Evaluation and Analysis of Interferograms from an InSAR Radar Encrypted by an AES-Based Cryptosystem with The Five Encryption Modes

Riad Saidi[1,2], Tarek Bentahar[1], Nada Cherrid[3], Atef Bentahar[4] and Hichem Mayache[5]

[1](LABGET) Laboratory, Larbi Tébessi Tébessa University, Tébessa-12000, Algeria
[2](LAAAS) Laboratory, Mostapha Benboulaid Batna-2 University, Batna- 05000, Algeria
[3]Electronic Department, Mostapha Benboulaid Batna-2 University, Batna- 05000, Algeria
[4] (LAMIS) Laboratory, Larbi Tébessi Tébessa University, Tébessa-12000, Algeria
[5]Higher School of Industrial Technologies-Annaba, Annaba-23000, Algeria
riad.saidi@univ-tebessa.dz, tarek.bentahar@ univ-tebessa.dz , h.mayache@esti-annaba.dz,
n.cherrid@univ-batna2.dz, atefbentahar@gmail.com

Abstract: This paper falls within the framework of the security of satellite images, in particular interferograms from an Interferometric Synthetic Aperture Radar (inSAR) system. The innovation of this work consists in the application of a cryptosystem based on two algorithms Advanced Encryption Standard (AES) and the Rivest, Shamir and Adleman (RSA) encryption algorithm for securing interferograms of inSAR systems. AES employs five encryption modes Electronic Code Book (ECB), Cipher Bloc Chaining (CBC), Cipher FeedBack (CFB), Output FeedBack (OFB), and counter-mode encryption (CTR). The use of the AES algorithm alone can only ensure the confidentiality function. In the proposed cryptosystem confidentiality is ensured by the AES algorithm, authenticity is guaranteed by the RSA algorithm, and integrity is ensured by two parameters; the correlation function between the adjacent pixels and the SSIM parameters (structural similarity index SSIM). For evaluation and analysis of security performance for interferogram encryption, several test metrics are employed. These metrics are: Analysis of histograms of the encrypted interferograms, correlation between the adjacent pixels, between the original interferogram and the encrypted interferogram, SSIM between the original interferogram and the decrypted one. Moreover, we exploit the analysis of resistance to error propagation for the five modes.
The obtained results show a superiority of the OFB and CTR modes for the encryption of inSAR interferograms compared to ECB, CFB, and CBC modes. It is noteworthy, that the main criteria that can be used to choose between OFB and CTR for encryption of satellite images are propagation of errors and the complexity material for their locations on the edges of the satellites propagation of errors and the complexity material for their locations on the edges of the satellites. OFB mode is employed in satellites to minimize the number of on-board circuits, which is decisive for satellites. CTR mode is recommended by the CCSDS (Consultative Committee for Space Data Systems) for telemetry (TM) and remote control (TC) encryption.

Keywords: Cryptography; Encryption mode (ECB, CBC, CFB, OFB, CTR); Interferograms inSAR; Symmetric encryption; AES; RSA; SSIM.

1. Introduction

Satellite images have become an essential tool for several fields [1]. Images must be secured against unauthorized access (confidentiality), protected against unauthorized changes (integrity), and available to an authorized entity when necessary (Authentication) [2]. The images used are interferograms from the inSAR system. Interferometric synthetic aperture radar (InSAR) is one of the radar imaging systems [3]. It is an active system comparing to the optical one by dint of its light-independent scan. According to the backscattered signal from different imaged points, inSAR can provide two images: magnitude and phase (commonly called interferogram [4]. InSAR interferogram is the only useful data for surface change monitoring and surface digital elevation model. But this valuable data is not directly used, phase unwrapping process

Received: March 7th, 2020. Accepted: December 3rd, 2020
DOI: 10.15676/ijeei.2020.12.4.13

[5] must be performed due to the wrapping measurement of such system. Indeed, all interferogram phases are wrapped into [–π, +π] and to recover the true phase value, the real cycle number to be added must be correctly found. For a noise-free interferogram, the phase unwrapping is a simple integration in the wrapped space. In reality, all interferograms are subject to a particular noise called residues. To avoid error propagation in a noisy interferogram, the phase unwrapping has to be residue-immune. For this aim, several single-baseline phase unwrapping algorithms have been proposed in two main categories: path-following and optimization-based methods. Among the skillful methods, we find Constantini's algorithm [6] of optimization-based group. Constantini's algorithm provides a high quality and accuracy of the unwrapped image with an acceptable running time.

Throughout history, mankind has tried to send information securely. Information encryption has been used as a security tool for military strategies and the exchange of secret data. Secure information transfer is necessary and widely used in the digital world. Digital networks have evolved considerably in recent years and have become inevitable for modern communication. The interferograms transmitted on these networks are specific data because of their large amount of information. The transmission of these requires us to meet the three basic criteria of security which are confidentiality, authentication and data integrity.

To meet these requirements, several encryption techniques are proposed; the symmetric public algorithm AES (Advanced Encryption Standard) [7] which has proven its robustness against different types of attacks nowadays, the asymmetric RSA algorithm (Rivest, Shamir and Adleman) [8], and the International Data Encryption Algorithm (IDEA) [9]. But if we apply these algorithms separately for the transmission of images or data, they can only ensure confidentiality, for this we offer a hybrid encryption cryptosystem based on the two algorithms AES and RSA to ensure the three main axes of security: confidentiality, authenticity, integrity. To ensure confidentiality in this cryptosystem, among the site algorithms, our choice fell on the AES algorithm with its five operating modes [10], given its low consumption of memory space, less complicated, plus easy to implement, very fast and it hasn't broken until today.

Knowing that, some satellite uses the 3-DES algorithm to encrypt images, whereas in our cryptosystem we use the AES which is the successor to DES [11], for encryption not of images but of interferograms.

We have used RSA to ensure secure exchange of keys and satisfy authentication, as it is very fast and very secure. Our cryptosystem also includes a procedure based on the correlation between the pixels neighboring the interferograms and the calculation of the structural similarity index SSIM between the original interferogram which is the reference and the one deciphered to ensure integrity. Although there are many encryption algorithms available, the use of encryption technology in spacecraft lags far behind terrestrial systems [12]. It is difficult to establish a precise state of the art on the encryption methods used on board satellites since most of the manufacturers and owners of satellites do not share this type of information, in particular the encryption of interferograms. While, some document cites the encryption algorithms used in some space missions [13]. But also, it is important to remember that AES is the algorithm recommended by the CCSDS (Consultative Committee for Space Data Systems) for the encryption of data for civil space missions.

2. The Algorithms Used

In this work we have used two encryption algorithms, one symmetrical which is AES, the other asymmetrical which is RSA.

A. AES main algorithm

The Advanced Encryption Standard (AES) is the standard approved by the National Institute of Standards and Technology (NIST) for symmetric data encryption [14]. AES is widely used due to its simplicity, flexibility and ease of implementation. It is implemented, in Software or in Hardware, on a wide variety of applications.

In addition, AES is the only standard recommended by the CCSDS for encrypting data on board satellites [15]. In this work, the transmitter and the receiver use the same key for encryption and decryption. The AES algorithm has an iterative structure that processes 128-bit data blocks using 128-bit cryptographic keys, 192 or 256 bits [16]. The number of iterations is determined by the size of the key used. For the three key sizes of 128, 196 and 256 bits, a number of 10, 12 and 14 turns are required, respectively. The design of the AES algorithm is based on the concept of substitution-permutation network in which the bytes of the plaintext message are substituted and swapped each turn through four operations (transformations) called SubBytes, ShiftRows, MixColumns and AddRoundKey [17]. The AddRoundKey transformation is the point where the secret key enters the encryption process and contributes to the end result. These four operations are repeated each round except in the last round which does not use the Mix-Columns transformation. Decryption is simply the reverse operation of encryption because the four transformations are reversible. Figure 1 shows the general structure of the AES algorithm [18].

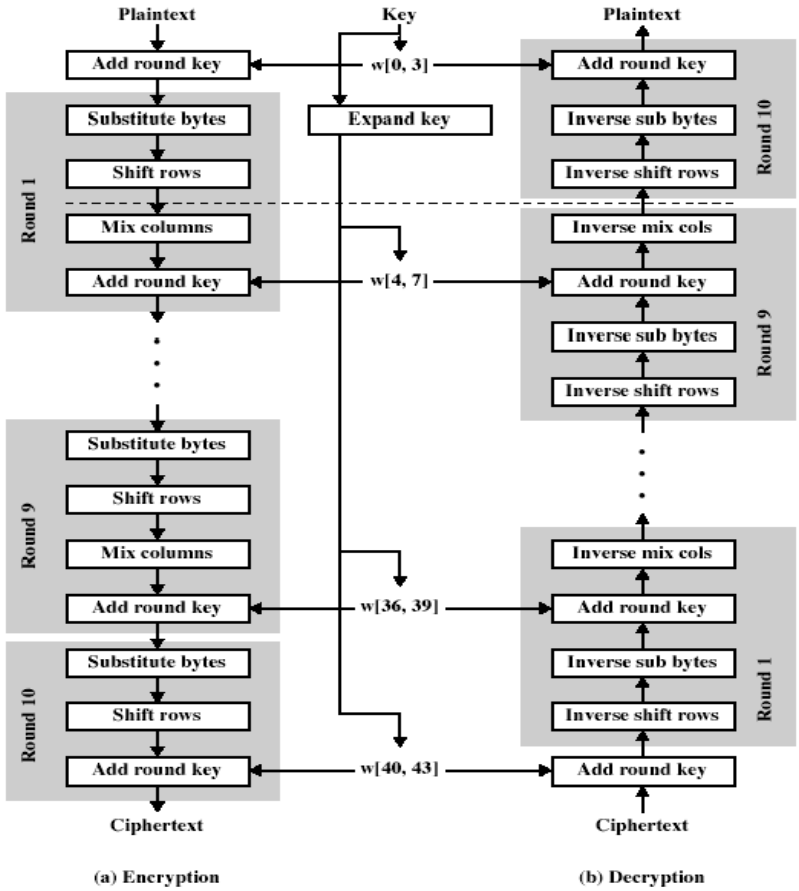


Figure 1. AES algorithm [17]

This algorithm can be combined with a series of modes to reinforce security without penalizing its efficiency. This combination is called encryption mode, several encryption modes exist which are:

1. Electronic Code Book (ECB)
2. Cipher Block Chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)

5. CounTeR (CTR)

These are encryption modes (ECB, CBC, CFB, OFB and CTR mode) [19], ensures confidentiality the last three modes (CFB, OFB and CTR) are similar to encryption by streams. They generate a flow of pseudo-random numbers which depends or not on the clear message [20].

B. RSA algorithm

The RSA algorithm (named by the initials of its three inventors: Ronald Rivest, Adi Shamir and Leonard Adleman) is an asymmetric encryption algorithm, widely used in e-commerce, and more generally to exchange confidential data on the Internet. In our cryptosystem that we have designed, this algorithm is used to secure the exchange of keys, and to ensure the authentication function [21].

3. The encryption modes used by AES

In this work, it's fashion will allow us to meet the criterion of confidentiality of transmission.

A. ECB mode

In ECB mode Figure 2, the encryption is applied directly and independently to each block of the clear message. The resulting sequence of output blocks is the encrypted message [21].

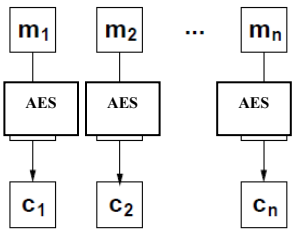


Figure 2. ECB block encryptions mode [21]

B. CBC mode

CBC mode, represented by Figure 3, is the mode in which the clear message blocks, before being encrypted, is xored with the previously encrypted blocks, an initial vector C_0 must be used to initialize the process. It replaces the first block which has not yet been defined. The initial vector C_0 which is noted IV on Fig .3, does not need to be kept secret but must be a nonce, a value which is never repeated with the same encryption key [22].

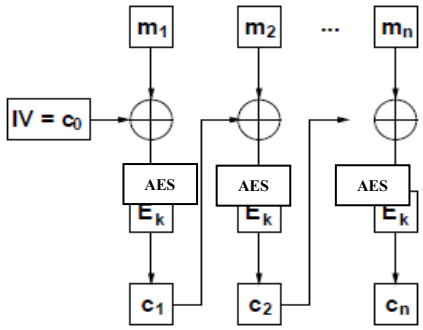


Figure 3. CBC block encryptions mode [21]

C. CFB mode

In this mode, which is illustrated by the Figure 4, an initial vector C_0 is used to start the encryption process and generate the first encrypted block, the latter is used as an input to en-

crypt the second block of the clear message. The process repeats sequentially until the last block [23]. The conditions applied on the IV are the same as those detailed in the CBC mode CBC mode.

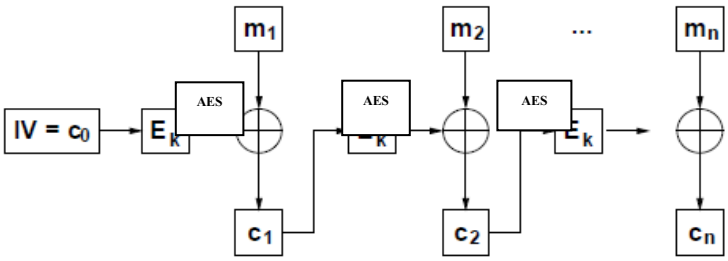


Figure 4. CFB block encryptions mode [21]

D. OFB mode

In this mode Figure 5, an initial vector C_0 is initially encrypted to start the process, the key flow at the output of this block will be reinjected at input to calculate the next key flow.

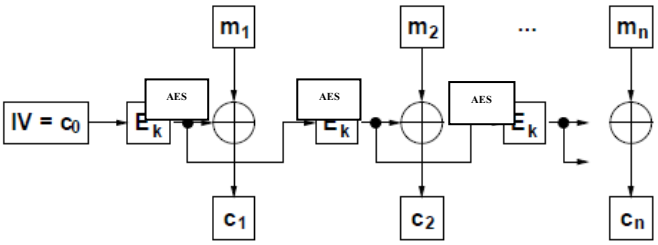


Figure 5. OFB block encryptions mode [21]

Using this mode, the preprocessing of the key flow is possible because it does not depend on a clear message.

E. CTR mode

This mode is simple, it creates a flow of pseudo-random numbers independent of the plain text. The Figure 6 shows the counter mode (CTR). In this mode, the key flow is obtained by encrypting successive values of a counter (T) which is then exorited with a block of the message in clear to generate a block of the encrypted message [24].

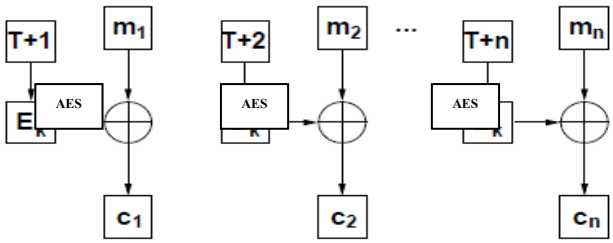


Figure 6. CTR block encryptions mode [21]

The counter values used with an encryption key must be nonce, because the key flow must never be repeated. In this mode, unlike the others, there is no feedback or sequential processing of the blocks. Consequently, it is possible to perform several ciphers in parallel, a significant advantage in high performance applications [25]. This mode is recommended by the CCSDS (Consultative Committee for Space Data Systems) for the encryption of remote measurements (TM) and remote controls (TC) [15].

4. Related works

In this section, a description of the cryptosystem used for the encryption of interferograms is presented. The proposed cryptosystem is a hybrid encryption of two algorithms AES and RSA using the five modes (ECB, CBC, CFB, OFB, and CTR). This cryptosystem aims to secure the inSAR interferograms transmitted between two blocks. One for Transmission and the other for reception, through a transmission channel as illustrated in Figure 7.

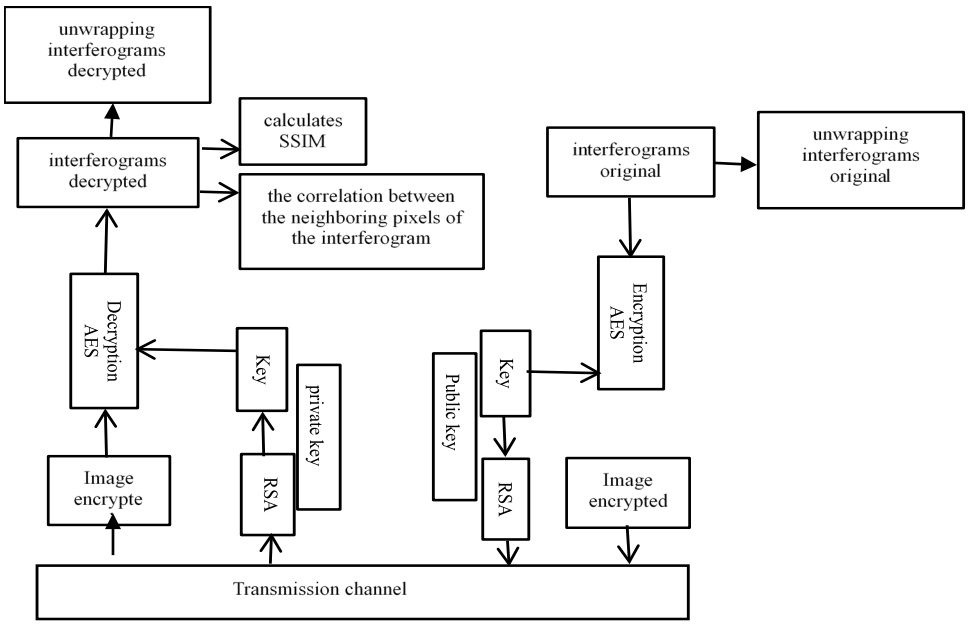


Figure 7. Cryptosystem for interferogram transmission

5. The proposed cryptosystem

In this section, we will give an explanation to the proposed cryptosystem, it is composed of two blocks:

A. Transmission block

The transmission consists of three main stages in the following order:

1. The original interferogram before its encryption, must be unrolled for a possible comparison on reception as shown in fig. 7.
2. After step one, the original interferogram switches to encryption with AES using one of the five modes each time (ECB, CBC, CFB, OFB and CTR mode).
3. After step two, the key used for encrypting the original interferogram with AES is in turn encrypted with the RSA algorithm with a public key, and transmitted in parallel with the interferogram to the receiving blocks.

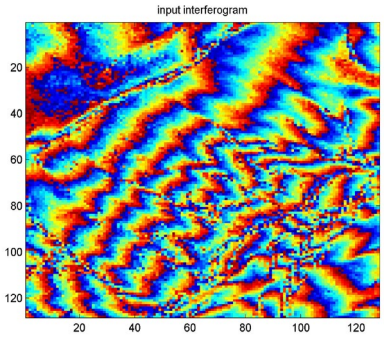
B. Reception block

On receipt of the reverse functions are performed for the reconstruction of the original interferogram transmitted, following this order:

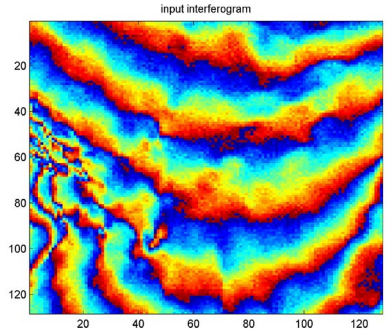
1. On reception, the key encrypted with RSA in the transmission block will be decrypted with the RSA algorithm with a private key.
2. After step one, the encrypted interferogram in the transmission block will be decrypted by the AES each time using one of the five modes (ECB, CBC, CFB, OFB and CTR mode) as shown in fig.7.

3. After step two, the interferogram decrypted for integrity verification proceeds to the following steps:
   - Calculation of SSIM between deciphered interferogram and original interferogram
   - Calculation the correlation of adjacent pixels.
   - The decrypted interferogram is unwound for examination with that from the unwinding operation performed on the original interferogram at the start of the transmission block. For verification of integration as shown in figure. 7

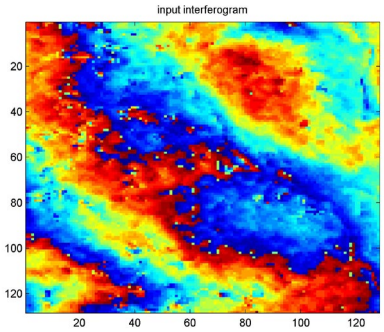
6. Results and analysis



(a).



(b)



(c).

Figure 8(a). interferogram1 (int1) (b). interferogram 2 (int2)
(c) interferogram 3 (int3)

The simulation and performance analysis of the various operating modes of the AES were carried out with a 2.53 GHz Pentium I-5 PC with Windows 7 and 4 GB of RAM. The software used is Matlab.

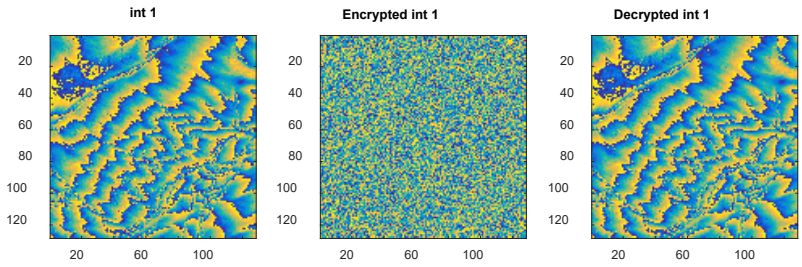
Three interferograms from the inSAR system with different information and from different geographic regions which are indicated by the Table 1, were used to assess their qualities after encryption and decryption as well as security performance, using AES, using different modes.

Table 1. Characteristics of interferograms

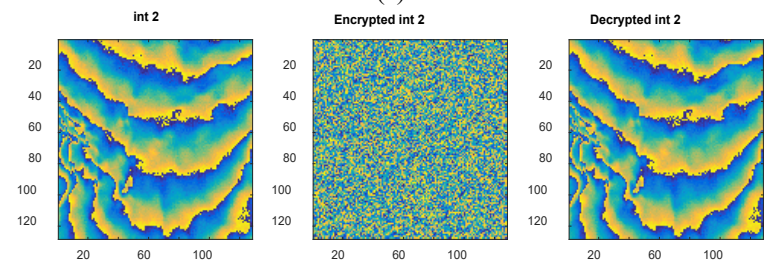
	Imaged region	Taken on	Orbit	Baseline(m)	Residues rate (%)
Int1	Sardinia	Aug2, 1991	241	126	0,0621
Int2	Chilcotin	Apr 11, 1995	Not provided	42	0,0151
Int3	Vatnajökull	Dec 31, 1995	23315	Not provided	0,0112

In this part we will present the results of the encryption of the three illustrated interferograms by the Figure 8 for the CTR mode as an example, illustrated by Figure 9, since the figures that represent encryption and decryption with the four encryption modes (ECB, CBC, CFB, OFB) remain the same, gold their analyzes which shows the difference between the five modes.

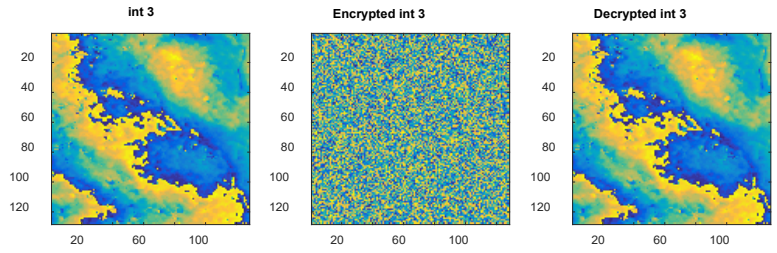
A. Encryption with CTR mode:



(a).



(b).

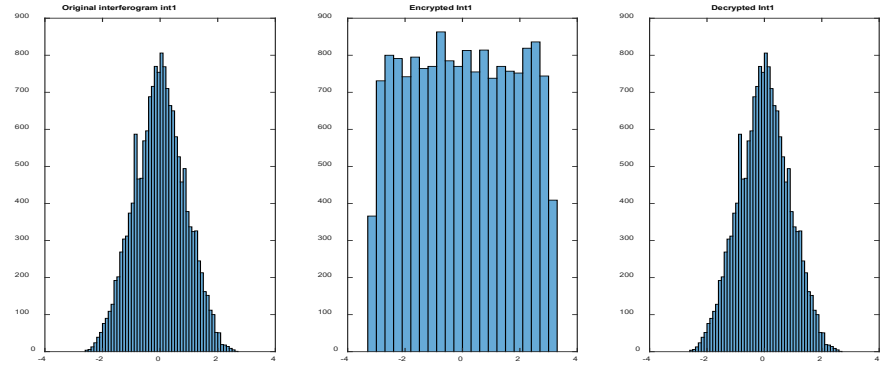


(c).

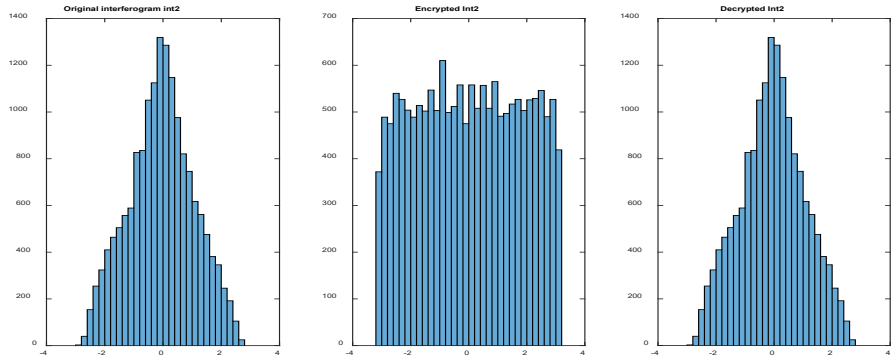
Figure 9. Encryption and decryption results of the three interferograms in CTR mode, a) interférogramme1 (int 1), b) interférogramme2 (int2), c) interférogramme3 (int3)

We have Figure 9, which represent the encryption and decryption results of the three interferograms with CTR mode, through the cryptosystem of figure 7.

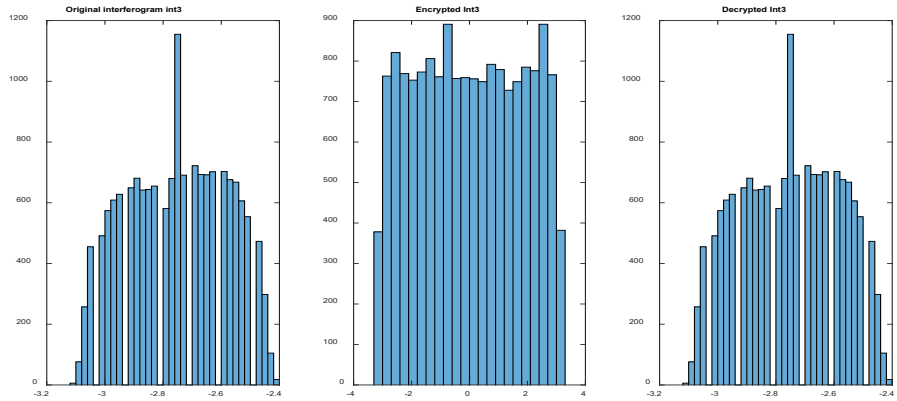
B. Evaluation criteria



(a).



(b).



(c).

Figure 10. Histogram of the three interferograms with AES -ECB, (a) Histogram of the interferogram int 1, (b) Histogram of the interferogram int 2, (c) Histogram of the interferogram int 3.

Among these are five encryption modes, there is no universal powerful mode for any type of application. The analysis by a simple visual inspection of the results obtained from the encryption remains insufficient to judge the effectiveness and quality of the deciphered interferograms, and the robustness of the encryption mode, as well as the constraints applied and the resources available which determine the most suitable mode for this type of image which are

(interferograms). Two main stages are used in this work for the evaluation and analysis of the results which are:

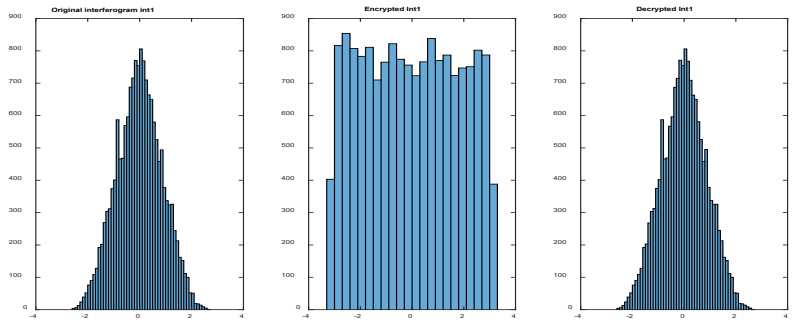
1. Security performances for the encryption of interferograms.
   a. Analysis of histograms,
   b. The correlation between the adjacent pixels, between the original interferogram and the encrypted interferogram,
   c. The calculation of SSIM to check the integrity.
2. Resistance against error propagation,

1. Security performance for interferogram encryption.

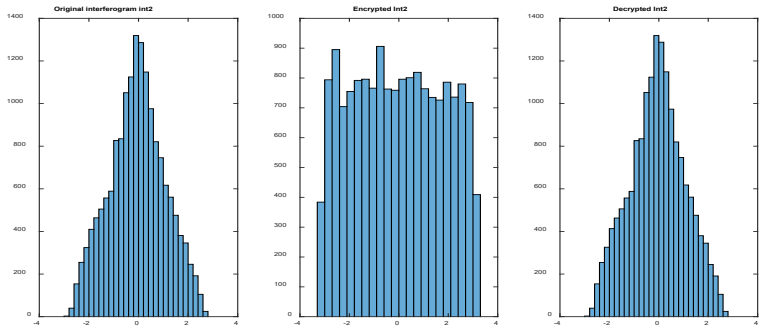
A. Analysis of histograms

The histogram of the encrypted interferogram must have two properties [2]:

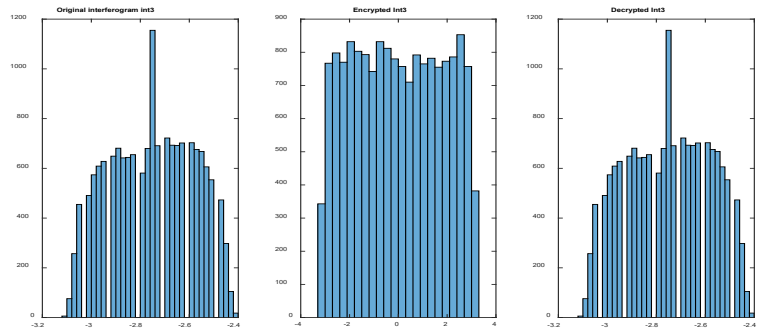
1. Must be completely different from the histogram of the original interferogram.
2. Must have a uniform distribution, which means that the probability of occurrence of any value is the same.



(a).



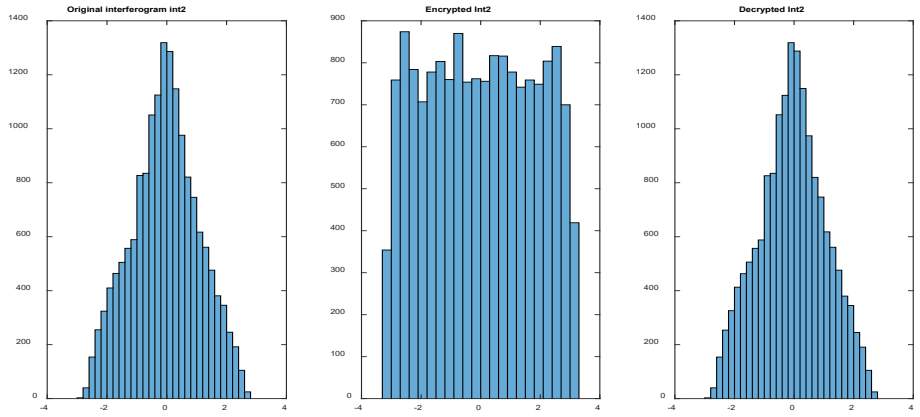
(b).



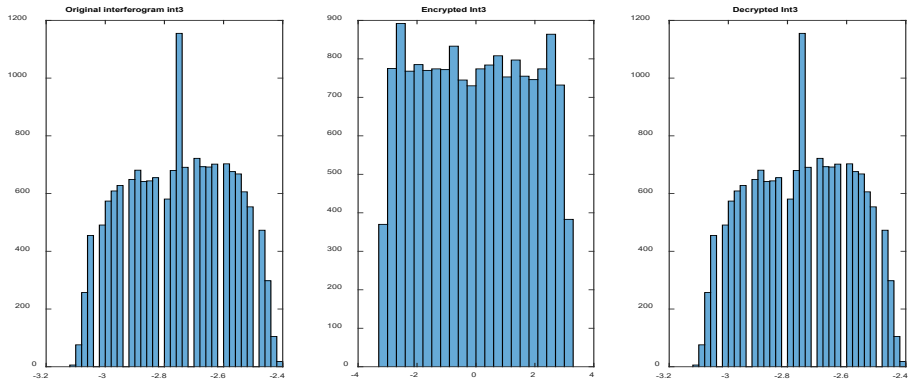
(c).

Figure 11. Histogram of the three interferograms with AES -CBC, (a) Histogram of the interferogram int 1, (b) Histogram of the interferogram int 2, (c) Histogram of the interferogram int 3

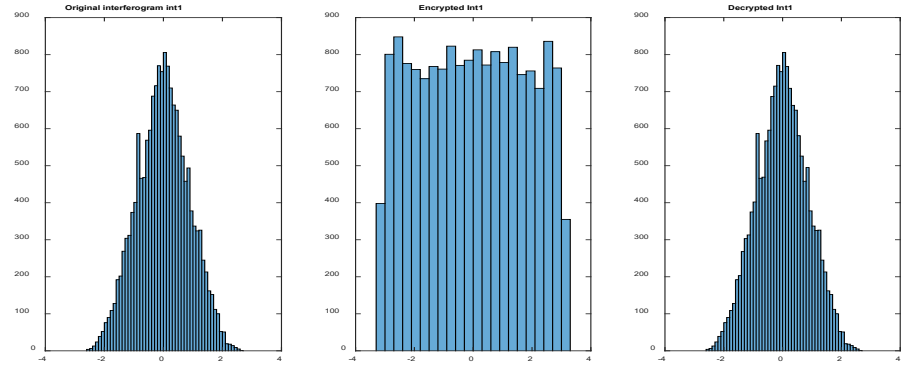
ed interferograms are completely different from the histograms of the original interferograms for the five modes (ECB, CBC, CFB, OFB and CTR). These tell us that they have a uniform distribution, which means that the probability of occurrence of any value is the same, since they have almost the same gray level compared to the histograms of the original or deciphered interferograms.



(a).

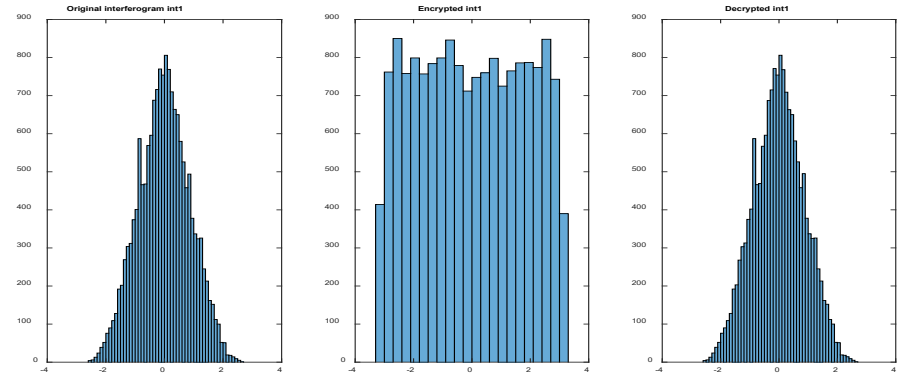


(b).

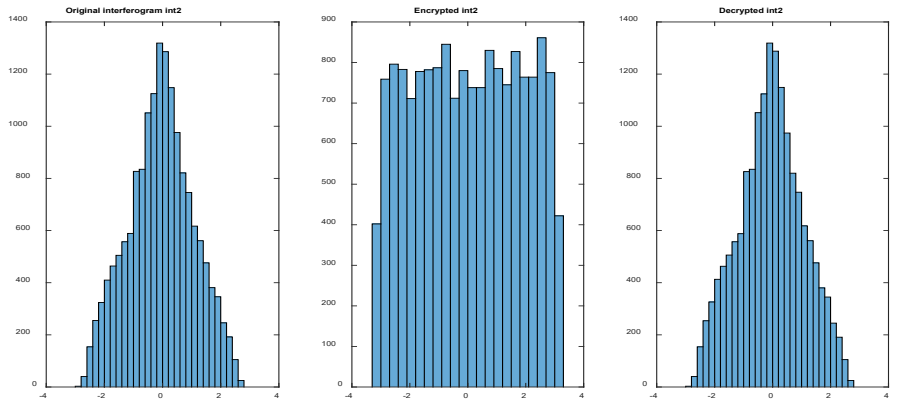


(c).

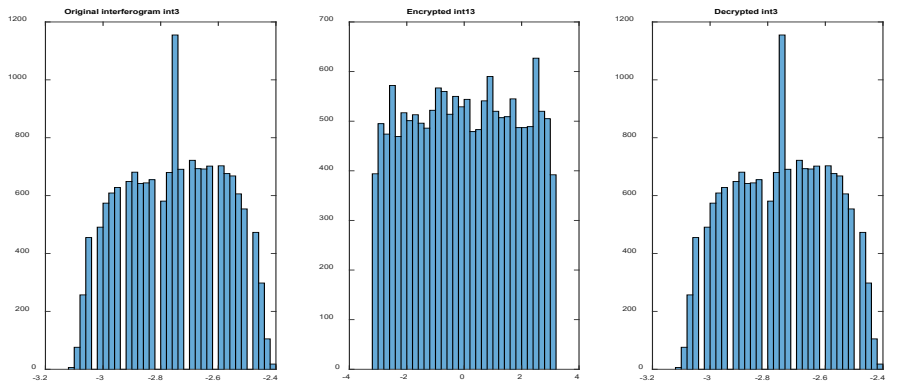
Figure 12. Histogram of the three interferograms with AES -CFB, (a) Histogram of the interferogram int 1, (b) Histogram of the interferogram int 2, (c) Histogram of the interferogram int 3



(a).

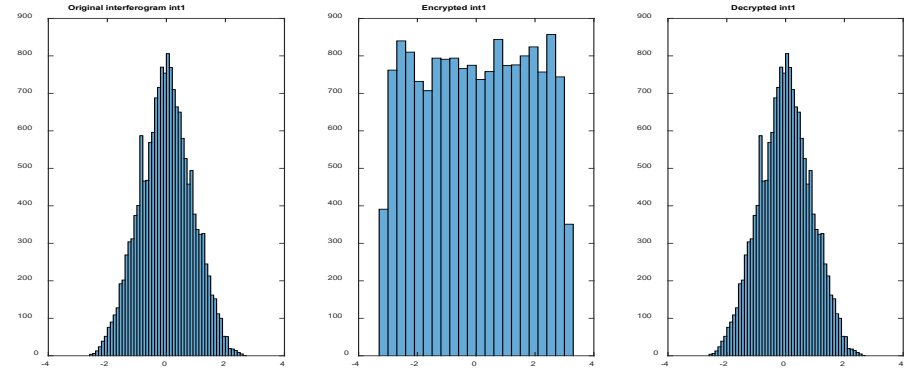


(b).

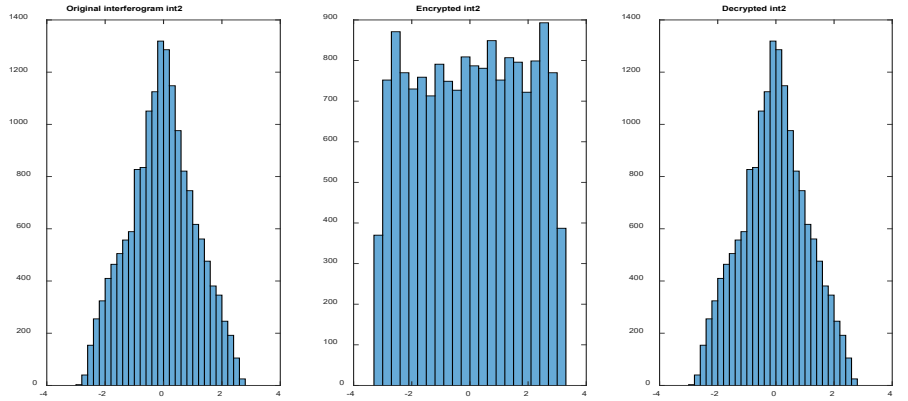


(c).

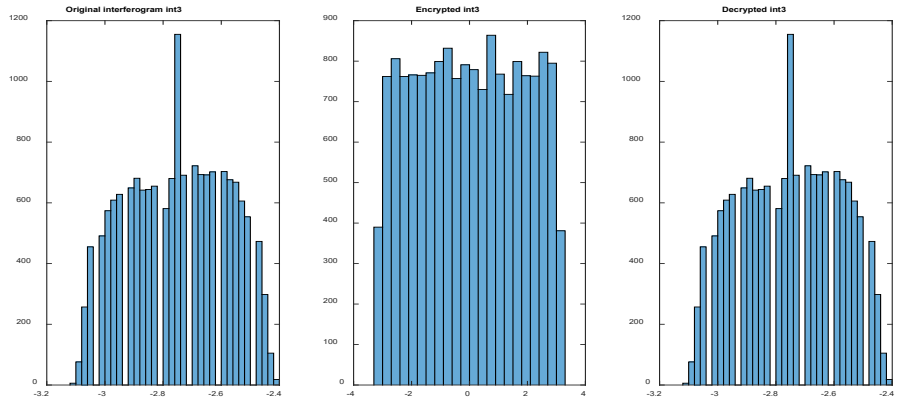
Figure 13. Histogram of the three interferograms with AES -OFB, (a) Histogram of the interferogram int 1, (b) Histogram of the interferogram int 2, (c) Histogram of the interferogram int 3.



(a).



(b).



(c).

Figure 14. Histogram of the three interferograms with AES -CTR, (a) Histogram of the interferogram int 1, (b) Histogram of the interferogram int 2, (c) Histogram of the interferogram int 3

B. Analysis of correlation coefficients

In this part we will see the correlation between original and encrypted interferogram.

1. *Correlation between the original interferogram and the encrypted interferogram [26-27]*

Usually in an image, a pixel is generally strongly correlated with its adjacent pixels in horizontal directions, vertical or diagonal. These high correlation properties can be quantified as a correlation coefficient for comparison. The correlation coefficient is calculated as follows:

$$r = \frac{cov(x,y)}{\sqrt{D(x)*D(y)}} \quad (1)$$

Where:

r: correlation coefficient.

x, y: pixel intensity values.

cov (*x, y*), *D*(*x*) and *D*(*y*) are calculated as follows:

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

$$cov(x) = \frac{1}{N}\sum_{i=1}^{N}(x(i) - E(x))(y(i) - E(x)) \quad (3)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x(i)) \quad (4)$$

The correlation coefficient *r* is expressed between -1 and +1, where:

r = -1: Means that the encrypted image is the reverse of the ordinary image,

-1 < *r* < 0: (Negative correlation) indicates a negative relationship between the pixels.

r = 0: Indicates no correlation between pixels.

0 < *r* ≤ 1: (Positive correlation) indicates a positive relationship between the pixels.

Table 2. Correlation coefficients of the adjacent pixels of the original and encrypted interferogram

Correlation coefficients of interferogram Int 1				
Horizontal				
ECB	CBC	CFB	OFB	CTR
0.0042	0.0059	0.0013	0.9993	-0.0041
Vertical				
ECB	CBC	CFB	OFB	CTR
0.0033	0.0054	0.0011	1	-0.0044
Diagonal				
ECB	CBC	CFB	OFB	CTR
0.1084	0.1095	-0.0667	0.9997	0.0781

Correlation coefficients of interferogram Int 2				
Horizontal				
ECB	CBC	CFB	OFB	CTR
0.0033	0.0067	0.0035	0.9986	-0.0018
Vertical				
ECB	CBC	CFB	OFB	CTR
0.0024	0.0070	0.0043	1	-0.0002
Diagonal				
ECB	CBC	CFB	OFB	CTR
-0.0509	0.075	-0.151	0.9999	-0.1149

Correlation coefficients of interferogram Int 3				
Horizontal				
ECB	CBC	CFB	OFB	CTR
0.0012	0.0032	0.0088	1	-0.0005
Vertical				

ECB	CBC	CFB	OFB	CTR
0.0013	0.0032	0.0087	1	-0.0005
Diagonal				
ECB	CBC	CFB	OFB	CTR
-0.0761	-0.0137	0.0816	1	-0.0386

The Table 2, inform us about the correlation coefficients of the adjacent pixels of the original and encrypted interferograms. It can be clearly seen that the encrypted interferograms obtained from different modes retain low correlation coefficients (positive correlation) in all directions, which confirms the integrity of the deciphered interferogram.

C. Analysis of the SSIM Structural Similarity Index

In this work, we have used the Structural Similarity index as a metric for the evaluation and measurement of the integrity of deciphered interferograms. SSIM is a method for measuring the similarity between two digital images, which is given by the Table 3.

The SSIM index can be considered as a measure of the quality of one of the compared images, to a reference image provided that the latter is considered of perfect quality. This is an improved version of the Universal Image Quality Index [28]. The idea of SSIM is to measure the similarity of structure between the two images. The underlying assumption is that the human eye is more sensitive to changes in the structure of the image [29], its optimal value is 1.

The SSIM metric is calculated on several windows of an image. The measurement between two windows *x* and *y* of size *N*x*N* is: [28]

$$SSIM(x,y) = l(x,y).c(x,y).s(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_x\sigma_y+c_2)(cov_{xy}+c_3)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)(\sigma_x\sigma_y+c_3)} \quad (5)$$

With

μ_x : *the average of x*

μ_y : *the average of y*

σ_x^2 : *the average of x*

σ_y^2 :*the variance of y*

cov_{xy}: *the covariance of x and y*

$$c_1 = (k_1L)^2, c_2 = (k_1L)^2 \; et \; c_3 = \frac{c_2}{2}$$

Are three variables intended to stabilize the division when the denominator is very low.

L: the dynamic range of pixel values, is 255 for images coded on 8 bits. k_1=0.01 and k_2=0.03 by default.

Table 3. Structural Similarity index

Interferograms	Structural similarity index				
	AES-ECB	AES-CBC	AES-CFB	AES-OFB	AES-CTR
Int1	0.9984	0.9986	0.9968	0.9968	1
Int2	1	0.9976	0.9976	0.9976	1
Int3	1	1	1	1	1

Table 3 shows the structural similarity index calculated by SSIM. The obtained results show that the similarity rates of the decrypted interferograms compared to those of the original interferograms are very close to the optimum value of the SSIM which 1 for all modes (ECB, CBC, CFB, OFB, and CTR). These results allow the satisfaction of the criterion of integrity of the interferograms decrypted compared to those of origin. Furthermore, SSIM values for the CTR mode are optimal and equal to 1, which confirms the reordering of the CCSDS (Consultative Committee for Space Data Systems) of this mode for the encryption of telemetry (TM) and remote controls (TC).

2. Resistance against error propagation

A single bit error occurring during the encryption process can spread and cause several errors in the encrypted data. In this part, we study the possibility of the propagation of an error for the different modes used with the AES.

The works of (R. Banu & Vladimirova) [29], in 2006 describes these sources of errors and estimates the amount of damage caused to the data after an encryption process by the different modes. The results observed, for each mode, which are summarized in the Table 4.

Table 4. Error propagation due to one-bit error during encryption and transmission

	Mode ECB	Mode CBC	Mode CFB	Mode OFB	Mode CTR
Amount of data affected during encryption	One block	One block	One block	Full data from the point where the fault occurred	One block
Quantity of data allocated during the transmission	One block	Two block	Two blocks	No propagation	No propagation

In all three modes ECB, OFB and CTR, the encrypted blocks are independent of each other. Therefore, if an encrypted block is affected during transmission, the error does not spread to other blocks. The error only affects the corresponding bits in the decrypted message. CTR mode is recommended by the CCSDS for the encryption of telemetry (TM) and remote controls (TC). OFB mode is exploited in satellites to minimize the number of on-board circuits, which is a decisive factor for satellites [21]. ECB mode is not suitable for image encryption in general. Since, images in general have often high redundancy. Therefore, if the blocks with the same content are encrypted in the same way, it can be detected as repeated blocks in the encrypted message. We performed a test to see the influence of error propagation, as indicated in red in the manuscript section (Resistance against error propagation). As an example, we will perform a pixel shift in the original interferogram, which is considered an error, and then encrypt the original interferogram with AES-CBC mode as an example.

For a pixel change in the original int1 interferogram. The following procedure was applied:

1. Encrypt the original interferogram (int 1) to generate the first encrypted interferogram (C1).
2. Change a pixel in int 1 to obtain a second original interferogram (int 2). int 1 and int 2 are the same with a difference of only one pixel, this pixel is chosen at the beginning, in the middle or at the end of the first block.
3. Encrypt the original interferogram (int 2) to generate the second encrypted interferogram (C2).
4. Finally, calculate the SSIM between the two interferograms (C1 and C2).
5. From figure 15, we can clearly see, if we consider that the pixel change is an error, see its influence and the propagation of the error from C1 to C2, through the difference that exists between the histogram of C1 and C2.

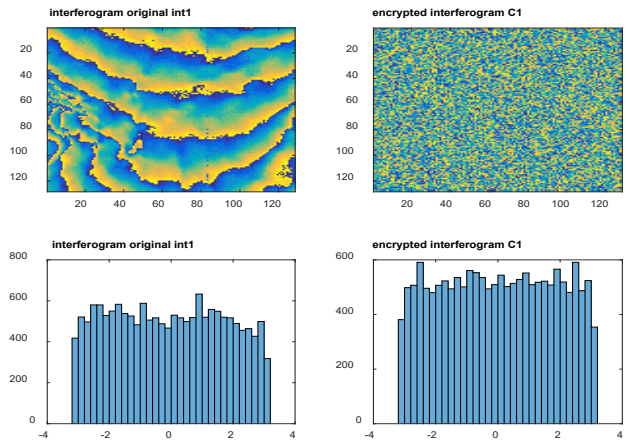


Figure 15. Encrypted interferogram and AES-CBC mode histogram,
(a) interferogram int1, (b) interferogram int2

According to the table. 5, the value of the SSIM informs us that the two interferograms (C1 and C2) are completely different which shows the error propagation, which will influence the quality of the deciphered interferogram.

Table 5. SSIM between original interferogram C1 and C2

SSIM between C1 and C2	AES-CBC
	0.6416

7. Unwinding operation deciphered interferograms and original interferograms

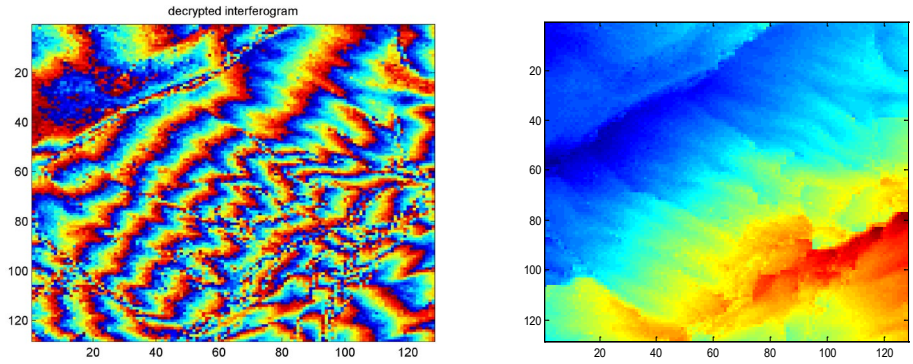
The interferograms after being deciphered will undergo an unwinding operation as shown in Figure 16.

We also calculated the SSIM between the images resulting from the unwinding of the original interferograms before encryption and those of the interferograms deciphered as indicated in Table 5.

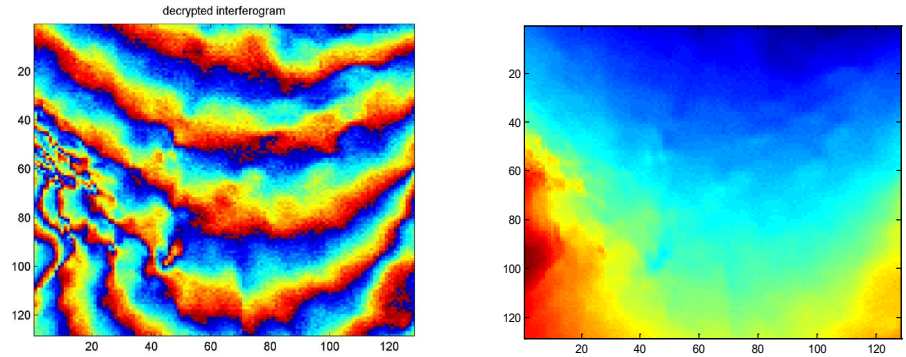
Table 5. Structural Similarity index interferogram takes place

Interferograms	Structural similarity index				
	AES-ECB	AES-CBC	AES-CFB	AES-OFB	AES-CTR
Int1	1	0.9973	0.9967	0.9746	1
Int2	1	0.9967	0.9967	0.9967	1
Int3	1	0.9986	0.9986	0.9986	1

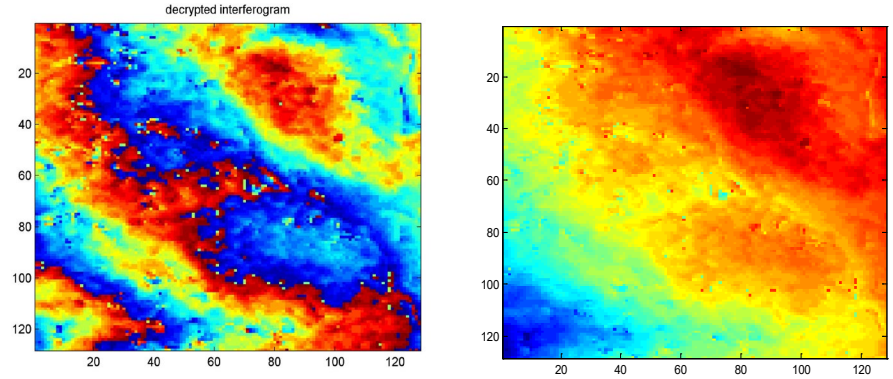
The above table shows clearly that the obtained values are very close to the optimal values. This demonstrates that the images of the interferograms unwound after decryption are identical to the images of the original interferograms before encryption. These results indicate that our proposed cryptosystem shows a high credibility in securing the interferograms of an inSAR system.



(a).



(b).



(c)

Figure 16. The three interferograms deciphered with their unrolled images, (a) original interferogram int1 after decryption and its unwound image, (b) original interferogram int 2 after decryption and its unwound image, (c) original interferogram int 1 after decryption and its unwound image

8. Discussion

After comparing the results of the encryption and decryption with the five encryption modes (ECB, CBC, CFB, OFB, CTR), the most favorable modes for the encryption of inSAR interferograms are OFB and CTR modes. First, on the basis of the results obtained after evaluations, which have been very satisfactory.

Second, on the basis that the main criteria that can be used to choose between these modes for inSAR interferogram encryption are the error propagation is as we have seen that in both OFB and CTR modes, the cipher blocks are independent of each other. others. Therefore, if an

encrypted block is assigned during transmission, the error does not propagate to other blocks. The error affects only the corresponding bits in the decrypted message, and the complexity of the hardware. Consequently, OFB mode is chosen for use in satellites since it allows us to reduce the number of on-board circuits. For CTR mode, it is recommended by the CCSDS for encryption of telemetry (TM) and remote controls (TC).

9. Conclusion

In this study, we proposed a hybrid cryptosystem based on AES and RSA Algorithms to secure a type of satellite image which is the interferograms from an inSAR system. Furthermore, a comparison of five encryption modes (ECB, CBC, OFB, CFB, and CTR) is conducted in order to select the most appropriate mode that best meets the safety requirements of inSAR interferograms.

For the evaluation and analysis of encrypted interferograms, we assessed several metrics such as: the histogram analysis, the correlation between adjacent pixels, between the original interferogram and the encrypted interferogram, the SSIM to verify integrity, as well as the resistance to error propagation. The results show that the histograms of the encrypted images are uniform for all operating modes (ECB, CBC, CFB, OFB, CTR), which satisfy the confidentiality criterion. Moreover, a random distribution of information is established since the pixels are strongly decorrelated for the five encryption modes. Using our transmission cryptosystem, the original interferograms and those deciphered are strongly decorrelated. The calculation of the SSIM also allowed us to verify the integrity of the interferograms resulting from the decryption against the original interferograms, and the resistance to error propagation. A decrypted interferogram unwinding operation is performed to calculate the SSIM between the original interferograms unwinding before encryption and the interferograms unwinding after decryption. The results are very satisfying for all modes.

This paper demonstrates that most favorable modes for the encryption of inSAR interferograms are OFB and CTR modes. Knowing that, the other modes (ECB, CFB, CBC) have given good results. It is noteworthy that the main criteria that can be used to choose between OFB and CTR for encryption of inSAR interferograms are error propagation and hardware complexity. As a result, OFB mode is employed in satellites in order to reduce the number of on-board circuits. CTR mode is recommended by CCSDS for encryption of telemetry (TM) and remote controls (TC).

For the future work of this research foreseeing us, the use of other encryption algorithms such as: the ECC algorithm (Cryptography on Elliptical Curves), and chaotic systems, for the securing of inSAR interferograms.

9. References

[1]. Lavender, S, and Lavender, A. "Practical handbook of remote sensing, "CRC Press, 2015.

[2]. El-Samie, F. E. A, Ahmed, H. E. H., Elashry, I. F, Shahieen, M. H, Faragallah, O. S, El-Rabaie, E.-S. M, and Alshebeili, S. A. "*Image encryption: a communication perspective*," CRC Press, 2013.

[3]. K. Raney, "Radar, Altimeters, " in Encyclopedia of Remote Sensing, Springer New York, 2014, pp. 525–532.

[4]. A. Moreira, P. Prats-Iraola, M. Younis, G. Krieger, I. Hajnsek, and K. P. Papathanassiou, "A tutorial on synthetic aperture radar, " *IEEE Geoscience and Remote Sensing Magazine*, vol. 1, no. 1, pp. 6–43, Mar. 2013.

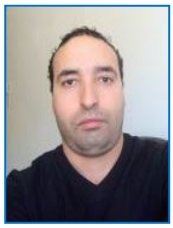
[5]. H. Yu, Y. Lan, Z. Yuan, J. Xu, and H. Lee, "Phase Unwrapping in InSAR: A Review," *IEEE Geoscience and Remote Sensing Magazine*, vol. 7, no. 1, pp. 40–58, Mar. 2019.

[6]. Haixia bi, Z.-Q. Wei, " A new phase unwrapping method based on region recognition and region expansion, " International Journal of Remote Sensing, vol.37, no. 22, pp. 813–821, 2016.

[7]. Abdulkarim amer shtewi, m. hasan, and Abd el fatah, A. hegazy, "an efficient modified advanced encryption standard (MAES) adapted for image cryptosystems, " *IJCSNS inter-*

national journal of computer science and network security, vol.10 no.2,pp.226-232 february 2010.
[8]. R. stinson, "cryptography: theory and practice, (discrete mathematics and its applications), " chapman & hall/ crc press, new york, november 2005.
[9]. Bruce schneier, "applied cryptography, " CRC press, united states of America, 1996, p. 780.
[10]. Morris dworkin, "recommendation for block cipher modes of operation, " NIST special publication 800-38 ,2001 edtion.
[11]. Robert pre, "system DVB MSG, " fontana roberto software, EUMET cast, p. 22, 2008.
[12]. Peng, J., You, M., Yang, Z., & Jin, S, "Research on a block encryption cipher based on chaotic dynamical system, Paper presented at the Natural Computation, Third International Conference on 2007, ICNC 2007
[13]. https://directory.eoportal.org/web/eoportal/satellite-missions, 2018.
[14]. FIPS, P. (2009). 197, "Advanced Encryption Standard (AES) ", National Institute of Standards and Technology, US Department of Commerce, November 2001.
[15]. CCSDS, "CCSDS cryptographic algorithms," 350.9-G-1, 2012.
[16]. Katz, J., & Lindell, Y. (2014). "Introduction to modern cryptography, " CRC press.
[17]. Ako, .M Abdullah, " Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, " Department of Applied Mathematics & Computer Science Eastern Mediterranean University – Cyprus, 2017.
[18]. Touradj Ebrahimi, Franck Leprévost, Bertrand Warusfel, "Cryptographie et sécurité des systèmes et réseaux, " Hermès – Lavoisier, 2006.
[19]. Dworkin, M, "Recommendation for block cipher modes of operation, " Special Publication 800-38A, 2001.
[20]. Hudde, H, "Building stream ciphers from block ciphers and their security, " Seminararbeit Ruhr-Universität Bochum, February, 2009.
[21]. Jean-Guillaume. Dumas, Jean-Louis Roch Éric Tannier Sébastien Varrette, "théorie des codes compression, cryptage, correction, " Dunod, Paris, 2007 ISBN 9-78-210-050692-7.
[22]. Sandeep, K.R., Dindayal. M., Danish, A.K., " A Survey on Advanced Encryption Standard Handbook of information and communication security, " *International Journal of Science and Research (IJSR)*, 6(1), 711-774, 2017.
[23]. Katz, J., & Lindell, Y, "Introduction to modern cryptography, " CRC press, 2014.
[24]. Stavroulakis, P., & Stamp. M, "*Handbook of information and communication security, " Springer Science & Business Media*, 2010.
[25]. McGrew. D, "Counter mode security: Analysis and recommendations, " Cisco Systems, November, 2, 4, 2002.
[26]. Napa, S.B, Somkait, U., "Noise Reduction based on Multiple Copies Color Image Noise Estimation, " International Journal on Electrical Engineering and Informatics, 11(3), 515-528, 2019.
[27]. Jamal, N., Bani, S., " A New Approach for Securing Medical Images and Patient's Information by Using A hybrid System, " *IJCSNS International Journal of Computer Science and Network Security*, 19(4), 28-39, April 2019.
[28]. https://fr.wikipedia.org/wiki/Structural_Similarity, 2019.
[29]. Vladimirova, T., Banu, R., & Sweeting.M, "Investigation of Fault Propagation in Encryption of Satellite Images Using the AES Algorithm, " *IEEE Military Communications conference* 2006, MILCOM 2006.

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 and researcher in electrical engineering at the electrical engineering department of Larbi Tébessi University Tébessa, Algeria. He is a member of a research team in the laboratory of electrical engineering LABGET, electrical engineering department of Larbi Tébessi University Tébessa, Algeria and also member of a research team in the laboratory in the LAAAS laboratory of Mostapha Benboulaid Batna-2 University - Algeria. His interests include telecommunications, mobile phone systems, as well as cryptography and network security.



Tarek BENENTAHAR was born in 1980 in Batna-Algeria. 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 an associate professor at Larbi Tébessi Tébessa University. His area of interests includes: Telecommunication and network systems, Remote sensing, Radar, image and signal processing.

Nada CHERRID 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.

Atef BENTAHAR was born in 1981 in Batna-Algeria. In 2016 he had his master degree in computer science from Larbi Tébessi University. Currently 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

Hichem MAYACHE received the engineering degree in communication from the University of Annaba, Algeria (2005), and the magister degree in communication and digital computing from the University of Annaba, Algeria (2008). He received the Ph.D. degree in communications from the Badji Mokhtar University, Annaba (2018). He is associate professor in the Higher School of Industrial Technologies-Annaba, Algeria. His research interests include: communication systems, embedded system, Network-on-Chip, signal processing, FPGA design and Real time implementation. He can be reached at h.mayache@esti-annaba.dz.