

An encryption algorithm for satellite images based on chaotic sequences and a rotation system

M.NAIM ^{a,*} - A. ALI PACHA ^a – C.SERIEF ^b

Corresponding authors*: *mohammed.naim@univ-usto.dz, adda.alipacha@univ-usto.dz, serief7@hotmail.com

^a Laboratory of Coding and Security of Information

University of Sciences and Technology of Oran Mohamed Boudiaf

PoBox 1505 Oran M'Naouer 31000 Algeria

^bSatellite Development Center

Ilot T12, Bir El Djir, 31130 Oran, Algeria

Reçu le : 02/06/2020

Accepté le : 17/06/2020

Abstract -In recent years, the demand for conserving the secure transmission of satellite images from satellites to ground stations is increasing. To avoid hacking these images from illegal usage and unauthorized access. The most efficient solution for secure transmission is image encryption, which is an effective technique for protecting sensitive and important images, although that the encryption algorithms which, used in present satellite missions are typically obsolete and not suitable algorithms nowadays such as DES, 3 DES and AES due to their intrinsic characteristics such as size, high redundancy, strong correlation between adjacent pixels, etc.

In this paper, we propose an efficient encryption algorithm based on Lorenz Chaotic System and proposed a rotation system for encryption and decryption satellite images on board. Experimental and analysis results shows that the proposed algorithm is efficient method and evaluated security performances and has less time for encryption and decryption when compared to recent works in term of intrinsic characteristics and avoid threats and problems in classical algorithms.

Keywords— Encryption algorithms/ Chaotic Lorenz System/ Satellite images/ Cyclic Rotation/ Earth observation.

Résumé-Ces dernières années, la demande de conservation de la transmission sécurisée des images satellite des satellites aux stations au sol augmente. Pour éviter de pirater ces images à partir d'une utilisation illégale et d'un accès non autorisé. La solution la plus efficace pour une transmission sécurisée est le cryptage d'images, qui est une technique efficace pour protéger les images sensibles et importantes, bien que les algorithmes de cryptage qui, utilisés dans les missions satellitaires actuelles, soient généralement obsolètes et ne conviennent pas de nos jours comme DES, 3 DES et AES en raison de leurs caractéristiques intrinsèques telles que la taille, la redondance élevée, la forte corrélation entre les pixels adjacents, etc.

Dans cet article, nous proposons un algorithme de cryptage efficace basé sur Lorenz Chaotique System et un système de rotation pour le cryptage et le décryptage des images satellites à bord. Les résultats expérimentaux et d'analyse montrent que l'algorithme proposé est une méthode efficace et a évalué les performances de sécurité et a moins de temps pour le chiffrement et le déchiffrement par rapport aux travaux récents en termes de caractéristiques intrinsèques et évite les menaces et les problèmes dans les algorithmes classiques.

Mots-clés- Algorithmes de chiffrement/ Système Lorenz chaotique/ Images satellites/ Rotation cyclique/ Observation de la Terre.

1. INTRODUCTION

The development of encryption and protection of images in space science and technology attracted scientists, researchers and industrial communities to create and propose new and efficient algorithms used to consider mechanisms capable of securing images in the satellites (on board), the earth station, and during transmission. In addition, with these mechanisms, we must consider the methods that can protect data confidentiality, integrity and authentication. The encryption is the most common and acceptable solution to secure and protect satellite images against external attacks and to ensure high confidentiality. The classical encryption algorithms such as: Digital Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Triple Data Encryption Standard (3-DES), are not efficient with the rapid development in the space domain [1], moreover these algorithms are complex and take time to encrypt large and bulky satellite images and some of them have security weaknesses due to their

small key size, except the Advanced Encryption Standard (AES) which, still used for encrypting satellite images.

Nowadays chaotic maps are used as an effective method for encrypting images, due to their efficiency characteristics such as high sensitivity to initial conditions, unpredictability, pseudo-randomness and ergodicity. They used to create new and efficient algorithms or develop classic ones presented an overview of recent research related to the image data protection and cryptanalysis.

With the large utilization of chaotic maps in the current cryptosystems we can be classified existing chaotic maps into two categories: the chaotic maps one-dimensional (1D) and chaotic maps high dimension (HD) [2], [3] explain the two categories of chaotic maps. The chaotic maps (1D) have one variable and simple structures and orbits. Such as the Logistic, Gaussian, Sine and Tent maps. With the development of techniques to estimate chaotic signals, when little information is extracted, it is easy to predict its parameters and initial values; therefore, it is not appropriate in many areas of security. While the (HD) chaotic maps have more than one variable and a complex structure with high chaotic performance compared with (1D) maps so that their chaotic orbits are very difficult to predict. Therefore, chaotic maps must be developed with high performance and low implementation costs.

In this paper, the proposed encryption algorithm consist of Lorenz Chaotic System which contain three equations with (1D&2D) chaotic maps parameters and an efficient rotation system to reduce the complexity which usually used in works which, used chaotic maps and give more simplicity to understand the work [4]. Through the results of tests, the proposed encryption algorithm is robust against attacks and give a high level of security, which makes it applicable on board Earth observation satellites (EOS). In addition to satellite images, the proposed algorithm is better suited to the secure encryption of normal digital images. One of the main advantages of our proposed algorithm is the concentrated in the simplicity of using and understanding when compared with the recent works of encrypting satellite images. Therefore, we used an efficient chaotic system (Lorenz Chaotic System) with fast and efficient rotation

system. We will explain the systems used in the next sections.

2. CHAOS-BASED ENCRYPTION

2.1. LOGISTIC MAP

Logistic map is a very simple chaotic map. Its mathematical expression formula is as follows:

$$x_{n+1} = x_n \times \mu \times (1 - x_n) \quad (1)$$

$\mu \in [0, 4]$ is called Logistic parameters. When $\mu \in [3.569946, 4]$, Logistic map works in a chaotic state, and produces non-periodic sequence [5]. Figure 1 shows two logistic maps with small change error of one parameter ($\mu=3.9999$, first logistic map initial condition $x_0 = 0.1$ and second one $x_0 = 10000001$) to confirm the high sensitivity of the logistic map (Sensitivity to initial condition).

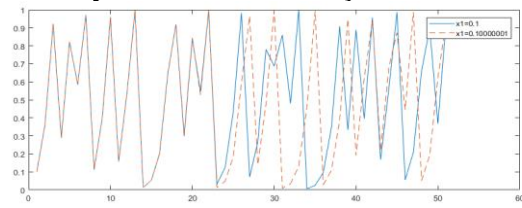


Figure 1: Two logistic maps

2.2. CHAOTIC LORENZ SYSTEM

The Lorenz system is the first numerical study of chaos[6]. The model was reported and published for the first time by E.N Lorenz in [7]. It was a classical chaotic systems and applied in scientific studies as a cause of the "butterfly effect" with the attractor has two wings like butterflies[8]. Consequently, it has been widely studied in chaos theory, dynamic system modeling, chaotic control and synchronization phenomenon. The chaotic Lorenz equation is a 3D dynamic system, defined by x, y and z. The system of equations gives a chaotic behavior compared to the initial parameters of the system. Apart from any chaotic 1D or 2D system, the Lorenz system has a much more complicated chaotic behavior. The Lorenz system is a system of ordinary differential equations. LvJinhu and Chen Guanrong proposed a model of three-dimensional continuous unified chaotic system to link the chaotic Lorenz system and the chaotic Chen system with a parameter in 2001.

When $0 \leq \alpha < 0.8$, Lorenz equation:

$$\frac{dx}{dt} = \sigma(y - x) \quad (2)$$

$$\frac{dy}{dt} = Rx - y - xz \quad (3)$$

$$\frac{dz}{dt} = xy - \beta z \quad (4)$$

Typical values for the parameters are $R=28$, $\sigma=10$, and $\beta=8/3$.

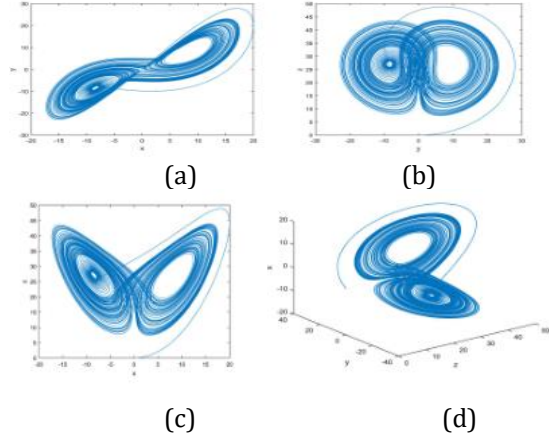


Figure 2: The projections of attractor on the planes (a) x-y, (b) x-z, (c) y-z and (d) Lorenz attractor in 3D

By using the discretization, we can get the differential equations. Here we choose the Euler method for discretization of the equation. Defined by the definition of the derivative, for sufficiently small:

$$\frac{y(x_{n+1}) - y(x_n)}{h} \approx y'(x_n) \approx f(x_n, y(x_n)) \quad (5)$$

Through it we can draw $(x_{n+1}) \approx y(x_n) + hf(x_n, y(x_n))$, according to the Lorenz equation method for the use of the derivative with respect to discrete:

$$\begin{cases} x_{n+1} = x_n + \sigma(y_n - x_n)h \end{cases} \quad (6)$$

$$\begin{cases} y_{n+1} = y_n + (Rx_n - y_n - x_n z_n)h \end{cases} \quad (7)$$

$$\begin{cases} z_{n+1} = z_n + (x_n y_n - \beta z_n)h \end{cases} \quad (8)$$

Typical values for the parameters are $h=0.0001$, $R=28$, $\sigma=10$, and $\beta=8/3$. [15]. And we will use these three equations in our algorithm.

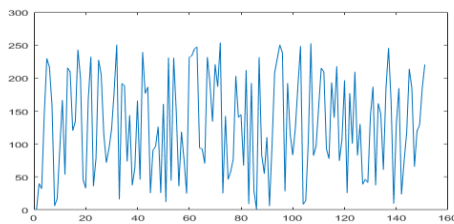


Figure 3: The plot of Lorenz systems for x along t-axis for $\alpha = 10, \beta = 28, \gamma = 8/3$

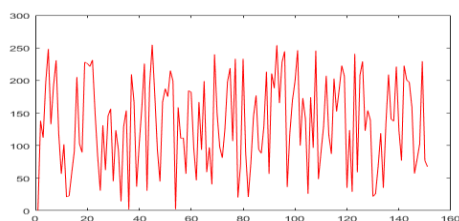


Figure 4: Plot of Lorenz systems for y along t-axis for $\alpha = 10, \beta = 28, \gamma = 8/3$

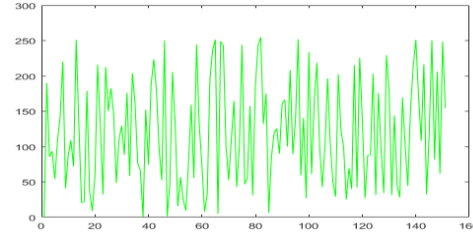


Figure 5: Plot of Lorenz systems for z along t-axis for $\alpha = 10, \beta = 28, \gamma = 8/3$

The three histograms of the three equations of Lorenz Chaotic System present the trajectory of each equation and like we regard here the trajectory is randomly and that's behavior what we want in our proposed algorithm.

3. PROPOSED ALGORITHM

In the proposed algorithm, we used the combination between Chaotic Lorenz System and Cyclic Rotation Technique for encrypting satellite images. Figure 6 shows the detailed procedure of the proposed algorithm.

The following four steps obtain the desired results, which we need:

1. Select one equation from (x_{n+1}) or (y_{n+1}) according to (z_{n+1}) by $((Z) \bmod 2)$.
2. XORed the original image with the equation determined according to the previous step.
3. Apply the cyclic rotation technique to the result obtained from the previous step.
4. The encrypted image.

Step 1: Select one equation from (x_{n+1}) or (y_{n+1}) according to (z_{n+1}) by $((Z) \bmod 2)$, therefore increasing the encryption complexity. With x_{n+1} is the iterated value by (Generator (x)) the first equation of Chaotic Lorenz System $(x_{n+1} = x_n + \sigma(y_n - x_n)h)$, y_{n+1} is the iterated value by (Generator (y)) the second equation of Chaotic Lorenz System $(y_{n+1} = y_n + (Rx_n - y_n - x_n z_n)h)$ and z_{n+1} is the modulo (2) of $(x+y)$ iterated by the third equation of Chaotic Lorenz system (Generator (x, y)).

Step 2: The original image is randomly mixed with chaotic keys generated by one of the two equations of Chaotic Lorenz System $(x_{n+1} \text{ OR } y_{n+1})$.

$$IC = \begin{cases} x_{n+1} \oplus 10 & \text{if } z_{n+1} = 0 \\ y_{n+1} \oplus 10 & \text{if } z_{n+1} = 1 \end{cases} \quad (9)$$

Where **IO** is the original image, **IC** is the cipher image. This confusion is sensitive to the original data and fulfills one cryptosystem validity condition.

Step 3: in the Diffusion operation, we use the Cyclic Rotation Technique with using the logistic map, which choose the parameter of rotation, and we apply that on the cipher image after the first encryption to give the desired result by permutation the pixels positions with using the following steps:

1. The logistic map specify the following parameters: A, B, C, and D. that control the offset number per pixel. All are controlled by the following equations:

$$C = \text{mod}(\text{floor}(xx_{n+1}(1) * AP), 256) \quad (10)$$

$$D = \text{mod}(\text{floor}(xx_{n+1}(2) * AP), 256) \quad (11)$$

$$A = \text{mod}(\text{floor}(xx_{n+1}(3) * AP), 256) \quad (12)$$

$$B = \text{mod}(\text{floor}(xx_{n+1}(4) * AP), 256) \quad (13)$$

Where $\text{floor}(xx_{n+1})$ mean the integrated value of (X), and **AP** is amplifier used to increase the values of the parameters.

2. We use the logistic map to controller and select which operation will use in each iteration, by using the following equation:

$$T = \text{mod}(\text{floor}(xx_{n+1}), 4) \quad (14)$$

- a. If the value of (T) equal zero, the pair rows will be shifted to the right by the value of the parameter (C) and the impair rows stay fix.
- b. If the value of (T) equal one, the impair rows will be shifted to the left by the value of the parameter (D) while the pair rows stay fix.
- c. If the value of (T) equal two, the pair columns will be shifted to the up by the value of the parameter (A) and the impair columns stay fix.
- d. If the value of (T) equal three, the impair columns will be shifted to the down by the value of the parameter (B) and the pair columns stay fix.

4. Repeat the third step (N) times to give the desired results of our proposed cycle rotation technique.

Step 4: We have the encrypted image.

By comparing the proposed algorithm with others works according the desired results and performances, our proposed algorithm used only one efficient chaotic system (Lorenz Chaotic System(3D)) which divided on three different equations, that's give simplicity in using and understanding, while the others works [9], [10] used more than one chaotic system (1D, 2D and 3D) which give more complexity in using and

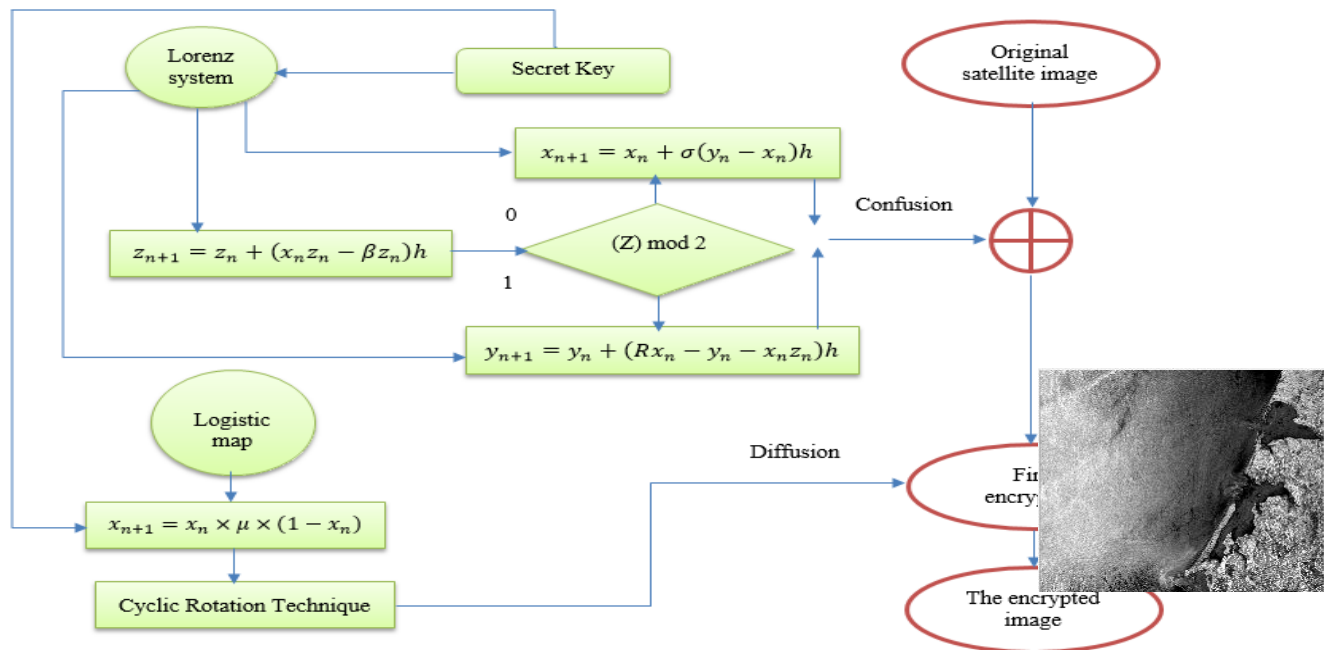


Figure 6: Block diagram of the encryption algorithm

3. In each iteration:

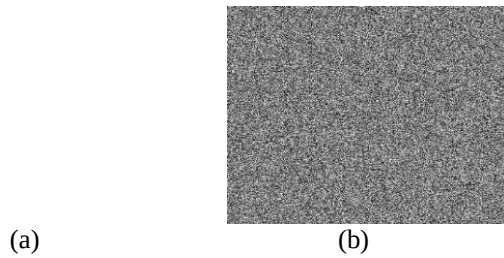
understanding and in otherwise there are works [11], [12] which used Advanced Encryption

Standard AES with chaotic systems used such as key or in confusion operation, and also there are a high complexity in these works and some disadvantages.

On the other hand, we used a simple and fast cycle rotation technique to give more encryption on the concerned image, while almost of recent works did not use a cycle rotation technique. The obtained and desired results shown in the following section in details.

4. PERFORMANCE AND EXPERIMENT RESULTS AND ANALYSIS

We have implemented the proposed algorithm using MATLAB, and observed the results on an Intel Core i3- 4030U CPU 1.9 GHz PC with 4 GB RAM. We use satellite image: Alaska image image[13] as shown in Figure 7. The initial parameters are: $x(0)=0.1$, $y(0)=0.2$, $z(0)=0.3$, $h(0)=0.0001$, $xx(0)=0.1$ and the repeating times $N=5$.



4.1. Histogram analysis

It is very important to protect the information of the original image to resist the statistical attacks, and to not found any statistical similarity between the original and encrypted images. The histogram of the encrypted image has to be uniform. The hackers and attackers find a difficulty to extract the pixels' statistical nature of the plain-image from the cipher-image, and the algorithm can resist a chosen-plaintext or known-plaintext attack. To examine the statistical distribution, we analyze several tests results of

the proposed algorithm by calculating and analyzing the histograms of this image. The histogram analysis was performed on a satellite image of 256 (gray-scale) pixels of Alaska and its corresponding cipher image as shown in Figure 8.

As shown in Fig.8, the histogram for encryption image has uniform distribution, which are significantly different from the original image histogram with no statistical similarity in appearance. Therefore, the proposed encryption algorithm can resist statistical attack.

4.2. Key space

To secure sensitive and critical satellite imagery from brute force and similar attacks, the encryption algorithm should have a large key space and be sensitive to a secret key. According to the IEEE-754 the computational precision of the 64-bit double precision number is about 10^{-15} . The total key

Figure 9: Secret key sensibility in the encryption process. (a) Encrypted image with $x_1 + 10^{-15}$. (b) Encrypted image with $y_1 + 10^{-15}$. (c) Encrypted image with $z_1 + 10^{-15}$. (d) Encrypted image with $h + 10^{-15}$. (e) Subtraction of (a) and Fig. 7(b). (f) Subtraction of (b) and Fig. 7(b). (g) Subtraction of (c) and Fig. 7(b). (h) Subtraction of (d) and Fig. 7(b).

Figure 7: (a) Original image of Alaska, (b) encrypted image of Alaska

space of the proposed algorithm is:

$$\text{Key} = (x(0) = 10^{15}) \times (y(0) = 10^{15}) \times (z(0) = 10^{15}) \times (h = 10^{15}) \times (xx(0) = 10^{15}) \times (N = 10) = 10^{76} \approx 2^{250} > 2^{100}$$

The key space is large enough to reduce the risk of brute force attack. The key space is sufficient for practical use for real-time satellite imaging applications.

4.3. Key sensitivity analysis

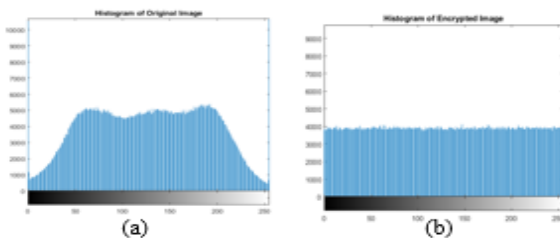
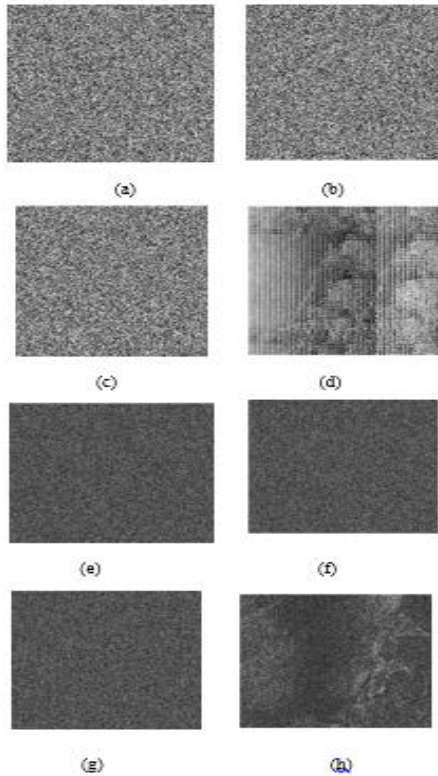


Figure 8: (a) is histogram of Fig. 7 (a), (b) is histogram of Fig. 7 (b).

Images	Size	Correlation coefficient			Entropy	NPCR	UACI	HD
		Horizontal l	Vertical	Diagonal				
Satellite image of Alaska	1000×1000	0.0007	-0.0002	0.0015	7.9998	99.5997	33.4913	50.0242

To confirm the ideality of an image encryption algorithm, it should be sensitive to the inputs (secret key and original image). If a single bit had been changed in either the secret key or original image, it should produce a completely different output results. Therefore, we

guarantees the security of encryption algorithm against external attacks and even a tiny change in the secret key. We take the Alaska image (1000*1000) as the plain image, then the results of the sensibility analysis shown in Fig9. There are a quite difference between the ciphers images as shown below proposed algorithm is sensitive to secret keys in both processes.



implement a sensitivity analysis on the secret key and original image to prove the robustness of the proposed encryption algorithm. The secret key, should be with a high sensitivity in the cryptosystem of satellite image, this high sensitivity leads to don not decrypted correctly the encrypted image, if there is only a slight difference between secret key. In addition, that

Table 1: Performance of the proposed algorithm

4.4. Correlation coefficients analysis

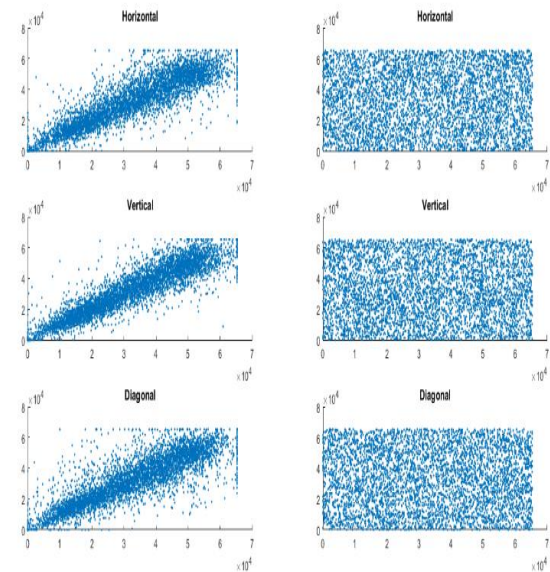


Figure 10: Adjacent pixels correlation at horizontal, vertical, and diagonal directions: (a) Plaintext image,

To evaluate the correlation coefficients of the encrypted images in three different directions: horizontal, vertical and diagonal, we choose randomly 5000 pairs of neighboring pixels. The table 1 shows the correlation coefficients values of both plain and encrypted images. The correlation of adjacent pixels for the plain and ciphered image shown in Fig. 10 in the three directions: horizontal, vertical, and diagonal. The proposed encryption scheme can resist the statistical attacks. By Fig. 10, we cannot be observed the difference of the three directions of encrypted image by a naked eye thus for the accurate comparison, we computed the correlation coefficient for the encrypted satellite image.

Therefore, we used the following correlation coefficients formula:

$$r_{xy} = \frac{Con(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (15)$$

$$Con(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (16)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (17)$$

$$E(y) = \frac{1}{N} \sum_{i=1}^N y_i \quad (18)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (19)$$

$$D(y) = \frac{1}{N} \sum_{i=1}^N (y_i - E(y))^2 \quad (20)$$

Where:

r_{xy} : The correlation coefficient of two adjacent pixels

$E(x), E(y)$: The expectation of variable

$D(x), D(y)$: The variance of variable

As shown in table 1 the correlation coefficients of the proposed algorithm are very low or practically zero. Thus, the proposed algorithm resisted to statistical attacks.

4.5. Differential attack analysis

There are three performance indices used to test the effect of a 1-bit change in the plain-image on the corresponding cipher-image. They are the number of pixels change rate (NPCR), the unified average changing intensity (UACI) and Hamming Distance (HD). Suppose cipher image before and after one pixel change in a plain image are C^1 and C^2 , respectively; the pixel value at grid (i, j) in C^1 and C^2 are denoted as $C^1(i, j)$ and $C^2(i, j)$; and a bipolar array is defined in Eqn. (21). Then the NPCR, UACI and HD can be mathematically defined by Eqns. (22), (23) and (24) respectively, where symbol T denotes the total number pixels in the cipher text, symbol F denotes the largest supported pixel value compatible with the cipher text image format, n_b is the number of bits per pixel, and $|\cdot|$ denotes the absolute value function.

$$D(i, j) = \begin{cases} 0, & \text{if } C^1(i, j) = C^2(i, j) \\ 1, & \text{if } C^1(i, j) \neq C^2(i, j) \end{cases} \quad (21)$$

$$NPCR: N(C^1, C^2) = \sum_{i,j} \frac{D(i, j)}{T} \times 100\% \quad (22)$$

$$UACI: U(C^1, C^2) = \sum \frac{|C^1(i, j) - C^2(i, j)|}{F \times T} \times 100\% \quad (23)$$

$$HD: H(C^1, C^2) = \sum \frac{|C^1(K) XOR C^2(K)|}{n_b \times T} \times 100\% \quad (24)$$

Thus for several satellite images, the mean values of NPCR, UACI, and HD are equal to 99.61%, 34.33%, and 50.72%, respectively. The results shown in Table 1 indicate that the differential attack analysis tests the best values of NPCR, UACI, and HD.

4.6. Information Entropy analysis

The information entropy is one of the criteria to measure the strength of the cryptosystem. It measures the average information per bit in an image. Therefore, the entropy of an encrypted image means each pixel has equal probability with uniform distribution [8]. The statistical measure used to test the effectiveness of the proposed encryption system is the $H(m)$ entropy given in next equation:

$$H(m) = \sum_{i=0}^{255} P(m_i) \log_2 \frac{1}{P(m_i)} \quad (25)$$

Where $P(m_i)$ represents the probability of occurrence of m_i . The values of information entropy of encrypted images in table 1 are very close to the ideal value; therefore, the proposed algorithm has confirmed its strength and quality against attacks.

4.7. Computation time performance analysis

A very important issue is the performance and efficiency for computation time applications while doing satellite images encryption and decryption. We will compare the computation time of our proposed algorithm with AES Classic to observe the computation time of every algorithm. The results of some experiments given in table 2 to prove the high performance and efficiency of the proposed algorithm.

Table 2: Comparative speed test experiment results of the proposed algorithm and AES Classic

Images & size (pixels)	Proposed Algorithm (Encryption Time (s))	AES Classic (Encryption Time (s))
Alaska (1000×1000)	0.2424 (s)	0.6888 (s)

As shown in table 2 the proposed algorithm is faster in speed as compare to other traditional image encryption algorithms AES and has edge in performance.

4.8. Fault propagation analysis (Single Event Upsets & Transmission errors)

As its illustrate in Table 3, we can confirm that the encrypted images have slightly different from each other and that transmission errors are not propagating to the other image pixels and SEU affect just one block by the obtained small NPCR and UACI values. Consequently, our proposed encryption scheme can resist error propagation against the effect of SEUs and transmission errors.

Table 3: Impacts of SEU and transmission errors

The Type	NPCR	
----------	------	--

of error		UACI
SEUs	2.0000 e-04	1.0941-04
Transmission errors	1.0000e-04	3.9216e-05

5. CONCLUSION

In this paper a new technique based on Chaotic Lorenz System and Cyclic Rotation Technique is proposed specifically designed to secure satellite imagery from unauthorized access and illegal use. The idea of utilizing chaotic techniques is to ensure confusion and diffusion operations and the main goal of this method is to achieve a high level of security. First, a complete confusion based on the Lorenz system generators has been used to increase the complexity of data encryption, is applied. Then, cyclic rotations were used to improve the resistance to single image attacks. The experimental results have assured that the proposed algorithm is able to resist differential, brute force, statistical, and image attacks, and is therefore highly secure and efficient. The speed of encryption and decryption is fast compared to other chaos-based encryption algorithms and adequate for satellite imagery.

REFERENCES

- [1] B. PokhaliSayedRoohi, « Satellite On-Board Encryption », University of Surrey, 2007.
- [2] Z. Hua, Y. Zhou, C.-M. Pun, et C. L. P. Chen, « 2D Sine Logistic modulation map for image encryption », *Information Sciences*, vol. 297, p. 80-94, mars 2015, doi: 10.1016/j.ins.2014.11.018.
- [3] Z. Hua et Y. Zhou, « Image encryption using 2D Logistic-adjusted-Sine map », 2016.
- [4] S. El Assad, M. Farajallah, et C. Vladeanu, « Chaos-based Block Ciphers: An Overview », 2014.
- [5] L. Li-Hong, B. Feng-Ming, et H. Xue-Hui, « New Image Encryption Algorithm Based on Logistic Map and Hyper-Chaos », in *2013 International Conference on Computational and Information Sciences*, Shiyang, China,

- juin 2013, p. 713-716, doi: 10.1109/ICCIS.2013.193.
- [6] F. Özkaynak et A. Özer, « A method for designing strong S-Boxes based on chaotic Lorenz system », 2010.
- [7] X.-Y. Wang et Y.-X. Xie, « Cryptanalysis of a chaos-based cryptosystem with an embedded adaptive arithmetic coder », *Chinese Phys. B*, vol. 20, n° 8, p. 080504, août 2011, doi: 10.1088/1674-1056/20/8/080504.
- [8] Q. Zhang, Y. Guo, W. Li, et Q. Ding, « Image Encryption Method Based on Discrete Lorenz Chaotic Sequences », 2016.
- [9] M. Usama, M. K. Khan, K. Alghathbar, et C. Lee, « Chaos-based secure satellite imagery cryptosystem », *Computers & Mathematics with Applications*, vol. 60, n° 2, p. 326-337, juill. 2010, doi: 10.1016/j.camwa.2009.12.033.
- [10] E.-H. Bensikaddour, Y. Bentoutou, et N. Taleb, « Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher », 2018.
- [11] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, et N. Bounoua, « An improved image encryption algorithm for satellite applications », *Advances in Space Research*, p. S0273117719306908, sept. 2019, doi: 10.1016/j.asr.2019.09.027.
- [12] F. Bin Muhaya, « Chaotic and AES cryptosystem for satellite imagery », 2011.
- [13] « <https://directory.eoportal.org/web/eoportal/satellite-missions/e/eros-a> ».
- [14] M. Kaur et V. Kumar, « A Comprehensive Review on Image Encryption Techniques », 2018.