Research Article

Image Encryption with Fusion of Two Maps

Yannick Abanda ^{1,2}, **Alain Tiedeu** ^{1,2,3} and **Guillaume Kom** ⁴

¹Signal Image and Systems Laboratory, HTTTC Ebolowa, University of Yaoundé I, P.O. Box 886, Yaoundé, Cameroon

²Centre for Research, Experimentation and Production, HTTTC Ebolowa, University of Yaoundé I, P.O. Box 886, Ebolowa, Cameroon

³Ingénierie Mathématique et Systèmes d'Information, National Advanced School of Engineering, University of Yaoundé I, P.O. Box 8390, Yaoundé, Cameroon

⁴Laboratoire d'Automatique et d'Informatique Appliquée (LAIA), Department of Engineering, IUT-FV Bandjoun, University of Dschang, Dschang, Cameroon

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

Received 9 October 2020; Revised 3 June 2021; Accepted 5 July 2021; Published 15 July 2021

Academic Editor: Goi Bok-Min

Copyright © 2021 Yannick Abanda et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we propose a fusion technique for image encryption combining two maps and generate a new optimized map by fusing Hartley and Duffing chaotic oscillators. In order to measure and quantify the amount of chaos present in data sequences, the resultant map is tested by a new method of nonlinear time series analysis. This test ensures its robustness during its use to construct an encrypted image when combined with some mathematical function that we have designed. The cryptosystem was tested on images such as Lena, Barbara, Mandrill, and Man. The results were compared to those in the literature and proved satisfactory.

1. Introduction

The need to preserve privacy and confidentiality in communications has triggered the rapid development of cryptographic techniques. This has spurred an intense research activity in the field of cryptography. Thanks to their excellent properties of unpredictability, ergodicity, and sensitivity to their parameters and initial values, chaotic maps are good candidates for encryption algorithms. Over the years, many generators of chaos have been used in cryptosystems. However, robustness is still a major challenge in chaos-based cryptosystems. This is shown through the important number of attacked and broken cryptosystems [1–14]. Security defects in cryptosystems are from different origins. Remarkable flaw is the insufficient robustness of chaotic maps used in some encryption algorithms. Indeed, in some chaos-based encryption systems, the link between the control parameters and the secret key is not carefully established. This is because of disappearance of chaos in some portions of the map used, culminating in reduction of the entropy level in the

encrypted image and consequently vulnerability of the system to attacks. Those shortcomings were studied by Huang and Guan [5] and Pareek et al. [6]. Another flaw is the fact that eavesdropper can estimate the control parameters from a chaotic orbit and finally, through this, break the cryptosystem. The work by Skrobek [7] presents the methodology to do that. Several encryption algorithms perform transformation from original to encrypted image by many rounds. For each round, the chaotic map is iterated k times. Then, they use the number of rounds and k as part of the key. Such cryptosystems can be broken through a timing attack which analyzes the encryption/decryption time. An illustration is given in the paper of Pisarchik et al. [8] which was cryptanalyzed by Arroyo and al. [9].

The cryptosystems, in which the transformation from plaintext to ciphertext roughly corresponds to a mapping that depends only on the key, have been found to succumb to known and/or chosen plaintext attacks. For example, the two cryptosystems developed by Patidar et al. [12] have been broken, using different approaches, by Rhouma et al. [2] and

Li et al. [4]. Another example is the algorithm of Guan et al. [10] that has been cryptanalyzed by Çokal and Solak [11].

Insufficient key space has also in the past accounted for a number of cryptosystems being broken. However, this flaw is rather rare these last years, especially with the optimization of one-dimensional (1D) chaotic generators for digital image encryption. This is justified by their ease of implementation, their discretized forms, and their flexibility when it comes to optimizing them [15, 16]. To solve this problem and improve the chaotic maps, many researchers claim that high dimensional (HD) digital chaotic maps have better security and mixing method permits the extension of the period length of chaotic systems in order to get closer to robust chaos. In addition, the absence of periodic windows and coexisting attractors in some neighborhood of the parameter space means the improvement of the dynamic degradation.

In this paper, we develop a new cryptosystem that covers some of the security flaws enumerated above. Our cryptosystem is based on a chaotic map derived from the fusion of samples from time series data from Hartley and Duffing chaotic oscillators, coupled with mathematical transformation function. One of the main contributions in this work is the production of a new chaotic map resulting from the piecewise linearity introduced in the variables of Hartley's oscillator, but this oscillator was also merged with another one in order to produce chaotic and quite robust data maps.

In our generated sequences, we have chosen a new technique to quantify the quality of the chaos. A comparative study was conducted on several traditional techniques such as MLE, Shannon entropy, and permutation entropy [17–24], but this study revealed that they were all time consuming and therefore less suitable for real-time systems [25]. A new algorithm was developed, the PLSE (permutation large slope entropy).

This technique has the advantage of being more appropriate for experimental data, for continuous time systems, and for the analysis of data coming from systems without a well-defined mathematical model in order to quantify the chaos. Another contribution is the modeling of an encryption function whose complexity is based on the principle of affine cryptography. This function uses an external key alpha which is added to the initial conditions of the chaotic oscillators to build the main secret key. The cryptosystem has the following advantages:

- (i) Firstly, the chaos generated is robust.
- (ii) Secondly, even if the attacker succeeds to correctly estimate the parameters and recovers a map, he cannot get the exact map which was actually used for encryption because it has been truncated, and it is therefore difficult for the attacker to know which part has been cut.
- (iii) Thirdly, in the proposed algorithm, only one round is necessary for encryption, and therefore there is no way of breaking the scheme based on time analysis.

(iv) Fourthly, the transformation from plaintext to ciphertext is not a simple mapping function dependent on the initial conditions only. Therefore, as will be seen in the security analysis section, neither the plaintext nor the ciphertext attack can break the proposed cryptosystem.

(v) Finally, the key space is large enough to resist all forms of brute attack.

The paper is organized as follows. Section 2 presents the chaotic map generation followed by the encryption algorithm. In Section 3, results and performance of the algorithm are given. Section 4 deals with the cryptanalysis of the system. In Section 5, the proposed cryptosystem is compared to some recent ones. The paper is concluded in Section 6.

2. Chaotic Maps and Encryption Algorithm

2.1. Chaotic Maps. This section presents the two chaotic seed maps. These are Duffing and Hartley maps. They are combined to generate the final map as will be described later. The set of equations (6)–(8) describes the Hartley oscillator while the set of equations (11) governs the Duffing oscillator.

2.1.1. Hartley Oscillator. The circuit of the Hartley oscillator is given in Figure 1. Applying Kirchhoff laws (KL), we obtained the following system of equations:

$$\begin{cases} C \frac{dV_c}{dt} = (I_1 - I_2) - \frac{V_c}{R_C}, \\ L_1 \frac{dV_{I_1}}{dt} = (V_1 - V_{EC} - V_c) - I_1 R_{L1}, \\ L_2 \frac{dI_2}{dt} = (V_c - I_2 R_{L2}) - (I_2 - I_B) R_L. \end{cases} \quad (1)$$

Let us model the BJT by the following systems:

$$I_B = \begin{cases} \frac{-V_{EB} - V_{TH}}{R_{ON}}, & V_{EB} > V_{TH}, \\ 0, & V_{EB} \leq V_{TH}, \end{cases} \quad (2)$$

$$V_{EC} = \begin{cases} V_{EC0}, & V_{EB} > V_{TH}, \\ (V_{TH} - V_{EB})k, & V_{EB} \leq V_{TH}, \end{cases} \quad (3)$$

where V_{TH} is the threshold voltage and R_{ON} is the small-signal on-resistance of the base-emitter junction; V_{EB} can also be written from the circuit in Figure 1 as

$$V_{EB} = V_1 - (I_2 - I_B) R_L. \quad (4)$$

Let us use the following dimensionless variables and (4) to build the nonlinear functions F and F^* and transform systems (1)–(3). We obtain (6)–(8).

FIGURE 1: Circuit of Hartley oscillator used.

$$\begin{aligned}
 \text{gam} &= \frac{(R_L + R_{0N})}{R_{0N}}, \\
 \alpha &= \frac{R_L}{R_{0N}}, \\
 a &= \frac{\text{rau}}{R_C}, \\
 \text{rau} &= \sqrt{\frac{L_1}{C}}, \\
 \tau &= \sqrt{L_1 C}, \\
 x_1 &= \frac{V_C}{V_1}, \\
 y_1 &= \text{rau} \times \frac{I_1}{V_1}, \\
 z_1 &= \text{rau} \times \frac{I_2}{V_1}, \\
 t &= \frac{t}{\tau}, \\
 s &= \frac{V_{EC0}}{V_{TH}}, \\
 q &= \frac{V_1}{V_{TH}}, \\
 f &= \frac{(L_1 \times R_L)}{(L_2 \times V_{TH})}, \\
 b &= \frac{R_{L1}}{\text{rau}}, \\
 d &= \frac{L_1}{L_2}, \\
 e &= \frac{\tau(R_L + R_{L2})}{L_2}, \\
 g &= \frac{(V_{TH} - V_1)}{(R_{0N} \times \text{gam})}, \\
 h &= \frac{(V_{TH} - V_1)((\text{gam} \times R_{0N}) - R_L) \times k}{(R_{0N} \times \text{gam})}, \\
 m &= \frac{(R_L \times V_{TH} \times k)(\text{gam} - \alpha)}{(\text{gam} \times \text{rau})}, \\
 a_1 &= \frac{(\alpha \times V_{TH})}{(\text{gam} \times \text{rau})}, \\
 \text{lamda} &= \text{gam} \times \left(\frac{\text{rau}}{R_L} \right) \times \left(\frac{\alpha}{\text{gam}} \right) + \left(\frac{V_1}{(\text{gam} \times V_{TH})} - 1 \right), \\
 F(z_1) &= \begin{cases} -\frac{1}{V_{TH}} (h + m \times z_1), & z_1 \geq \text{lamda}, \\ s, & z_1 < \text{lamda}, \end{cases}
 \end{aligned} \tag{5}$$

$$F(z_1) = \begin{cases} -\frac{1}{V_{TH}} (h + m \times z_1), & z_1 \geq \text{lamda}, \\ s, & z_1 < \text{lamda}, \end{cases} \tag{6}$$

$$F^*(z_1) = \begin{cases} 0, & z_1 \geq \text{lamda}, \\ f(g + a_1 z_1), & z_1 < \text{lamda}, \end{cases} \quad (7)$$

$$\begin{cases} \dot{x}_1 = y_1 - z_1 - ax_1, \\ \dot{y}_1 = q - x_1 - by_1 - F(z_1), \\ \dot{z}_1 = dx_1 - ez_1 + F^*(z_1). \end{cases} \quad (8)$$

The following values were used for systems (1) and (8):

$$\begin{aligned} R_C &= 95.5\Omega, \\ R_{L1} &= 1.5\Omega, \\ R_L &= 78\Omega, \\ R_{0N} &= 100\Omega, \\ R_{L1} &= 1.5\Omega, \\ V_{TH} &= 0.75 \text{ V}, \\ C &= 22 \text{ nF}, \\ L_1 &= 100 \mu\text{H}, \\ L_2 &= 100 \mu\text{H}, \\ V_{EC0} &= 0.2 \text{ V}, \\ \alpha &= 0.76, \\ \text{gam} &= 2.3158, \\ \text{rau} &= 67.42, \\ k &= 900, \\ a &= 0.706, \\ a_1 &= 0.0037, \\ \alpha &= 0.76, \\ b &= 0.0222, \\ d &= 1, \\ e &= 1.1495, 101.3333, \\ g &= -0.013, \\ h &= -1.8139 \times 10^{-3}, \\ \text{lamda} &= 3.0554 \text{ m}, \\ q &= 5, \\ s &= 0.2667. \end{aligned} \quad (9)$$

2.1.2. Duffing Oscillator. The Duffing oscillator is one of the nonautonomous equations (10) that produces nonlinear dynamics, leading to the presence of chaos when it is well calibrated [26]. It can be transformed into an autonomous 3D system by introducing a new state variable $z = t$. The new 3D system is given in (11).

$$\ddot{x} + \varepsilon \dot{x} + bx^3 = B \cos(\omega t), \quad (10)$$

$$\begin{cases} \dot{x} = y; \\ \dot{y} = -\varepsilon y - bx^3 + B \cos(\omega z); \\ \dot{z} = z. \end{cases} \quad (11)$$

The following parameters have been selected in order to simulate chaotic behavior:

$$\begin{aligned} \varepsilon &= 0.1, \\ b &= 0.25, \\ B &= 400, \\ \omega &= 0.8. \end{aligned} \quad (12)$$

The sets of equations for each of the two oscillators were numerically solved using Runge–Kutta algorithm with a step $\Delta t = 0.01$. Figure 1 displays phase portraits yielded for each oscillator in the chaotic mode.

We can see from Figures 2(a) and 2(b) that each oscillator's phase portrait is a strange attractor.

This, however, does not automatically mean that these oscillators are chaotic. To prove the chaotic nature of these oscillators, Lyapunov analysis was carried out for each of them. In Figures 3(a) and 3(b), the dynamics of Lyapunov exponents are displayed. The computation of the Lyapunov exponents of Hartley system gives us a positive exponent by changing in Figure 1 the voltage value at the Emitter V_1 from 3.75 V to 2.75 V. $L_{E1} = 0.0585 > 0$, and the other two are negative $L_{E2} = -0.8709 < 0$ and $L_{E3} = -2.8722 < 0$, which proves that the system is chaotic. The bifurcation diagram in Figure 4 also proves this. By setting the parameters L_1 and C , the control parameter is the resistance R_c . This resistance is associated with the control parameter a in (8). Thus, R_c can be chosen between the values **10.5** and **170.5** ohm and the parameter a between **0.39** and **6.742**.

Lyapunov exponents represent the average exponential rates of divergence or convergence of nearby orbits in the phase space. Chaotic systems exhibit exponential orbital divergence. This is manifested by the fact that small differences in initial conditions which we may not be able to resolve get magnified rapidly leading to loss of predictability. Figure 3 displays the dynamics of Lyapunov exponents for Hartley and Duffing oscillators used with initial conditions $x_{10}, y_{10}, z_{10} = (0.2, 0.5, 0.5)$ and $x_{20}, y_{20}, z_{20} = (0, 1, 1)$, respectively. By solving the two systems using 4th order Runge–Kutta technique with step 0.01, three series of values,

FIGURE 2: 2D numerical phase portraits in X - Y plane of Hartley (a) and Duffing (b) oscillators with initial conditions $(0.2, 0.5, 0.5)$ and $(0, 1, 1)$, respectively.

FIGURE 3: Dynamics of Lyapunov exponents for (a) Hartley oscillator and (b) Duffing oscillator.

L_{E1} , L_{E2} , and L_{E3} , were obtained and plotted for each of the oscillators. For each oscillator, one series is positive, the second one nil, and the third one negative. These prove the chaotic nature of the oscillators [17].

2.2. Encryption Algorithm. The encryption algorithm has two steps. The first consists in combining the two original chaotic maps to generate a third one which is used in the

encrypting function. The second step is the implementation of the mathematical encrypting function.

2.2.1. Fusion Technique and New Chaotic Map. Let (x_1, y_1, z_1) be the state variables of the first oscillator while (x_2, y_2, z_2) are those of the second oscillator. Each iteration i generates sets of state variables (x_{1i}, y_{1i}, z_{1i}) and (x_{2i}, y_{2i}, z_{2i}) . Let $m \times n$ be the size of the image to be encrypted. After a given

FIGURE 4: Bifurcation diagram of Hartley oscillator: x_1 , y_1 , z_1 versus R_c .

number of iterations, the resultant map K'_{ij} can be obtained as follows:

```

while  $u \leq m * n$ 
  for  $i = 1$  to  $m$ 
    for  $j = 1$  to  $n$ 
       $K_{ij} = \text{mod}(x_{1u} + y_{1u} + z_{1u} + x_{2u}, 1)$ 
    End
  End
   $u = u + 1$ 
End
 $K'_{ij} = \text{Trunc}(K_{ij})$ 

```

The truncation function represents the way that data mask can be extracted from the data obtained by merging the two oscillators. The notion of periodicity is lost when the combination of two chaotic maps extends the cycle length of the chaotic orbit and improves the chaotic behavior of the pseudorandom generator. For the new map obtained, we choose the variables that have more nonlinearity in their state equations and therefore provide high probability of more random data to merge. In order to preserve the parameter estimation and be sure that the orbit of the new system is bounded, we take values from the established mathematical equations and combine them, emphasizing the unpredictable side of the newly calculated data with the modulo operator at the output. K_u represents the chaotic map when we merge the oscillators. You can see the phase portrait in Figure 5.

2.2.2. Chaotic Nature of the Resultant Map. The resultant map is a truncated fusion of two chaotic maps. However, this resultant map may not automatically be chaotic. The goal of this section is to prove that it is chaotic.

In order to prove that a map is chaotic, a number of techniques such as 0-1 test [18, 19], 3ST test [27], and permutation entropy (PE) [21, 22] can be used. They help to distinguish the regularity or irregularity of the map and also measure the complexity of the finite data sequence coming

from system, in order to make sure that the latter is chaotic. To characterize data, all the above-mentioned techniques are directly applied to the time series. This permits the detection of the chaotic nature of the corresponding dynamics thanks to either its chaos indicator or the entropy. The entropy is a metric to characterize the complexity of time series and helps to distinguish between regular (periodic, for example), random, and chaotic signals and to quantify their complexity. Most of prementioned tests have been successfully applied to continuous time systems [18, 23] and discrete time systems [20]. Furthermore, they are robust in presence of noise and require neither phase space reconstruction nor modeling equations of the underlying system. However, some of them are time consuming and cannot be used for real-time implementation [24]. Recently, a new test proposed by Eyebe Fouda et al. [25] was used efficiently with interesting results. Its principle is described below and then used to test our data series.

2.2.3. Description of the Permutation Largest Slope Entropy (PLSE) Test Method. Let $\{X_t\}_{t=1, \dots, T}$ be a time series of length T , where t is the time index. The permutation entropy (PE) of order n is defined as a measure of the probabilities of permutations of order n . Permutations of order n are obtained from the comparison of neighboring values (increasing order) in embedding vectors $X_t = (X_{t+1}, X_{t+1+\tau}, \dots, X_{t+1+(n-1)\tau})$, where n is the number of values of X_t and τ the distance between two values in X_t . Assuming that the permutation P_t of order n derived from X_t is a piecewise linear function, we consider the slope of each linear function as the difference between pairs of neighboring values in P_t as follows:

$$s_i = P_t(i+1) - P_t(i), \quad 1 \leq i \leq n-1. \quad (13)$$

We thus defined the largest slope of P_t as $S_t = \max - (S_i)$ as the maximum value of $\{S_i\}$. It has been shown that $L = \lim_{n \rightarrow \infty} |S_t|$ for regular dynamics and that L -periodic dynamics are characterized by a single value of largest slope if the embedding dimension n is such that $L < n$ [20]. As a result, the entropy related to the distribution of the largest

FIGURE 5: Phase portrait of Ku versus X_1, X_2, X_3, Z_2 .

slopes may be equal to zero in the case of regular dynamics. The normalized permutation largest slope entropy (PLSE) of order $n \geq 2$ is

$$h_s(n) = -\frac{1}{\ln(n-1)} \sum p(s) \ln(p(s)), \quad (14)$$

where

$$p(s) = \frac{Nb\{t|t \leq T-n, S_t = S\}}{T-N+1}, \quad (15)$$

where $p(s)$ is the probability of S and Nb denotes the number of slopes apparition. For regular dynamics, $h_s(n) = 0$ with period $L < n$, and for irregular dynamics, $0 < h_s \leq 1$. Indeed, regular dynamics are characterized by a single value of largest slope $S_t = S$, for all t and $h_s = 0$ as $p(S) = 1$; for irregular dynamics, S_t takes different values.

2.2.4. Application of PLSE Test. The algorithm of PLSE is applied to the resultant map, and only the maximal value of the corresponding entropies is retained. Choosing $\tau > 1$ allows reducing detection errors due to small values of embedding dimensions n while $1 < t_0 < n$ allows considering smaller observation time T for detection purposes. Moreover, choosing $1 < t_0 < n$ speeds up the scanning time of the time series under study [23]. Three sequences of data were tested depending on control parameter B in the Duffing oscillator. The following parameters were used.

For the PLSE test (Figure 6),

$$t_0 = 1,$$

$$\tau = 1,$$

$$T = 10000,$$

$$n = 20,$$

$$(x_{10}, y_{10}, z_{10}) = (0.2, 0.5, 0.5),$$

$$(x_{20}, y_{20}, z_{20}) = (0, 1, 1), \quad (16)$$

$$\text{sequence 1: } = 580,$$

$$H_s = 0.3944,$$

$$\text{sequence 2: } B = 400,$$

$$\text{sequence 3: } H_s = 0.4892,$$

$$H_s = 0.7601.$$

2.3. Transformation Function

2.3.1. Theory. Given a plain image $\mathbf{O}_{ij}$ of size $m \times n$ and a chaotic map X_{ij} , apply the following equation; the mathematical transformation function is implemented by the following equation to obtain the ciphered image $\mathbf{T}_{ij}$.

$$\begin{aligned} \mathbf{T}_{ij}^{n+1} = & (\text{round}(\alpha \times 255) \times \mathbf{O}_{ij} \\ & + \text{round}((1 - \alpha)X_{ij} \times 10^{16}) \bmod(256)) \\ & \bmod(256) \oplus \text{SHA256}(\mathbf{T}_{ij}^n), \end{aligned} \quad (17)$$

FIGURE 6: Flowchart of the PLSE test.

where SHA256 is the hash algorithm in order to scramble image deterministically. T_{ij} is encrypted image and α a parameter.

2.3.2. Pseudocode of the Encryption Process.

- (1) Load the plain image O_{ij} of size $n \times m$.
- (2) Choose six values which represent the initial conditions for the two chaotic systems.
- (3) Choose the unsigned parameter $\alpha = 0.05$. For a good choice of α , $0 < \alpha < 0.8$.

- (4) Create a 1D signal of chaotic sequences $\{X_t\}_{t=1, \dots, L}$ by modular addition of the two chaotic maps which are solutions of (8) and (11) as follows.
- (5) Use PLSE Test in the resultant vector X_t and select the chaotic map with the maximum value of the entropy.
- (6) Use mathematical transformation described in Section 2.3.1 to process the plain image O_{ij} using K'_{ij} as chaotic map to obtain encrypted image T_{ij} .

$$\begin{aligned}
 T_{ij}^1 &= (\text{round}(\alpha \times 255) \times O_{1,1} + \text{round}((1 - \alpha)K'_{1,1} \times 10^{16}) \bmod(256)) \bmod(256) \oplus \text{SHA256}(T_{ij}^0), \\
 T_{ij}^{n+1} &= (\text{round}(\alpha \times 255) \times O_{ij} + \text{round}((1 - \alpha)K'_{ij} \times 10^{16}) \bmod(256)) \bmod(256) \oplus (T_{ij}^n).
 \end{aligned} \tag{18}$$

3. Results and Performances of the Cryptosystem

3.1. Test Images. In this section, we present results yielded by our cryptosystem and analyze them. Four images (Figure 7) were used to test our algorithm. The statistical properties of the plaintext images are summarized in Table 1. Two images of this testing set were of gray-level type while the other two were color ones. They were of size $m \times n$ with $m \neq n$ for one of them and $m = n$ for the rest. This permits us to test the various combinations.

3.2. Cipher Evaluation. Visual examples of plain, encrypted, and decrypted images are given in Figure 8.

Brute force attack, speed, histogram, correlation, key space, and key sensitivity analyses were also carried out for the proposed cryptosystem. With a laptop equipped with a 2.0 GHz Core Duo and 2Go DDR, we had encryption times

of 1.2 seconds for a 512×512 resolution Lena image, 1.2 seconds for a 512×512 resolution Barbara image, 1 second for a 480×500 resolution Mandrill image, and 3 seconds for a 1024×1024 resolution Man image.

3.2.1. Key Space Analysis. The secret key of the proposed cryptosystem contains 7 real numbers (6 initial conditions and many parameters). By considering only the initial conditions of the two oscillator models, let us use real data type to attenuate effect caused by discretization. In the event of using a programming language compatible with IEEE Standard 754-2008 [21], it is necessary to use the double data type, which stores real numbers on 8 bytes (64 bits), with an accuracy of 15 decimal positions. In this case, the secret key length will be 448 bits (7 numbers $\times$ 64 bits). This means that the size of the secret key space will be equal to $2^{448} \approx 7.26 \times 10^{134}$, which is sufficiently large to resist all kinds of known brute force attack.

FIGURE 7: Test images: (a) Mandrill; (b) Barbara; (c) Lena; (d) Man.

TABLE 1: Statistical properties of plaintext images: HC: horizontal correlation; VC: vertical correlation; DC: diagonal correlation; H : entropy.

Image	Size	HC	VC	DC	H
Lena	512×512	0.972	0.985	0.959	7.45
Mandrill	480×500	0.933	0.912	0.866	7.21
Barbara	512×512	0.954	0.892	0.884	7.34
Man	1024×1024	0.9813	0.9774	0.9671	7.52

FIGURE 8: Visual examples: (a), (d), (g) (j) plain images; (b), (e), (h), (k) encrypted images; (c), (f), (i), (l) decrypted images.

3.2.2. Histogram Analysis. Histogram analysis refers to quality of the frequency distribution of pixels in an image. When the grayscale frequencies in the ciphered image are approximately in the same level, this will result in a flat histogram and excellent resistance to statistical analysis

attacks. As illustrated in Figure 9, the three histograms of the ciphered images are almost flat.

We can notice that, contrary to those of plain images that clearly exhibit some modes, histograms of ciphered images are roughly flat which is a good indication for a cipher. As for

FIGURE 9: Histograms: (a), (d), (g), (j) plain images of Barbara, Lena, Man, and Mandrill, respectively; (b), (e), (h), (k) encrypted images; (c), (f), (i), (j), (l) decrypted images.

the correlation analysis, Figure 10 displays results yielded by the proposed cryptosystem.

3.3. Further Analyses. A number of common metrics such as image entropy (19), number of pixel change rate ((20) and (21)), unified average changing intensity (22), and variance of histogram (23) were computed to evaluate the proposed system.

$$H = \sum_{i=1}^{2^k} p(m_i) \log_2(p(m_i)), \quad (19)$$

$$\text{NPCR} = \left(\frac{1}{MN} \right) \sum_{i=1}^M \sum_{j=1}^N D(i, j), \quad (20)$$

where

FIGURE 10: Continued.

FIGURE 10: Correlation between pixels' pairs for Man image (a-c), Barbara image (g-i), Lena image (m-o), and Mandrill image (s-u). Horizontal, vertical, and diagonal direction correlation for plain images (d-f), (j-l), (p-r), and (v-x), respectively. Encrypted images of Man, Barbara, Lena, and Mandrill correlation in horizontal, vertical, and diagonal directions.

$$D(i, j) = \begin{cases} 0 & \text{if } \text{Im}_o(i, j) = \text{Im}_c(i, j), \\ 1 & \text{if } \text{Im}_o(i, j) \neq \text{Im}_c(i, j), \end{cases} \quad (21)$$

$$\text{UACI} = \left(\frac{100}{MN} \right) \sum_{i=1}^M \sum_{j=1}^N \frac{|\text{Im}_o(i, j) - \text{Im}_c(i, j)|}{255}, \quad (22)$$

$$\text{Var}(Z) = \frac{1}{n^2} \sum_{i=1}^n \sum_{j=1}^n \frac{1}{2} (z_i - z_j)^2, \quad (23)$$

where Z is the vector of the histogram values. $Z = \{z_1, z_2, \dots, z_{256}\}$, with z_i and z_j being the numbers of pixels whose gray values are equal to i and j , respectively. The results are summarized in Tables 2 and 3.

The average value of NPCR which is 99.464 falls into the bracket of what the literature presents. That of UACI is 33.8, a bit higher than 33.3 which is the average value in the literature. The observation of Table 3 shows that, from plain to ciphered images, there is a ratio of 10^3 as concerns the values of variances of histograms.

3.3.1. Key Sensitivity Analysis. The security of a cryptosystem is clearly related to the sensitivity of the key. Thus, for a chaos-based encryption algorithm, the smallest difference in the key or in the plaintext image leads to a failure to decrypt the encrypted image. To test the sensitivity to the encryption key, we encrypt the color and grayscale images "Lena (512×512)", "Barbara (512×512)", and "Man (1024×1024)" with the key $x_{10} = 0.12345678919876$; then, this key will be slightly modified and used for decryption. Figure 11 clearly shows that the image encrypted by the x_{10} is not correctly decrypted by using the key $x_{10} + 10^{-15}$. Accordingly, it can be

concluded that the proposed scheme is very sensitive to the key.

3.3.2. Pixels' Resemblance Analysis. The pixels' resemblance reveals the similarity between different digital contents [28]. The quality of the encrypted image compared to the original image can be measured using mathematical tools such as PSNR (Peak Signal Low Noise Ratio between images) and SSIM (Structured Similarity Index Measure). The most widely used classical metric for objectively estimating the distortion between two images is the PSNR which is considered to be a reliable indicative measure. To calculate PSNR (25), first we have to calculate the MSE using the following expression:

$$\text{MSE} = \frac{1}{MN} \sum_i^M \sum_j^M (P_{ij} - C_{ij})^2, \quad (24)$$

where P_{ij} and C_{ij} refer to the pixels' position at i th row and j th column of plain and ciphered images distinctly. MSE is the mean square error.

$$\text{PSNR} = 10 \log \frac{R^2}{\text{MSE}}, \quad (25)$$

where R^2 , R is the maximum fluctuation in the input image data type.

The higher the PSNR, the better the quality of compressed or reconstructed image. If the input image has double-precision floating point data type, the R is 1; if it has 8 bit unsigned integer data type, R is 255 etc. PSNR and MSE are used to compare image compression quality.

SSIM determines the structural similarity of images in order to be closer to visual perception than the PSNR is

TABLE 2: Values of common metrics.

	Lena	Mandrill	Barbara	Man
NPCR	99.5771	99.4712	99.346	99.5
UACI	35.082	32.9123	33.406	33.41
H	7.996	7.995	7.997	7.999

TABLE 3: Variances of histograms for plain and ciphered images from the proposed scheme.

Image	Plain	Ciphered
Mandrill	6.13×10^5	1049.5
Lena	1.018×10^6	935.54
Barbara	7.32×10^5	934.22
Man	1.139×10^7	4535.3

FIGURE 11: Key sensitivity analysis: (a), (e), (i) plain images; (b), (f), (j) encrypted images by x_{10} ; (c), (g), (k) decrypted images by changing x_{10} by $x_{10} + 10^{-15}$; (d), (h), (l) difference images between (b) and (c), (f) and (g), (j) and (k), respectively.

and is used to compare contrast of plain and enciphered contents too. For plain and ciphered images P_{ij} and C_{ij} with mean values μ_p , μ_c and the standard deviation σ_{pc} , the SSIM (26) has values between 0 and 1. If the value is close to 1, there will be more resemblance between plain and ciphered contents; if the value approaches 0, there will be dissimilarity between contents. Pixels' resemblance analysis of proposed approach is given in Table 4.

$$\text{SSIM} = \frac{(2\mu_p\mu_c + C_1)(2\sigma_{pc} + C_2)}{(\mu_p^2 + \mu_c^2 + C_1)(\sigma_p^2 + \sigma_c^2 + C_2)}. \quad (26)$$

4. Cryptanalysis of the System

As far as the security analysis is concerned, the cryptosystem was submitted to the CPA (Chosen-Plaintext Attack). In this attack, we have an adversary model in which an eavesdropper is presumed to have the ability to encrypt a plain image to obtain its corresponding cipher but does not have the secret key. The eavesdropper has access to the encryption mechanism or process and encrypts a neutral image, in the hope of discovering the secret key. According to [26], it can be summarized by the following equation:

$$A = A' \oplus (B' \oplus \text{Map}), \quad (27)$$

TABLE 4: Pixels resemblance and pixels disparities analyses between plain encrypted images and their comparison with existing methods.

Reference [29]	SSIM	—	—	—	—
	PSNR	—	—	8.4865	—
	MSE	—	—	5201.746	—
Reference [28]	SSIM	0.02308	—	—	—
	PSNR	9.2570	—	—	—
	MSE	4666.515	—	—	—
Plain encrypted disparity	SSIM	0.0070	0.0059	0.0069	0.0079
	PSNR	5.7177	4.9159	5.4884	7.6769
	MSE	17431	20965	18333	11102
Images		Lena	Barbara	Mandrill	Man

FIGURE 12: CPA cryptanalysis attack: (a) Barbara; (b) neutral image; (c) encrypted image of Barbara; (d) extracted key map; (e) decrypting (c) with (d).

TABLE 5: Comparison of some ciphers using Lena as test image: TR: time required; RND: round numbers of diffusion; AC: average correlation; KS: key space; H : entropy; VH: variance of histograms.

Algorithm	TR (s)	RND	AC	KS	H	VH	UACI (%)	NPCR (%)
Proposed scheme	1.2	1	0.0024	7.2×10^{134}	7.9993	1091.1	33.41	99.6
[28]	1.69		0.017		7.9984		31.71	99.42
[30]	5.5		0.032	7.86×10^{366}	7.9993	819.48	33.47	99.64
[31]			0.0005		7.9998		33.47	99.64
[32]		1	0.0112	10^{79}	7.997		33.45	99.6
[27]	0.006	5	0.059	7.2×10^{134}	7.819		31.15	99.63

where A is the decrypted image, A' is its cipher, B' is the eavesdropper's encrypted image obtained from an extreme plaintext, " $\oplus$ " is the machinery, and Map is the presumed key. Two test images were used, and the results obtained are shown in Figure 12. We note that the eavesdropper does not reveal any keys or patterns in the plain image.

5. Comparison with Other Cryptosystems

Not all published cryptosystems present an extensive evaluation of the system. Our system was compared to recent papers in the literature based on performances with a common image which is Lena. Results are displayed in Table 5.

We can see from the table that one first advantage of the proposed system is the fact that one round is enough to encrypt an image. This also means a short encryption time and therefore possibility of real-time encryption. Furthermore, the key space of our cryptosystem and that of Choi

et al. [27] are the largest. We can also notice from Table 5 that the average UACI, NPCR, and entropy yielded by the proposed scheme are among the best. Finally, its NPCR and entropy are among the best in literature.

6. Conclusion

In this work, we have suggested a chaos-based cryptosystem. A new data chaotic map has been built by combining two oscillators. To do this, we first introduce continuous functions in the dynamics of the Hartley oscillator; then, by modular addition, we perform a fusion with the Duffing oscillator. The robustness of the resulting data chaotic maps is evaluated by the PLSE algorithm. Furthermore, the resulting chaotic map is combined with a new iterative mathematical transformation function we have proposed to encrypt images.

The encryption and decryption process are tested on 4 very popular images and evaluated using very common

metrics such as NPCR, UACI, SSIM, PSNR, and variance of histograms. The system was further analyzed in terms of speed, correlation, and attacks. Results obtained were compared to very recent systems in the literature and proved to be of equal or better quality. We aim to carry out the experimental setup in future work.

Data Availability

The images used in this paper to support our results were Lena, Mandrill, and Barbara. These can be found via the following links: <https://www.programmersought.com/article/40272792839/> for Lena image; <http://www.hlevkin.com/TestImages/baboon.bmp> for Mandrill image; <https://homepages.cae.wisc.edu/~ece533/images/Barbara.png> for Barbara image. Mandrill image can also be found in Matlab database. More generally, images for testing encryption algorithm can be found at <https://homepages.cae.wisc.edu/~ece533/images/>.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution-diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.
- [2] R. Rhouma, E. Solak, and S. Belghith, "Cryptanalysis of a new substitution-diffusion based image cipher," *Communications in Nonlinear Science and Numerical Simulation*, vol. 15, no. 7, pp. 1887–1892, 2010.
- [3] 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," *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011.
- [4] C. Li, S. Li, and K.-T. Lo, "Breaking a modified substitution-diffusion image cipher based on chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 2, pp. 837–843, 2011.
- [5] F. Huang and Z.-H. Guan, "Cryptosystem using chaotic keys," *Chaos, Solitons & Fractals*, vol. 23, no. 3, pp. 851–855, 2005.
- [6] N. K. Pareek, V. Patidar, and K. K. Sud, "Discrete chaotic cryptography using external key," *Physics Letters A*, vol. 309, no. 1–2, pp. 75–82, 2003.
- [7] A. Skrobek, "Approximation of a chaotic orbit as a cryptanalytical method on Baptista's cipher," *Physics Letters A*, vol. 372, no. 6, pp. 849–859, 2008.
- [8] A. N. Pisarchik, N. J. Flores-Carmona, and M. Carpio-Valadez, "Encryption and decryption of images with chaotic map lattices," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 16, no. 3, Article ID 033118, 2006.
- [9] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, and V. Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 18, no. 3, Article ID 033112, 2008.
- [10] Z.-H. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1–3, pp. 153–157, 2005.
- [11] C. Çokal and E. Solak, "Cryptanalysis of a chaos-based image encryption algorithm," *Physics Letters A*, vol. 373, no. 15, pp. 1357–1360, 2009.
- [12] G. Alvarez and S. Li, "Breaking an encryption scheme based on chaotic baker map," *Physics Letters A*, vol. 352, no. 1–2, pp. 78–82, 2006.
- [13] G. Alvarez, S. Li, and L. Hernandez, "Analysis of security problems in a medical image encryption system," *Computers in Biology and Medicine*, vol. 37, no. 3, pp. 424–427, 2007.
- [14] G. Álvarez, F. Montoya, M. Romera, and G. Pastor, "Cryptanalysis of a discrete chaotic cryptosystem using external key," *Physics Letters A*, vol. 319, no. 3–4, pp. 334–339, 2003.
- [15] Y. P. K. Nkandeu and A. Tiedeu, "An image encryption algorithm based on substitution technique and chaos mixing," *Multimedia Tools and Applications*, vol. 78, no. 8, pp. 10013–10034, 2019.
- [16] L. M. Y. Heuchen, A. Tiedeu, and G. Kom, "A robust and fast image encryption scheme based on a mixing technique," *Security and Communication Network*, vol. 2021, Article ID 6615708, 17 pages, 2021.
- [17] G. Kenfack and A. Tiedeu, "Chaos-based encryption of ECG signals: experimental results," *Journal of Biomedical Science and Engineering*, vol. 7, no. 6, pp. 368–379, 2014.
- [18] R. Gopal, A. Venkatesan, and M. Lakshmanan, "Applicability of 0-1 test for strange nonchaotic attractors," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 23, no. 2, Article ID 023123, 2013.
- [19] G. A. Gottwald and I. Melbourne, "A new test for chaos in deterministic systems," *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 460, no. 2042, pp. 603–611, 2004.
- [20] J. S. A. Eyebe Fouda, J. Y. Effa, M. Kom, and M. Ali, "The three-state test for chaos detection in discrete maps," *Applied Soft Computing*, vol. 13, no. 12, pp. 4731–4737, 2013.
- [21] C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," *Physical Review Letters*, vol. 88, no. 17, Article ID 174102, 2002.
- [22] Y. Cao, W. W. Tung, J. B. Gao, V. A. Protopopescu, and L. M. Hively, "Detecting dynamical changes in time series using the permutation entropy," *Physical Review E, Statistical, Nonlinear, and soft Matter Physics*, vol. 70, Article ID 046217, 2004.
- [23] J. S. A. Eyebe Fouda and W. Koepf, "Detecting regular dynamics from time series using permutations slopes," *Communications in Nonlinear Science and Numerical Simulation*, vol. 27, no. 1–3, pp. 216–227, 2015.
- [24] J. S. A. Eyebe Fouda and W. Koepf, "Efficient detection of the quasi-periodic route to chaos in discrete maps by the three-state test," *Nonlinear Dynamics*, vol. 78, no. 2, pp. 1477–1487, 2014.
- [25] J. S. A. Eyebe Fouda, B. Bodo, G. M. D. Djeufa, and S. L. Sabat, "Experimental chaos detection in the Duffing oscillator," *Communications in Nonlinear Science and Numerical Simulation*, vol. 33, pp. 259–269, 2016.
- [26] Y. Abanda and A. Tiedeu, "Image encryption by chaos mixing," *IET Image Processing*, vol. 10, no. 10, pp. 742–750, 2016.
- [27] J. Choi, S. Seok, H. Seo, and H. Kim, "A fast ARX model-based image encryption scheme," *Multimedia Tools and Applications*, vol. 75, no. 22, pp. 14685–14706, 2016.
- [28] S. I. Batool and H. M. Waseem, "A novel image encryption scheme based on Arnold scrambling and Lucas series,"

- Multimedia Tools and Applications*, vol. 78, no. 19, pp. 27611–27637, 2019.
- [29] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, and M. R. Mosavi, “A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process,” *Multimedia Tools and Applications*, vol. 71, no. 3, pp. 1469–1497, 2014.
 - [30] B. Ali, “Designing digital image encryption using 2D and 3D reversible modular chaotic maps,” *Journal of Information Security and Applications*, vol. 47, pp. 188–198, 2019.
 - [31] M. Essaid, I. Akharraz, A. Saaidi, and E. A. Mouhib, “Image encryption scheme based on a new secure variant of hill cipher and 1D chaotic maps,” *Journal of Information Security and Applications*, vol. 47, pp. 173–187, 2019.
 - [32] X. Wang and C. Liu, “A novel and effective image encryption algorithm based on chaos and DNA encoding,” *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6229–6245, 2016.