From Diffusion to Confusion of RGB Pixels Using a New Chaotic System for Color Image Encryption

Salma Ben Mamia, Pauline Puteaux, William Puech, Kais Bouallegue

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

From diffusion to confusion of RGB pixels using a new chaotic system for color image encryption

SALMA BEN MAMIA[1,2], PAULINE PUTEAUX[3] (Member, IEEE), WILLIAM PUECH[2] (Senior Member, IEEE), and KAIS BOUALLEGUE[4]

[1]Electronics and Microelectronics laboratory, University of Monastir, TUNISIA (e-mail: salma.ben-mamia@lirmm.fr)
[2]LIRMM, Université de Montpellier, CNRS, FRANCE (e-mail: william.puech@lirmm.fr)
[3]CRIStAL, CNRS, Univ. Lille, Centrale Lille, Lille (e-mail: pauline.puteaux@cnrs.fr)
[4]Department of Electrical Engineering, Higher Institute of Applied Sciences and Technology of Sousse, TUNISIA (e-mail: Kais_bouallegue@yahoo.fr)

Corresponding author: William Puech (e-mail: william.puech@lirmm.fr).

This work was supported in part by LIRMM, University of Montpellier, CNRS, FRANCE and University of Monastir, TUNISIA.

ABSTRACT Over the past decade, the transmission of images over digital and social networks, as well as their archiving on clouds, has increased dramatically. It has become necessary and urgent to secure them during their transmission or when archiving. In this paper, we propose a new color image encryption (CIE) scheme based on a single scroll chaotic system, using neurons with two dendrites. The originality of the proposed CIE scheme is that the main encryption step is based only on color pixel scrambling, which is traditionally used for diffusion. Based on the proposed CIE scheme we have developed three different approaches. From color pixel scrambling (CPS), to full color pixel component scrambling (FCPCS), passing through intra-color pixel component scrambling (ICPCS), we show that color pixel component scrambling can act not only as a permutation, but also as a substitution, ensuring both confusion and diffusion properties. The experimental results show that using the proposed scheme, regardless of the approach used, we can efficiently obtain encrypted color images. In particular, the results obtained with the FCPCS approach show that statistical and differential attack analyses are comparable to those obtained with current state-of-the-art methods that combine permutation and substitution steps.

INDEX TERMS chaotic system, cryptography, diffusion-confusion, color image encryption, multimedia security.

I. INTRODUCTION

Multimedia security plays an important role in all fields, especially in highly sensitive areas, such as military and medical worlds. With the development of cloud computing, the growth of information technology has led to some serious security challenges. Privacy, authentication, and integrity are constantly compromised by illegal activities such as hacking, copying, or malicious use of information. Encryption methods have been developed to protect the privacy of data by creating many robust security techniques [1].

Image encryption technology is an important way to ensure security [2], [3]. Several methods and areas of research, including some traditional data encryption algorithms such as IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard) and AES (Advanced Encryption Standard), have been developed to encrypt and protect text information [4]–[7]. These algorithms are not suitable for real-time image encryption due to their high computational complexity. To improve and solve this particular problem, many chaotic systems have been proposed for image encryption.

Chaotic systems have attracted the attention of researchers due to several properties, such as initial sensitivity, unpredictability, and pseudo-randomness [8], [9]. A simple change in the initial state of the system will output a different sequence. Based on these properties, extensive research has been carried out in this vein [10], [11]. Chaotic systems are also used to perform chaotic-based cryptography according to Shannon information theory, which consists of two operations: confusion and diffusion. In the confusion process, pixel positions are first randomly scrambled. Then, during the diffusion process, all pixel values are substituted by other

values. After both these steps, the visual content of the image is no longer recognizable.

Image encryption algorithms based on chaotic systems can be divided into two categories: one dimension (1D) and high dimension. Chaotic 1D maps include the logistic map, the tent map and the chaotic circle map. However, due to their simplicity, they are easy to compromise. The second category is high dimensional chaotic maps, such as the Henon and Ikeda maps, which have a larger key space and provide good chaotic behavior [12].

Nonlinear chaotic systems have been exploited for either the most significant and least significant bits or n bits of a pixel. Selective image encryption techniques are another important spatial classification for chaotic image encryption. They reduce the computational cost of encrypting images to real-time encryption. The second major class of chaotic image encryption techniques are frequency domain-based methods. These patterns basically use different frequency filters to encrypt digital content. Many transforms, such as the discrete cosine and sine transforms, the fast Fourier transform and wavelet chaotic dynamical systems are used to encrypt images [7], [13]–[16].

Recently, many chaos-based image encryption systems have been introduced [17]. Ben Slimane *et al.* developed a new chaotic image encryption system based on DNA sequence operations and a unique neuron model [18]. They also designed a chaotic multi-croll system by exploiting the map with the fractal process [19].

In this paper, we propose an original scheme based on a single scroll chaotic system for encrypting color images. With this new scheme, we show that it is possible to achieve effective color image encryption, by only scrambling the components of color pixels (R, G and B). The proposed scheme involves the integration of a new chaotic attractor using neurons with two dendrites used to perform color image encryption. From naive color pixel scrambling (CPS), to intra-color pixel component scrambling (ICPCS), and finally, to full color pixel component scrambling (FCPCS), we show that scrambling acts not only as a permutation, but it can also act as a substitution, ensuring both confusion and diffusion properties. Our experiments on real images show that the proposed color image encryption scheme, regardless of the approach used, is efficient. Indeed, the results of both statistical and differential attack analyses are comparable with those obtained by current state-of-the-art methods that combine permutation and substitution steps.

The rest of the paper has the following structure. In Section II, related works on chaotic systems and color image encryption are presented. In Section III, we propose our new single scroll chaotic system, while in Section IV, we present with details the new scheme with three approaches of color image encryption. In Section V, several experimental results and security analysis of the proposed color image encryption approaches are presented. Finally, the conclusion and perspectives are given in Section VI.

II. PREVIOUS WORK

This section introduces the most common methods of chaotic systems and color image encryption to date. In Section II-A, traditional chaotic systems are described, while in Section II-B, previous color image encryption methods are presented.

A. TRADITIONAL CHAOTIC SYSTEMS

In this section, we introduce traditional chaotic systems, such as Logistic Map, Lorenz, Chua, and Roessler systems.

The logistic map is known for its simple mathematical properties as well as its dynamical features [20]. It has been extensively used in various fields. The logistic map is defined by:

$$x_{i+1} = \alpha x_i(1 - x_i), \tag{1}$$

where $\alpha \in [0, 4]$, $x_i \in [0, 1]$, x_i represents the value of the i-th iteration of the map.

The Lorenz system, originally studied by Lorenz in 1960, is a dynamical system defined by a nonlinear system of standard differential equations [21]:

$$\begin{cases} \dot{x} = \alpha(y - x), \\ \dot{y} = (\beta - z)x - y, \\ \dot{z} = xy - \gamma z, \end{cases} \tag{2}$$

where α, β, γ are the control parameters, x, y, z the state variables, and $\dot{x}, \dot{y}, \dot{z}$ stand for the time derivatives of the state variables.

Given control parameters and initial values x_0, y_0, z_0 of the state variables, Eq. (2) is usually solved numerically. The simulation of the chaotic attractor gives a picture that looks like a butterfly.

In late 1983, Chua proposed the Chua's circuit. He was the first to discover a chaotic phenomenon in a computer simulation and a practical circuit. The fundamentals of Chua's circuit is a three-dimensional, self-sustaining, oscillating system. The system consists of four linear components: the inductor L, the resistor R, the capacitors C_1 and C_2, and the nonlinear resistor N_R (called the Chua diode [22]). The equation of a state of Chua's circuit is:

$$\begin{cases} \dot{V}_1 = \frac{1}{C_1}\left[\frac{1}{R}(V_2 - V_1) - f(V_1)\right], \\ \dot{V}_2 = \frac{1}{C_2}\left[\frac{1}{R}(V_1 - V_2) + I_3\right], \\ \dot{I}_3 = -\frac{1}{L}V_2, \end{cases} \tag{3}$$

where V_1 and V_2 denote the voltage across C_1 and C_2 respectively, I_3 refers to the current through L, and $f(V_1)$ is the piecewise-linear function of Chua's Diode:

$$f(V_1) = G_b V_1 + 0.5(G_a - G_b)\left[|V_1 + E| - |V_1 - E|\right], \tag{4}$$

where G_a and G_b denote the slopes of internal and external broken lines in volt-ampere characteristic respectively, and E is the breakpoint voltage.

The Rossler system is a prototype of a continuous dynamical system that has many similarities to the Lorenz system,

defined by the following nonlinear differential equations [23]:

$$\begin{cases} \dot{x} = (y + z), \\ \dot{y} = x + \alpha y, \\ \dot{z} = \beta + z(x\gamma), \end{cases} \tag{5}$$

where α, β and γ are non-negative parameters. It approaches chaos in a period that doubles the bifurcation.

B. COLOR IMAGE ENCRYPTION

The rapid progress of chaos theory and its associated applications has led to the development of a variety of image encryption techniques.

Wu *et al.* have presented a color image encryption method using a combination of the rectangular transform and the chaotic tent map principle [24]. The three color components are encrypted simultaneously and are related to each other. Moreover, the key sensitivity is improved by using both the secret key and the content of the original image in generating the key stream. Later, Zhu and Sun showed that this model is not secure against attacks using selected plaintext tests [25]. They also proposed a similar, but more secure method based on a logistic tent map and a parameter related to the SHA -3 hash value of the original image.

In addition, Liu *et al.* developed an algorithm for simultaneous scrambling and diffusion of color images based on a chaotic Hopfield neural network [26]. They performed the first diffusion simultaneously with the first scrambling. Then, the second diffusion is completed to improve both the key sensitivity and the resistance to selected-plaintext attacks. Finally, a second encryption is performed for some special pixels.

Malik *et al.* presented an algorithm for encrypting color images based on hyperchaos and DNA computing [27]. The three components of an original color image are split. They are first diffused at the decimal level and then permuted. After that, DNA coding is performed on the channels. To increase security, diffusion is also performed at the DNA level.

Hu *et al.* proposed an algorithm for encrypting color images based on dynamic chaos and matrix convolution [28]. The chaotic sequence is used to permute the pixel coordinates of the mosaic images of the three components of a color image. Then, each element of the chaotic sequence is used as an algorithm for a matrix convolution cloud, which alternately updates the input value of the matrix convolution operation and the pixel value to obtain the new position of each pixel. Finally, a substitution is performed.

Qian *et al.* described a novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques [29]. During the diffusion process, the three-dimensional chaotic logistic map is introduced to modify the pixel values. In the confusion process, the three-dimensional chaotic Arnold cat map is applied for scrambling purposes.

Asl *et al.* have presented a scale-invariant color image encryption method using three-dimensional chaotic maps [30]. First, an original color image is converted to three-dimensional space by dividing the three color components into several square sub-images with gray levels. To create confusion and diffusion, 3D substitution and permutation are performed on the sub-image

Recently, Abduljabbar *et al.* have proposed a fast algorithm for encrypting color images based on various chaotic map types and an S-box based on a hyperchaotic map principle [31]. First, three key matrices are generated by a hybrid technique that uses two low-complexity chaotic maps, namely a 1D logistic map and a 3D Hénon map. The substitution is then performed.

III. A NEW SINGLE SCROLL CHAOTIC SYSTEM USING NEURONS WITH TWO DENTRITES

In this section, based on a new class of neurons presented in [32]–[34], we propose to develop a generation of chaotic attractors using neurons with two dendrites. Based on the work proposed by Ben Mamia *et al.* [35], [36], these new chaotic attractors allow us to increase the systems precision. In Section III-A, we present a simulation of the proposed neuron with two dentrites, while in Section III-B we develop the analysis of the bifurcation of the system.

A. SIMULATION OF THE PROPOSED NEURON WITH TWO DENTRITES

In this section, we present a simulation of the proposed model with two dentrites in order to increase the precision of the system. The variable structure model of neuron (VSMN) is described by a nonlinear system of standard differential equations based on the two functions $f_1()$ and $f_2()$:

$$\begin{cases} \dot{u} = f_1(u, v), \\ \dot{v} = f_2(u, v), \end{cases} \tag{6}$$

with:

$$f_1(u, v) = u + \alpha(-u + \beta\gamma v(u + p_1) \times (u + p_2)) \times g(v) \times \frac{h(u)}{2}, \tag{7}$$

$$f_2(u, v) = v + \alpha(-\lambda v - \lambda\beta\gamma v(u + q_1)^{n_1} \times (u + q_2)^{n_2}) \times h(u), \tag{8}$$

where:

$$g(v) = e^{-\gamma v^2/2}, \tag{9}$$

and:

$$h(u) = e^{-\gamma((u+p_1)\times(u+p_2))^2}, \tag{10}$$

with u and v being the states of activity of the neurons, n_1, n_2, q_1 and q_2 being related to the behaviour of the dendrites and p_1 and p_2, to the positions of the dentrites, and $g(v)$, $h(u)$, α, β, γ and λ being the control parameters.

To get the chaotic behavior, in the proposed model, we have added two oscillators that generate the dynamic of neurons:

$$x_{n_0} = sin(2\pi k_{n_0}), \tag{11}$$

and:

$$x_{n_2} = 2cos(2\pi k_{n_2}) x_{n_1} - x_{n_0}, \tag{12}$$

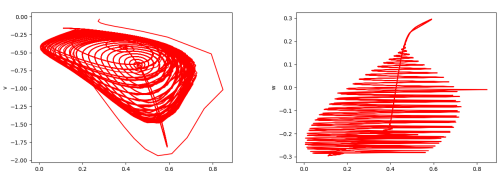
where k_{n_0}, k_{n_2} and x_{n_1} are control parameters.

Fig. 1 and Fig. 2 illustrate the implementation results of the VSMN presented in Eq. (7) and Eq. (8), with $u = 0.5$ and $v = 0.25$ as initial conditions in this case. But later, when it comes to encryption methods, these initial conditions will be the key generators. Based on the work proposed by Ben Mamia *et al.* [35], [36], the other initial conditions values are illustrated in Table 1.

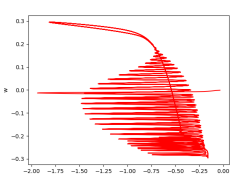
TABLE 1: Initial conditions of single scroll chaotic system [35], [36].

p_1	p_2	q_1	q_2	α	β	γ	λ	k_{n_0}	k_{n_2}	x_{n_1}
-0.8	0.6	p_1	p_2	0.1	9	25	1.5	$\frac{1}{8000}$	1	0

Fig. 1 presents the different two dimensional phase trajectories of the proposed chaotic system (Fig. 1.a illustrates the trajectory on u, v plane, Fig. 1.b, on u, w plane, and Fig. 1.c, on v, w plane). Fig. 2 presents the three dimensional phase trajectories of the proposed system (Fig. 2.a illustrates the 3D trajectory on u, v, w space, and Fig. 2.b on u, w, v space). The trajectories illustrate a spiral chaotic behavior with two orbits connected with a linear straight line. They are called hidden chaotic attractors.



(a) u, v plane. (b) u, w plane.



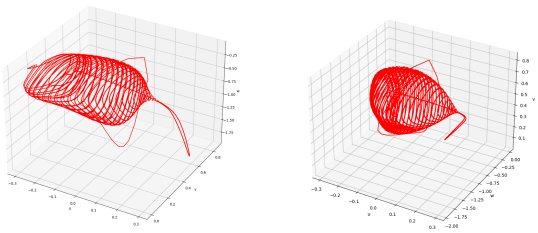
(c) v, w plane.

FIGURE 1: The 2D phase trajectories of the proposed chaotic system: a) u, v plane, b) u, w plane, c) v, w plane.

A simulation of the system with its bifurcation diagrams is presented in Section III-B.

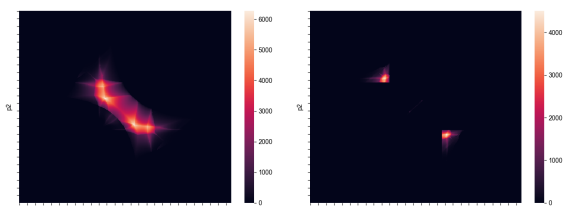
B. ANALYSIS OF THE BIFURCATION OF THE PROPOSED SYSTEM

Over the past two decades, a great deal of bifurcation and chaos analysis has been developed [37]. This is why the study of this particular aspect of this phenomenon has become an appealing undertaking. In this section, we analyse the time-delay influence on the stability of the steady state by taking p_1 as bifurcation parameter and fixing the value of

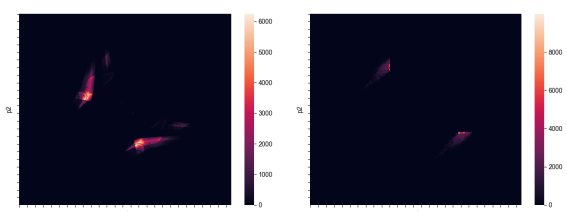


(a) u, v, w space. (b) u, w, v space.

FIGURE 2: The 3D phase trajectories of the proposed chaotic system: a) u, v, w space, b) u, w, v space.



(a) $n_1 = 0$ and $n_2 = 0$. (b) $n_1 = 2$ and $n_2 = 2$.



(c) $n_1 = 1$ and $n_2 = 1$. (d) $n_1 = 3$ and $n_2 = 3$.

FIGURE 3: 2D bifurcation diagram illustrating the steady state behavior of Eq. (7) and Eq. (8) with four different gain pairs (p_1, p_2).

p_2 [37]. The stability of Eq. (7) and Eq. (8) is modified, and a family of periodic orbits bifurcates from equilibrium with an increase of p_1. Four 2D bifurcations showing the steady state behavior of Eq. (7) and Eq. (8) for different pairs (p_1, p_2) are illustrated in Fig. 3. It can easily be deduced that as p_1 increases, then the first period (stable) behavior shown in orange is extended for higher values of p_1 [38]. Indeed, Fig. 3 depicts in orange the zones of the first period mode and this matches the higher periods. Furthermore, the chaotic zones are also shown as parameters p_1 and p_2 vary [39]. In particular, when $p_1 = 0$, we observe that as p_2 raises, the output of a period of 6,000 becomes a period of 5,000. For a short interval of p_1, it becomes a period of 4,000 before it goes into the black period, which corresponds to the chaotic mode. We can conclude from Fig. 3 that when n_1 and n_2 increase, the system takes a short period to reach the chaotic zone.

This new chaotic system is therefore used as a pseudo-

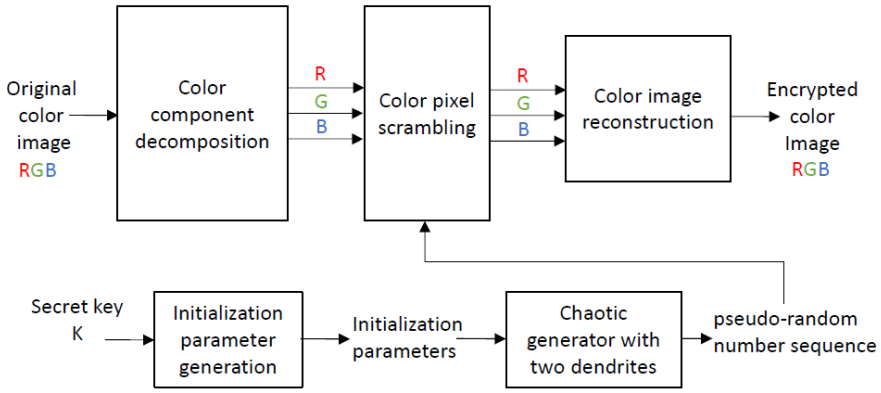


FIGURE 4: Overview of the proposed color image encryption (CIE) scheme.

random number generator (PRNG) to encrypt color images, as presented in Section IV.

IV. THE PROPOSED COLOR IMAGE ENCRYPTION (CIE) SCHEME

In this section, we present with details the proposed color image encryption (CIE) scheme. With this new CIE scheme, we show that color pixel component scrambling acts not only as a permutation, but it can also act as a substitution. This proposed CIE scheme integrates the new chaotic system using neurons presented in Section III.

Firstly, in Section IV-A, we give an overview of the proposed CIE scheme. Then, we present the different approaches that have been developed to encrypt a color image based on scrambling approaches. In Section IV-B, we introduce a naive approach, called color pixel scrambling (CPS), which consists in scrambling all the color pixels of an image, while in Section IV-C, we present a second approach, called intra-color pixel component scrambling (ICPCS), where the red, green, and blue components of color pixels are scrambled separately. In Section IV-D, we develop a third approach, called full color pixel component scrambling (FCPCS), which consists of scrambling together the red, green and blue components of image color pixels. Finally, we give details on the decryption phase in Section IV-E.

A. OVERVIEW OF THE PROPOSED CIE SCHEME

In this section, an overview of the proposed CIE scheme is detailed. This overview is illustrated in Fig. 4.

Let a color image I be a matrix of $M \times N$ pixels $p(i,j)$, with $0 \leq i < M$ and $0 \leq j < N$. Each color pixel $p(i,j)$ is composed of three color components and can be seen as a color triplet $(r(i,j), g(i,j), b(i,j))$, where each color component is encoded on 256 gray levels (8 bits/component).

Let an encrypted color image I_e be a matrix of $M \times N$ pixels $p(i',j')$, with $0 \leq i' < M$ and $0 \leq j' < N$. Each color pixel $p(i',j')$ of the encrypted image is also composed of three color components and can be seen as a color triplet $(r(i',j'), g(i',j'), b(i',j'))$, where each color component is encoded on 256 gray levels (8 bits/component).

As illustrated in Fig. 4, from a secret key K, the necessary initialization parameters of the chaotic system presented in Section III are generated. From the chaotic generator we obtain a pseudo-random number sequence (PRNS) S with elements $s(i,j)$.

On the color image side I, the first step of the proposed scheme, as illustrated in Fig. 4, consists first in decomposing the three color components. The next steps are based on the PRNS S, this consists of separately scrambling all color components $r(i,j)$, $g(i,j)$ and $b(i,j)$ of each pixel $p(i,j)$. The last step of the proposed CIE scheme is color image reconstruction in order to obtain an encrypted color image I_e.

Based on this proposed CIE scheme, in Sections IV-B, IV-C and IV-D we develop three different approaches. We start with a naive color pixel scrambling (CPS), passing through an intra-color pixel component scrambling (ICPCS) and finally a full color pixel component scrambling (FCPCS). Whatever the approach we used, our proposed CEI scheme is of complexity $O(n)$. Based on these three approaches, we show that scrambling acts not only as a permutation, but it can also act as a substitution, ensuring both confusion and diffusion properties.

B. COLOR PIXEL SCRAMBLING (CPS) APPROACH

In this section, based on the CIE scheme presented in Section IV-A, we develop the color pixel scrambling (CPS) approach. In the CPS approach, the three color components of each pixel are not dissociated. This means that for the CPS approach there is no decomposition step as illustrated in Fig. 4. In this case, as illustrated in Fig. 5, each pixel $p(i,j) = (r(i,j), g(i,j), b(i,j))$, of the original image I is moved to the position of $p(i',j') = (r(i',j'), g(i',j'), b(i',j'))$ in the encrypted image I_e such that:

$$p(i,j) \rightarrow p(i',j') \text{ with } \begin{cases} i' &= \lfloor s(i,j)/N \rfloor, \\ j' &= s(i,j) \ mod \ N, \end{cases} \quad (13)$$

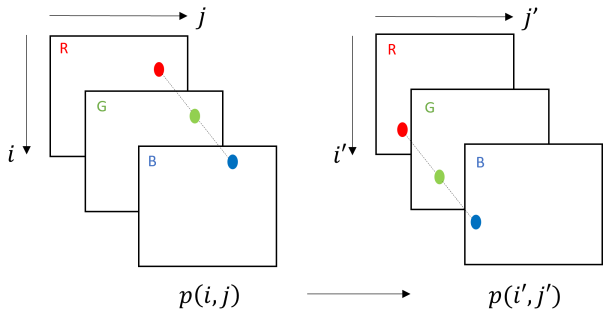


FIGURE 5: The proposed color pixel scrambling (CPS) approach.

where S is the PRNS generated by the chaotic generator, with $0 < s(i,j) \leq M \times N$, $|S| = M \times N$, $0 \leq i' < M$ and $0 \leq j' < N$.

When the sequence S generates a position which is already occupied, collision management is applied by moving this position to the next that is available.

Note that by applying the CPS approach, not only do the three 2D histograms related to the three color components R, G, and B of the original image remain unchanged, but the associated 3D histogram also stays identical.

C. INTRA-COLOR PIXEL COMPONENT SCRAMBLING (ICPCS) APPROACH

In this section, based on the CIE scheme presented in Section IV-A, we develop the intra-color pixel component scrambling (ICPCS) approach. In the ICPCS approach, as illustrated in Fig. 6, after the decomposition step, the three color components of each pixel of the original image I are scrambled separately within their own color component. In this case, the three color components $r(i,j)$, $g(i,j)$ and $b(i,j)$ of a pixel $p(i,j)$ of the original image I are moved separately within their own color component of the encrypted image I_e to the positions of $r(i',j')$, $g(i',j')$ and $b(i',j')$ respectively, such that:

$$r(i,j) \rightarrow r(i',j') \text{ with } \begin{cases} i' = \lfloor s(3N \times i, j)/3N \rfloor, \\ j' = s(3N \times i, j) \ mod \ N, \end{cases} \tag{14}$$

$$g(i,j) \rightarrow g(i',j') \text{ with } \begin{cases} i' = \lfloor s(3N \times i, j+N)/3N \rfloor, \\ j' = s(3N \times i, j+N) \ mod \ N, \end{cases} \tag{15}$$

$$b(i,j) \rightarrow b(i',j') \text{ with } \begin{cases} i' = \lfloor s(3N \times i, j+2N)/3N \rfloor, \\ j' = s(3N \times i, j+2N) \ mod \ N, \end{cases} \tag{16}$$

where S is the PRNS generated by the chaotic generator, with $0 < s(i,j) \leq 3 \times M \times N$, $|S| = 3 \times M \times N$, $0 \leq i' < M$ and $0 \leq j' < N$.

It can be noted that with this approach the length of the sequence S is three times longer than the one generated for the CPS approach. Collision management is also taken into account for this approach.

We can observe that by applying the ICPCS approach, even if the three 2D histograms related to the three color components R, G, and B of the original image remain unchanged, the associated 3D histogram extends and tends towards a uniform distribution. Indeed, after decomposing the original color image, by changing the positions of the color components within their own component, new combinations of color pixels are created. The distribution of the color cloud of the encrypted image seems to be uniformly distributed in a rectangular parallelepiped (bounding box).

D. FULL COLOR PIXEL COMPONENT SCRAMBLING (FCPCS) APPROACH

In this section, based on the CIE scheme presented in Section IV-A, we develop the full color pixel component scrambling (FCPCS) approach. In the FCPCS approach, as in the ICPCS approach, the three color components of each pixel of the original image I are scrambled separately after the decomposition step. But in this case, contrary to the ICPCS approach, as illustrated in Fig. 7, the three color components $r(i,j)$, $g(i,j)$ and $b(i,j)$ of a pixel $p(i,j)$ of the original image I are moved separately in the full encrypted image I_e to the positions of $c_0(i',j')$, $c_1(i',j')$ and $c_2(i',j')$ respectively, such that:

$$r(i,j) \rightarrow c_0(i',j') \text{ with } \begin{cases} i' = \lfloor s(3N \times i, j)/3N \rfloor, \\ j' = s(3N \times i, j) \ mod \ 3N, \end{cases} \tag{17}$$

$$g(i,j) \rightarrow c_1(i',j') \text{ with } \begin{cases} i' = \lfloor s(3N \times i, j+N)/3N \rfloor, \\ j' = s(3N \times i, j+N) \ mod \ 3N, \end{cases} \tag{18}$$

$$b(i,j) \rightarrow c_2(i',j') \text{ with } \begin{cases} i' = \lfloor s(3N \times i, j+2N)/3N \rfloor, \\ j' = s(3N \times i, j+2N) \ mod \ 3N, \end{cases} \tag{19}$$

where S is the PRNS generated by the chaotic generator, with $0 < s(i,j) \leq 3 \times M \times N$, $|S| = 3 \times M \times N$, $0 \leq i' < M$ and $0 \leq j' < 3N$.

The length of the sequence S is also three times longer than the one generated for the CPS approach. Collision management is also taken into account for this approach.

With the FCPCS approach, all the color pixel components of the image are scrambled together in the whole image. We can note that from Eq. (17), (18) and (19) we obtain three color components $c_0(i',j')$, $c_1(i',j')$ and $c_2(i',j')$ that do not necessary form a color triplet. This is due to the fact that to calculate j' we apply an operation $mod \ 3N$ (instead of $mod \ N$), and so we obtain values between 0 and $3 \times M \times N - 1$.

Finally, to obtain three color components of three different pixels of the encrypted image I_e, for each of the three values obtained $c_k(i',j')$, with $0 \leq k \leq 2$, we have to analyze if the value is less than N, less than $2N$ or less than $3N$:

$$c_k(i',j') = \begin{cases} r(i',j') \text{ if } 0 \leq j' < N, \\ g(i',j') \text{ if } N \leq j' < 2N, \\ b(i',j') \text{ if } 2N \leq j' < 3N. \end{cases} \tag{20}$$

Based on the values generated by the PRNS S, we can obtain different scenarios with the encrypted image I_e. For

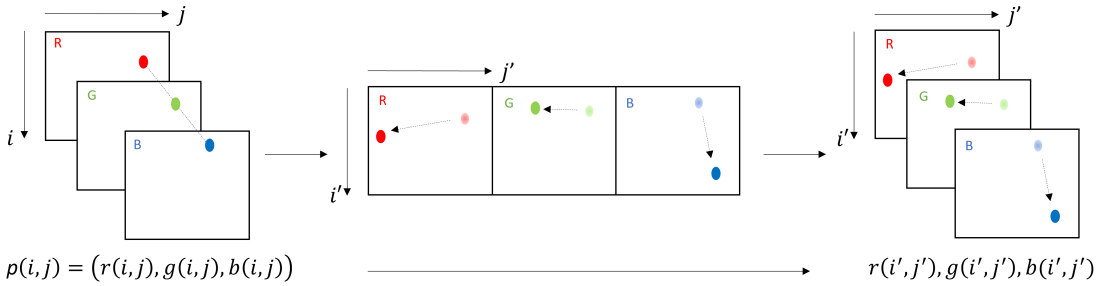


FIGURE 6: The proposed intra-color pixel component scrambling (ICPCS) approach.

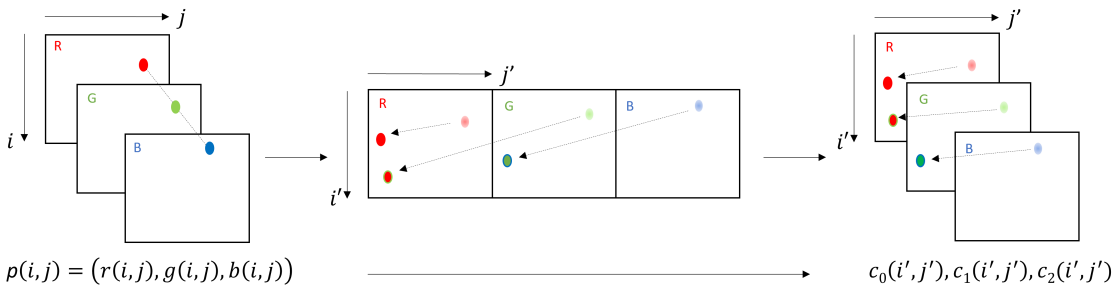


FIGURE 7: The proposed full color pixel component scrambling (FCPCS) approach.

example, the three $c_k(i', j')$ can be on the same color component R, G or B. It is also possible for every $c_k(i', j')$ to be in different color components.

Note that by applying the FCPCS approach, because a full scrambling is performed, the three 2D histograms related to the three color components R, G, and B of the original image are modified: they become almost identical. In addition, the expansion of the associated 3D histogram is more important than using the ICPCS approach and tends towards a uniform distribution. Indeed, the color cloud is larger than this corresponding to the two previous approaches. For the FCPCS approach, the rectangular parallelepiped is a cube (bounding box).

E. DECRYPTION OF AN ENCRYPTED COLOR IMAGE

For the decoding step, from the same secret key K, the necessary initialization parameters of the chaotic system presented in Section III are generated. From the chaotic generator, we obtain the same pseudo-random number sequence (PRNS) S with elements $s(i, j)$ that is used to reconstruct the original image from the encrypted one, regardless of the approach used (CPS, ICPCS or FCPCS). The original image is then reconstructed from the first pixel $p(0, 0)$ to the last one $p(M - 1, N - 1)$.

V. EXPERIMENTAL RESULTS

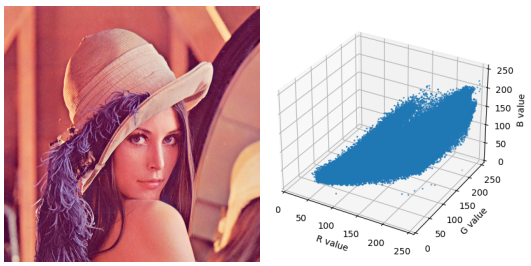
In this section, we present several results we obtained by applying our proposed CEI scheme to encrypt color images. Experiments and security analysis are presented to show the effectiveness and the originality of the proposed CIE scheme. Regarding the encryption phases, whatever the approach we used, the encryption applied to the images is based on the parameters detailed in Table 1. Based on a 256-bit encryption key K, we generate initial conditions for u and v. In our examples, we have $u = 0.00111870372955887447930711663025$ and $v = -0.98372466509577250354298356128242$.

In Section V-A, our CIE scheme is applied to the color image of Lena and presented in detail by applying and comparing the three proposed approaches. In Section V-C and Section V-D respectively, statistical analysis and differential attack analysis are presented and compared to current state-of-the-art methods combining permutation and substitution steps.

A. A FULL EXAMPLE

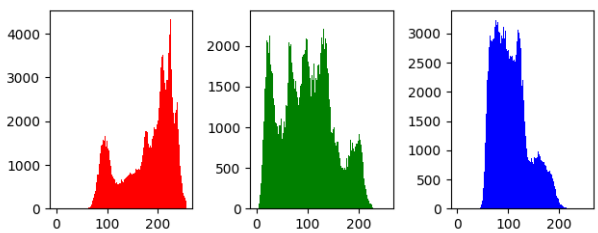
In this section, we develop our proposed scheme in detail by applying it to the color image of Lena, illustrated in Fig. 8a. The 3D histogram of the color image of Lena is illustrated in Fig. 8b. In addition, Fig. 9 shows the histograms, $\mathcal{H}_R(I)$ $\mathcal{H}_G(I)$ and $\mathcal{H}_B(I)$, of the three color components red, green and blue of the Lena color image respectively.

In Fig. 8b, we note that the distribution forms a color cloud with a connected envelope that does not cover the 3D RGB point cloud of 2^{24} possible colors. In Fig. 9, we observe a significant difference in the distributions of the three histograms as well as a significant variability. Moreover, in the histogram $\mathcal{H}_R(I)$ illustrated in Fig. 9a, the non-zero values of the distribution are between 56 and 255, while in the histogram $\mathcal{H}_G(I)$ illustrated Fig. 9b, the non-zero



(a) Lena color image (b) Lena 3D histogram

FIGURE 8: a) Original Lena color image, b) Its 3D histogram.



(a) $\mathcal{H}_R(I)$ (b) $\mathcal{H}_G(I)$ (c) $\mathcal{H}_B(I)$

FIGURE 9: Histograms of the three color components of the Lena color image: a) Red, b) Green, c) Blue.

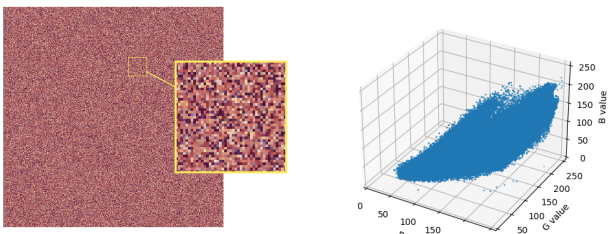
values of the distribution are between 3 and 248, and in the histogram $\mathcal{H}_B(I)$ illustrated in Fig. 9c, the non-zero values of the distribution are between 41 and 225.

In Section V-A1, we illustrate the obtained results on the Lena color image by applying the CPS approach. In Section V-A2, we present the obtained results on the Lena color image by applying the ICPCS approach. In Section V-A3, we show the obtained results on the Lena color image by applying the FCPCS approach. Finally, in Section V-A4, we propose to compare the obtained results with our proposed approaches with those obtained by a method combining permutation and substitution.

1) Color pixel scrambling (CPS) approach

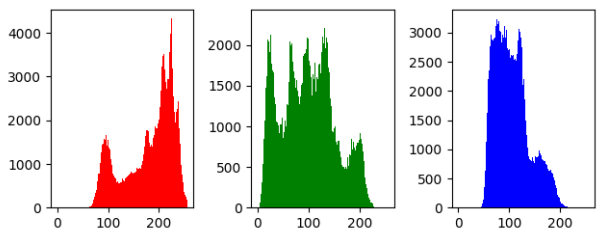
After applying the proposed CPS approach on the Lena color image illustrated in Fig. 8a, we obtain the encrypted image illustrated in Fig. 10a. In this encrypted image, we can no longer visually recognize its original content. However, we can observe that the red and orange colors of the encrypted image are those of the original image, which is normal since only the order of the color pixels has been scrambled.

Moreover, when we examine the histograms, both the 3D histogram displayed in Fig. 10b and the histograms of the three color components shown in Fig. 11 are exactly the same as those of the original image. Even if we present a statistical analysis in Section V-C, we can already say that this approach is not secure enough.



(a) CPS-based encrypted Lena color image (b) CPS 3D histogram

FIGURE 10: Encryption of the Lena color image by applying the proposed CPS approach: a) Encrypted Lena color image, b) The corresponding 3D histogram.

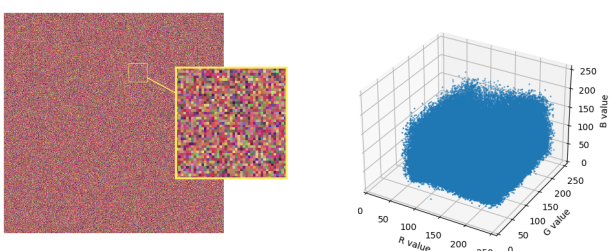


(a) $\mathcal{H}_R(I_e)$ (b) $\mathcal{H}_G(I_e)$ (c) $\mathcal{H}_B(I_e)$

FIGURE 11: Histograms of the three color components after applying the CPS approach to the Lena color image: a) Red, b) Green, c) Blue.

2) Intra-color pixel component scrambling (ICPCS) approach

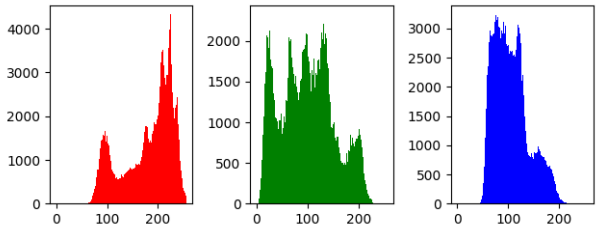
After applying the proposed ICPCS approach on Lena color image illustrated in Fig. 8a, we obtain the encrypted image illustrated in Fig. 12a. In this encrypted image, we can no longer visually recognize its original content. However, as with the CPS approach, we can notice that, with the ICPCS approach, the red and orange colors of the encrypted image also look like those of the original image.



(a) ICPCS-based encrypted Lena color image (b) ICPCS 3D histogram

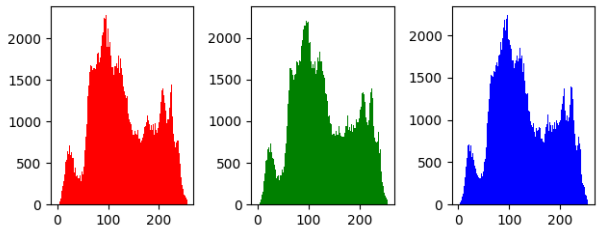
FIGURE 12: Encryption of the Lena color image applying the proposed ICPCS approach: a) Encrypted Lena color image, b) The corresponding 3D histogram.

Moreover, we can observe that the histograms of the three color components, $\mathcal{H}_R(I_e)$, $\mathcal{H}_G(I_e)$ and $\mathcal{H}_B(I_e)$, illustrated in Fig. 13, are exactly the same as those of the original image.



(a) $\mathcal{H}_R(I_e)$ (b) $\mathcal{H}_G(I_e)$ (c) $\mathcal{H}_B(I_e)$

FIGURE 13: Histograms of the three color components after applying the ICPCS approach to the Lena color image: a) Red, b) Green, c) Blue.



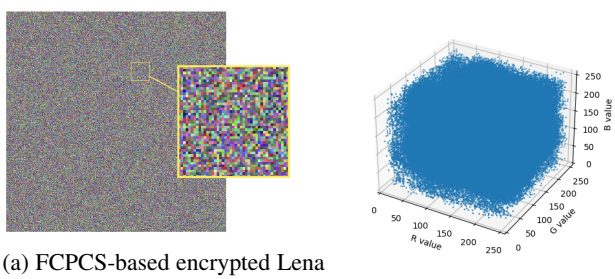
(a) $\mathcal{H}_R(I_e)$ (b) $\mathcal{H}_G(I_e)$ (c) $\mathcal{H}_B(I_e)$

FIGURE 15: Histograms of the three color components after applying the FCPCS approach to the Lena color image: a) Red, b) Green, c) Blue.

However, when we examine the 3D histogram displayed in Fig. 12b, we notice that the color cloud is different from the original image shown in Fig. 8b. Indeed, after decomposing the original color image, by changing the positions of the color components $r(i,j)$, $g(i,j)$ and $b(i,j)$ within their own component, we create new combinations of color pixels that occupy a larger space in the color cube. Then, based on the color components $r(i,j)$, $g(i,j)$ and $b(i,j)$ in the original image, the distribution of the color cloud of the encrypted image seems to be uniformly distributed in a rectangular parallelepiped (bounding box). As illustrated in Fig. 8b, this rectangular parallelepiped (bounding box) has edge lengths $\mathcal{R} = 200$, $\mathcal{G} = 246$ and $\mathcal{B} = 185$.

3) Full color pixel component scrambling (FCPCS) approach

After applying the proposed FCPCS approach on the Lena color image displayed in Fig. 8a, we obtain the encrypted image illustrated in Fig. 14a. In this encrypted image, as with the two previous approaches, we can no longer visually recognize its original content. But this time, with the FCPCS approach, we can notice that the red and orange colors contained in the original Lena color image have disappeared. Indeed, the encrypted image shown in Fig. 14a seems to cover the whole range of colors and therefore no color is prevalent.



(a) FCPCS-based encrypted Lena color image (b) FCPCS 3D histogram

FIGURE 14: Encryption of the Lena color image by applying the proposed FCPCS approach: a) Encrypted Lena color image, b) The corresponding 3D histogram.

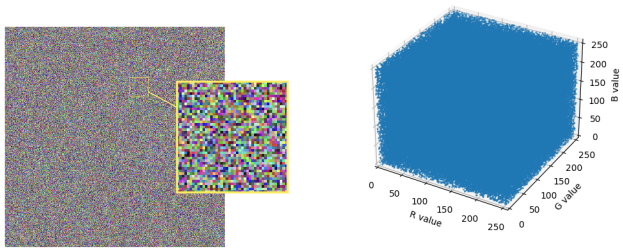
With the FCPCS approach, after decomposing the original color image, the positions of the color components $(r(i,j)$, $g(i,j)$ and $b(i,j))$ are moved separately in the entirety of the three color components to the positions $c_0(i',j')$, $c_1(i',j')$ and $c_2(i',j')$. As illustrated in Fig. 15, the FCPCS approach transforms the histograms of the three color components, $\mathcal{H}_R(I_e)$, $\mathcal{H}_G(I_e)$ and $\mathcal{H}_B(I_e)$ into three very similar histograms. Indeed, after the decomposition and the scrambling of all the original color components, we obtain a unique histogram in which the total number of occurrences is $3 \times M \times N$. This is why we obtain three very similar histograms after the reconstruction of the encrypted color image. We can observe that the first non-zero value of the three histograms illustrated in Fig. 15 is 3 which corresponds to the first non-zero values of the three original histograms $(min(56, 3, 41))$. In the same manner, the last non-zero value is 255, because $255 = max(255, 248, 225)$. Fig. 14b shows the obtained 3D histogram, where the color cloud is larger than that corresponding to the two previous approaches. For the FCPCS approach, the rectangular parallelepiped is a cube (bounding box) of edge length 253.

In Section V-A4, we compare the results obtained with our proposed scheme with those obtained if we add a substitution step to the FCPCS approach.

4) XOR full color pixel component scrambling (XOR-FCPCS)

In this section, we propose to compare the obtained results from our proposed approaches with those obtained with a method combining permutation and substitution. For this purpose, based on the FCPCS approach, we add an exclusive-OR (XOR) operation between the encrypted image obtained by the FCPCS approach (illustrated in Fig. 14a for the Lena color image) to obtain the final encrypted image illustrated in Fig. 16a. In order to apply the XOR operation, from the chaotic system using neurons presented in Section III, we generate a second PRNS.

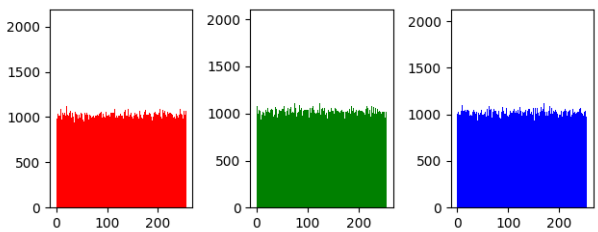
We can observe, in Fig. 17, that the histograms of the three color components are all uniform, due to the confusion process added to the proposed FCPCS approach and applied to the original color image of Lena. Fig.16 illustrates the 3D histogram of the obtained encrypted image, this shows that



(a) XOR-FCPCS-based encrypted Lena color image (b) XOR-FCPCS 3D histogram

FIGURE 16: Encryption of the Lena color image by applying an XOR-FCPCS approach: a) Encrypted Lena color image, b) The corresponding 3D histogram.

the obtained distribution forms a color cloud covering the entire 3D RGB point cloud of 2^{24} possible colors. For the XOR-FCPCS approach, the rectangular parallelepiped is a cube with edge length 256.



(a) $\mathcal{H}_R(I_e)$ (b) $\mathcal{H}_G(I_e)$ (c) $\mathcal{H}_B(I_e)$

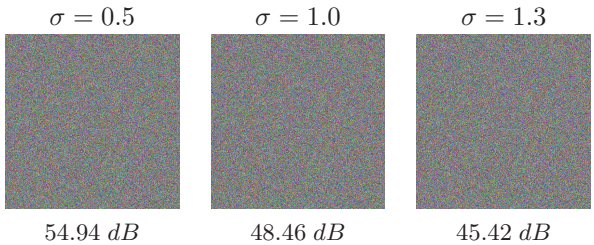
FIGURE 17: Histograms of the three color components after applying an XOR operation to the proposed FCPCS approach to the Lena color image: (a) Red, (b) Green, (c) Blue.

From this full example applied to the color image of Lena we can conclude that scrambling – in particular with our proposed FCPCS approach – acts not only as a permutation, but also as a substitution. This provides both confusion and diffusion properties, in particular on the 3D histogram of the encrypted color image. Although the histograms of the three color components are not completely uniform with our proposed approaches, we note that the distribution of the colors in the 3D histogram tends toward some uniformity, which allows us to achieve a certain level of security.

In section V-B, we propose to analyze the robustness of the proposed CEI scheme to noise and data loss.

B. ROBUSTNESS ANALYSIS TO NOISE AND DATA LOSS

In this section we analyze the robustness to noise and data loss of the proposed CEI scheme by comparing the proposed FCPCS approach and an XOR-FCPCS approach. We first analyze the robustness to Gaussian noise. Fig. 18 illustrates the results obtained when adding a Gaussian noise in the FCPCS-based encrypted color images, with a standard deviation $\sigma = 0.5$, $\sigma = 1.0$ or $\sigma = 1.3$. We note in Fig. 18a that when the standard deviation of the Gaussian noise increases the PSNR decreases. Since the FCPCS-based encrypted color images is only based on permutations, in the decrypted noised images illustrated in Fig. 18b we note that the PSNR obtained are exactly these obtained in the encrypted domain. This shows the robustness to noise of the proposed FCPCS approach.



(a) Noised FCPCS-based encrypted color images

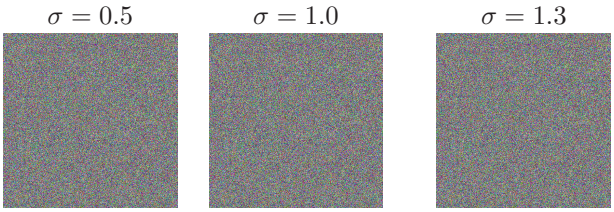
(b) Decrypted noised FCPCS-based encrypted color images

FIGURE 18: Robustness analysis to Gaussian noise of the proposed FCPCS approach: a) Noised FCPCS-based encrypted Lena color images by adding a Gaussian noise with a standard deviation $\sigma = 0.5$, $\sigma = 1.0$ or $\sigma = 1.3$, b) Corresponding decrypted noised FCPCS-based encrypted Lena color images.

On the contrary, if we add the same Gaussian noise on the XOR-FCPCS-based encrypted color images as illustrated in Fig. 19, we note that the results obtained are very different. Indeed, even if in the encrypted domain the PSNR are very similar to those obtained with the FCPCS approach (Fig. 19a), in the clear domain after the decryption we note that the PSNR decrease drastically. In Fig. 19b, for $\sigma = 0.5$, we obtain a $PSNR = 33.58\ dB$ instead of a $55.94\ dB$, and for $\sigma = 1.3$, we obtain a $PSNR = 26.62\ dB$ instead of a $45.42\ dB$. This shows that our FCPCS approach is much more robust to noise than an XOR-FCPCS approach since our FCPCS approach does not amplify Gaussian noise during the decryption.

In a second step we analyze the robustness to data loss. In Fig. 20, we illustrated the results obtained by simulating a data loss with a black box of square 50 pixels or 100 pixels in the center of the encrypted image and finally a black box of square 100 pixels shifted from the center.

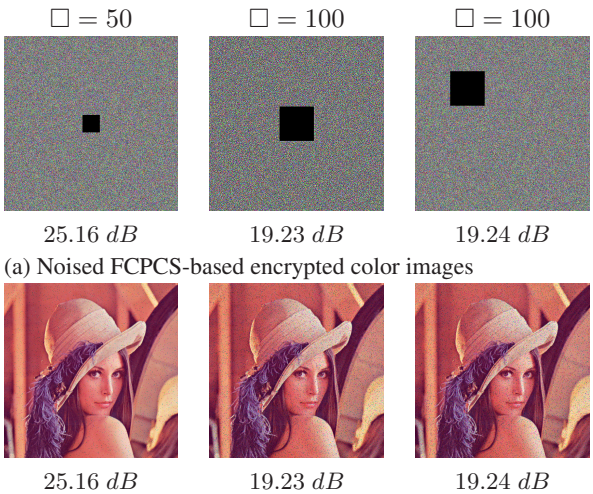
In this case, we note that the results we obtained are almost similar between the two approaches and only depend on the size of the black box and not on its position. Since the FCPCS-based encrypted color images is only based



(a) Noised XOR-FCPCS-based encrypted color images

(b) Decrypted noised XOR-FCPCS-based encrypted color images

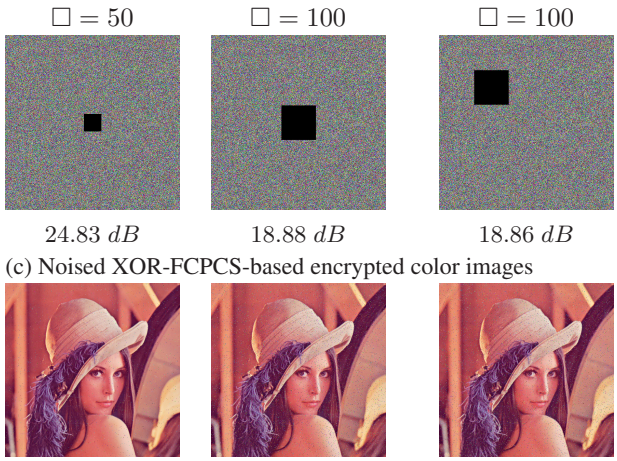
FIGURE 19: Robustness analysis to Gaussian noise of an XOR-FCPCS approach: a) Noised XOR-FCPCS-based encrypted Lena color images by adding a Gaussian noise with a standard deviation $\sigma = 0.5$, $\sigma = 1.0$ or $\sigma = 1.3$, b) Corresponding decrypted noised XOR-FCPCS-based encrypted Lena color images.



(a) Noised FCPCS-based encrypted color images

(b) Decrypted noised FCPCS-based encrypted color images

FIGURE 20: Robustness analysis to data loss of the proposed FCPCS approach: a) Noised FCPCS-based encrypted Lena color images with a black box of square 50 pixels or 100 pixels in the center of the encrypted image or shifted from the center, b) Corresponding decrypted noised FCPCS-based encrypted Lena color images.



(c) Noised XOR-FCPCS-based encrypted color images

(d) Decrypted noised XOR-FCPCS-based encrypted color images

FIGURE 21: Robustness analysis to data loss of an XOR-FCPCS approach: a) Noised XOR-FCPCS-based encrypted Lena color images with a black box of square 50 pixels or 100 pixels in the center of the encrypted image or shifted from the center, b) Corresponding decrypted noised XOR-FCPCS-based encrypted Lena color images.

on permutations, in the decrypted noised images illustrated in Fig. 20b, once again, we note that the obtained PSNR values are exactly these obtained in the encrypted domain. This shows the robustness and stability to noise of the proposed FCPCS approach. With an XOR-FCPCS approach, in Fig. 21b, we notice that the PNSR values increase by 3 dB compared to the FCPCS approach we proposed. Indeed, with the XOR operation, the pixels of the black box are transformed during decryption into other values which, statistically, are more probable to be close to the original values of the lost pixels.

In conclusion, we can say that our FCPCS approach is more robust to noise than a method based on an XOR operation. In section V-C, we propose to develop and present a statistical analysis of the proposed CEI scheme to confirm this level of security.

C. STATISTICAL ANALYSIS

To demonstrate the effectiveness of the proposed CIE scheme against statistical attacks, statistical tests are performed and the results are shown in this section. Based on the work proposed by [40] and [41], in Section V-C1, we present the results obtained by analyzing the correlation coefficients between adjacent pixels, both in the original and encrypted images. In Section V-C2, the obtained peak signal to noise ratios (PSNR) between the original and the encrypted images are presented, and finally in Section V-C3 we analyze the obtained Shannon entropy values and compare them with current state-of-the-art methods combining both permutation and substitution steps.

1) Correlation coefficient analysis (CCA) of two adjacent pixels

The calculation of the correlation coefficients of adjacent pixels in an encrypted image is one of the main metrics to give insight on the confusion and diffusion properties [8], [18], [40], [41]. To do so, we randomly select N (in our case, $N = 5,000$) pairs of two adjacent pixels x_i and y_i in horizontal and vertical directions from the original and encrypted images, and then calculate the correlation coefficients:

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{21}$$

where $C(x,y)$ is the co-variance between two gray level values of adjacent pixels x and y in an image:

$$C(x,y) = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{N}, \tag{22}$$

with $E(x)$ the average the pixel values of x:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{23}$$

and $D(x)$ the standard deviation of the pixel values of x:

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2. \tag{24}$$

The value of this correlation coefficient ranges between -1 and 1, where an absolute value close to 1 indicates a strong correlation and 0 indicates no correlation. Fig. 22 shows the correlation distribution of horizontally and vertically adjacent pixels in the three color components of the original Lena color image. As we can see in Fig. 22, the correlation between the neighboring pixels of the original image is very strong.

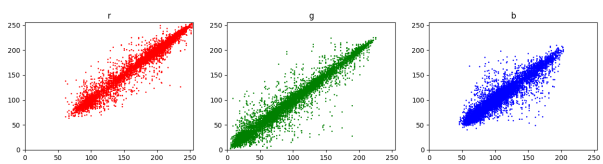


FIGURE 22: Correlation distribution of horizontally and vertically adjacent pixels in the three color components of the original Lena color image in Fig. 8a.

This high correlation for the original Lena color image is confirmed in Table 2. Indeed, whatever the color component or the direction, since the values of the neighboring pixels in the clear domain are highly correlated, the average correlation coefficient is equal to 0.9675.

Fig. 23 shows the correlation distribution of horizontally and vertically adjacent pixels in the three color components of the CPS-based encrypted Lena color image illustrated Fig. 10a. In this case, the correlation between neighboring pixels of the CPS-based encrypted Lena color image significantly decreases because the pixel positions have changed. In Table 2, for the CPS approach we can see that the average correlation coefficient is equal to 7.9 10^{-3}.

TABLE 2: Correlation coefficients of horizontally and vertically adjacent pixels in the three color components of the original Lena color image and the three proposed CIE approaches.

Image		Direction	Original image	CPS	ICPCS	FCPCS	XOR
Lena	R	Horizontal	0.9787	0.0008	0.0008	0.0078	0.0009
		Vertical	0.9895	-0.0133	-0.0012	-0.0020	-0.0004
Lena	G	Horizontal	0.9647	-0.0036	0.0108	-0.0014	-0.0033
		Vertical	0.9823	0.0057	0.0029	0.0017	-0.0026
Lena	B	Horizontal	0.9323	0.0146	0.0000	0.0124	0.0007
		Vertical	0.9573	0.0094	-0.0009	0.0006	0.0026
Average			**0.9675**	**0.0079**	**0.0028**	**0.0043**	**0.0017**

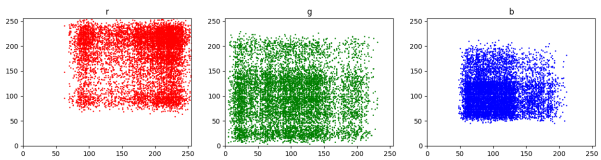


FIGURE 23: Correlation distribution of horizontally and vertically adjacent pixels in the three color components of the CPS-based encrypted Lena color image Fig. 10a.

However, we also observe on Fig. 23 that the coefficients are not totally diffused on the map. This is normal since the histograms of the three color components of the CPS-based encrypted Lena color image do not cover all the possible values, as shown in Fig. 11.

Fig. 24 shows the correlation distribution of horizontally and vertically adjacent pixels in the three color components of the ICPCS-based encrypted Lena color image illustrated in Fig. 12a. As in the CPS approach, the correlation between neighboring pixels of the CPS-based encrypted Lena color image significantly decreases because the pixel positions have changed. In Table 2, for the ICPCS approach, we can see that the average correlation coefficient is equal to 2.8 10^{-3}, which is similar to CPS approach.

Moreover, since the original histograms of the three color components are still preserved (Fig. 13), we notice on Fig. 24 that the coefficients are not totally diffused on the map, in a similar way as the CPS approach.

Fig. 25 shows the correlation distribution of horizontally and vertically adjacent pixels in the three color components of the FCPCS-based encrypted Lena color image illustrated in Fig. 14a. With the FCPCS approach, since the three color components of each pixel of the original image are moved separately in the full encrypted image, we can observe in Fig. 25 that the correlation between neighboring pixels considerably decreases. Indeed, the correlation coefficients

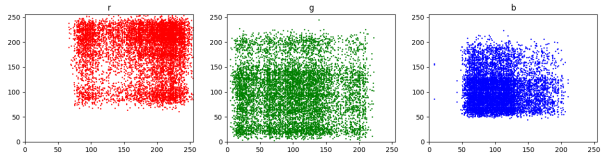


FIGURE 24: Correlation distribution of horizontally and vertically adjacent pixels in the three color components of the ICPCS-based encrypted Lena color image in Fig. 12a.

are spread over the whole map. In Table 2, for the FCPCS approach we can see that the average correlation coefficient is equal to $4.3\ 10^{-3}$.

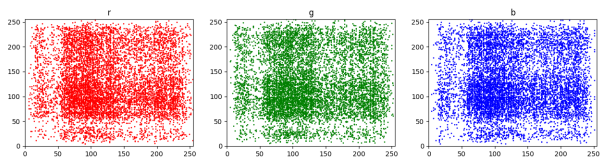


FIGURE 25: Correlation distribution of horizontally and vertically adjacent pixels in the three color components of the FCPCS-based encrypted Lena color image in Fig. 14a.

In order to make comparisons between our proposed approaches and an approach in which a substitution step has been added by performing an XOR operation, Fig. 26 shows the correlation distribution of horizontally and vertically adjacent pixels in the three color components of the XOR-FCPCS-based encrypted Lena color image shown in Fig. 16a. In this case, the diffusion is indeed more uniform than with our approach, but in Table 2, for the XOR-FCPCS approach, we can see that the average correlation coefficient is very similar than that obtained with all the proposed approaches (equal to $1.7\ 10^{-3}$.).

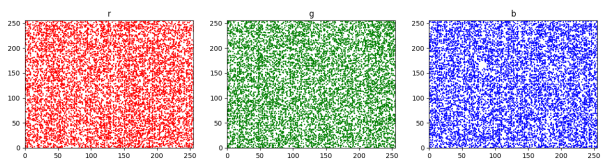
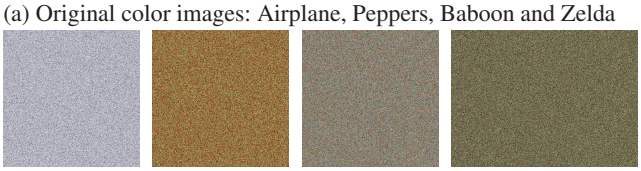


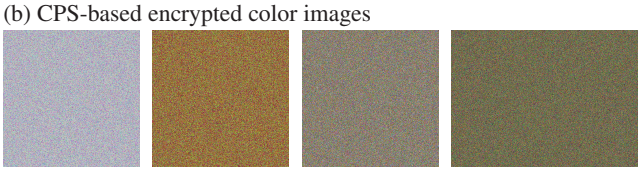
FIGURE 26: Correlation distribution of horizontally and vertically adjacent pixels in the three color components of the XOR-FCPCS-based encrypted Lena color image in Fig. 16a.

Fig. 27 illustrates the results obtained with our proposed CEI scheme when applying to four well-known color images, namely Airplane, Peppers, Baboon and Zelda. Table 3 sum-

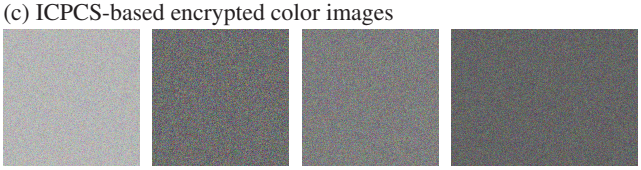
(a) Original color images: Airplane, Peppers, Baboon and Zelda



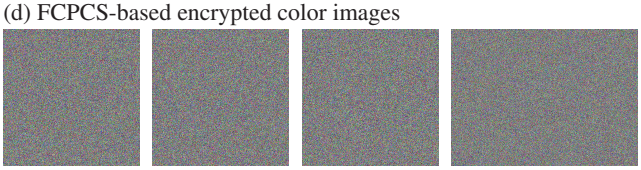
(b) CPS-based encrypted color images



(c) ICPCS-based encrypted color images



(d) FCPCS-based encrypted color images



(e) XOR-FCPCS-based encrypted color images

FIGURE 27: a) Original color images Airplane, Peppers, Baboon and Zelda, b) CPS-based encrypted color images, c) ICPCS-based encrypted color images, d) FCPCS-based encrypted color images, e) XOR-FCPCS-based encrypted color images.

TABLE 3: Correlation coefficients of horizontally and vertically adjacent pixels in the three color components of the original color images and the three proposed CIE approaches applied to the five studied color images.

Image	Direction	Original image	CPS	ICPCS	FCPCS	XOR
Lena	Horizontal	0.9586	0.0063	0.0039	0.0072	0.0016
	Vertical	0.9764	0.0095	0.0017	0.0014	0.0018
Baboon	Horizontal	0.8987	0.0039	0.0054	0.0016	0.0043
	Vertical	0.8384	0.0055	0.0080	0.0034	0.0050
Airplane	Horizontal	0.9596	0.0031	0.0025	0.0044	0.0033
	Vertical	0.9549	0.0039	0.0033	0.0041	0.0044
Peppers	Horizontal	0.9669	0.0058	0.0053	0.0019	0.0046
	Vertical	0.9710	0.0078	0.0047	0.0050	0,0041
Zelda	Horizontal	0.9900	0.0038	0.0010	0.0048	0.0017
	Vertical	0.9886	0.0014	0.0047	0.0033	0.0045
Average		**0.9503**	**0.0051**	**0.0040**	**0.0037**	**0.0035**

marizes the correlation coefficients obtained when applying our proposed approaches to five well-known color images, namely Lena, Baboon, Airplane, Peppers and Zelda. The correlation coefficients obtained for the original color images are high and close to 1, with an average of 0.9503. In contrast, all the correlation coefficients obtained for the encrypted images with our proposed approaches are very close to 0. On average, for the CPS and ICPCS approaches, the correlation coefficients are $5.1\ 10^{-3}$ and $4.0\ 10^{-3}$ respectively, while for the FCPCS approach, we reach an average correlation coefficient of $3.7\ 10^{-3}$, which is very similar to the value obtained with the XOR-FCPCS approach ($3.5\ 10^{-3}$). Thus, this analysis shows the efficiency of the proposed CIE scheme in eliminating the correlation of adjacent pixels.

2) Peak signal-to-noise ratio analysis

To evaluate the reliability of the proposed approaches, this section presents the peak signal-to-noise ratio (PSNR) values obtained between the original and encrypted images. The PSNR is based on the mean square error (MSE) which measures the average squared error between the original pixel values and the encrypted pixel values:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (p(i,j) - p'(i,j))^2, \qquad (25)$$

where $M \times N$ is the number of pixels in the image, $p(i,j)$ the original pixel values and $p'(i,j)$ the encrypted ones.

From a MSE, we can then calculate the corresponding PSNR, that is measured in decibels (dB):

$$\text{PSNR} = 10\ log_{10} \frac{R^2}{\text{MSE}}, \qquad (26)$$

where R is the maximum gray level value of a pixel. In our case, since each color component is encoded on 256 gray levels (8 bits/component), we have $R = 255$.

TABLE 4: PSNR between the three original color components and the corresponding encrypted components with our proposed CIE approaches for the five studied color images.

PSNR (dB)					
Image		CPS	ICPCS	FCPCS	XOR
Lena	R	11.30	11.32	8.79	7.85
	G	10.65	10.66	9.60	8.56
	B	14.47	14.48	11.03	9.62
Baboon	R	10.23	10.24	10.11	8.78
	G	11.53	11.53	10.77	9.26
	B	9.31	9.32	9.59	8.36
Airplane	R	12.15	12.15	12.18	8.15
	G	10.82	10.84	11.46	7.85
	B	14.95	14.96	13.28	7.93
Peppers	R	12.02	12.02	9.12	9.10
	G	7.62	7.61	8.10	7.63
	B	12.19	12.18	8.95	7.65
Zelda	R	9.64	9.64	9.89	8.52
	G	10.81	10.82	10.56	8.86
	B	12.20	12.21	10.84	8.28
Average		**11.33**	**11.33**	**10.29**	**8.43**

Table 4 shows the PSNR obtained for the five studied color images. The results we obtained show that, whatever the CIE approach, the PSNR values are very low (less than 15 dB). For the CPS and ICPCS approaches, the average PSNR is $11.33\ dB$, while for FCPCS approach, the average PSNR decreases to $10.29\ dB$ and to $8.43\ dB$ for the XOR-FCPCS approach. Note that from a visual security point of view, a PSNR lower than $12\ dB$ guarantees a confidential level [42].

3) Shannon entropy

To be resilient to a statistical attack, the histogram of the encrypted image must be as uniform as possible and also different from that of the original image. In this section, we propose to calculate the Shannon entropy $H(I)$ to measure the uniformity of the distribution of the encrypted images generated by our proposed approaches:

$$H(I) = \sum_{i=0}^{2^l-1} P(g_i) log_2 \frac{1}{P(g_i)}, \qquad (27)$$

where I is an image with pixels encoded with l bits, and $P(g_i)$ is the probability related to the gray level g_i.

The value of entropy is given in bits per pixel (bpp) and is between 0 bpp and l bpp. In our case, the maximum value of the entropy is 8 bpp.

Table 5 lists the entropy values of the original and encrypted images obtained using our proposed CIE approaches applied to the five studied color images. While the entropy values associated with the encrypted images generated by the CPS and ICPCS approaches are exactly the same as the original images (7.265 bpp on average), we can note that the entropy values associated with the encrypted images generated by the FCPCS approach increase and tend towards 8 bpp (7.503 bpp on average). For the XOR-FCPCS approach, the average Shannon entropy is 7.999 bpp. This indicates that the FCPCS approach has a good random performance.

TABLE 5: Shannon entropy (in bpp) of the three color components of the original and encrypted images with the three proposed CIE approaches applied to the five studied color images.

Image	Original image	CPS	ICPCS	FCPCS	XOR
Lena	7.272	7.272	7.272	7.749	7.999
Baboon	7.644	7.644	7.644	7.762	7.999
Airplane	6.577	6.577	6.577	6.663	7.999
Peppers	7.298	7.298	7.298	7.669	7.999
Zelda	7.532	7.532	7.532	7.671	8.000
Average	**7.265**	**7.265**	**7.265**	**7.503**	**7.999**

In Table 6, we compare the values we obtained using our proposed approaches with the results of Ben Slimane *et al.* [2], [18], Wu *et al.* [24], Hu *et al.* [28] and Lone *et al.* [43] methods. All of these state-of-the-art methods generate both diffusion and confusion because they are all based on permutation and substitution steps. Note that only three color images (Lena, Baboon and Peppers) are used for comparisons due to the availability of the results in the

TABLE 6: Shannon entropy (in *bpp*) comparisons with previous work for CIE.

Entropy (*bpp*)			
Image	Lena	Baboon	Peppers
CPS	7.272	7.644	7.298
ICPCS	7.272	7.644	7.298
FCPCS	7.749	7.762	7.669
XOR	7.999	7.999	7.999
Ben Slimane *et al.* [2]	7.999	7.999	N/A
Ben Slimane *et al.* [18]	7.998	7.998	7.998
Wu *et al.* [24]	7.997	7.999	N/A
Hu *et al.* [28]	7.994	N/A	7.996
Lone *et al.* [43]	7.994	N/A	7.996

other papers. We can see that our results with the FCPCS approach, even though they do not reach the maximum value of 8 *bpp*, are comparable with those obtained with previous work.

D. DIFFERENTIAL ATTACK ANALYSIS

In this section, differential attack analyses are presented and compared with current state-of-the-art methods combining both permutation and substitution steps. Section V-D1, develops on the results obtained for the number of pixel change rates (NPCR), while Section V-D2, presents the results for the unified average changing intensity (UACI). Finally, Section V-D3 illustrates three examples of key sensitivity for the decryption step.

1) Number of pixel change rate (NPCR)

NPCR is used to calculate the percentage of different pixel counts between an original image and an encrypted image, or between two images encrypted with two different keys:

$$\text{NPCR} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} D(i,j) \times 100, \qquad (28)$$

where:

$$D(i,j) = \begin{cases} 1, \text{ if } p(i,j) \neq p'(i,j), \\ 0, \text{ else,} \end{cases} \qquad (29)$$

with $M \times N$ is the image pixel number, $p(i,j)$ the original pixel values and $p'(i,j)$ the encrypted ones.

A high value (close to 100 %) of NPCR indicates that the encryption algorithm can better resist differential attacks.

Table 7 presents the NPCR obtained between the three original color components and the corresponding encrypted color components with our proposed CIE approaches for the five studied color images. We can notice that all the values obtained are very high and very close to 100%. We can note that, for the FCPCS approach, we obtain an average for the NPCR of 99.26%, while with the XOR-FCPCS approach, the average NPCR value is 99.61%.

In Table 8, the results obtained with our proposed CIE approaches are compared with previous work (Ben Slimane *et al.* [2], [18], Wu *et al.* [24], Hu *et al.* [28] and Lone *et al.* [43]). Note that only three color images (Lena, Baboon and Peppers) are used for comparison due to the availability of the results in the other papers. We can observe that the NPCR obtained with our CIE scheme, in particular with the FCPCS approach (very close to 99.5%), is very similar to those obtained by other current state-of-the-art methods that combine permutation and substitution steps.

TABLE 7: NCPR between the three original color components and the corresponding encrypted color components with our proposed CIE approaches for the five studied color images.

Image		NPCR (%)			
		CPS	ICPCS	FCPCS	XOR
Lena	R	99.24	99.25	99.54	99.62
	G	99.45	99.44	99.53	99.62
	B	99.08	99.06	99.38	99.62
Baboon	R	99.50	99.46	99.54	99.61
	G	99.40	99.41	99.53	99.60
	B	99.49	99.49	99.38	99.59
Airplane	R	98.61	98.54	98.58	99.60
	G	98.60	98.58	98.54	99.61
	B	97.98	97.93	98.27	99.60
Peppers	R	99.29	99.29	99.56	99.63
	G	99.12	99.15	99.34	99.60
	B	98.91	98.88	99.30	99.61
Zelda	R	99.50	99.48	99.49	99.62
	G	99.42	99.43	99.47	99.62
	B	99.32	99.31	99.41	99.62
Average		**99.13**	**99.11**	**99.26**	**99.61**

TABLE 8: NPCR comparisons with previous work for CIE.

NPCR (%)			
Image	Lena	Baboon	Peppers
CPS	99.26	99.46	99.11
ICPCS	99.25	99.45	99.11
FCPCS	99.48	99.48	99.40
XOR	99.62	99.60	99.61
Ben Slimane *et al.* [2]	99.63	99.61	99.63
Ben Slimane *et al.* [18]	99.71	99.72	99.74
Wu *et al.* [24]	99.67	N/A	99.61
Hu *et al.* [28]	99.76	99.71	99.62
Lone *et al.* [43]	99.60	99.63	N/A

2) Unified average changing intensity (UACI)

UACI is also used to measure the average intensity of the differences between two images, which can be an original image and a corresponding encrypted image:

$$\text{UACI} = \frac{100}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} \frac{|p(i,j) - p'(i,j)|}{R}, \qquad (30)$$

with $M \times N$ is the image pixel number, $p(i,j)$ the original pixel values, $p'(i,j)$ the encrypted ones, and R the maximum gray level value of a pixel (in our case $R = 255$).

Table 9 presents the UACI obtained between the three original color components and the corresponding encrypted color components with our proposed CIE approaches for the five studied color images. We note that the average UACI for the CPS and the ICPCS approaches are very similar and

equal to 21.75% and 21.74% respectively. We can also note, in Table 9, that the average UACI for the FCPCS approach increases significantly and is equal to 24.84%, while the average UACI for the XOR-FCPCS approach is equal to 33.64%.

TABLE 9: UACI between the three original color components and the corresponding encrypted color components with our proposed CIE approaches for the five studied color images.

Image		UACI (%)			
		CPS	ICPCS	FCPCS	XOR
Lena	R	21.38	21.35	30.08	33.12
	G	23.76	23.72	26.74	33.60
	B	14.96	14.95	22.48	33.61
Baboon	R	24.90	24.87	30.08	33.92
	G	21.58	21.59	26.74	33.50
	B	27.36	27.36	22.48	33.29
Airplane	R	17.65	17.66	17.37	33.94
	G	20.26	20.21	18.68	33.07
	B	12.19	12.16	14.80	33.80
Peppers	R	19.95	19.97	28.71	33.97
	G	33.48	33.49	32.10	33.91
	B	18.77	18.78	29.01	33.88
Zelda	R	26.77	26.76	26.01	33.76
	G	23.28	23.26	24.09	33.66
	B	19.95	19.92	23.25	33.52
Average		**21.75**	**21.74**	**24.84**	**33.64**

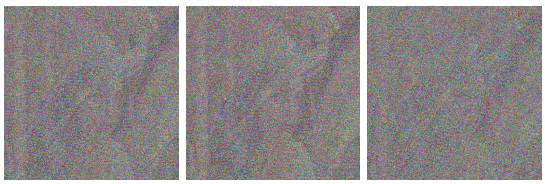
TABLE 10: UACI comparisons with previous work for CIE.

UACI (%)			
Image	Lena	Baboon	Peppers
CPS	20.03	24.61	24.07
ICPCS	20.00	24.61	24.08
FCPCS	26.43	26.43	29.93
XOR	33.44	33.57	33.95
Ben Slimane *et al.* [2]	33.43	33.40	N/A
Ben Slimane *et al.* [18]	33.45	33.49	33.53
Wu *et al.* [24]	33.38	N/A	33.47
Hu *et al.* [28]	33.38	N/A	33.38
Lone *et al.* [43]	33.28	33.25	N/A

In Table 10, the results obtained with our proposed CIE approaches are also compared with previous work (Ben Slimane *et al.* [2], [18], Wu *et al.* [24], Hu *et al.* [28] and Lone *et al.* [43]). Note that only three color images (Lena, Baboon and Peppers) are used for comparisons due to the availability of the results in the other papers. We can observe that the UACI obtained with the proposed FCPCS approach increases a lot, and tends towards those obtained by current state-of-the-art methods that combine permutation and substitution steps.

3) Illustration of key sensitivity analysis

From the color image of Lena encrypted by FCPCS with the 256-bit encryption key K, shown in Fig. 14a, for the decryption, if we replace the key K with another 256-bit key K', then the decryption does not work at all. Indeed, as illustrated



(a) K' (b) K'' (c) K'''

FIGURE 28: Decryption of the FCPCS-based encrypted Lena color image shown Fig. 14a, with another 256-bit key: a) K' modifying the initial value of u, b) K'' modifying the initial value of v, c) K''' modifying the initial values of u and v.

in Fig. 28, the three decrypted images with another 256-bit key are not correct. In Fig. 28a the 256-bit key K' modifies the initial value of u for the decryption step. In this case, between the original color image of Lena and this decrypted image, we obtain $PSNR = 10.13\ dB$, $NPCR = 89.11\%$ and $UACI = 23.88\%$. In Fig. 28b the 256-bit key K'' modifies the initial value of v for the decryption step and in this case, we obtain $PSNR = 10.20\ dB$, $NPCR = 87.70\%$ and $UACI = 23.50\%$. Finally, in Fig. 28c the 256-bit key K''' modifies both the initial values of u and v for the decryption step. In this case, we obtain $PSNR = 9.96\ dB$, $NPCR = 93.12\%$ and $UACI = 24.88\%$.

VI. CONCLUSION

In this paper, we have described a new CIE scheme based on a single scroll chaotic system for encrypting color images. After decomposing the color components of a color image, we apply color pixel scrambling that uses a PRNS generated by the proposed chaotic generator system, to finally obtain an encrypted color image. Based on the proposed CIE scheme, we then developed three approaches to encrypt color images, all uniquely based on a scrambling step. While in the CPS approach, the color pixels of the original image are scrambled, the ICPCS approach scrambles the components of the color pixels separately. The third proposed approach, called the FCPCS approach, involves scrambling together the red, green and blue components of the image color pixels.

The experimental results we have obtained show that the proposed CIE scheme, in particular the FCPCS approach, is efficient. Indeed, the results of both statistical and differential attack analyses tend towards those obtained by the current state-of-the-art methods that combine permutation and substitution steps. Thus, we can confirm that scrambling can act not only as a permutation, but also as a substitution, ensuring both confusion properties and diffusion properties.

Then we can ask ourselves the question of the boundary between the diffusion step, which often occurs through a scrambling and the confusion step, which often occurs through a substitution. Especially when performing a CIE, we have noted in this paper that a specific scrambling of color pixel components, produces, in addition to the diffusion,

a confusion. What would happen if we went even further and scrambled the together of each color pixel component together? We would then obtain a complete confusion, generated only by scrambling.

In perspective, the robustness of the proposed FCPCS approach could be analyzed. In addition, the new chaotic system could be coupled with multidendrites and the applications of the proposed CIE system could be applied on a larger database.

ACKNOWLEDGMENT

This work was supported in part by the university of Monastir, Tunisia and in part with the LIRMM laboratory, Université de Montpellier, CNRS, France.

REFERENCES

[1] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 7, pp. 1670–1681, 2018.

[2] N. B. Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "An efficient nested chaotic image encryption algorithm based on DNA sequence," *International Journal of Modern Physics C*, vol. 29, no. 7, p. 1850058, 2018.

[3] C. Abikoye Oluwakemi, S. Adewole Kayode, and J. Oladipupo Ayotunde, "Efficient data hiding system using cryptography and steganography," *International Journal of Applied Information Systems*, vol. 4, no. 11, pp. 6–11, 2012.

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

[5] P. P. Dang and P. M. Chau, "Image encryption for secure internet multimedia applications," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 3, pp. 395–403, 2000.

[6] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Processing*, vol. 90, no. 9, pp. 2714–2722, 2010.

[7] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools and Applications*, vol. 78, no. 18, pp. 26 203–26 222, 2019.

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

[9] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve elgamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017.

[10] M. K. Khan, J. Zhang, and X. Wang, "Chaotic hash-based fingerprint biometric remote user authentication scheme on mobile devices," *Chaos, Solitons & Fractals*, vol. 35, no. 3, pp. 519–524, 2008.

[11] S. Kumari, X. Li, F. Wu, A. K. Das, H. Arshad, and M. K. Khan, "A user friendly mutual authentication and key agreement scheme for wireless sensor networks using chaotic maps," *Future Generation Computer Systems*, vol. 63, pp. 56–75, 2016.

[12] A. Qayyum, J. Ahmad, W. Boulila, S. Rubaiee, Arshad, F. Masood, F. Khan, and W. J. Buchanan, "Chaos-based confusion and diffusion of image pixels using dynamic substitution," *IEEE Access*, vol. 8, pp. 140 876–140 895, 2020.

[13] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari, and B. Gupta, "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain," *Multimedia Tools and Applications*, vol. 76, no. 18, pp. 18 451–18 472, 2017.

[14] J.-H. Huh, "PLC-integrated sensing technology in mountain regions for drone landing sites: focusing on software technology," *Sensors*, vol. 18, no. 8, p. 2693, 2018.

[15] J.-H. Huh and K. Seo, "Blockchain-based mobile fingerprint verification and automatic log-in platform for future computing," *The Journal of Supercomputing*, vol. 75, no. 6, pp. 3123–3139, 2019.

[16] M. A. Alsmirat, F. Al-Alem, M. Al-Ayyoub, Y. Jararweh, and B. Gupta, "Impact of digital fingerprint image quality on the fingerprint recognition accuracy," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3649–3688, 2019.

[17] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Optics & Laser Technology*, vol. 101, pp. 30–41, 2018.

[18] N. Ben Slimane, N. Aouf, K. Bouallegue, and M. Machhout, "A novel chaotic image cryptosystem based on DNA sequence operations and single neuron model," *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30 993–31 019, 2018.

[19] N. Ben Slimane, K. Bouallegue, and M. Machhout, "Designing a multi-scroll chaotic system by operating logistic map with fractal process," *Nonlinear Dynamics*, vol. 88, no. 3, pp. 1655–1675, 2017.

[20] S. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Physical review E*, vol. 51, no. 4, p. 3670, 1995.

[21] J. L. Kaplan and J. A. Yorke, "Preturbulence: a regime observed in a fluid flow model of Lorenz," *Communications in Mathematical Physics*, vol. 67, no. 2, pp. 93–108, 1979.

[22] E. Bilotta, P. Pantano, and F. Stranges, "A gallery of Chua attractors: Part I," *International journal of Bifurcation and chaos*, vol. 17, no. 1, pp. 1–60, 2007.

[23] A. Belazi, R. Rhouma, and S. Belghith, "A novel approach to construct S-box based on Rossler system," in *11th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2015, pp. 611–615.

[24] X. Wu, B. Zhu, Y. Hu, and Y. Ran, "A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps," *IEEE Access*, vol. 5, pp. 6429–6436, 2017.

[25] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18 759–18 770, 2018.

[26] L. Liu, L. Zhang, D. Jiang, Y. Guan, and Z. Zhang, "A simultaneous scrambling and diffusion color image encryption algorithm based on Hopfield chaotic neural network," *IEEE Access*, vol. 7, pp. 185 796–185 810, 2019.

[27] M. A. Malik, Z. Bashir, N. Iqbal, and M. A. Imtiaz, "Color image encryption algorithm based on hyper-chaos and DNA computing," *IEEE Access*, vol. 8, pp. 88 093–88 107, 2020.

[28] X. Hu, L. Wei, W. Chen, Q. Chen, and Y. Guo, "Color image encryption algorithm based on dynamic chaos and matrix convolution," *IEEE Access*, vol. 8, pp. 12 452–12 466, 2020.

[29] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, "A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques," *IEEE Access*, vol. 9, pp. 61 334–61 345, 2021.

[30] A. M. Asl, A. Broumandnia, and S. J. Mirabedini, "Scale invariant digital color image encryption using a 3D modular chaotic map," *IEEE Access*, vol. 9, pp. 102 433–102 449, 2021.

[31] Z. A. Abduljabbar, I. Q. Abduljaleel, J. Ma, M. A. Al Sibahee, V. O. Nyangaresi, D. G. Honi, A. I. Abdulsada, and X. Jiao, "Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map," *IEEE Access*, vol. 10, pp. 26 257–26 270, 2022.

[32] K. Bouallegue, "A new class of neural networks and its applications," *Neurocomputing*, vol. 249, pp. 28–47, 2017.

[33] G. Bouallegue, R. Djemal, and K. Belwafi, "Artificial EEG signal generated by a network of neurons with one and two dendrites," *Results in Physics*, vol. 20, p. 103699, 2021.

[34] S. Nasr, K. Bouallegue, and H. Mekki, "Fractal, chaos and neural networks in path generation of mobile robot," *International Journal of Modelling, Identification and Control*, vol. 34, no. 1, pp. 41–50, 2020.

[35] S. B. Mamia, W. Puech, and K. Bouallegue, "Generation of chaotic attractors using neurons with multidentrites," *International Journal of Modelling, Identification and Control*, vol. 40, no. 1, pp. 92–104, 2022.

[36] ——, "Impact of neuron network on the generation of chaotic attractors," in *8th International Conference on Control, Decision and Information Technologies (CoDIT)*, vol. 1. IEEE, 2022, pp. 332–336.

[37] N. Li, W. Tan, and H. Zhao, "Hopf bifurcation analysis and chaos control of a chaotic system without Silnikov orbits," *Discrete Dynamics in Nature and Society*, vol. 2015, 2015.

[38] Y. Miladi and M. Feki, "Bifurcation, quasi-periodicity, chaos, and co-existence of different behaviors in the controlled H-bridge inverter," in *Handbook of Research on Advanced Intelligent Control Engineering and Automation*. IGI Global, 2015, pp. 301–332.

[39] B. Robert, M. Feki, and H. H. Iu, "Control of a PWM inverter using proportional plus extended time-delayed feedback," *International Journal of Bifurcation and Chaos*, vol. 16, no. 01, pp. 113–128, 2006.
[40] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 2022, no. 21, pp. 917–935, 2022.
[41] J. Ahmad and S. O. Hwang, "A secure image encryption scheme based on chaotic maps and affine transformation," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13 951–13 976, 2016.
[42] N. L. Philippe, V. Itier, and W. Puech, "Visual saliency-based confidentiality metric for selective crypto-compressed JPEG images," in *24th IEEE International Conference on Image Processing (ICIP)*. IEEE, 2017, pp. 4347–4351.
[43] P. N. Lone, D. Singh, and U. H. Mir, "Image encryption using DNA coding and three-dimensional chaotic systems," *Multimedia Tools and Applications*, vol. 81, no. 4, pp. 5669–5693, 2022.

SALMA BEN MAMIA received her M.S. Intelligent Systems Road Traffic Control (Hit4med), from the University of Sousse, Tunisia, in 2019. She is currently pursuing her Ph.D. degree with the Laboratory of Electronics and Microelectronics in the University of Monastir, Tunisia. Her work has focused on the generation of new chaotic systems applied in image encryption by neural network. She has published one journal article and two conference papers in 2022.

PAULINE PUTEAUX received her M.S. degree in Computer Science and Applied Mathematics with specialization in Cybersecurity from the University of Grenoble, France, in 2017 and her PhD degree in computer science from the Université de Montpellier, France, in 2020. She is currently working as a researcher for the CNRS (French National Centre for Scientific Research) with the Centre de Recherche en Informatique, Signal et Automatique de Lille (CRIStAL), France. Her work has focused on multimedia security, and in particular, image analysis and processing in the encrypted domain. Since 2016, she has published eight journal articles and thirteen conference papers. She is a reviewer for Signal Processing (Elsevier), the Journal of Visual Communication and Image Representation (Elsevier), the IEEE Transactions on Circuits & Systems for Video Technology, and the IEEE Transactions on Dependable and Secure Computing. She has been a member of the IEEE Information Forensics and Security TC since 2023.
Photo credit: © Xavier PIERRE / CNRS

WILLIAM PUECH received the diploma of Electrical Engineering from the Univ. Montpellier, France (1991) and a Ph.D. Degree in Signal-Image-Speech from the Polytechnic National Institute of Grenoble, France (1997) with research activities in image processing and computer vision. He served as a Visiting Research Associate to the University of Thessaloniki, Greece. From 1997 to 2008, he has been an Associate Professor at the Univ. Montpellier, France. Since 2009, he is a full Professor in image processing at the Univ. Montpellier, France. His current interests are in the areas of image forensics and security for safe transfer, storage and visualization by combining data hiding, compression, cryptography and machine learning. He is head of the ICAR team (Image and Interaction) in the LIRMM and has published more than 50 journal papers and 160 conference papers and is associate editor for 4 journals (SPIC, SP, JVCIR and IEEE TDSC) in the areas of image forensics and security and senior area editor for IEEE TIFS. Since 2017 he has been the general chair of the IEEE Signal Processing French Chapter. He has been a member of the IEEE Information Forensics and Security TC between 2018 and 2020 and then again since 2022. Since 2021 he has also been member of the IEEE Image, Video and Multidimensional Signal Processing TC.

KAIS BOUALLEGUE is a Professor in the Higher Institute of Applied Sciences and Technology of Sousse, Tunisia. He got his PhD from National Engineering School of Sfax. He is active member in different industrial companies. He has served a reviewer for technical papers. His current research interests include fractal, chaos and complex system.