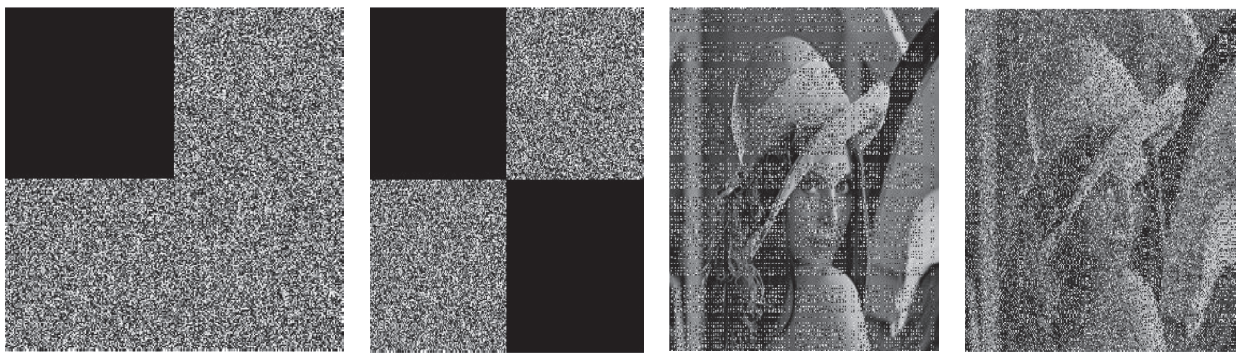
$$\text{PSNR} = 10 \log_{10}\left(\frac{255^2}{\text{MSE}}\right) (\text{dB}), \tag{17}$$

where MSE is the mean square error defined by

$$\text{MSE} = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M \times N}. \tag{18}$$

Table 8 presents the values of MSE and PSNR of the proposed cryptosystem. We can notice from this table that the values of MSE are low, then leading to best values of PSNR.

5.7. Comparison of the Proposed Scheme with Other Recent Encryption Algorithms. Table 9 shows the performance of the proposed algorithm compared to mostly cited and good standing ones in the literature. Comparative tests were carried out, and the Lena image of size 512×512 was used as an example. From Table 9, we can observe that the proposed encryption algorithm has the best value of entropy, a large key space that gets close to the best performances presented in [62, 63, 69–71], and a good encryption time compared to others. As for UACI and NPCR, they are very close to the



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

Figure 14: Encrypted and decrypted Lena (512 × 512) image with occlusion noise. (a) Encrypted image with 25% occlusion noise. (b) Encrypted image with 50% occlusion noise. (c) Decrypted image with 25% occlusion noise. (d) Decrypted image with 50% occlusion noise.

Table 8: Values of the MSE and PSNR of the proposed cryptosystem.

Image	Size	MSE	Proposed scheme	PSNR (dB)		
				[61]	[44]	[60]
Cameraman	(256 × 256)	1.01402×10^4	8.0700	7.436	—	—
Lena	(512 × 512)	1.12934×10^4	7.6030	8.586	8.604	8.1102
Plane	(900 × 600)	1.341780×10^4	6.8540	—	7.975	—
Mixture	(512 × 512)	1.274205×10^4	7.0780	—	—	—

Table 9: Comparison of some recent works with the proposed one.

	Key space	Key sensitivity	Average correlation	Entropy	NPCR	UACI	Encryption time (s)
Proposed algorithm	10^{165}	99.62	0.004	7.9993	99.62	33.46	0.2880
[62] (2020)	10^{238}	—	0.003	7.9980	99.68	33.47	—
[51] (2020)	10^{112}	99.60	0.004	7.9970	99.61	33.43	0.251
[63] (2020)	10^{206}	—	0.004	7.9976	99.60	33.47	—
[64] (2020)	10^{120}	—	0.051	7.9991	99.56	33.43	—
[65] (2020)	10^{142}	—	0.023	7.9992	99.61	33.45	—
[66] (2020)	10^{105}	99.04	0.003	7.9975	99.60	—	0.52
[67] (2020)	10^{135}	—	0.0202	7.9974	99.60	33.55	0.5156
[68] (2020)	2^{192}	—	0.002	7.9974	99.59	33.45	—
[37] (2020)	10^{120}	—	0.003	7.9993	99.59	33.50	0.402
[69] (2020)	$(28 \times 28)! \times 2196644$	—	0.005	7.9972	99.60	33.50	1.9143
[70] (2020)	$2^{(8 \times 65536 + 1)}$		0.004	7.9972	99.62	30.91	—

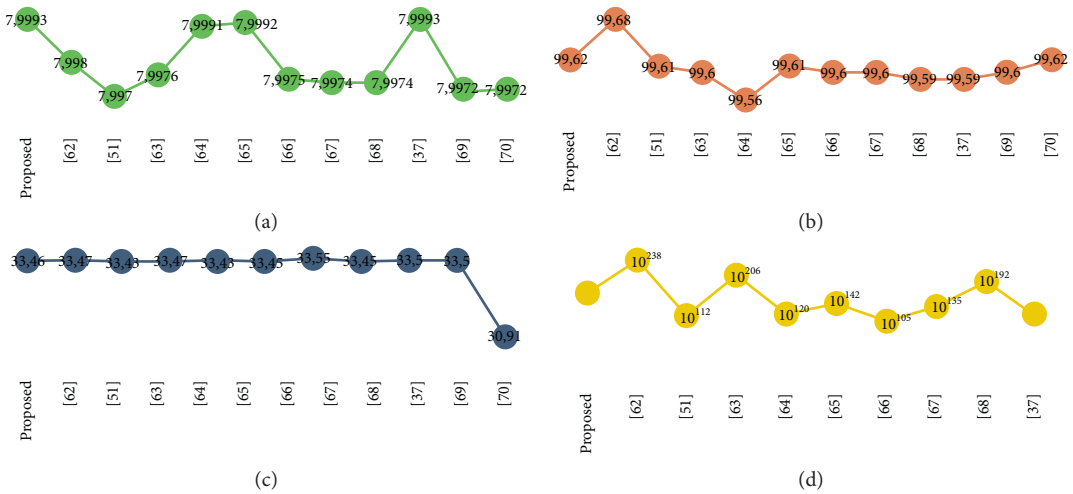


Figure 15: Plot of some metrics of the proposed scheme compared with recent others: (a) entropy, (b) NPCR, (c) UACI, and (d) key space.

theoretical optimal values expected, i.e., 33.4635% for UACI and 99.6904% for NPCR [9]. Finally, our cryptosystem exhibits a good correlation value. The good performances of the proposed schemes compared with recent others are clearly illustrated in Figure 15.

6. Conclusion

In this paper, a new two-step image encryption algorithm was designed. After partitioning the image into subblocks, the first step consisted of carrying out a pseudo-random block permutation (using the May-Gompertz map) followed by a pseudo-random pixel permutation (using the PWLCM). In the second step, the result of the first step is divided into 4 subimages, which were then fused by means of pseudo-random matrices obtained from May-Gompertz and PWLCM concurrently. The key space of the proposed cryptosystem is large, and some elements of the keys are dependent on image pixels' values in such a way that each cipher image is specific to the original plain image. The analysis of experimental results reveals that the new algorithm is very efficient and secure, which is suitable for practical image encryption. The proposed cryptosystem particularly exhibits best results for $p = 2$ rounds. Moreover, encryption/decryption time is short enough for the proposed scheme to be used for multimedia communication, especially for video encryption. Finally, the proposed algorithm exhibits high security due to the improvement of chaotic properties of the maps used. It also offers the possibility of multiple-image encryption and proved to be robust when faced with noise and data loss.

Data Availability

The data used to support the findings of this study were taken from the internet. (https://homepages.cae.wisc.edu/~ece533/images/ for most).

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

The authors wish to thank Ms. Shemminra Yunnus from the University of Cape Coast, Ghana, for proofreading this paper.

References

[1] A. Bisht, M. Dua, and S. Dua, "A novel approach to encrypt multiple images using multiple chaotic maps and chaotic discrete fractional random transform," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 9, pp. 3519–3531, 2019.

[2] S. Pan, J. Wei, and S. Hu, *A Novel Image Encryption Algorithm Based on Hybrid Chaotic Mapping and Intelligent Learning in Financial Security System*, pp. 9163–9176, Springer, New York, NY, USA, 2020.

[3] K. Dharavathu and S. Anuradha, *Efficient Transmission of an Encrypted Image through a MIMO – OFDM System with Different Encryption Schemes*, Springer, New York, NY, USA, 2020.

[4] X. Zhang and X. Wang, *Multiple-image Encryption Algorithm Based on DNA Encoding and Chaotic System*, pp. 7841–7869, Springer, New York, NY, USA, 2019.

[5] H. Chen, C. Tanougast, Z. Liu, W. Blondel, and B. Hao, "Optical hyperspectral image encryption based on improved Chirikov mapping and gyrator transform," *Optics and Lasers in Engineering*, vol. 107, pp. 62–70, 2018.

[6] Y. A. S. Hi, Y. O. L. Iu, W. E. I. S. Heng, D. A. B. O. Z. Hu, and J. I. W. Ang, "Rotations of a random phase mask with spatially incoherent illumination," *Optics Express*, vol. 27, no. 18, pp. 26050–26059, 2019.

[7] W.-H. Chen, S. Luo, and W. X. Zheng, "Impulsive synchronization of reaction-diffusion neural networks with mixed delays and its application to image encryption," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 27, no. 12, pp. 2696–2710, 2016.

[8] A. Belazi, M. Talha, S. Kharbech, W. Xiang, and S. Member, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.

[9] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.

[10] C. Wu, Y. Wang, Y. Chen, J. Wang, and Q.-H. Wang, "Asymmetric encryption of multiple-image based on compressed sensing and phase-truncation in cylindrical diffraction domain," *Optics Communications*, vol. 431, pp. 203–209, 2019.

[11] X. Yuan, L. Zhang, J. Chen, K. Wang, and D. Zhang, "Multiple-image encryption scheme based on ghost imaging of Hadamard matrix and spatial multiplexing," *Applied Physics B*, vol. 125, no. 9, pp. 1–13, 2019.

[12] R. Hamza and K. Muhammad, "Hash based encryption for keyframes of diagnostic hysteroscopy," *Computer Vision and Image Analysis*, vol. 5, 2018.

[13] M. Alfalou, "AymJridi and An, "Real-time and encryption efficiency improvements of simultaneous fusion , compression and encryption method based on chaotic generators," *Optics and Lasers in Engineering*, vol. 102, pp. 59–69, 2018.

[14] J. Chen, L. Chen, L. Y. Zhang, and Z.-L. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 301–322, 2019.

[15] M. Li, D. Lu, Y. Xiang, Y. Zhang, and H. Ren, "Cryptanalysis and improvement in a chaotic image cipher using two-round permutation and diffusion," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 31–47, 2019.

[16] X. Zhang and Z. Zhao, "Chaos-based image encryption with total shuffling and bidirectional diffusion," *Nonlinear Dynamics*, vol. 75, no. 1-2, pp. 319–330, 2014.

[17] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.

[18] X. Li, X. Meng, X. Yang et al., "Multiple-image encryption based on compressive ghost imaging and coordinate sampling," *IEEE Photonics Journal*, vol. 8, no. 4, p. 1, 2016.

[19] I. Mehra and N. K. Nishchal, "Wavelet-based image fusion for securing multiple images through asymmetric keys," *Optics Communications*, vol. 335, pp. 153–160, 2015.

[20] Y. Qin, Q. Gong, Z. Wang, and H. Wang, "Optical multiple-image encryption in diffractive-imaging-based scheme using spectral fusion and nonlinear operation," *Optics Express*, vol. 24, no. 23, p. 26877, 2016.

[21] M. I. Elements, T. D. Chaotic, and E. Map, "Encryption algorithm of multiple-lmage using mixed lmage elements and two dimensional chaotic economic map," *Entropy*, vol. 20, no. 801, pp. 1–21, 2018.

[22] J. S. Teh, M. Alawida, and Y. C. Sii, "Implementation and practical problems of chaos-based cryptography revisited," *Journal of Information Security and Applications*, vol. 50, Article ID 102421, 2020.

[23] S. Dongfeng, H. Jian, W. Yingjian et al., "Simultaneous fusion, imaging and encryption of multiple objects using a single-pixel detector," *Scientific Reports*, vol. 7, no. 1, Article ID 13172, 2017.

[24] X. Liu, W. Mei, and H. Du, "Simultaneous image compression, fusion and encryption algorithm based on compressive sensing and chaos," *Optics Communications*, vol. 366, pp. 22–32, 2016.

[25] A. Alfalou, C. Brosseau, N. Abdallah, and M. Jridi, "Simultaneous fusion, compression, and encryption of multiple images," *Optics Express*, vol. 19, no. 24, p. 24023, 2011.

[26] M. Khurana and H. Singh, "An asymmetric image encryption based on phase truncated hybrid transform," *3D Research*, vol. 8, no. 3, 2017.

[27] G.-L. Zhu, "Mixed image element encryption algorithm based on an elliptic curve cryptosystem," *Journal of Electronic Imaging*, vol. 17, no. 2, Article ID 023007, 2008.

[28] J. S. Zhenjun and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps," *Optics and Lasers in Engineering*, vol. 80, pp. 1–11, 2016.

[29] G. Thoms, R. Muresan, and A. Al-Dweik, "Design of chaotic block cipher operation mode for intelligent transportation systems," in *Proceedings of the 2019 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–4, Las Vegas, NV, USA, 2019.

[30] I. F. Elashry, W. El-Shafai, E. S. Hasan et al., "Efficient chaotic-based image cryptosystem with different modes of operation," *Multimedia Tools and Applications*, vol. 79, no. 29-30, pp. 20665–20687, 2020.

[31] O. S. Faragallah, A. Afifi, W. El-Shafai et al., "Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications," *IEEE Access*, vol. 8, pp. 103200–103218, 2020.

[32] J. A. P. Artiles, D. P. B. Chaves, and C. Pimentel, "Image encryption using block cipher and chaotic sequences," *Signal Processing: Image Communication*, vol. 79, pp. 24–31, 2019.

[33] M. Alawida, A. Samsudin, J. S. Teh, and W. H. Alshoura, "Deterministic chaotic finite-state automata," *Nonlinear Dynamics*, vol. 98, no. 3, pp. 2403–2421, 2019.

[34] M. Alawida, A. Samsudin, and J. S. Teh, "Enhanced digital chaotic maps based on bit reversal with applications in random bit generators," *Information Sciences*, vol. 512, pp. 1155–1169, 2020.

[35] B. Yang and X. Liao, "A new color image encryption scheme based on logistic map over the finite field ZN," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 21803–21821, 2018.

[36] W. Wang, "An encryption algorithm based on combined chaos in body area networks," *Computers & Electrical Engineering*, vol. 65, pp. 282–291, 2018.

[37] Y. P. K. Nkandeu, J. R. Mboupda Pone, and A. Tiedeu, "Image encryption algorithm based on synchronized parallel diffusion and new combinations of 1D discrete maps," *Sensing and Imaging*, vol. 21, no. 55, pp. 1–36, 2020.

[38] Y. Pascal, K. Nkandeu, and A. Tiedeu, "An image encryption algorithm based on substitution technique and chaos mixing," *Multimedia Tools and Applications*, vol. 78, pp. 10013–10034, 2019.

[39] G. Za, "Sécurisation par dynamiques chaotiques des réseaux locaux sans fil au niveau de la couche MAC," Ph.D. thesis, University of Toulouse, Toulouse, France, 2013.

[40] L. Liu, Y. Lei, and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation," *IEEE Access*, vol. 8, pp. 27361–27374, 2020.

[41] X. Wang and H. Zhao, "Fast image encryption algorithm based on parallel permutation-and-diffusion strategy," *Multimedia Tools and Applications*, vol. 79, no. 27-28, pp. 19005–19024, 2020.

[42] 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 Dynamics*, vol. 77, no. 4, pp. 1191–1207, 2014.

[43] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," *IET Image Processing*, vol. 10, no. 10, p. 742, 2016.

[44] M. Kumari and S. Gupta, "A novel image encryption scheme based on intertwining chaotic maps and RC4 stream cipher," *3D Research*, vol. 9, no. 1, pp. 1–20, 2018.

[45] W. M. H. Company, *Modern Cryptography: Theory and Practice*, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2003.

[46] A. A. Alzaidi, M. Ahmad, M. N. Doja, E. Al Solami, and M. M. S. Beg, *A New 1D Chaotic Map and β -Hill Climbing for Generating Substitution-Boxes*, IEEE, Piscataway, NJ, USA, pp. 1–9, 2018.

[47] X. Zhang and X. Wang, "Multiple-image encryption algorithm based on mixed image element and permutation," *Optics and Lasers in Engineering*, vol. 92, pp. 6–16, 2017.

[48] S. Koppu and V. M. Viswanatham, "A fast enhanced secure image chaotic cryptosystem based on hybrid chaotic magic transform," *Modelling and Simulation in Engineering*, vol. 2017, Article ID 7470204, 12 pages, 2017.

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

[50] B. Mirzakuchaki, "SattaNorouzi and R, "breaking an image encryption algorithm based on the new substitution stage with chaotic functions," *Optik*, vol. 127, no. 16, 2016.

[51] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, R. Amirtharajan, and R. Amirtharajan, "Hopfield attractor-trusted neural network: an attack-resistant image encryption," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11477–11489, 2020.

[52] M. Ahmad, M. N. Doja, and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *Journal of King Saud University - Computer and Information Sciences*, vol. 33, no. 1, p. 77, 2021.

[53] R. Rhouma and S. Belghith, "Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem," *Physics Letters A*, vol. 372, no. 36, pp. 5790–579410.1016/j.chaos.2007.10.054, 2008.

[54] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.

[55] M. Asgari-chenaghlu, M.-A. Balafar, and M.-R. Feizi-Derakhshi, "A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation," *Signal Processing*, vol. 157, p. 1, 2019.
[56] 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 Dynamics*, vol. 81, no. 1-2, pp. 511–529, 2015.
[57] C.-Y. Song, Y.-L. Qiao, and X.-Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik - International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3329–3334, 2013.
[58] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "An efficient quasigroup based image encryption using modified nonlinear chaotic maps," *Sensing and Imaging*, vol. 15, no. 1, 2014.
[59] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-elyazeed, "Generalized double-humped logistic map-based medical image encryption," *Journal of Advanced Research*, vol. 10, pp. 85–98, 2018.
[60] K. K. Butt, G. Li, and S. Khan, *Fast and Efficient Image Encryption Algorithm Based*, pp. 1–28, 2020.
[61] S. El Assad, *Novel Models of Image Permutation and Diffusion*, 2020.
[62] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Medical & Biological Engineering & Computing*, vol. 58, no. 7, pp. 1445–1458, 2020.
[63] S. Aashiq Banu and R. Amirtharajan, "Tri-level scrambling and enhanced diffusion for DICOM image cipher- DNA and chaotic fused approach," *Multimedia Tools and Applications*, vol. 79, no. 39-40, pp. 28807–28824, 2020.
[64] M. A. B. Farah, R. Guesmi, A. Kachouri, and M. Samet, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Optics & Laser Technology*, vol. 121, Article ID 105777, 2020.
[65] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," vol. 171, 2020.
[66] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," *Neural Computing and Applications*, vol. 32, no. 9, pp. 4961–4988, 2020.
[67] M. Alawida, J. Sen, A. Samsudin, and W. Hamdan, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Processing*, vol. 13, pp. 1–39, 2019.
[68] F. Yu, "Chaos-based application of a novel multistable 5d memristive hyperchaotic system with coexisting multiple attractors," *Complexity*, vol. 2020, Article ID 8034196, , 2020.
[69] A. Rengarajan, "Chua ' S diode and strange attractor: a three-layer hardware-software co-design for medical image confidentiality," *IET Image Processing*, vol. 14, no. 7, pp. 1354–1365, 2020.
[70] R. Sivaraman, S. Rajagopalan, J. Bosco, and B. Rayappan, "Ring oscillator as confusion-diffusion agent: a complete TRNG drove image security," *IET Image Processing*, vol. 14, no. 13, pp. 2987–2997, 2020.
[71] Y. P. K. Nkandeu, J. R. Mboupda Pone, and A. Tiedeu, "Image encryption algorithm based on synchronized parallel diffusion and new combinations of 1D discrete maps," *Sens Imaging*, vol. 21, p. 55, 2020.