The Impact of A Chaotic Map on The Encryption Quality of Insar Interferograms

Karim Benamara[1], Riad Saidi[2*], Nada Cherrid[3], Tarek Bentahar[4], Hanane Djellab[5] and Atef Bentahar[6]

[1]Department of Electronics and Telecommunications, Laboratory of Mathematics Informatics and Systems, University Echahid Cheikh Larbi Tebessi Tebessa, Road of Constantine, 12002, Tébessa, Algeria [2]Electronics Department, Laboratory of Signals and Smart Systems, University Mustapha Ben Bboulaid-Batna2, 53 road of Constantine Fesdis, 05078, Batna, Algeria, University Echahid Cheikh Larbi Tébessi Tébessa, road of Constantine, 12002, Tébessa, Algeria [3]Electronics Department, University Mustapha ben boulaid-Batna2,53 Road of Constantine Fesdis, 05078, Batna, Algeria [4]Higher National School of Renewable Energies, Environment & Sustainable Development, Laboratory of Signals and Smart Systems, Constantine Road, Fesdis, Batna 05078, Algeria. University Echahid Cheikh Larbi Tébessi Tébessa, road of Constantine, 12002, Tébessa, Algeria [5]Department of electronics and Telecommunications, University Echahid Cheikh Larbi Tebessi Tebessa, Road of Constantine, 12002, Tébessa, Algeria, LTI laboratory of Guelma, University Guelma, BP 401 24000, Guelma Algeria [6]Department of Mathematics and Computer Science, Center Si El'Houès -Barika, Batna, Algeria
*Corresponding author: r.saidi@univ-batna2.dz
karim.benamara@univ-tebessa.dz, n.cherrid@univ-batna2.dz, tarek.bentahar@univ-tebessa.dz, hanane.djellab@univ-tebessa.dz, atef.bentahar@cu-barika.dz

Abstract: The transmission of satellite images to Earth is vulnerable to various threats, both accidental and intentional, which can compromise the confidentiality and integrity of the data. Recognizing this risk, satellite manufacturers have emphasized the need for robust data security measures, leading to a growing demand for encryption algorithms that can effectively protect transmitted images.

The primary aim of this work is to enhance the security of InSAR interferograms by implementing a multi-stage encryption process to safeguard transmitted data against potential threats.

The encryption process is executed in three stages. Initially, the interferogram undergoes encryption using the Advanced Encryption Standard (AES) in two modes: Output Feedback (OFB) and Counter Mode (CTR), both employing a 256-bit key generated by a GEFFE generator. To ensure secure transmission, In the third stage, a chaotic logistic map with predefined initial parameters is applied to the interferogram previously encrypted using both AES-256-OFB and AES-256-CTR modes. This additional encryption layer further secures the already processed interferogram, providing enhanced protection against potential attacks.

The effectiveness of the encryption process was evaluated using several image quality and security metrics, including Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM). Additionally, statistical analyses were performed, such as histogram analysis of encrypted interferograms, entropy calculation, and differential analyses like the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI). These evaluations confirmed the robustness of the encryption approach.

The proposed multi-stage encryption method demonstrated strong security performance, effectively protecting InSAR interferograms during transmission. The positive results from various security and quality metrics indicate that this approach enhances key security and rovide a reliable means of securing satellite image data.

Received: March 28th, 2025. Accepted: June 25th, 2025
DOI: 10.15676/ijeei.2025.17.2.14

Keywords: Interferogram InSAR; AES-256; OFB mode; CTR mode; GEFFE generator; logistic map.

1. Introduction

Satellite images are captured by observation instruments on satellites, covering Earth or other planets. These images are utilized in diverse fields such as agriculture, meteorology, forestry, urban planning, military operations, and more. Satellite imagery has become an essential tool across many domains [1]. Ensuring their security against unauthorized access (confidentiality) and protecting them from unauthorized modifications (integrity) are critical concerns. Additionally, satellite images must be accessible to authorized entities when required (authentication) [2].

The images analyzed in this study are interferograms from the inSAR system, which uses an independent light scanning technique. This method illuminates surfaces with its own source of electromagnetic waves [3][31]. inSAR interferograms are employed in various applications, including Earth observation, meteorology, and cartography [4][5].

The inSAR system produces two types of images: an amplitude image and a phase image. These images are derived from the complex correlated signal captured by two separate antenna acquisitions. The phase image, also known as an interferogram, is inherently wrapped within the range of $[-\pi, +\pi]$. To obtain the true phase values, an unwrapping process is required. This process involves determining the cycle number that needs to be added to each pixel [6]. Encryption has been used for a long time as a security measure in military strategies and for exchanging classified data. In today's digital world, secure information transfer is crucial and widely practiced. Interferograms are particularly noteworthy due to the large volume of data they encompass. Several encryption techniques have been proposed to secure satellite images, including the symmetric encryption algorithm AES (Advanced Encryption Standard). Endorsed as a standard by the National Institute of Standards and Technology (NIST), AES is widely adopted by organizations globally. AES is a symmetric block cipher where both the sender and receiver use the same key for encryption and decryption. It processes 128-bit (16-byte) data blocks and supports cryptographic keys of 128, 192, or 256 bits [7]. In practical applications, the AES algorithm is often supplemented with a series of straightforward operations to enhance security while preserving efficiency. This approach is referred to as a cryptographic mode and includes methods such as CBC (Cipher Block Chaining), OFB (Output Feedback), and Counter-mode encryption, which are utilized in this paper. These modes are techniques for applying block ciphers, as detailed in [8].

A GEFFE generator that utilizes three variable-length Linear Feedback Shift Registers (LFSRs) to produce the desired sequence. Two of these LFSRs operate as input multiplexers, while the third functions as a controller, ensuring the GEFFE generator produces high-quality pseudo-random sequences [9]. It should be noted that AES is the only encryption standard recommended by CCSDS for onboard satellite data encryption [10].

Some satellites use the 3-DES algorithm for image encryption, but our work utilizes the AES algorithm, the successor to DES [11], for encrypting interferograms. Despite the availability of various encryption algorithms, the adoption of encryption technology in spacecraft has lagged behind its use in Earth-based systems [12]. Obtaining a comprehensive overview of encryption methods used in satellites is challenging, as most manufacturers and satellite operators do not disclose this information. However, some documents do reference the encryption algorithms used in specific space missions [13].

To enhance AES encryption performance, several modifications have been proposed in previous studies [14]. Additionally, research has explored advancements in cryptography, such as a study [15] that introduced a new encryption algorithm for digital images by combining a chaotic system with a modified version of AES. Another approach, detailed in [16], presents a hybrid fractal-chaos image encryption technique designed to ensure highly secure transmission. The study described in [17] involves dividing the InSAR interferogram into three equal segments and encrypting each segment separately using the AES-256 algorithm in Output

Feedback (OFB) mode to enhance security. Given the extensive use of image data across various fields, numerous encryption algorithms have been developed to protect this data. In this context, [18] provides a comparative analysis of two image encryption algorithms: one based on AES and the other using a chaotic cryptosystem that employs a logistic map. The study aims to evaluate and compare their robustness in terms of security.

2. Algorithms used in our work

This work employs three algorithms: AES with a key length of 256 bits, a logistic map, and an asymmetric algorithm, which is RSA. The encryption process utilizes OFB and CTR modes illustrated in Figure 1.

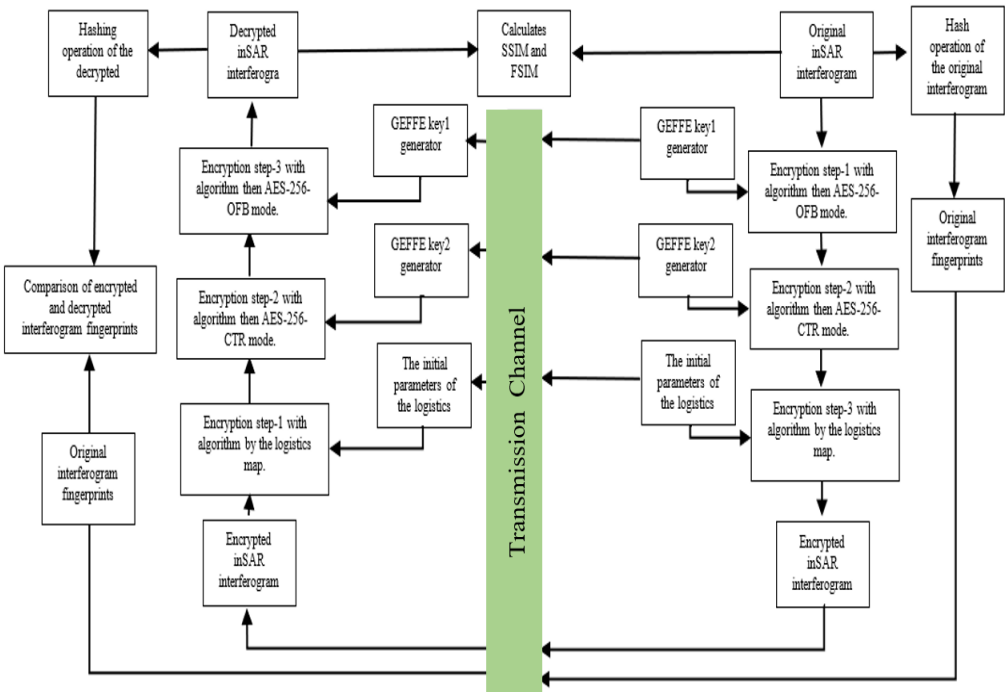


Figure 1. Transmission cryptosystem

A. AES algorithm

AES is a symmetric, secret-key block encryption system. It offers the possibility of working on blocks of 128, 192 or 256 bits. Standard AES only uses a block size of 256 bits. The encryption key can be 128, 192, or 256 bits. The calculation time for "sub-keys" is low. This is a strong and interesting point when used in a rapidly changing security context [3][19]. This work implements the AES -256 encryption algorithm. The encryption process for the AES algorithm is as follows:

- Generate all the sub-keys that will constitute the keys of each round, from the initial key.
- Initialize the 128-bit data matrix which represents the plain text.
- Add the initial key to the data matrix.
- Perform nine encryption cycles per round on the state matrix.
- Copy the final state matrix as encrypted data (encrypted text).

The encryption process is the reverse process of decryption, which is illustrated in Figure 2.

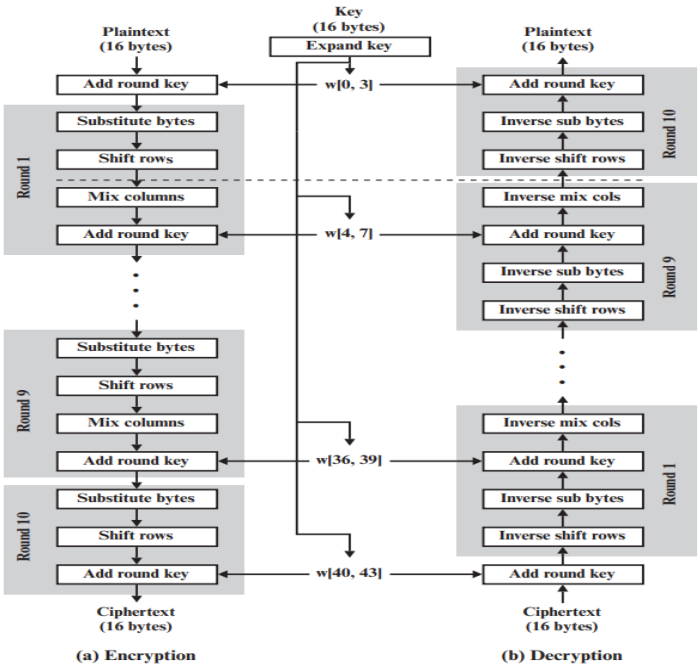


Figure 2. AES algorithm [20]

In addition, AES is the only standard recommended by the CCSDS for encrypt data on board satellites [20].

B. GEFFE key generator for AES-256

In our study, the GEFFE generator is employed to create an encryption key for AES-256. This process involves three linear feedback shift registers (LFSRs) of varying lengths to generate the desired sequence, as shown in Figure 3. Two of these LFSRs function as input multiplexers, while the third LFSR serves as a controller. To guarantee that the GEFFE generator produces a high-quality pseudo-random sequence, each LFSR must be straightforward in design [9], see Figure 3.

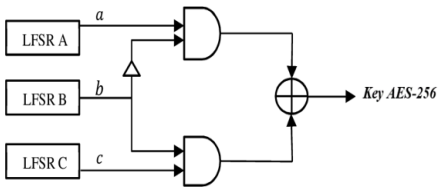


Figure 3. Scheme of GEFFE generator [9]

$$keystream = (a \wedge (\neg b) \oplus (b \wedge c)) \quad (1)$$

$$f(a,b,c) = a(1 \oplus b) \oplus b.c = a \oplus a.b \oplus b.c \quad (2)$$

Where:

a, b, c: represent the output bits of the 03 LFSR.

$\neg b$: represents the logical negation of bit b.

$\oplus$: represents the XOR (or exclusive) logical operation.

The product: presents the logical AND operation.

In our work the GEFFE generator is used as the key generator for AES-256 for both OFB and CTR modes, we used a GEFFE generator of three linear feedback shift registers (LFSR) as shown in Table 1.

Table 1. Parameter of the three LFSR registers

The three registers	LFSR A	LFSR B	LFSR C
Length(bits)	11	13	17
Feedback coefficients	[2,7]	[7,11]	[3,13]

The maximum period of each LFSR is according to equality (2^n-1) [11], with n being the number of bits in the LFSR register.

LFSR A= $(2^{11}-1)$;

LFSR B= $(2^{13}-1)$;

LFSR C= $(2^{17}-1)$.

The maximum period of a GEFFE generator is the product of the maximum periods of the individual shift registers. The maximum period of GEFFE = $(2^{11}-1)\ (2^{13}-1)\ (2^{17}-1)$.

By generating a sequence of size 256 bits from each LFSR, we then apply the GEFFE generator formula to generate the key sequence of size 256 bits to use for AES for encryption and decryption.

C. Output Feedback (OFB) Mode

In this mode, the process starts by encrypting an initial vector. The resulting key stream is then fed back into the input to generate the subsequent key stream, as illustrated in Figure 4 [9].

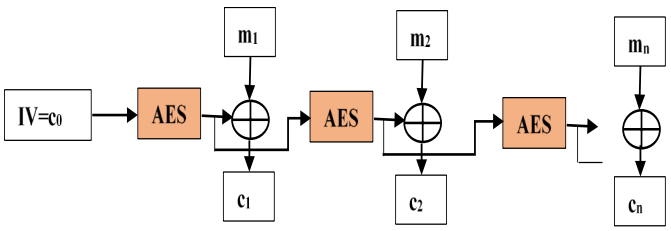


Figure 4. OFB block encryption mode [4]

This mode is useful in satellites where minimizing the number of on-board circuits is crucial.

D. Counter-mode encryption (CTR) Mode

This mode is entirely symmetric and can be easily parallelized. It involves encrypting an initial counter value T, as illustrated in Figure 5 [9].

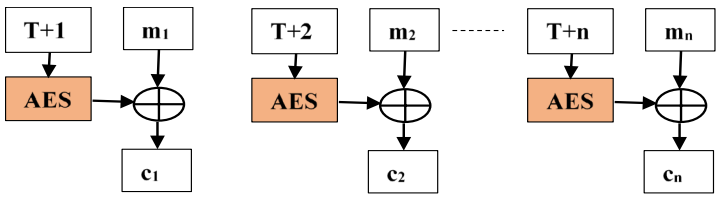


Figure 5.CTR block encryption mode [4]

E. Chaotic Logistic Map in inSAR Interferogram Cryptography

Chaotic systems possess several key characteristics that make them advantageous for securing communications [21]:

- Determinism: Chaotic systems are governed by specific mathematical equations that dictate their behavior.
- Butterfly Effect (sensitivity to initial conditions): When a chaotic map is iteratively applied to two points that are initially close, the iterations quickly diverge and become uncorrelated over time. This property allows chaotic systems to function as pseudo-random number generators.

Due to these appealing features, chaos is considered a highly promising approach for cryptosystem design [22].

The core concept involves the transmitter generating a chaotic signal to obscure the original interferogram. At the receiver's end, a second chaotic system is used to synchronize with the transmitted, encrypted interferogram. A simple subtraction operation then reveals the decrypted interferogram. In this study, a chaotic logistic map used.

F. The Logistic Map

Chaotic maps are dynamic systems governed by recurrence relations. The Logistic map, in particular, is a polynomial mapping whose behavior is dictated by a simple nonlinear dynamic equation. The equation for the chaotic Logistic map is provided in (3) [23]:

$$x(n+1)=r.\ x(n).(1-x(n)) \tag{3}$$

Where:

x : is variable in the interval [0, 1][23].

n : is the number of iterations.

r : is a number defined in the interval [0, 1].

G. Lyapunov Exponent

The Lyapunov exponent is a quantitative measure of chaos; from this, Lyapunov demonstrated that the number of Lyapunov exponents is equal to the dimension of the phase space. [24].

Let us consider a one-dimensional discrete system and $x0$ and $x0+\varepsilon$ two very close initial conditions, let us assume that they deviate on average at an exponential rate.

We will be able to find; a real λ such that after n iterations we will have (4) [24]:

$$\left|f^n(x_0+\varepsilon)-f^n(x_0)\right| \cong \varepsilon e^{n\lambda} \tag{4}$$

Hence:

$$n\lambda \cong ln\frac{\left|f^n(x_0+\varepsilon)-f^n(x_0)\right|}{\varepsilon}=\frac{1}{n}ln\left|\frac{df^n(x_0)}{dx_0}\right| \tag{5}$$

$$\cong \frac{1}{n}ln\left|\frac{df^n(x_0)}{dx_0}\right|\left|\frac{df^{n-1}(x_0)}{dx_0}\right|....\left|\frac{df^1(x_0)}{dx_0}\right| \cong \frac{1}{n}\sum_{i=0}^{n-1}\left|\frac{df(x_i)}{dx_i}\right| \tag{6}$$

Est pour $n\to\infty$ on a :

$$\lambda=\lim_{n\to\infty}\frac{1}{n}\sum_{i=0}^{n-1}\left|\frac{df(x_i)}{dx_i}\right| \tag{7}$$

According to (7), λ is called the Lyapunov exponent, indicating the average divergence rate:

- If $\lambda > 0$, there is sensitivity to initial conditions.
- If $\lambda < 0$, there are trajectories that converge and information on the initial conditions is lost [24].

H. Encryption Method

This section explains the encryption phase executed by the cryptosystem depicted in Figure. 1, which clearly details the steps required to encrypt and decrypted the interferogram.

Step 1: Reading the original interferogram.
Step 2: Conversion of the interferogram to grayscale: If the interferogram is in color, it is converted to grayscale using the `rgb2gray` function.
Step 3: The interferogram undergoes a hashing operation, producing a fingerprint of the original interferogram, which will be transmitted for comparison with the fingerprint of the decrypted interferogram at the receiver's end.
Step 4: First, the original interferogram is encrypted using the AES-256 algorithm in OFB mode, with the key generated by a GEFFE generator.
Step 5: In the second phase, the interferogram encrypted in Step 4 is encrypted again using the AES-256 algorithm in CTR mode, where the same key used in Step 4 is applied. This key will then be transmitted for the decryption phase.
Step 6: The interferogram encrypted in Step 5 is further encrypted using a chaotic Logistic map, where:

- The initial parameters (r, x0) of the chaotic Logistic map are initialized.
- A sequence of chaotic numbers is generated using the chaotic logistic map: The logistic map is used to generate a sequence of chaotic numbers through iteration. This sequence is produced to cover the entire size of the interferogram (number of rows × number of columns).
- The pixels of the interferogram are permuted using the generated sequence of numbers: The chaotic number sequence is sorted, and the sorting indices are recorded. The image pixels are then permuted using these indices, resulting in a random mixing of the pixels, which produces an encrypted interferogram.
- The initial parameters of the Logistic map will be transmitted for the decryption phase.

Step 7: Upon reception, a decryption operation is completed, followed by a hashing operation on the decrypted interferogram, resulting in a fingerprint that will be compared to that of the original interferogram. Finally, the SSIM and FSIM between the original and decrypted interferograms are calculated to confirm the integrity criterion.

3. Results and analysis

The study in this article was carried out on a PC equipped with a Pentium I-5 2.53 GHz processor, running Windows 10, and 20GB of RAM, using MATLAB 2020b software. The image analyzed is an inSAR system interferogram, detailing the geographical region of Sardinia, as specified in Table 2. This interferogram is utilized to assess both the encryption and decryption quality, along with the security performance of the AES-256 algorithm, using a key generated by a GEFFE generator. The encryption process combines two modes, OFB and CTR, with a cascading logistic map, as illustrated in Figure 1.

Table 2. Characteristics of the interferogram studied

Interferogram	Imaged region	Taken on
Input Interferogram	Sardinia	Aug2, 1991
	Orbit	Baseline(m)
	241	126
	Residue’s rate (%)	
	0,0436	

In this part, the encryption and decryption results of the input interferogram, presented in Figure 6, with the cryptosystem of Figure 1, are illustrated in Figure 7.

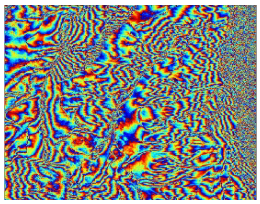


Figure 6. The original input interferogram

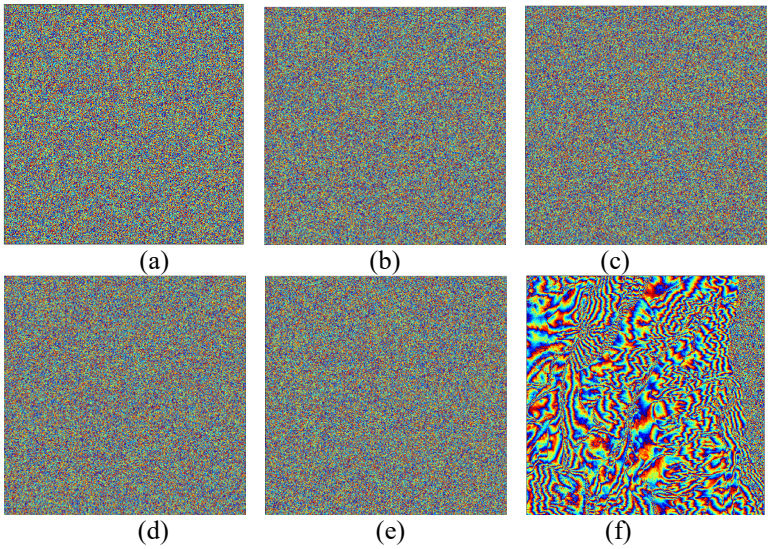


Figure 7. Input Interferogram encryption and decryption results, (a) Encrypted with AES-256-OFB, (b) Encrypted with AES-256-CTR, (c) Encrypted with logistics map, (d) Decrypted with logistics map, (e) Decrypted with AES-256-CTR, (f) Decrypted with AES-256- OFB.

Figures (a), (b) and (c) which represent the interferogram encrypted with AES-256-OFB, AES-256-CTR and the logistic map, respectively. Figures (d), (e) and (f) represent the interferograms decrypted with the logistic map, AES-256-CTR and AES-256-OFB, respectively. At first glance, we can clearly see that figure (f) is similar to the original, but measurements are needed to confirm this with certainty, which we will explore in more detail in this work.

A. The quality assessment of encrypted and decrypted interferogram

In this study, various metrics are employed to evaluate the quality of the encrypted and decrypted interferogram. A statistical and differential analysis is conducted to compare the results of encryption and decryption using the OFB and CTR modes, along with the chaotic logistic map, through an objective evaluation. The aims of these analyses are to: (i) assess the quality of the encrypted and decrypted interferograms, and (ii) demonstrate the contribution of the chaotic logistic map in conjunction with both modes to enhance the security of inSAR interferograms.

1. *Statistical Analyses*: Typically, image encryption can be effectively decrypted through statistical analysis. To assess the robustness of the cryptosystem and its resilience to statistical attacks, a comprehensive statistical analysis was conducted. Several key metrics were evaluated, including histogram analysis, entropy analysis, MSE, PSNR, Feature

Similarity Index (FSIM) SSIM for Image Quality assessment. These metrics provide valuable insights into the security and effectiveness of the encryption system, helping to determine its resistance to various statistical attacks.

a. Histogram analysis: The histogram of an encrypted image should have two properties [25]:

- It must be completely different from the histogram of the original image.
- It should have a uniform distribution.

Histogram analysis is used to illustrate the pixel intensity distribution in the interferogram Input Interferogram. It is important to note that the images in this work are interferograms from the inSAR system. Figure 8 and 9 show the histograms of the original and encrypted interferograms using the OFB-CTR modes with the AES-256 algorithm and the chaotic Logistic map. It is evident that both operational modes, as well as the Logistic map, meet the aforementioned properties. As shown in Figure 8 and 9, the histogram of the encrypted interferogram Input Interferogram is completely different from the original and exhibits a uniform distribution.

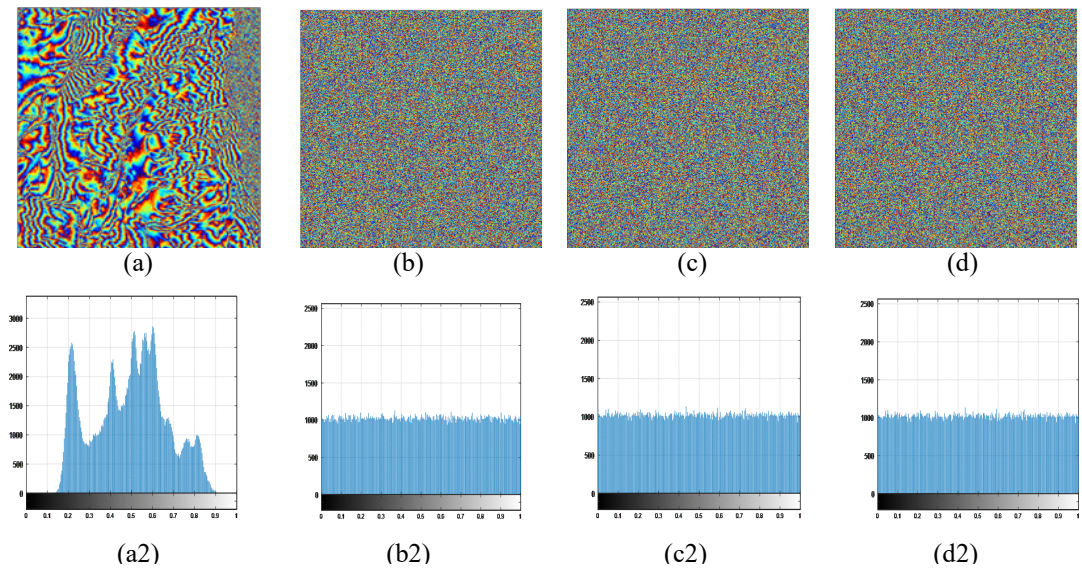


Figure 8. Histograms of the encrypted interferogram, (a, a2) Original Input, (b, b2) Encrypted with AES-256-OFB, (c, c2) Encrypted with AES-256-CTR, (d, d2) Encrypted with AES-256-logistics map.

From Figures 8 and 9, we can also observe that the histograms of the encrypted interferograms (b2), (c2), and (d2) satisfy the two key properties of encrypted image histograms:

- They are entirely different from the histogram of the original interferogram.
- Their distribution is uniform.

This indicates a complete dissimilarity between them, which is characteristic of strong encryption.

Regarding the histograms (e2), (f2), and (g2), they represent the decrypted interferogram histograms. Here, we can clearly see that histogram (g2) matches the distribution of histogram (a) from the original interferogram, demonstrating their similarity and confirming the full recovery of information.

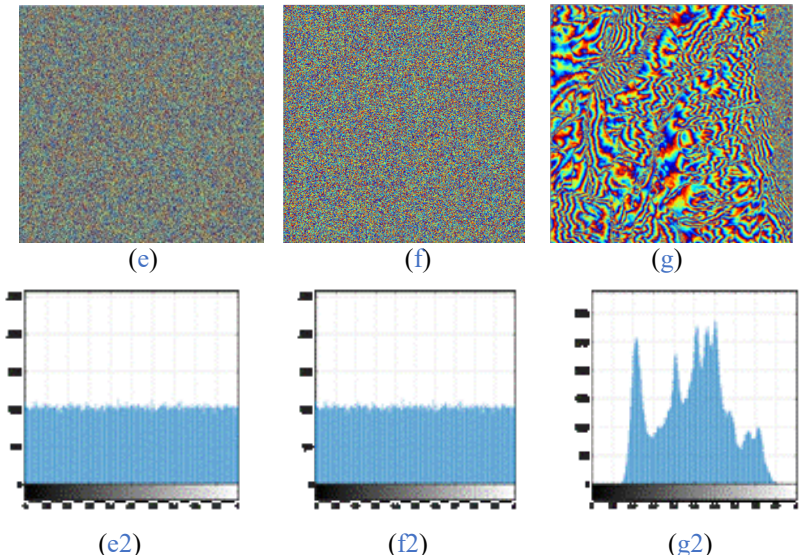


Figure 9. Histograms of the decrypted interferogram, (e, e2) Decrypted with AES-256-logistics map, (f, f2) Decrypted with AES-256-CTR, (g, g2) Decrypted with AES-256- OFB.

2. *Entropy analysis*: Shannon entropy, introduced by Claude Shannon, is a mathematical function that intuitively represents the amount of information contained in a source [20]. When applied to an image, entropy is used to characterize its texture. The entropy function is defined by (8) [20]:

$$H = -\sum p(i) * \log\left(p(i)\right) \quad (8)$$

Where:

p(i): represents the probability of a pixel having an intensity level i.(i=0,1,2…,N)

N: denotes the maximum intensity level a pixel can have.

For interferograms, the maximum intensity level ranges from [-π, +π]. Entropy is also defined as the number of bits needed to reconstruct the entire plaintext after decryption. For a receiver, higher entropy indicates that the source transmits more varied information. For example, if a source consistently sends the same symbol, such as the letter "d," its entropy is zero. As shown in Table 3, the entropy values for AES-256-OFB-CTR modes and the Logistic map can reach 2.3124, which is a very favorable value approaching the ideal entropy for interferograms. This suggests that the pixels in the encrypted interferograms are statistically independent of one another.

Table 3. Characteristics of the interferogram studied

Encryption	Entropy		
	AES-OFB	AES-CTR	Logistics map
Input Interferogram	2.3091	2.3124	2.3124

The Table. 3 clearly shows, that the maximum entropy is recorded by the CTR mode and the logistic map.

3. *Mean Square Error Analysis*: The decrypted interferogram, *I*, is compared to the original interferogram, $\hat{I}$ to assess their similarity. One commonly used measure is the MSE, which calculates the difference between the original and decrypted pixels using equation (9) [3][27]. In this context, the decrypted pixels are considered the degraded pixels.

$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} (I(m,n) - \hat{I}(m,n))^2 \quad (9)$$

Where: $(M \times N)$: is the size of the interferogram,
I and $\hat{I}$: are the amplitudes of the pixels in the original and decrypted interferograms, respectively.
It is likely that the human eye is more sensitive to large amplitude errors, which makes quadratic measures more significant. The different MSE values between the original and decrypted interferogram are presented in Table 4.

Table 4. Mean square error

Encryption	MSE
	AES-256-OFB-CTR-Logistics map
Input Interferogram	0

The results presented in Table 4 indicate that the MSE is zero, signifying an excellent outcome. This suggests a perfect match between the original and decrypted interferograms, and the result is deemed satisfactory.

4. *Peak signal-to-noise ratio analysis*: PSNR measures fidelity and is a function of MSE, as defined by equation (10). Its definition and usage originate from the field of signal processing [3][27]:

$$PSNR = 10log_{10}\left(\frac{I_{max}^2}{MSE}\right) \quad (10)$$

For a grayscale interferogram, Imax represents the maximum possible luminance. An infinite PSNR value signifies an undegraded interferogram, while this value decreases with increasing degradation. Consequently, PSNR reflects the relationship between MSE and the maximum energy of the interferogram. Table 5 presents the PSNR values of the decrypted interferogram, with a PSNR value reaching 99%, indicating a very favorable result.

Table 5. Peak signal-to-noise ratio

Encryption	PSNR in %
	AES-256-OFB-CTR-Logistics map
Input Interferogram	99

5. *Structural Similarity Index Analysis[3][28][17]*: The SSIM metric evaluates the similarity between two images, x and y. Rather than focusing solely on pixel differences, SSIM takes into account changes in visual perception related to luminance, contrast, and image structure [23][10][4], as expressed by Equation [29][17]:

$$SSIM(x,y) = [l(x,y)]^{\alpha} c[(x,y)]^{\beta} s[(x,y)]^{\gamma} \quad (11)$$

Where:

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{\mu_x^2 + \mu_y^2 + C_1} \quad (12)$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (13)$$

$$S(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (14)$$

For images x and y, the variables μ_x, μ_y, σ_x, σ_y, and σ_{xy} denote the local means, standard deviations, and cross-covariance, respectively.
$l(x, y)$: measures the luminance similarity between x and y.
$c(x, y)$: assesses the similarity in contrast between x and y.

s(x, y): represents the structural similarity between x and y.
C_1, C_2 , and C_3 are small constants that are given by:
$C_1=(K_1L)^2$, $C_2=C_3=(K_2L)^2$and $C_3=C_2/2$
Where:
K_1 and K_2: are two constants of very low values.
L=255: For grayscale images.
The similarity index is used to properly select the constants K_1 and K_2, allowing the assessment to be generalized across the entire image [30].
In our work, image is an interferogram from an inSAR system, the SSIM is calculated between the original interferogram and decrypted ones, the results are projected in table 6, which is a very acceptable value.
The similarity index is used to appropriately select the constants K_1 and K_2 to generalize the assessment across the entire image. In our study, the images are interferograms from an inSAR system. SSIM is computed between the original interferogram and the decrypted versions. The results, presented in Table 6, show very acceptable values.

Table 6. Structural similarity index

Encryption	SSIM
	AES-256-OFB-CTR-Logistics map
Input Interferogram	1

6. *Differential analysis:* Sensitivity to even minor deterioration of the original image, of an encryption or security system, must be significant.
This feature is crucial to defend against differential attacks [17]. Two parameters are employed to assess this sensitivity:
NPCR and UACI are used for evaluation. NPCR measures the proportion of pixels that change, while UACI reflects the average intensity change. Ideal values for NPCR and UACI are 99.61% and 33.46%, respectively [10]. A differential analysis is performed to evaluate the resistance of the cryptosystem against differential attacks.
   a. *NPCR:* NPCR is calculated by modifying a single pixel in the original image, then comparing the encrypted version of the original image to the encrypted version of the modified image using the same cryptosystem. This results in a percentage that reflects the rate of pixel change. A high NPCR value indicates a strong cryptosystem. The NPCR is determined using equations (15) and (16) [17]:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{M*N} * 100\% \quad (15)$$

$$D(i,j) = \begin{cases} 1 \; if \; C1(i,j) \neq C2(i,j) \\ 0 \qquad otherwise \end{cases} \quad (16)$$

Where:
C_1: the encrypted image without modification
C_2: the encrypted image with modification
*M*N*: indicates the dimensions of the image.

UACI: After altering a single pixel in the original image, UACI is computed to assess the average intensity difference between the encrypted original image and the modified encrypted image. This calculation is carried out using the following equation (17) [17]:

$$UACI = \frac{1}{M*N}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C1(i,j)-C2(i,j))}{255}\right] * 100\% \quad (17)$$

In this study, the image being analyzed is the interferogram Input Interferogram. The results for both the NPCR and UACI parameters are shown in Table 7.

Table 7. NPCR AND UACI

Inteferogram	AES-256-OFB		AES-256- CTR		Logistics map	
	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)	NPCR (%)	UACI (%)
Input Interferogram	99.62	30.8320	99.61	30.7665	99.62	30.8135
Ref [4]	99,62	33,52	99,60	30,62	---	------
Ref [3]	100	31,40	-----	------	------	-------

The results of the differential analysis, presented in Table 7, clearly show values close to those reported in the literature. The encryption system design shown in Figure 1 involves processing the interferogram through three distinct phases:
Two phases using AES-256 (OFB and CTR modes), each with keys generated by a GEFFE generator, a final phase using a logistic chaotic map with initial parameters
Thus, three different keys are used for both encryption and decryption of the interferogram, along with three encryption/decryption phases. This multi-stage approach significantly enhances transmission security through the communication channel, since to decipher to get to the information of the interferogram you need to find the three keys, knowing that the first two keys are random and change each time

7. *The function of SHA-256:* This function generates a fixed-size 256-bit hash value from input messages of variable length. The primary purpose of SHA-256, like other hash functions, is to ensure data integrity and authenticity by producing a unique hash value for each specific input message. This guarantees that even a minor change in the input message will result in a substantially different hash value [10].
According to the cryptosystem in Figure 1, an SHA-256 hash function is applied to the original interferogram at the beginning, then an SHA-256 hash function is applied to the decrypted interferogram, a comparison is made between the two fingerprints to verify the integrity criterion. The results of these two procedures are presented in the table 8.

Table 8. The hash value fingerprint of the original interferogram and the decrypted interferogram using sha-256-OFB-CTR-logistic map.

Interferogram	SHA-256 hash function
Input Interferogram	Imprint of the original interferogram
	0834573041a9af10970bf1dd3f3085f0ddd350799f15b77eb283520cb7a37fd9
	Imprint of the Interferogram deciphered
	0834573041a9af10970bf1dd3f3085f0ddd350799f15b77eb283520cb7a37fd9

The results presented in Table 8 reveal that the fingerprint values of the interferogram before encryption and after decryption are identical. This indicates that the interferogram retrieved after the decryption phase matches the original interferogram, thereby demonstrating that the data integrity and authenticity criteria are satisfied and are ensured by the cryptosystem shown in Figure 1.

4. Conclusion

This work proposes a cryptosystem for securing interferograms from an inSAR system, a form of satellite imagery. The interferogram is encrypted and decrypted using a system combining the AES-256 algorithm with two modes AES-256-OFB and AES-256-CTR with a GEFFE key generator and a logistic map.

Various evaluation methods were used to assess the quality of the encrypted and decrypted interferograms. Given that subjective evaluation can be impractical, time-consuming, and costly, we opted for an objective approach. This method assesses degradation through metrics such as MSE and PSNR, with PSNR being a widely recognized standard for image quality assessment in image processing. While PSNR is an objective metric, it can sometimes require subjective interpretation of the degradation.

Additionally, we employed other evaluation techniques that better reflect human perception, such as SSIM. The study is based on the premise that the human visual system is significantly influenced by the structural details in a scene.

Therefore, the focus is on measuring the structural degradation between the original and degraded images. Additionally, other methods such as statistical analysis, including histogram and entropy analysis of the encrypted interferograms, were employed.

The results show that encrypting the inSAR system's interferogram using both AES-256-OFB and AES-256-CTR modes, combined with the chaotic Logistic map, significantly improves security. The encryption process consists of three steps: the encryption and decryption of an InSAR system interferogram using AES-256-OFB, AES-256-CTR with two keys generated by a GEFFE generator, and finally, using a chaotic logistic map with predefined initial parameters as keys. The cryptosystem demonstrates excellent performance, maintaining high quality in the decrypted interferogram compared to the original and exhibiting overall effective encryption quality.

5. References

[1]. E. Bensikaddour, “Développement d'un cryptosystème basé sur le standard AES et la théorie du chaos pour le chiffrement des images satellitaires à bord d'un satellite d'observation de la terre,” Doctoral Thesis in Sciences, Communication Networks Architecture and Multimedia Laboratory (RCAM), Djillali Linkable University of Sidi Bel Abbes, pp 11-37, Algeria, 2019.

[2]. FE. A.El-Samie, HEH. Ahmed, IF. Elashry, MH. Shahieen, OS. Faragallah, and ESM. El-Rabaie, “ Image encryption : a communication perspective,” CRC PressTaylor & Francis, 2014.

[3]. R. Saidi, N. Cherrid, T. Bentahar, and A.Bentahar, “Evaluation of The Encryption Quality of an Insar Interferogram by a Crypto System Based on Two AES-256 and RSA Algorithms with Modes CTR and OFB,” *International Journal of Multimedia and Ubiquitous Engineering (IJMUE)*, vol.15, nº.2, pp.1-14, 2020 http://dx.doi.org/10.21742/ijmue.2020.15.2.01.

[4]. M.S. Bernardi, P.C. Africa, C. Falco and L. Formaggia, A. Menafoglio, S.Vantini, “On the Use of Interferometric Synthetic Aperture Radar Data for Monitoring and Forecasting Natural Hazards,” *Springer Mathematical Geosciences*, vol. 53, pp.1781–1812, 2021doi.org/10.1007/s11004-021-09948-8.

[5]. L Zhou, D Chai, Y Xia, P Ma, and H Lin, “Interferometric Synthetic Aperture Radar Phase Unwrapping,” *IEEE geoscience and remote sensing magazine*, vol. 9, iss. 2, pp. 10 – 28, 2021, doi: 10.1109/MGRS.2021.3065811.

[6]. H. Yu, Y. Lan, Z. Yuan, J. Xu, and H. Lee, “A Review on Phase Unwrapping in InSAR Signal Processing,” *IEEE Geoscience and Remote Sensing Magazine*, pp. 40-58, 2019, doi: 10.1109/MGRS.2018.2873644.

[7]. K. H. Brown, P.J. Bond, and D.L. Evans, “Advanced Encryption Standard (AES) ,” National Institute of Standards and Technology, Federal Information Processing Standards Publication (FIPS 197), US Department of Commerce, Updated: May 9, 2023, doi.org/10.6028/NIST.FIPS.197-upd1.

[8]. A. Bouadjemi, “Sécurité Informatique,” Course handout, University of Relizane Faculty of Sciences and Technologies Department of Computer Science, 2023, Algeria.

[9]. Din, M., Pal, S.K., Muttoo, S.K. (2019). Applying PSO Based Technique for Analysis of Geffe Generator Cryptosystem. In: Yadav, N., Yadav, A., Bansal, J., Deep, K., Kim, J. (eds) Harmony Search and Nature Inspired Optimization Algorithms. Advances in Intelligent Systems and Computing, vol 741. Springer, Singapore. https://doi.org/10.1007/978-981-13-0761-4_71

[10]. Space Data link security protocol Consultative Committee for Space Data Systems CCSDS. "Security Architecture For Space Data Systems," Informational Report CCSDS 351.0-M-1, Magenta Book, NASA, Washington, D.C., October.2012.

[11]. B. Schneider, "Applied cryptography," John Wiley & Sons, Inc, united states of America: CRC press, 1996, pp 780.

[12]. M. Mohammed, and B. Boukhatem, "Application des techniques de cryptage pour la transmission sécurisée d'images MSG," Computer engineering department of electronics and faculty of electrical Mouloud mammeri university, Tizi-ouzou, 2015, Algeria.

[13]. J. Peng, M. You, Z. Yang, and S. Jin, "Research on a block encryption cipher based on chaotic dynamical system," *IEEE Third International Conference* on, 2007.

[14]. European Union Agency for Network and Information Security, "Algorithms, key size and parameters report 2014," November 2014.

[15]. K.benammar, R.Saidi, T.Bentaher, H.Djallab, Nada Cherrid, and Yacine Belhocine, "Comparison of CTR-OFB Modes for AES-256- based InSAR Interferogram Encryption with a GEFFE Key Generator," *The 6th International Conference on Pattern Analysis and Intelligent Systems* (pais24), 2024.

[16]. M. Naim, and A. Pacha, "A new chaotic image encryption algorithm based on a modified version of the AES algorithm," Multimedia Tools and Applications, 10 July 2024, https://doi.org/10.1007/s11042-024-19842-0.

[17]. S.R.M.Halagowda, and S. K. Lakshminarayana, "Image Encryption Method based on Hybrid Fractal-Chaos Algorithm," *International Journal of Intelligent Engineering and Systems*, vol.10, nº.6, 2017, doi: 10.22266/ijies2017.1231.24.

[18]. K. Benamara, R. Saidi, T. Bentahar, H. Djellab, and N. Cherrid, "Technique for Securing Insar Interferograms using Cryptography," *International Journal on Electrical Engineering and Informatics*, vol. 16, n^0 .2, June 2024, doi: 10.15676/ijeei.2024.16.2.9

[19]. S.Hraoui, F.Gmira, A.W.Jarar, K.Satori, and A.Saaidi, "Etude comparative de deux cryptosystèmes: L'AES versus l'attracteur Chaotique," Mediterranean Telecommunication Journal, vol. 3, n0.2, july 2013.

[20]. B. Prakash, and V. Gupta, "An Improved Unified AES Implementation Using FPGA," International Journal of Embedded and Real-Time Communication Systems, vol 13, issue1, pp.1-12, 1 Jan 2022, doi.org/10.4018/IJERTCS.302110.

[21]. Y. Bentoutoua, E. Bensikaddoura, N. Talebb, and N. Bounouab, "An improved image encryption algorithm for satellite applications," Advances in Space Research, vol. 66, iss. 1, pp. 176-192, 2020, doi.org/10.1016/j.asr.2019.09.027.

[22]. J.G. Dumas, JL. Roch, É. Tannier, and S. Varrette, "Théorie des Codes compression, cryptage, correction," Dunod, ISBN 9-78-210-050692-7, 2007, pp. 39-41.

[23]. L. Xu, X. Gou, Z. Li, and J. LiA, "Novel chaotic image encryption algorithm using block scrambling and dynamic index-based diffusion," Optics and Lasers in Engineering, vol .91, pp. 41-5291, April 2017, doi: https://doi.org/10.1016/j.optlaseng.2016.10.012.

[24]. D. Zareai, M. Balafar, and F. Derakhshi, "EGPIECLMAC: efficient grayscale privacy image encryption with chaos logistics maps and Arnold Cat," Evolving Systems, vol.14, pp. 993–1023, 2023, Iran, doi: https://doi.org/10.1007/s12530-022-09482-w.

[25]. A. T. Azar, A.G. Radwan and S.Vaidyanathan, "Mathematical Techniques of Fractional Order Systems," Elsevier, Book 2018, DOI: https://doi.org/10.1016/C2016-0-05031-3.

[26]. M. Asif, J. Kiddy, K. Asamoah, M. M. Hazzazi, A. R. Alharbi, M. U Ashraf, A. M. Alghamdi, "A Novel Image Encryption Technique Based on Cyclic Codes over Galois Field," *Computational Intelligence and Neuroscience*, vol.2022, 2022, doi.org/10.1155/2022/1912603.

[27]. P. Patila, P. Narayankarb, D G. Narayan, and S M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *International Conference on Information Security & Privacy (ICISP2015)*, 2015, pp. 11-12, Nagpur, India.

[28]. N. Songose Awarayi, O. Appiah, B. jamin Asubam Weyori, and C. B. Ninfaakang, "A Digital Image Watermarking Using Dwt and L-shaped Tromino Fractal Encryption», *International Journal of Image*," Graphics and Signal Processing (IJIGSP) , vol. 13, no. 3, pp.33-43, 2021, doi: https://doi.org/10.5815/ijigsp.2021.03.03 .

[29]. S. M. Serag Eldin, A.Abd. El-latif, S. Chelloug, M.Ahmad, A. Eldeeb, T. Diab, W. Sobky, and H. N.Zaky, "Design and Analysis of New Version of Cryptographic Hash Function Based on Improved Chaotic Maps With Induced DNA Sequences," *IEEE acess*, vol. 11, pp. 101694- 101709, 2023, doi: 10.1109/ACCESS.2023.3298545.

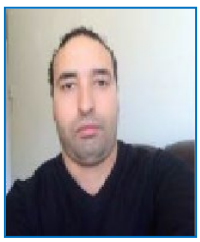
[30]. Z. Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli, "Image quality asssessment: From error measurement to structural similarity," *IEEE Trans. Image Processing*, vol. 13, no.4, , pp.600- 612, Apr .2004, DOI: 10.1109/TIP.2003.819861.

[31]. R. Saidi, T. Bentahar, N. Cherrid, A.Bentahar and H.Mayache, "Evaluation and Analysis of Interferograms from an InSAR Radar En-crypted by an AES-Based Cryptosystem with The Five Encryption Modes," *International Journal on Electrical Engineering and Informatics*, vol. 12, No. 4, December 2020, doi: 10.15676/ijeei.2020.12.4.13

Karim Ben Amara, born on 27/09/1989 in Khenchela, Algeria, is currently a doctoral student in telecommunications at Elchahid El-Arbi El-Tebessi University in Tebessa, Algeria. He obtained his baccalaureate in 2008 from Elchahid Othmani Ibrahim High School in the municipality of Kais, Khenchela province. Subsequently, he pursued his studies at Elchahid Abbas Laghrour University in Khenchela, where he obtained his bachelor's degree in 2011. In 2020, Karim joined the second cycle at Elchahid Hama Lakhdar University in El Oued, where he obtained his master's degree in 2022. In 2023, he successfully passed an admission competition for the third cycle of the LMD system.

Riad SAIDI was born in Khenchela, Algeria, in 1973. He received the option engineering control in 1997 from the electronics institute of the University of Batna, Algeria. He had the communication magister of the electrical engineering department of Mohamed Kidder University of Biskra in 2010. He received the Ph.D. degree in communications from the Mostapha Benboulaid Batna-2 University, Algeria (2018). He was a Research Associate at the Annaba Industrial Technology Research Unit of the welding and control center in Cheragua Alger, Algeria for two and a half years from 2011 to December 2013 as a Sensor Team Leader. Currently, he is a teacher-researcher in the common base department, faculty of technology at the University of Batna 2. He is a member of a research team, in the laboratory in the L3S laboratory of University Echahid Cheikh Larbi Tebessi Tebessa, road of constantine, 12002 *Tébessa*, Algeria. His interests include telecommunications, mobile phone systems, as well as cryptography and network security.

CHERRID Nada was born in Batna, Algeria, she worked on early auditory evoked potentials, received his Engineering Master degree from the electronics institute of the University of Batna, Algeria., in 1998 and the Ph.D. degree from Paris-Est Créteil Val de Marne (UPEC) University, Paris 12, France, in 2005. Currently, she is teacher researcher at the Electronics department, Mostapha Benboulaid Batna-2 University – Algeria.



Tarek BENENTAHAR was born in Batna, Algeria, in 1980. He received his telecommunication engineer diploma in 2004, magister degree in 2008, and Ph.D degree in 2017 from the University of Batna. He was a Lecturer in science and technological engineering department at Batna University from 2007 to 2010. He joined Bell Canada Corporation-Montreal in 2010 to 2011. Currently, he is a teacher-researcher at the Larbi Tébessi University of Tébessa, in addition to the higher school of renewable energies, environment and sustainable development Batna. His area of interests includes: Telecommunication and network systems, Remote sensing, Radar, image and signal processing.

Hannane Djellab Associat professor in Telecommunications, responsible for Huawei ICT Academy Tebessa and member of LTI laboratory Guelma. Doctor in Telecommunications of Badji Mokhtar University of Annaba, and a HDR of Tebessa University. Magister in automation and control in 2007. Engineer in communication from Tebessa University. She joined the company Algerie telecoms as an engineer at the CA amplification centre in 2003. Held the position of BSS Remote and AOR from 2005 to 2011 at Mobilis. Recruited at the University of Khanchla as an associate professor and transferred in 2015 at Tebessa University. These research works are focused on optical transmission FSO, VLC, 5G, Wireless network.

Atef BENTAHAR was born in Batna, Algeria, in 1981. In 2016 he had his master degree in computer science from Larbi Tébessi University, He received the Ph.D. degree in in computer science, option: Intelligent Systems Networks. Tébessa University, Algeria in 2022. Currently, he is a teacher-researcher at Si El'Houès University Center -Barika-Batna, Department of Mathematics and Computer Science he is a Ph.D student affiliated to Laboratory of Mathematics, informatics and systems (LAMIS) at Larbi Tébessi University. His area of interests includes: image processing, machine learning, pattern recognition, biometric systems, cryptography & network security and IoT security.