International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V70I6P104

Volume 70 Issue 6, 30-43, June 2022

Original Article

Performances Study of a New Chaos-based Video Encryption Algorithm

Tianandrasana Romeo RAJAONARISON[1], Paul Auguste RANDRIAMITANTSOA[2]

[1,2]*Doctoral School in Sciences and Technology of Engineering and Innovation, Research Laboratory Telecommunication, Automatic, Signal and Images, University of Antananarivo, BP 1500, Antananarivo101 – Madagascar.*

Received: 05 April 2022 Revised: 27 May 2022 Accepted: 11 June 2022 Published: 23 June 2022

Abstract - *The principle of chaos encryption consists of adding a chaotic signal to the message to be transmitted. the transmitter sends to a receiver this chaotic signal where the message is drowned. Knowing the characteristics of the initial chaotic signal lets the receiver know how to extract the message from the received signal. in this paper, we propose a new chaos-based video encryption method and study its performance. the approach of Chaos-based video encryption is implemented in Matlab to encrypt AVI format videos. Choosing an algorithm based on chaos allows us to improve the time/robustness ratio by making the best use of chaotic sequences. the results of tests and evaluations show the performances of our systems. Among these results, we obtained PSNR values up to 8.14, NPCR values around 99.99%, and entropy values up to 7.99.*

Keywords - *Attractor, Chaos, Confusion, Encryption, Video.*

1. Introduction

Nowadays, many videos are circulating in the mobile communication system via networks or even in the cloud, and in most cases, they are not secure. However, this causes many risks, such as the dissemination of intimate information in the network by pirates, which can lead to serious crimes such as suicides or access to paid videos by people who do not have the right or the discovery by competitors of the ideas of companies that hold their meetings by videoconference. Cryptography is an art already used by men for a very long time to conceal or hide information and secret messages. the evolution of computing allows us to use this art to secure all our digital information and face these threats. Many cryptographic techniques were then invented. We can cite those based on number theory such as Rivest Shamir Adleman (RSA) Encryption or those based on logical and mathematical operations such as the Advanced Encryption Standard (AES). the main problem of these systems is related to time because we need to increase the number of operations to increase robustness and escape the threats caused by the increase in the computing speed of computers. This article proposes using chaos-based video encryption to address these issues and threats. the nonlinearity, the sensitivity to the initial condition, and the random aspect while being deterministic of a chaotic sequence allows it to become one of the best options for cryptography. We will use this approach to establish our video encryption algorithm.

2. Materials and Methods

2.1. Discrete chaotic dynamical systems

Chaotic signal generators are strange attractors. and we can classify these attractors into two: the attractors which provide continuous chaotic signals and the attractors which provide discrete chaotic signals. This article only studies discrete attractors.

2.1.1. Logistics suite or logistics map

This function is given by equation (1) [1, 2, 14] :

$$X_{n-1} = rX_n(1 - X_n) \quad (1)$$

Xn is between 0 and 1, and r is a positive number between 1 and 4. the behavior is chaotic from r equal to 3,6. Figure 1 illustrates the bifurcation diagram (Xn as a function of r).

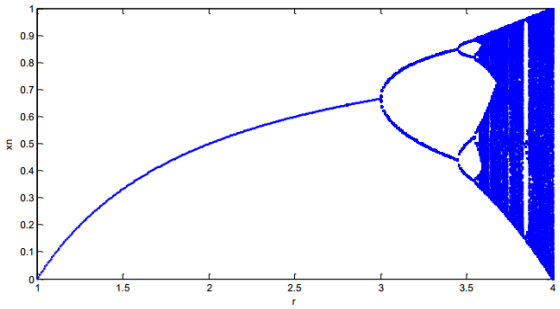

Fig. 1 Bifurcation diagram

2.1.2. Piecewise linear chaotic sequences

There are several piecewise linear chaotic recurrences like:

Tent Map

$$f(x) = \begin{cases} rx, & 0 \le x < 0{,}5 \\ (1-x)/(1-r), & 0{,}5 \le x \le 1 \end{cases} \quad (2)$$

Skew tent map

$$f(x) = \begin{cases} x/r & 0 \le x < r \\ (1-x)/(1-r), & r \le x < 1 \end{cases} \quad (3)$$

2.1.3. Hennon recurrence

It constitutes a discrete-time dynamical system introduced by the astronomer Michel Hénon in 1976. It is presented by the system of equation (4) [3, 19].

$$X_{n+1} = Y_n + 1 - aX_n^2$$
$$Y_{n+1} = bX_n \quad (4)$$

Figure 2 represents the Hénon attractor with a=1.4 and b=0.3.

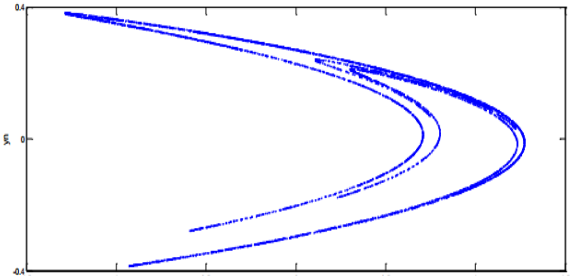

Fig. 2 Henon attractor

2.1.4. Gingerbreadman map

This attractor is presented by the system of equations (5) [3, 21].

$$X_{n+1} = 1 + |X_n| - Y_n$$
$$Y_{n+1} = X_n \quad (5)$$

Figure 3 represents the Gingerbreadman attractor.

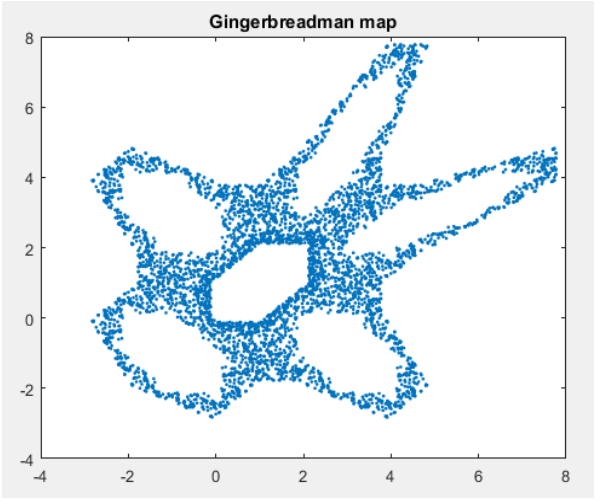

Fig. 3 Gingerbreadman attractor

2.1.5. Tinkerbell map

It is given by equations (6).

$$X_{n+1} = X_n^2 - Y_n^2 + aX_n + bY_n$$
$$Y_{n+1} = 2X_nY_n + cX_n + dY_n \quad (6)$$

Figure 4 represents the Tinkerbell attractor with a=0.9, b=0.6013, c=2, d=0.5.

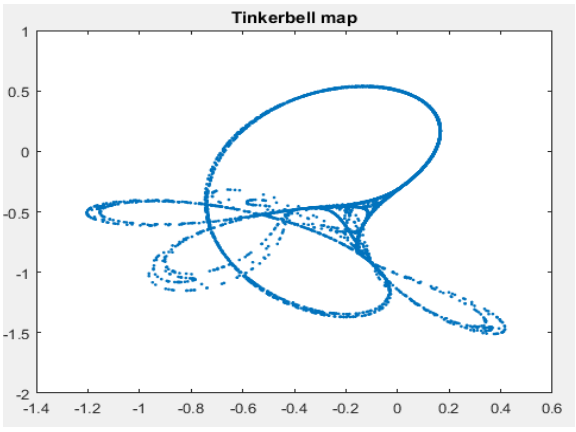

Fig. 4 Tinkerbell attractor

2.1.6. Burger's map

This chaotic system is presented as follows:

$$X_{n+1} = (1-\gamma)X_n - Y_n^2$$
$$Y_{n+1} = (1-\mu)Y_n + X_n Y_n \quad (7)$$

Figure 5 shows Burger's attractor.

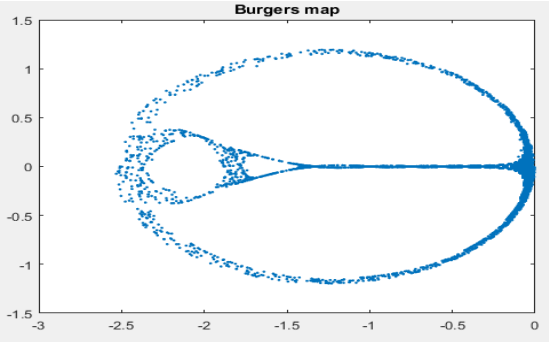

Fig. 5 Burger attractor

2.1.7. Ricker's map

Ricker's attractor is generated by the system of equations (8) :

$$X_{n+1} = aX_n e^X \quad (8)$$

Figure 6 represents Ricker's attractor with a=20.

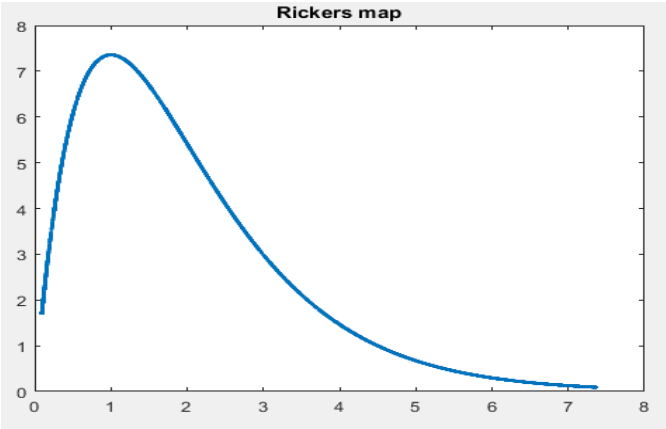

Fig. 6 Ricker's attractor

2.1.8. Cubic map

The Cubic attractor is generated by the system of equations (9) :

$$X_{n+1} = \alpha X_n + \beta X_n^3, \ 0 \le X_n \le 1/2$$
$$X_{n+1} = \alpha(1-X_n) + \beta(1-X_n)^3, \ 1/2 \le X_n \le 1 \quad (9)$$

Figure 7 represents the Cubic attractor.

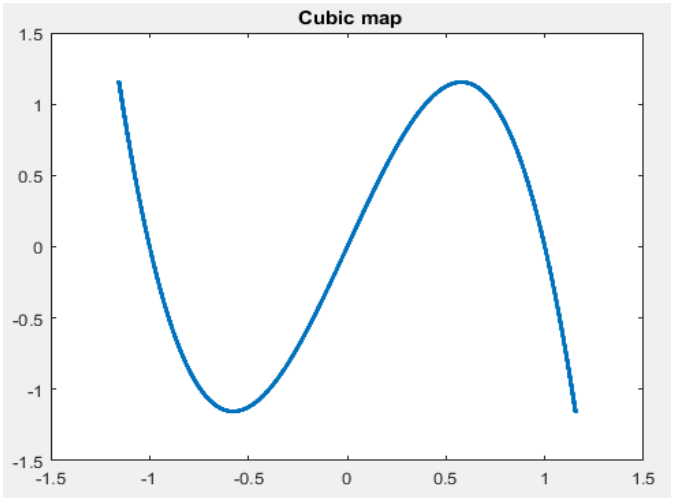

Fig. 7 Cubic attractor

2.1.9. Sin map

This chaotic system is presented as follows [1,2,4]:

$$X_{n+1} = \mu \sin(\pi X_n), \ X\epsilon[0;1], \mu > 0 \quad (10)$$

Figure 8 represents the Sin attractor.

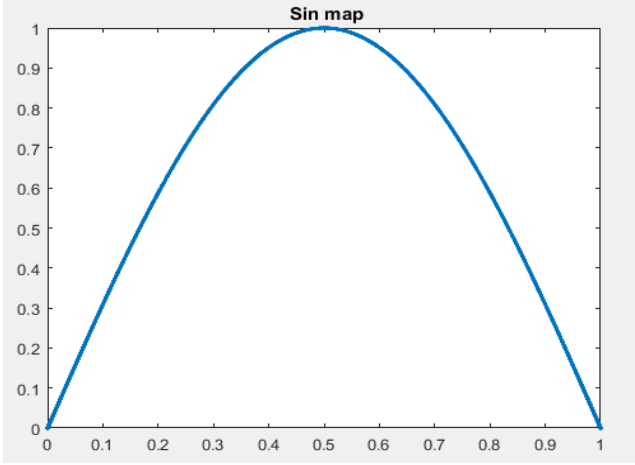

Fig. 8 Sin attractor

2.2. Differences between chaos and classical cryptography

Since the 90s, several researchers have noted an interesting relationship between chaos and cryptography. Indeed, several properties of chaotic systems have similar or almost similar correspondences with traditional cryptographic systems. the following table (Table 1) perfectly illustrates this correspondence. [14]

Table 1. Correspondence between Chaos theory and cryptography

Chaos theory	Cryptography
Chaotic systems	Pseudo-random system
Nonlinear transformation	Nonlinear transformation
the infinite number of states	the finite number of states
the infinite number of iterations	the finite number of iterations
Initial state	Plaintext
Final state	Ciphertext
Initial condition(s) and/or parameter(s)	Key(s)
Asymptotic independence of initial and final states	Confusion
Sensitivity to initial conditions and parameters	Diffusion

2.3. Chaos-based ciphers

Generally, a chaos encryption system is composed of two parts: the confusion part and the diffusion part, which consist respectively of the permutation of the original information elements and the replacement or substitution of these elements [2,5,6, 11].

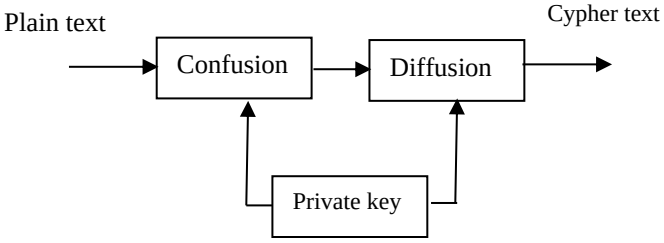

Fig. 9 General principle

2.3.1. Algorithm proposed by Chen and Mao

Chen used a 3D version of Arnold's Cat map for the substitution, the logistics map for the broadcast, and Chen's chaotic system as a key generator. the encryption algorithm is illustrated in the following figure 10 [2,5,6,11].

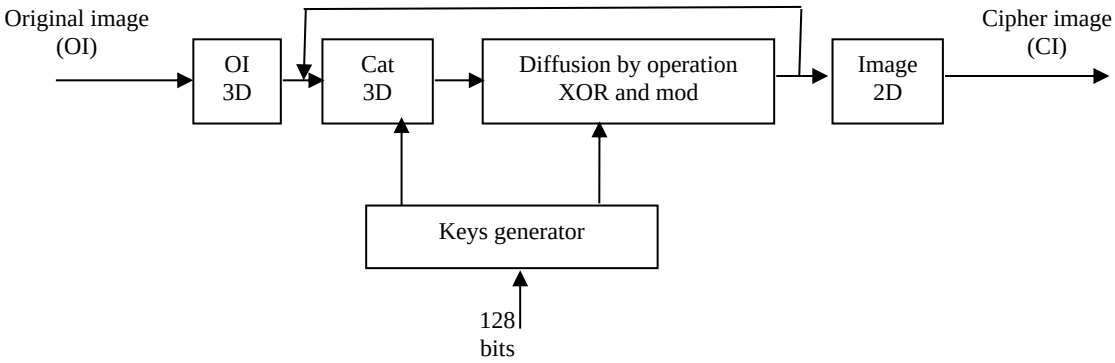

Fig. 10 Chen cipher principle

After converting the original image to 3D, the Arnold's Cat 3D map is defined as follows:

Where

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \\ Z_{n+1} \end{bmatrix} = A \begin{bmatrix} X_n \\ Y_n \\ Z_n \end{bmatrix} mod\ N \qquad (11)$$

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix} \qquad (12)$$

A is used to create confusion. Then, the following equation (13) is used to create the Diffusion

$$\boldsymbol{c(k) = \emptyset(k) \oplus \{[i(k) + \emptyset(k)] mod N\} \oplus c(k-1)} \quad (13)$$

Where

$\boldsymbol{\emptyset(k)}$ is generated using the logistic map, i(k) represents the current pixel value, and c(k) is the new pixel value.

Mao's Algorithm has the same idea as chen et al., except they used the 3D Baker map in the substitution step instead of the 3D Cat map. [18, 19, 21]

2.3.2. Lian proposed Algorithm

Lian proved that there are some weak keys (security problems) in the encryption techniques using the Baker and Cat chaotic maps and that the key space of the standard chaotic map is larger than these last two maps. They used the standard map for the substitution and the following function for the broadcast : [23, 24, 25]

$$\boldsymbol{C_i = V_i \oplus q[f(C_{i-1}), L]} \quad (14)$$

With

$$\boldsymbol{q[f(C_{i-1}), L] = 2^L \times f(C_{i-1})} \quad (15)$$

Where: Vi represents the pixel value of the permuted image, Ci denotes the pixel value of the diffused image, and the function f represents the logistic map. They also recommended at least four rounds of substitution and spread. Lian's Algorithm is well illustrated in Figure 11.

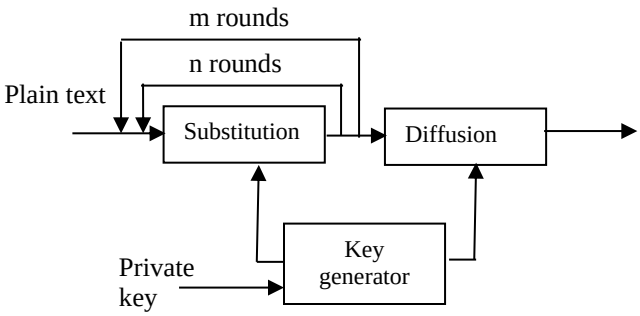

Fig. 11 Lian cipher principle

2.3.3. Algorithm proposed by V. Patidar

They proposed an encryption algorithm using the standard chaotic map and the logistic map with a 157-bit secret key to encrypt color images. the initial condition, the system parameter of the standard map, and the number of iterations together constitute the secret key. the first round of confusion is performed through XORing keys calculated from the secret key. Then, in the two diffusion rounds, the properties of the horizontally and vertically adjacent pixels are mixed, respectively. the fourth round achieves robust and efficient confusion using the standard and logistic map [2,5,6].

This Algorithm is well detailed in Figure 12.

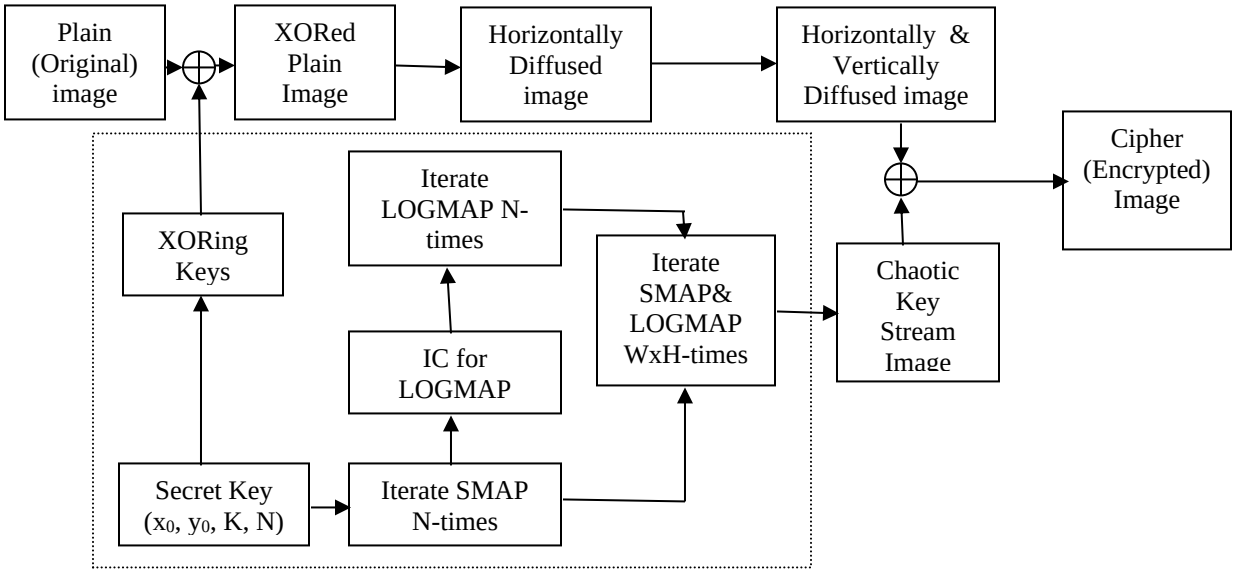

Fig. 12 Patidar cipher principle

2.4. Operation of the new chaotic-based encryption algorithm

2.4.1. Encryption

Reading: This step consists of reading the frames that make up the video for the image part and the sound samples for the audio part. in this step, information about the number of frames per second and the number of samples per second is recorded to synchronize the encrypted video.

Encryption: This step contains all the transformations performed on the video to make it unintelligible.

Synchronization: This step consists of rewriting the video file according to its initial parameters (frames per second, samples per second) but with encrypted frames and samples.

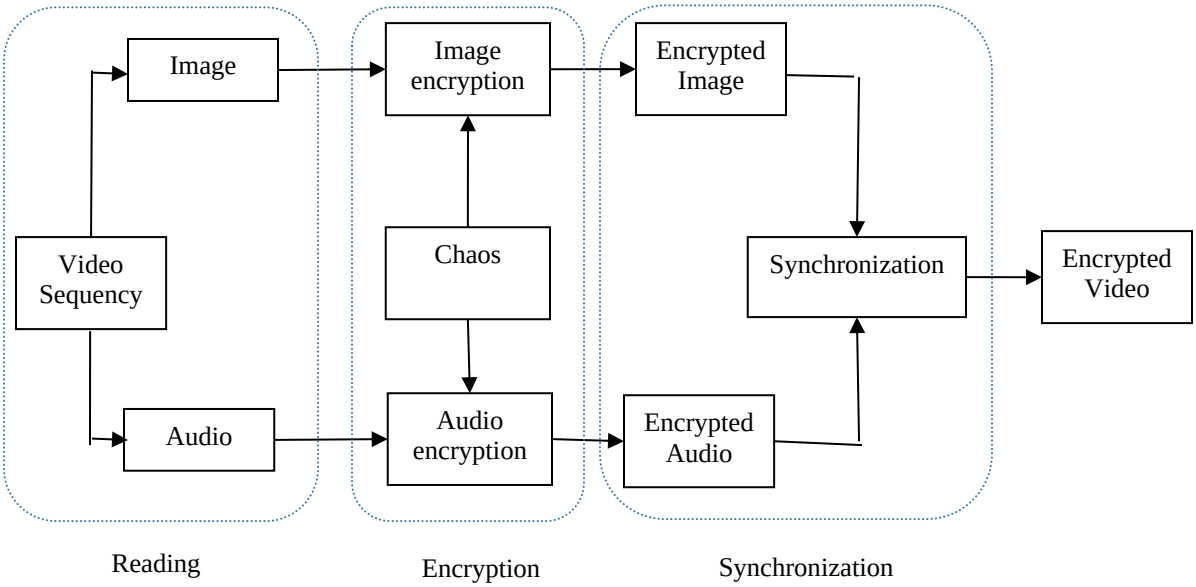

Fig. 13 Synoptic diagram of video encryption

2.4.2. Decryption

the decryption operation is done like the encryption operation, except that the input is the encrypted video here.

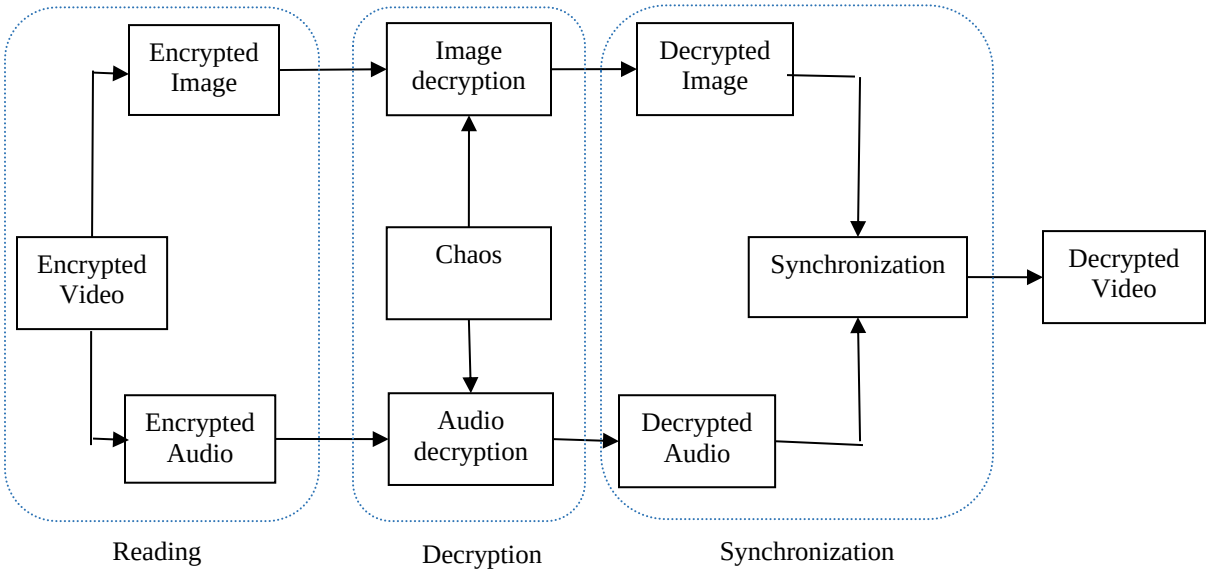

Fig. 14 Synoptic diagram of video decryption

2.4.3. Encryption principle

Key generation

We will use chaotic attractors to generate sequences that we will use as encryption keys. Therefore, the elements that must be kept secret are the attractor(s) used, these initial conditions, and the parameters of these equations. After its generation, its keys will be prepared/transformed to be used in each encryption part. in the confusion part, we must create the pairs where an element of the message and an element of the key. in the diffusion part, we must linearize the elements of the key between 0 and 255. Figure 15 shows the steps of the key generation.

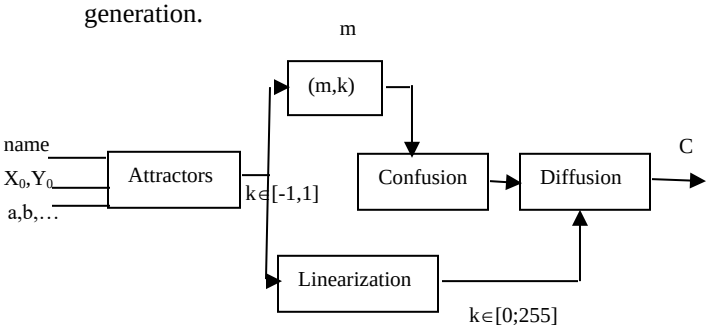

Fig. 15 Key generation

With the following initial conditions:

Attractor: Tinkerbell

Initial conditions: x_0= 0, y_0=0.5, a= 0.9, b= -0.6, c= 2, d= 0.5.

We get the following chaotic sequence:

0; -0.5500; -0.4050; -1.0130; 0.1894; -0.8727;-0.2201; -0.2240; -0.0947;-0.0162

Linearization consists of projecting this sequence into the interval [0; 255].

After linearization, the chaotic sequence becomes:

36; 164; 77; 138; 0; 45; 36; 31; 181; 17

This sequence is used as an encryption key.

Confusion from chaos

the objective of this step is to permute the image to remove any visual clues that may reveal the image's content. To perform this permutation, we will follow the following steps: first, form the pairs (m,k), then arrange the elements of k in ascending order without separating each pair.

$$(m_i, k_i) \Rightarrow (m_j, k_j) \quad (16)$$

Where

$i = \{1,2,\dots,N\},\ j = \{1,2,\dots,N\}, k_j < k_{j+1}$

Figure 16 shows three ways to permute an image: by row (a), by column (b), and by column over the entire image (c).

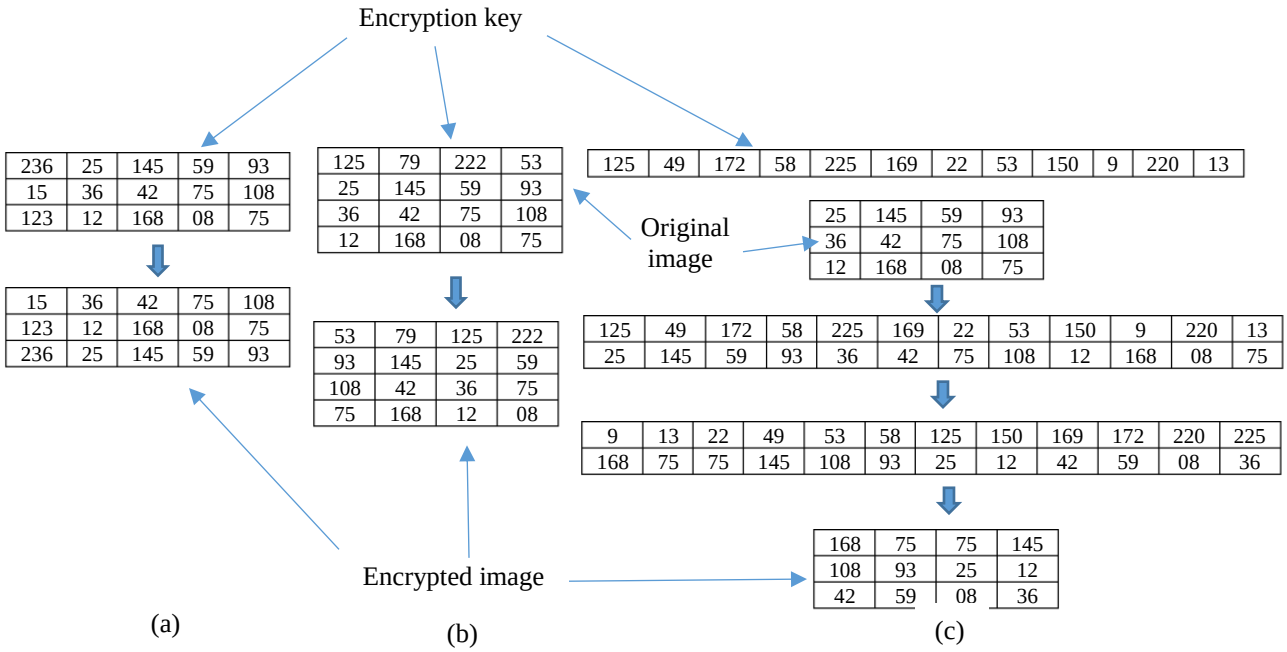

Fig. 16 Principle of confusion in ascending order

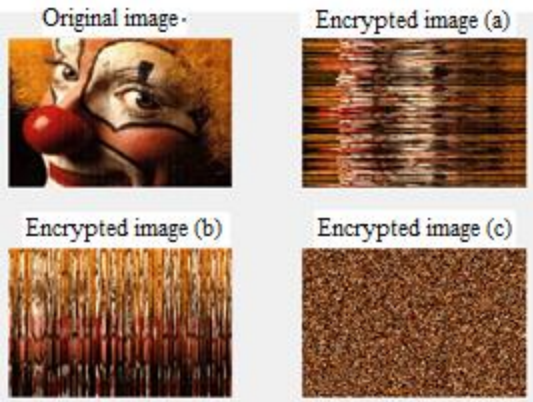

Fig. 17 Example of confusion by chaos

To perform the Decryption, we will use an intermediate key $k_{int} = \{1,2, \dots, N\}$. This key must be swapped with the key k used for Encryption. and this permuted k_{int} It is used for the Decryption of the message. Figure 18 shows the deciphering steps of "1-(a) confusion".

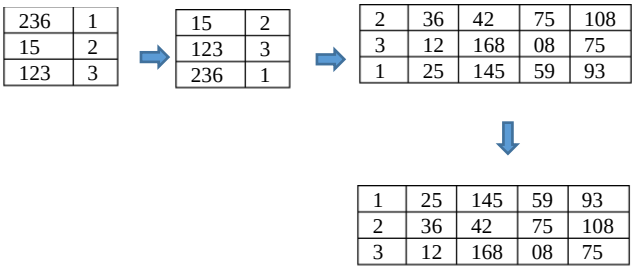

Fig. 18 Principle of deciphering confusion by chaos

Confusion from the image

This confusion step aims to create a dependency between the pixels of the encrypted image to avoid differential attacks. We, therefore, perform a permutation of neighboring pixels according to the value of a current pixel according to the following principle:

if $\big(p(i,1,1) \oplus p(i,1,2) \oplus p(i,1,3)\big) mod 3 \neq 1$

so $p(i+1,:,1) \Leftrightarrow p(i+2,:,1)$

$p(i+1,:,2) \Leftrightarrow p(i+2,:,2)$

$p(i+1,:,3) \Leftrightarrow p(i+2,:,3)$

Fig. 19 Example of confusion by the image itself

The Decryption follows the same Algorithm as the Encryption, but in the opposite direction; this means that if the Encryption is done from top to bottom, then the Decryption is from bottom to top. [22, 23]

Diffusion principle

During this step, we will change the values of each pixel to equalize the probability of the appearance of each level of color. For a size image $I \times c \times k$; where I, c, k indicate the number of lines, respectively, the number of columns, and the color of the component, this diffusion operation is defined by equation (17). the value of k will be 1 for the color red, 2 for the color green, and 3 for the color blue. the truth table of the EXCLUSIVE-OR operation is shown in Table 2.

Table 2. The truth table of the xor operation

A	B	A XOR B
0	**0**	**0**
0	**1**	**1**
1	**0**	**1**
1	**1**	**0**

Examples :

A=10 = 1010; B=12= 1100 donc A XOR B = 0110

$$P(i,j,k) = C(i,j) \oplus P(i,j,k) \quad (17)$$

where : $i = 1,2, \dots I,$

$j = 1,2, \dots c,$

k=1,2,3

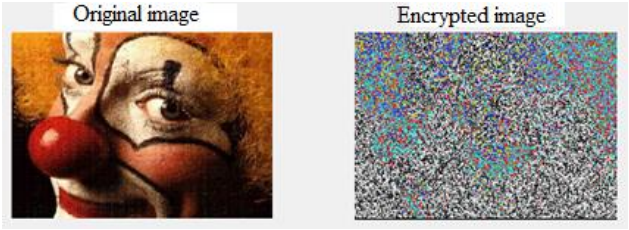

Fig. 20 Diffusion example

2.5. Algorithm proposed

the diagrams that we are going to propose will be based on these 3 types of Encryption, except that: the generation of the key, the principle of confusion or Diffusion, and the order of use of the steps will be permuted to have better results. After several tests, we propose the following diagrams, which can be used according to our needs. For ease of naming, we will name the confusion from the chaos "confusion 1" and that from the image "confusion 2" content.

2.5.1. Total confusion

in this scheme, we have favored the encryption time to the detriment of robustness. To achieve this Encryption, we will use an attractor to generate an encryption key. This key will perform "1-(c) confusion" on the current frame and the audio samples. Afterward, at the exit of this first confusion, the audio samples join the exit while the frame still passes through "confusion 2". Figure 21 shows how this scheme works. These steps are repeated for all frames of the video.

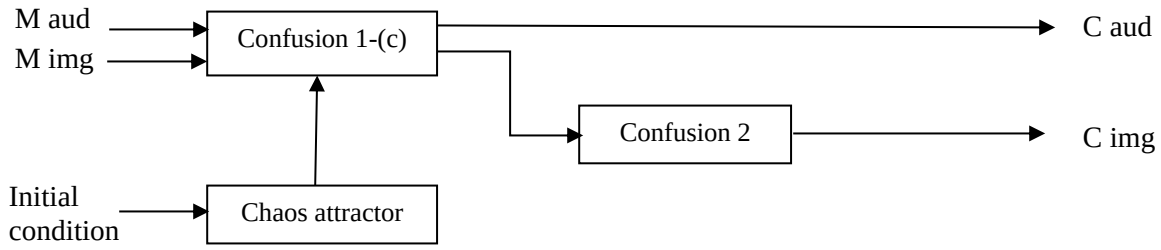

Fig. 21 Operation of the total confusion algorithm.

2.5.2. Total Diffusion and partial confusion

This scheme has a balanced time robustness ratio compared to the other two. This second diagram uses an attractor to generate the keys according to the method described in figure 15. Afterward, the image undergoes the "diffusion" stage before going through the "confusion 2" stage, and finally through a "confusion 1-(a)" stage. the audio samples are encrypted by the "confusion1-(c)" method. Figure 22 shows how this scheme works.

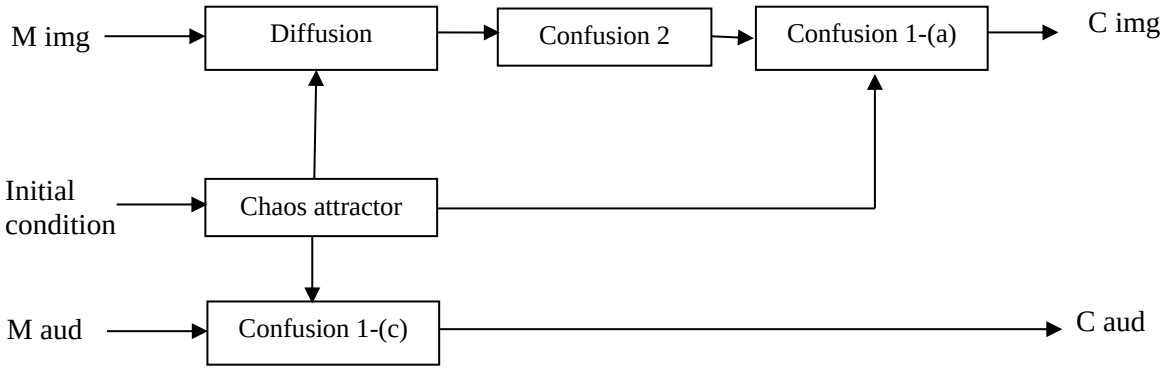

Fig. 22 Operation of the total and partial confusion algorithm

2.5.3. Diffusion and confusion

This third scheme allows strong Encryption but is quite time-consuming. in this diagram, we will use the key generation method in figure 15. Afterward, we successively carry out the steps of "diffusion," "confusion 2," and "confusion 1-(c)". the audio samples are encrypted by the "confusion1-(c)" method. Figure 23 shows the principle of this Encryption.

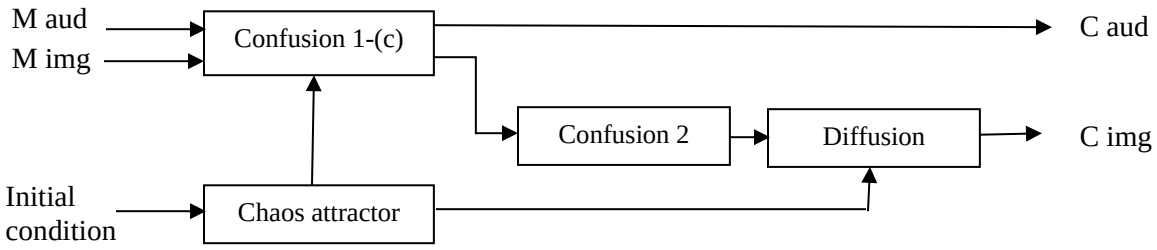

Fig. 23 Operation of the total diffusion and confusion algorithm

3. Results and Discussion

3.1. Statistical Analysis Measurement

in this section, we will present the results of our encryption methods. To analyze the performance of each approach, we will use a 2-second color video in the "avi" format of 640X480 pixels. the initial conditions used during the test are as follows: Attractors: Tinkerbell map with Initial conditions: x_0= 0, y_0=0.5, a= 0.9, b= -0.6, c= 2, d= 0.5.

3.1.1 Uniformity analysis

the histogram is a commonly used metric as a qualitative check of data distribution, intending to evaluate the robustness of the cryptosystem against statistical attacks. For a well-designed cryptosystem, such a metric should hide any noticeable information about the simple image or the relationship between it and the encryption image. An image histogram is a graphical representation showing the distribution of pixel values, plotting the number of pixels in each gray level value. the graphical representation of the encrypted image's histogram is important but insufficient to guarantee the uniformity of the distribution of the encrypted pixels. For this purpose, the Chi-square test indicates the uniformity characteristic of the given cipher image histogram. This statistical test is calculated by equation (18) [6,7]:

$$X_{exp}{}^2 = \sum_{i=1}^{N_V} \frac{(O_i - e_i)^2}{e_i} \tag{18}$$

Where N_V denotes the total number of levels ($N_V = 256$) for a grayscale image), O_i are the frequencies of occurrence of each gray level (0-255) and e_i Represents the expected frequency of occurrence of the uniform distribution, calculated by the equation (19).

$$e_i = \frac{M \times N \times P}{256} \tag{19}$$

Where: M is the number of rows, N number of columns, and P the number of planes; for the gray level image, P = 1.

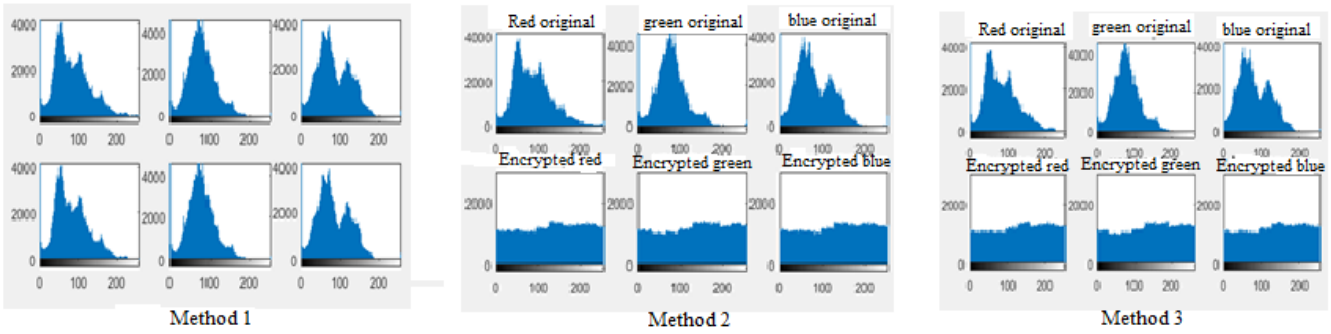

Fig. 24 Operation of the total diffusion and confusion algorithm

The curves in figure 24 represent the original and encrypted histograms of the three colors (Red, Green, and Blue) of methods 1, 2, and 3. the ordinate axis indicates the number of occurrences of each pixel of the axis of eastings. An encrypted image should have a flat histogram. the histogram in Figure 24 method 1 does not change because the method only swaps the pixels without changing their values. Methods 2 and 3 passes this test.

3.1.2 Correlation analysis

An image with its significant visual content is characterized by its strong correlation and redundancy between neighboring pixels in horizontal, vertical, or diagonal directions. A well-designed cryptosystem should conceal such relationships between adjacent pixels and exhibit zero correlation. To assess the immunity of a given cryptosystem to this type of attack, the first N pairs of neighboring pixels are randomly selected from the clear image and its corresponding cipher version in each direction. Next, the correlations of adjacent pixels in a given image are quantified by calculating the correlation coefficient of each pair using the following equations [8,9] :

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(X)}\sqrt{D(Y)}} \tag{20}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{21}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{22}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{23}$$

Where X_i and y_i represent the gray level values of i[th] the chosen pair of neighboring pixels in the image, and N is the integer number of samples.

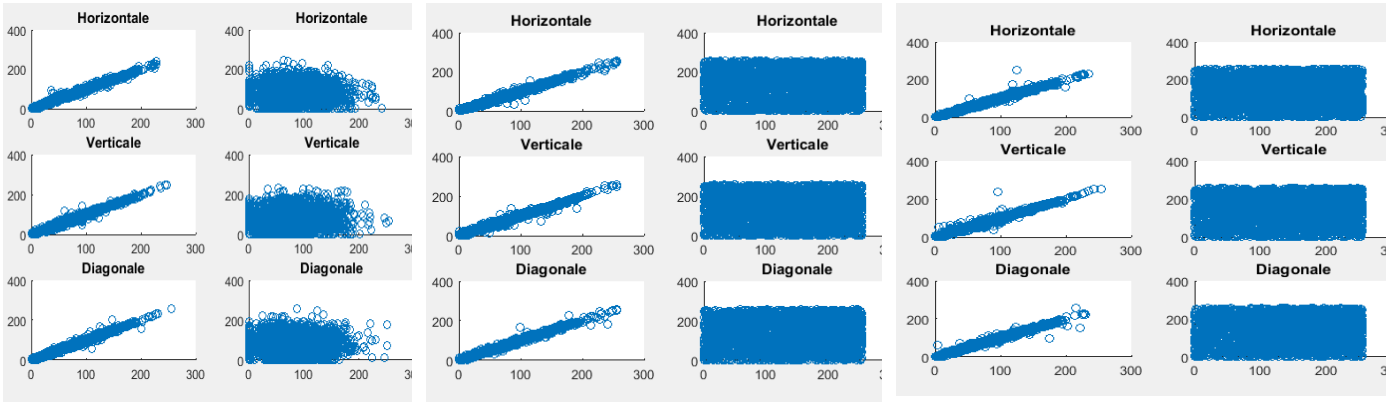

Fig. 25 Operation of the total diffusion and confusion algorithm

the curves in figure 25 respectively represent the comparisons of the correlation curves of the neighboring pixels between the original images (on the left) and the encrypted images (on the right). the points of the correlation figure for an encrypted image should be well scattered. the correlation of adjacent pixels from method 1 does not conform. However, the other two methods pass this test.

3.2 Sensitivity test

3.2.1 Robustness against differential attacks

For the sake of secret key recovery, an attacker could attempt to distinguish any noticeable information between the normal image and its cipher version by observing the influence of a one-pixel change on the overall system output. Encryption. A well-designed cryptosystem is one in which a minor modification of its simple image results in a major transformation of its encrypted image, and therefore such attacks are nullified. To experiment, the following procedure must be adopted:

1. the clear image P1 is encrypted to have an encryption image C1.

2. the simple image P2 is obtained by applying a minor change to a randomly selected pixel. the altered ordinary image P2 is encrypted using the same secret key to produce the corresponding encryption image C2.

Influence is measured quantitatively using two commonly used metrics:

- the number pixel change rate (NPCR): calculates the number of pixel differences between two images ciphered below C1 and C2 using equations 24 and 25 [7] :

$$NPCR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} D(i,j)}{H \times L} \times 100 \quad (24)$$

Where N and M denote the width and height of the image, respectively, and D(i;j) is defined as follows :

$$D(i,j) = \begin{matrix} 0 \; if \; C_1(i,j) = C_2(i,j) \\ 1 \; if \; C_1(i,j) \neq C_2(i,j) \end{matrix} \quad (25)$$

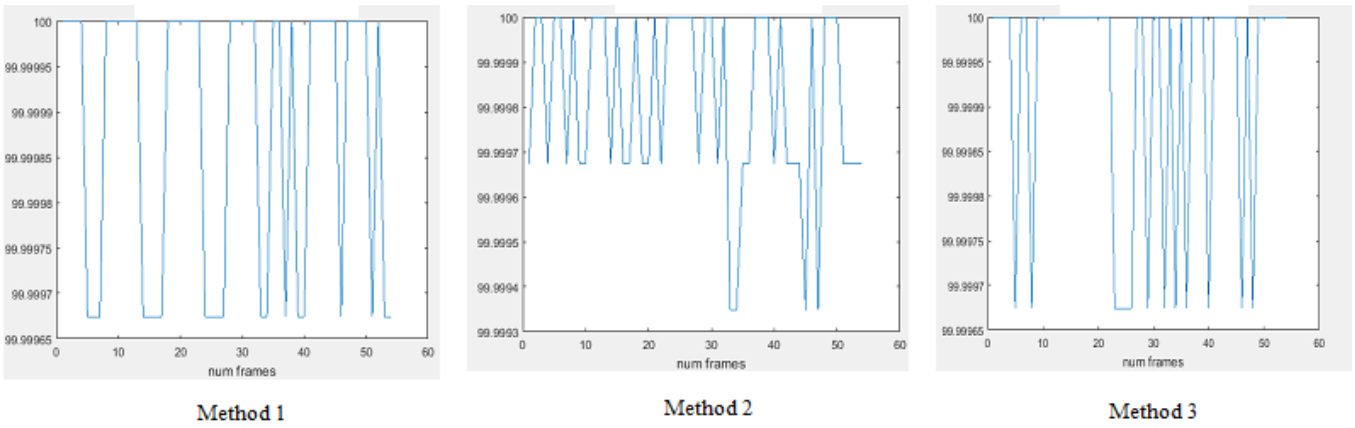

Fig. 26 Variation in NPCR value between original images C1 and encrypted C2

NPCR's benchmark for successful Encryption is 99.6094%. Figure 26 shows that our 3 methods pass this test because our values are all greater than 99.9993%. It means that our systems are resistant to differential attacks.

- Unified average change intensity (UACI): it calculates the average intensity of the differences between the original image C1 and the encrypted image C2 employing equation (26) [7] :

$$UACI = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}|C_1(i,j) - C_2(i,j)|}{H \times L \times 255} \times 100 \qquad (26)$$

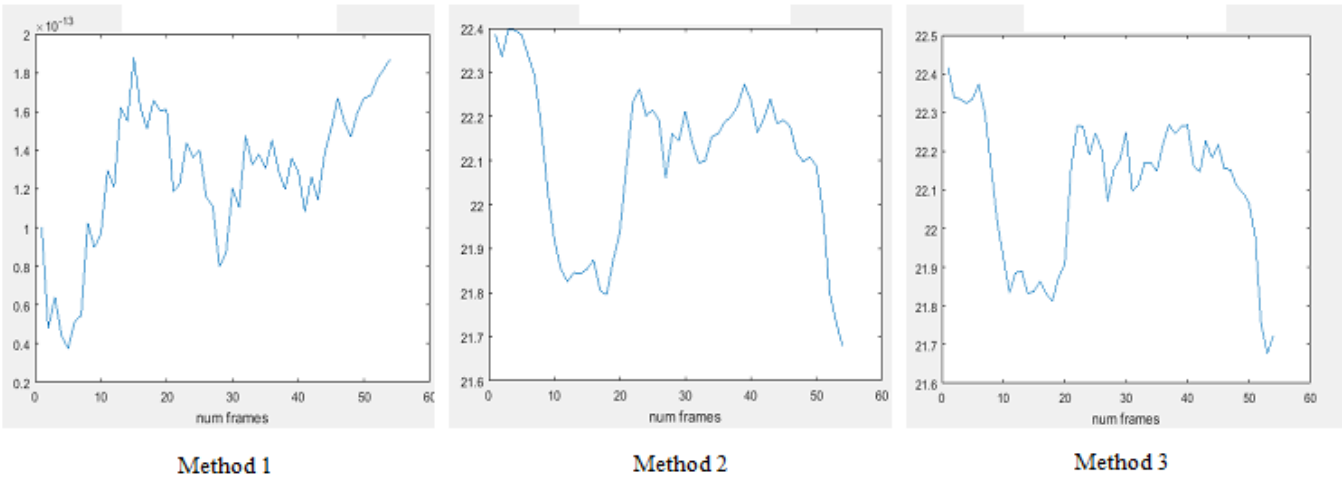

Fig. 27 Variation in UACI value between original images C1 and encrypted

the curves in Figure 27 show the variations in the UACI value of the 3 methods proposed. the reference value for this test is 33.4635%. the 1st method has results very far from this value. However, the other two methods have similar results.

3.2.2 Performance analysis measure:
Calculation speed estimates

Timing is also a crucial factor to consider in designing a secure crypto-system. Therefore, a good combination of computational performance and a satisfactory level of security is essential for real-time application scenarios. the performance of a given cryptosystem is determined by evaluating the execution speed, the latter being calculated using the average encryption and decryption times [8].

Result of method 1: 26.52 sec

Result of method 2: 13.39 sec

Result of method 3: 30.42 sec

Analysis of the signal-to-noise ratio

Peak Signal to Noise Ratio, often called PSNR, is a technical term for the ratio of the maximum possible power of a signal to the noise corruption power affecting the

fidelity of its representation. Because many signals have a wide dynamic range, PSNR is usually expressed on a logarithmic scale of decibels. the PSNR is most easily defined via the root mean square error (MSE). Given a noiseless monochrome image I and its noisy approximation K, MSE is defined as follows [9] :

$$MSE = \frac{1}{m \times n} \sum_{j=1}^{m} \sum_{i=1}^{n} [I(i,j) - K(i,j)]^2 \qquad (27)$$

the PSNR (in dB) is defined as follows :

$$PSNR = 10 \log \frac{255^2}{MSE} \qquad (28)$$

Use this simple array form; don't use the complex form:

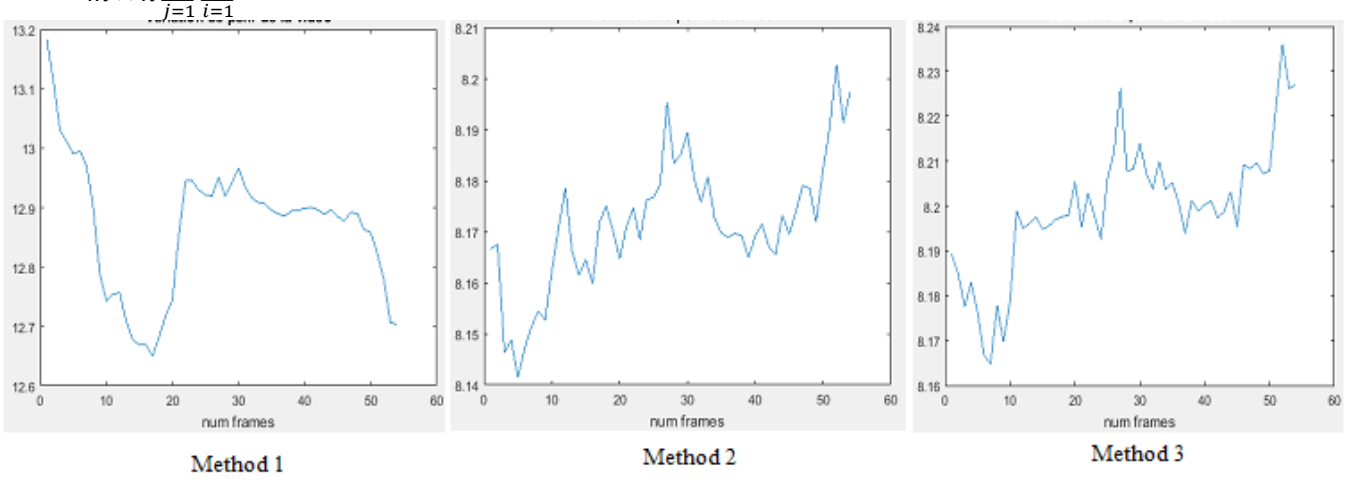

Fig. 28 Variation in PSNR value between original images C1 and encrypted

The curves in Figure 28 show the PSNR values. the PSNR of the 1st method is higher than those of the others. the 1st method is less efficient than the others because the reference value is 0.

Entropy

The entropy H(m) can be used as a performance indicator of a cryptosystem. It indicates the amount of information contained or delivered by a frame. It is related to the appearance probability distribution of each pixel and is calculated by equation (29). the value of entropy for an ideal cryptosystem is 8.

$$H(m) = -\sum_{i=0}^{L-1} p(m_i) \log\left(p(m_i)\right) \qquad (29)$$

With $p(m_i)$ the probability of appearance of the symbol m_i.

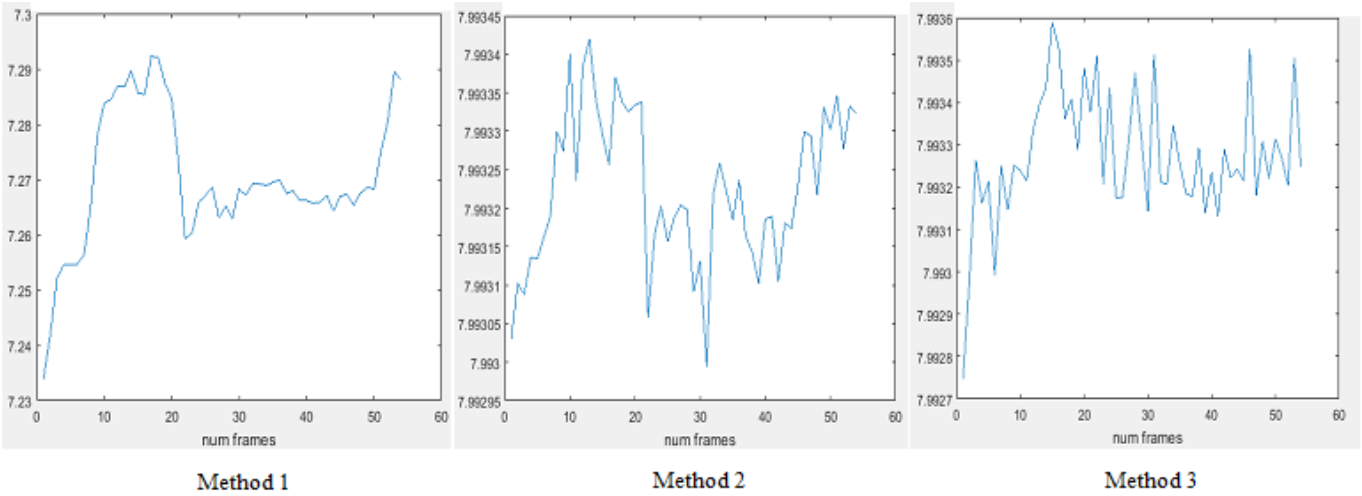

Fig. 29 Variation of entropy des in value of encrypted images

the reference value of entropy is 8. the 3 methods in figure 29 show that our results are not far from this value. It shows the effectiveness of our methods.

4. Conclusion

The need for confidentiality, integrity, and authentication of the mobile communication system forces people to run towards encrypting its data. in this article, we have created an encryption method based on chaos to protect our video data and to face several threats related to broadcasting or unauthorized access. This method reduces the complexity of calculating and generating encryption keys using chaotic attractors. the diffusion property is ensured by an "exclusive or" operation between the key and the pixel values of each frame. At the same time, the confusion is done by a permutation of the pixel values according to the order of magnitude of the encryption key. Afterward, we implemented our encryption method on Matlab. From the results obtained by the simulation, we carried out the tests and evaluations to qualify our system.

References

[1] G.D. Eddine, "Logistic Function and Chaotic Standard for the Encryption of Satellite Images," *Mentouri University of Constantine*, 2010.

[2] Al Nahian, S., "Hosen, Z. and Ahmed, P. "An Elementary Study of Chaotic Behaviors in 1-D Maps," *Journal of Applied Mathematics* and Physics, 2019 .

[3] L. Laurent., " Chaos Cryptography Using Nonlinear Delay Dynamics," *University of Franche-Comté*, 2002 .

[4] M. Madani, Y. Bentoutou, "Encryption of Medical Images Based on Chaotic Maps, *University of Sidi-Bel-Abbes*," 2015 .

[5] M. Nsreddine, "Clifford Attractor-Based Encryption," *Abou Bekr Belkaid University*, 2017 .

[6] A.S. Nassim, "Chaos-Based Cryptography and Image Encryption," *University of Applied Sciences Lucbeck Germany*, 2012 .PDCA12-70 Datasheet,Optospeedsa, Mezzovico, Switzerland.

[7] Junqin Zhao, Weichuang Guo, and Ruisong Ye, "A Chaos-Based Image Encryption Scheme Using Permutation-Substitution Architecture," *International Journal of Computer Trends and Technology* IJCTT , 2014 .

[8] S. Ahadpour, Y. Sandra, "A Chaos-Based Image Encryption Scheme Using Chaotic Coupled Map Lattices," *University of Mohaghegh Ardabili*, Iran, 2012 .

[9] G. A. Sathishkumar, K.B. Bagan, N. Sriraam, "Image Encryption Based on Diffusion and Multiple Chaotic Maps ," *International Journal of Network Security & Its Applications* IJNSA , 2011 .

[10] S. Abdullah, Z. Hosen, P. Ahmed, "Elementary Study of Chaotic," *Journal of Applied Mathematics and Physics*, Vol. 7, No. 5, 2019 .

[11] S. Li, G. Chen, X. Zheng, "Chaos-Based Encryption for Digital Image and Video," *Multimedia Encryption and Authentication Techniques and Applications*, CRC Press, 2006 .

[12] I. Yasser, M.A. Mohamed, A. S. Samra, F. Khalifa, "A Chaotic Based Encryption/Decryption Framework for Secure Multimedia Communications, Entropy," 2020 . Www.Mdpi.Com/Journal/Entropy.

[13] M.Alawida,, A. Samsudin, J.S Teh, Alkhawaldeh, R.S. "A New Hybrid Digital Chaotic System with Applications in Image Encryption. *Signal Process*, ", Vol. 160 , Pp. 45–58, 2019.

[14] S. Su, Y. Su, M. Xu, "Comparisons of Firefly Algorithm with Chaotic Maps. Comput. Model, " *New Technol*. Vol. 18, Pp.326–332, 2014.

[15] R. Enayatifar, "Image Encryption Via Logistic Map Function and Heap Tree," *Int. J. Phys. Sci*, Vol.6 , Pp.221–228, 2011.

[16] E. Chen, L.Q. Min, D.D. Han, "A Chaotic System with One Line Equilibria and Image Encryption with Avalanche Effects," in Proceedings of the 2015 International Conference on Electronics, *Electrical Engineering and Information Science-EEEIS2015*, Pp.737–754, 2015.

[17] J.Q. Kadhim, M.K. Alazawi, " Speech Scrambling Employing Lorenz Fractional Order Chaotic System," *J. Eng. Sustain. Dev*, Vol. 17 Pp. 195–211, 2013.

[18] S.F. Yousif, "Speech Encryption Based on Zaslavsky Map," *J. Eng. Appl. Sci*, Vol. 14 , Pp.6392–6399, 2019.

[19] J. Wu, X. Liao, B. Yang, "Image Encryption Using 2D Hénon-Sine Map and DNA Approach. *Signal Process*," Vol. 153 , Pp.11–23, 2018.

[20] S. Dhall, S.K. Pal, K. Sharma, "A Chaos-Based Probabilistic Block Cipher for Image Encryption," *Journal of King Saud University*, Pp. 1533-1543, 2018.

[21] I. Yasser, F. Khalifa, M.A. Mohamed, A.S. Samrah, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps," *Complexity*, 2020

[22] Z. Su, S. Lian, G. Zhang, J. Jiang, "Chaos-Based Video Encryption Algorithms," Chaos-Based Cryptography, *SCI 354*, Pp. 205–226, 2011.

[23] S. Lian, "Efficient Image or Video Encryption Based on Spatiotemporal Chaos System," *Chaos, Solitons and Fractals* , Vol.40, Pp. 2509–2519, 2009.

[24] L. Kocarev, Z. Galias, S. Lian, "Intelligent Computing Based on Chaos," Springer, *Heidelberg*, 2009 .

[25] S. Lian, J. Sun, G. Liu, Z. Wang, "Efficient Video Encryption Scheme Based on Advanced Video Coding," *Multimed. Tools Appl*, Pp. 75–89, 2008.