International Journal of Multimedia and Ubiquitous Engineering
Vol.15, No.2, (2020), pp.1-14
http://dx.doi.org/10.21742/ijmue.2020.15.2.01

Evaluation of The Encryption Quality of an Insar Interferogram by a Crypto-System Based on Two AES-256 and RSA Algorithms with CTR and OFB Modes

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

[1,3]Laboratory of electrical engineering-telecommunications (LABGET), Constantine Street 12002, Larbi Tébessi University, Tébessa, Algeria
[2]Electronic Department, CUB- Street Chahid BOUKHLOUF Mustapha ben boulaid Batna 2 University, Batna, 05000, Algeria
[4]Laboratory of Mathematics, Informatics and Systems (LAMIS), Constantine Street 12002, Larbi Tébessi University. Tébessa, Algeria
[1]riad.saidi@univ-tebessa.dz, [2]cherridnad@gmail.com, [3]tarek.bentahar@univ-tebessa.dz, [4]atefbentahar@gmail.com

Abstract

Many threats in turn transmit images from satellites to Earth which can affect the confidentiality of the data as well as its qualities. From this encryption algorithms capable of securing the transmitted images are used, to preserve the quality of origins. The satellite images often have a large volume and high redundancy. At the same time, the satellites work under tight limitations in terms of computing power and resources. In addition to that, it operates in a harmful environment and therefore, any electronics used onboard, including encryption electronics, may exhibit radiation-induced defects. Our objective in this work is to assess the quality of a particular type of satellite image, which is an interferogram from the InSAR system, encrypted using the AES-256 standard and the RSA asymmetric encryption algorithm using Counter-mode encryption (CTR) mode and Output Feedback (OFB) mode. The evaluation work covered, it's accomplished using different metrics, based on an objective evaluation with the methods using a complete reference image which is the original interferogram, the quantitative measures used are: The Mean Square Error (MSE), the Peak Signal to Noise Ratio (PSNR), Structural SIMilarity index (SSIM). Other statistical analyzes are used such as: the analysis of the original, encrypted and decrypted interferogram histogram, the entropy and the correlation coefficient between the adjacent pixels, the correlation between the original interferogram and the encrypted interferogram for the two modes under AES-256, as well as encryption speed, and execution time.

Keywords: *Interferogram quality assessment, Advanced encryptions standard (AES-256), SSIM, CTR and OFB mode*

1. Introduction

Observation means onboard satellites allow us to have so-called satellite images, which are images of the earth or other planets. These images are used in several fields such as agriculture, meteorology, forestry, urban traffic, the military and other fields. For several fields, they have

Article history:
Received (May 16, 2020), Review Result (July 5, 2020), Accepted (August 18, 2020)

Print ISSN: 1975-0080, eISSN: 2652-1954 IJMUE

evolved to a necessary means [1]. For this, they must be secured against unauthorized access (confidentiality), protected against unauthorized changes (integrity), and available to an authorized entity when necessary (Authentication) [2].

In this article, we used an interferogram from the InSAR system for our work, which is based on independent light scanning, by illuminating the surface with its source of electromagnetic waves. This type of image, are used in several fields of application such as: earth observation, meteorology and cartography [3][4]. The InSAR system provides two images: an amplitude image and the other phase image. The two inSAR images are produced from the complex correlated signal using two antenna acquisitions. The image of the InSAR phase; known as an interferogram, is naturally wrapped in [-π, + π], to recover the true phase value, an unwinding process must be performed. This process consists of finding the cycle number which will be added to each pixel [5]. Information encryption has been exploited as a security mechanism for military purposes and the exchange of secret data for a long time. Secure data transmission is necessary and widely used in the digital world. Interferograms are particular data because of their large amount of information. Various techniques exist for securing satellite images; we mention among them, the symmetric public algorithm AES (Advanced Encryption Standard), AES has been approved as an encryption standard by National Institute of Standards and Technology (NIST), is chosen by several organizations around the world. It is a symmetric block encryption process in which the transmitter and receiver use a single key for encryption and decryption. it processes blocks of data of 128 bits (16 bytes) using cryptographic keys of 128, 192 or 256 [6] proposed, as part of a practical implementation, the AES algorithm is combined with a series of simple operations to improve security without penalizing the efficiency of the algorithm. This combination is called a cryptographic mode, such as Cipher Block Chaining (CBC), Output Feedback (OFB), and Counter-mode encryption (CTR) mode, these modes are methods for using block ciphers, we speak of operating modes [7]. The Consultative Committee for Space Data Systems (CCSDS), recommends this standard for data encryption in civil space missions.

There are other encryption algorithms that exist such as the asymmetric RSA algorithm [8][9] proposed, and the International Data Encryption Algorithm (IDEA) proposed, some satellites using the 3- DES algorithm for encrypting images. In our work, the cryptosystem used is based on AES-256, which is the successor to DES proposed, for the InSAR interferogram encryption. The RSA algorithm ensure secure exchange of keys. Many encryption algorithms available exist, however the use of encryption technology in spacecraft is far behind compared to terrestrial systems [10]. This is why it is difficult to establish a true state of the art on the encryption methods used onboard satellites since most manufacturers and owners of satellites do not share this type of information. Whereas, some document cites the encryption algorithms used in some space missions [11].

2. Encryption algorithm

The algorithms used in this work are based on two encryption algorithms, one symmetrical which is AES-256, the other asymmetrical which is the RSA algorithm, which is illustrated in [Figure 1].

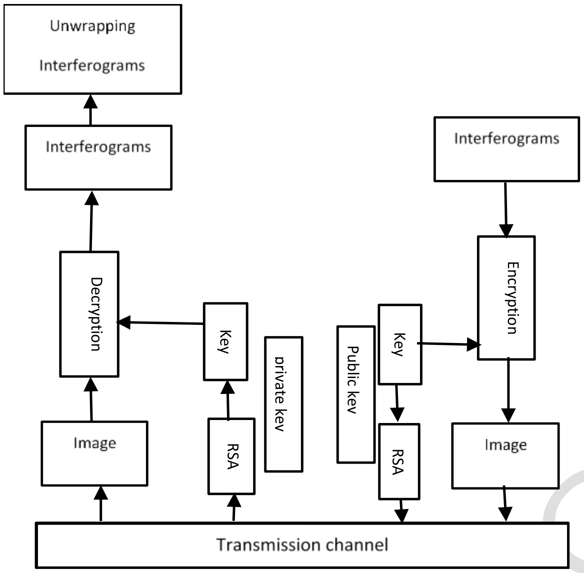


Figure 1. Transmission cryptosystem

3. Advanced Encryption Standard (AES) encryption modes

It's an algorithm that was developed in 1998 by Joan Daemen and Vincent Rijmen, based on block encryption with symmetric key. It processes all types of data, the data block length is fixed at 128 bits, while the key can take a length of 128, 192 or 256 bits. The AES algorithm allows data of 128-bit length to be divided into four basic operational blocks. They are considered as a byte array which is organized as a 4 × 4 dimension matrix which is also called state matrix and which in turn is subjected to various transformations. For a complete encryption, the number of turns used is variable N is equal to 10, 12, 14 according to the key length of 128 192 and 256 respectively. Each cycle of this algorithm uses the principle of permutation and substitution, and is suitable for both hardware and software implementation [12] In our work, the algorithm used is a key of length 256 which corresponds to several turns equal to 14 rounds. For civilian space missions, the CCSDS recommends using AES as symmetric encryption [6]. The AES algorithm can be combined with a series of simple encryption modes to improve security, without penalizing the efficiency of the algorithm itself [13][14], such as:

- Cipher Block Chaining (CBC).
- Cipher Feedback (CFB).
- Output Feedback (OFB).
- Counter-mode encryption (CTR).
- Electronic Code Book (ECB)

In the two OFB and CTR modes, the encrypted blocks are independent of each other. so, if an encrypted block is altered during transmission, the error does not spread to the other blocks. The error only affects the corresponding bits in the decrypted message. For this reason, the OFB and CTR modes are favored compared to the other modes.

The main criteria for choosing between OFB and CTR for the encryption of satellite images are [15]:

- Propagation of errors.
- Material complexity.

3.1. AES OFB mode

In this mode [Figure 2], an initial vector is initially encrypted to start the process, the key flow at the output of this block will be reinjected at the input to calculate the next key flow.

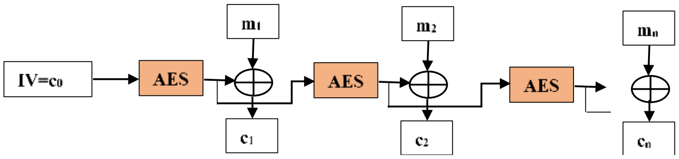


Figure 2. OFB block cipher mode

Using this mode, the preprocessing of the key flow is possible because it does not depend on a clear message. This mode is useful in satellites for which minimizing the number of on-board circuits is crucial [16].

3.2. AES CTR mode

CTR mode is simple, it creates a stream of pseudo-random numbers independent of the plain text. [Figure 3] shows Counter-mode encryption (CTR). In this mode, the key flow is obtained by encrypting successive values of a counter which is then XORE with the message in plain text to generate the encrypted message [17][18].

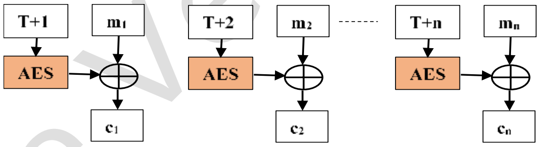


Figure 3. CTR block cipher mode

Counter values used with an encryption key must be nonce, because the key flow should never be repeated. because the key flow should never be repeated. In this mode, unlike other modes, there is no feedback or sequential processing of the blocks. Therefore, it is possible to perform several ciphers in parallel, a significant advantage in high performance applications [18]. This mode is recommended by the CCSDS for the encryption of telemetry (TM) and remote control (TC) [19].

4. RSA algorithm

The RSA algorithm founded in 1977 by the three inventors: Ronald Rivest, Adi Shamir and Leonard Adleman, RSA, is an asymmetric cryptographic algorithm. It generates two keys: a public key for encryption and the other private key for message decryption, it consists of three steps, the first step is the generation of keys which should be used as a key to encrypt and decrypt the data, the second step is encryption, where the actual process of converting plain text to encrypted text and the third step is decryption, where the encrypted text is converted to plain text. It is widely used and very efficient for exchanging keys of symmetric algorithms like

AES. In our cryptosystem, this algorithm is used for the secure exchange of keys, and to provide the authentication function. In this algorithm, it is impossible to find the decryption key despite the knowledge of the cryptographic algorithm and the encryption key. The RSA is based on two basic mathematical principles: the difficulty of factoring large numbers, and the arithmetic of congruences. The size of the key is from 1024 to 4096 bits [8][20].

5. Methodologies

The evaluation of an InSAR encrypts and decrypts interferogram, proposed in this article, is based on an AES-256 cryptosystem using two encryption modes (OFB, CTR). This evaluation of the encryption results by the two modes, to seek to determine the quality of the deciphered interferogram, which determine the most suitable mode for encrypting this type of image. The different evaluation criteria, concerning the quality of the results used in this article are: concerning quality of the results used in this article are:

The Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM). A statistical analysis is also made based on: Analysis of the histograms of the original, encrypted, and deciphered interferogram, the entropy and the correlation coefficient between the adjacent pixels, the correlation between the original interferogram and the encrypted interferogram, as well as the encryption speed.

The two modes of the AES-256 were simulated and evaluated on a 2.53 GHz Pentium I-5 PC with Windows 7 and 4 GB of RAM. The software used is Matlab. The [Figure 4] illustrates the interferogram studied, with different information and a geographic region which are indicated by the [Table 1].

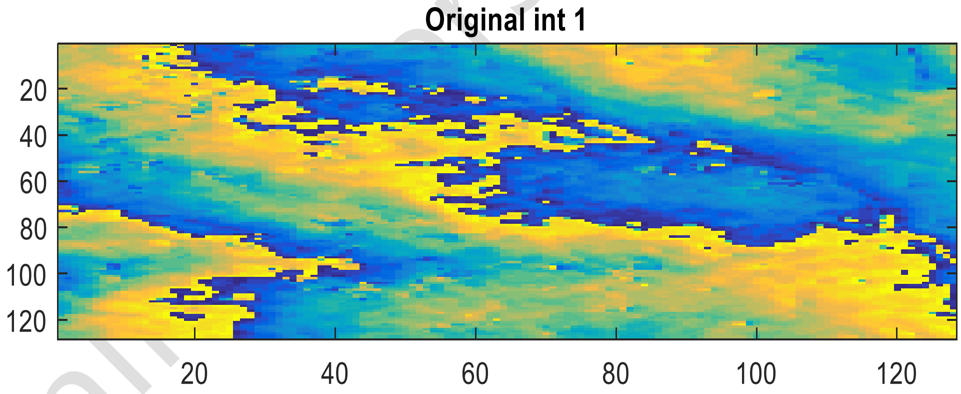


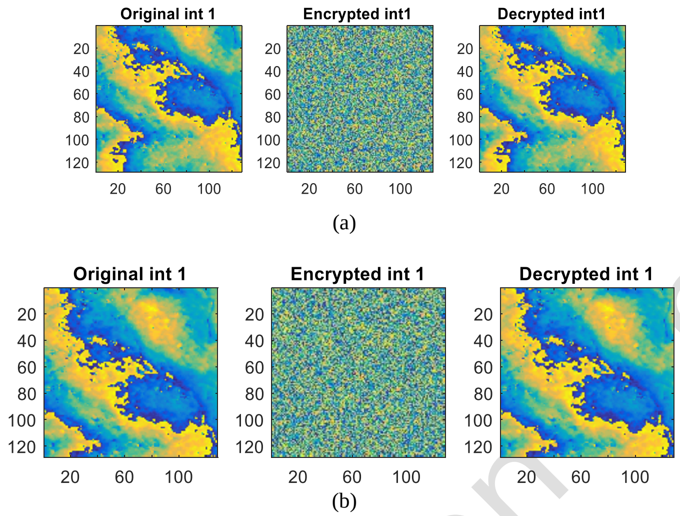
Figure 4. Interferogram original (int1)

Table 1. Characteristics of the interferogram being studied

	Imaged region	Taken on	Orbit	Baseline(m)	Residues rate (%)
Interferogram original (int 1)	Vatnajökull	Dec31, 1995	23315	Not provided	0,0112

6. Results and analysis

The results of the interferogram encryption are illustrated by [Figure 5] for the two AES-256-OFB and AES-256-CTR modes.



(a)

(b)

Figure 5. Interferogram original, encrypted, and decrypted (a) with AES-256 CTR mode, (b)With AES-256 OFB mode

In this part of assessing the quality of the encrypted and deciphered interferogram, several metrics are used.

6.1. Mean Square Error (MSE)

The interferogram deciphers Î is always compared to the original I to determine its likeness ratio. This criterion is the most used. It is based on the measurement of the mean square error (MSE) calculated between the original and degraded pixels [21] proposed in our case those deciphered:

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

Where (M × N) is the size of the interferogram, and I and $\hat{I}$ are the amplitudes of the pixels on the original interferograms and those deciphered, respectively. The eye likely takes much greater account of errors at large amplitudes, which favors quadratic measurement. ([Table 2])shows the different values of the mean square error between the original and deciphered interferograms for the three modes.

Table 2. Mean square error

Interferogram	MSE	
	AES-256-OFB	AES-256-CTR
Int 1	0	0

6.2. Peak Signal-to-Noise Ratio (PSNR)

The PSNR measures fidelity, which is related to quality. All the same, it is a function of MSE; its definition and use come from the field of signal processing [21]:

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

For a gray level interferogram, *I_{max}* designates the maximum possible luminance. An infinite PSNR value corresponds to a decrypted interferogram not degraded compared to the original. This value decreases as a function of the degradation. The PSNR therefore links the MSE to the maximum energy of the interferogram. [Table 3] gives the PSNR values of the interferogram decrypted for the two modes which is at a high value for the two modes. Indicating the non-degradation of the interferogram decrypted compared to the original.

Table 3. Peak signal to noise ratio

Interferogram	Peak signal to noise ratio in %	
	AES-256-OFB	AES-256-CTR
Int 1	99	99

6.3. Structural SIMilarity index (SSIM)

SSIM is a measure of similarity between two digital images. It was developed to measure the visual quality of a distorted image, compared to the original image. The idea of SSIM is to measure the similarity of structure between the two images, rather than a pixel-to-pixel difference like the PSNR does for example. The SSIM metric is calculated on several windows of an image. We denote x and y the original image and the distorted image respectively. The similarity compares the luminance, the contrast and the structure between each pair of windows. Luminance is estimated by measuring the average intensity of each window [22]:

$$\mu_x = \frac{1}{N}\sum_{1}^{N} x_i \tag{3}$$

N: the number of pixels in each window.
x_i: the intensity of a pixel.
The contrast for each window is measured by:

$$\sigma_x = \left(\frac{1}{N-1}\sum_{1}^{N}(x_i - \mu_x)^2\right)^{\frac{1}{2}} \tag{4}$$

The similarity is determined by the loss of correlation between the two windows:

$$\sigma_{xy} = \frac{1}{N-1}\sum_{1}^{N}(x_i - \mu_x)(y_i - \mu_y) \tag{5}$$

The luminance comparison function denoted by *l (x, y)* is a function of *x* and y. The contrast between two windows denoted by *c (x, y)*, compare the variances of *x* and *y*. The third function compares the structures of the two windows given by the function *s (x, y)* as a function of two normalized windows. Finally, the function measuring the similarity, is a function of *l (x, y)*, *c (x, y)* and *s (x, y)*.

It is of the form:

$$S\,(\mathrm{x},\mathrm{y}) = \mathrm{f}\,(l\,(x, y), c(x, y), s(x, y)) \tag{6}$$

A function to compare the luminance of the form [22]:

$$l(x,y) = \frac{2\mu_x\mu_y + (K_1L)^2}{\mu_x^2 + \mu_y^2 + (K_1L)^2} \tag{7}$$

K_1 is a constant of very low value. The constant *$(K_1L)^2$* avoids the instability of the comparison function when $\mu_{\mathrm{x}}^2 + \mu_{\mathrm{y}}^2$ are $\mu_x^2 + \mu_y^2$ very close to zero. Note that [Equation 7] conforms to Weber's law, widely used for modeling light adaptation in the SVH (human visual system). According to weber's law, the variation in luminance is proportional to the background luminance. In other words, the SVH is sensitive to relative variations in luminance between the two signals or between the two images.

The contrast comparison function takes a similar form:

$$c(x,y) = \frac{2\sigma_x\sigma_y + (K_2L)^2}{\sigma_x^2 + \sigma_y^2 + (K_2L)^2} \tag{8}$$

K_2 is a constant of very low value.

The structure comparison is carried out by the correlation between the two vectors after subtracting the luminance and normalizing by the variance. Note that the correlation between the two vectors is a simple and effective measure of structural similarity. Then the structural comparison function is given by:

$$s(x,y) = \frac{2\sigma_{xy} + (K_2L)^2}{2\sigma_x\sigma_y + (K_2L)^2} \tag{9}$$

Finally, the resulting similarity measure of the three comparisons is given by a simplified expression of the structural similarity index between *x* and *y*:

$$SSIM\,(\mathrm{x},\mathrm{y}) = l\,(x, y).\ c\,(x, y).\ s\,(x, y) \tag{10}$$

Or in a simplified form:

$$SSIM(x,y) = \frac{2\mu_x\mu_y + (K_1L)^2}{\mu_x^2 + \mu_y^2 + (K_1L)^2} * \frac{2\sigma_{xy} + (K_2L)^2}{\sigma_x^2 + \sigma_y^2 + (K_2L)^2} \tag{11}$$

The similarity index is used for an appropriate choice of the constants *K_1* and *K_2* to generalize the evaluation to the entire image. Based on the results shown in [Table 4], the value of the SSIM calculated between the original interferogram and that which deciphers, for the two modes are perfect, indicating that the original interferogram and that which deciphers are identical.

Table 4. Structural similarity index

Interferogram	SSIM	
	AES-256-OFB	AES-256-CTR

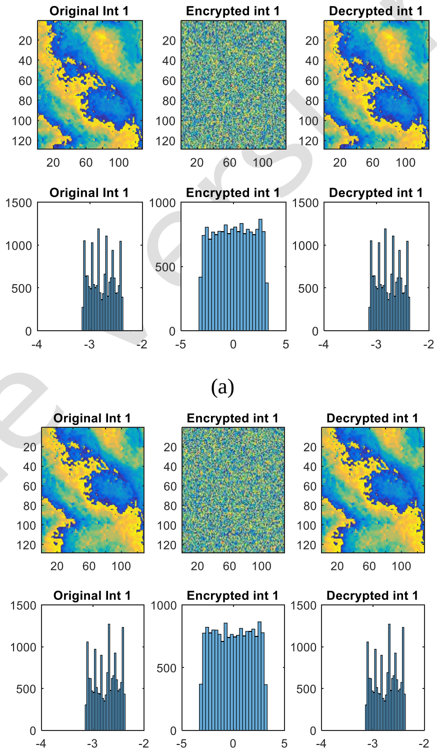
Int 1	1	1

We also calculated the SSIM between the interferogram resulting from the unwinding of the original interferogram and that of the deciphered interferogram, we had the results indicated in [Table 5].

Table 5. SSIM between the interferogram original unwinding and the deciphered interferogram unwinding

Interferogram	SSIM the interferogram unwinding	
	AES-256-OFB	AES256--CTR
Int 1	1	1

In the way that even the interferogram resulting from the unwinding of the original interferogram and that of the interferogram deciphered by AES-256-OFB and AES-256-CTR Mode, its identical.



(a)

(b)

Figure 8. Histogram of the interferogram original, encrypted, and decrypted, (a) with AES-256 -OFB, (b) with AES-256 -CTR

7. Statistical analysis

7.1. Histogram analysis

Two properties the histogram of the encrypted image(interferogram) must satisfy [23]:

1. the histogram of the encrypted image(interferogram) must be completely different from the histogram of the original image(interferogram).

2. the histogram of the encrypted image(interferogram) must have a uniform distribution, which means that the probability of occurrence of any value is the same.

Recall that the image in our work is an interferogram of the InSAR system. [Figure 8] represents the histogram of the original interferogram and encrypted by the two OFB-CTR modes with the AES-256 algorithm. It is quite observable that the two modes of operation respect the properties required for the histogram of the encrypted interferogram.

7.2. Entropy

Entropy of Shannon, due to Claude Shannon, is a mathematical function that intuitively corresponds to the quantity of information contained in an information source [24]. If this information source is an image, entropy is used to characterize the texture of the image. The entropy function is defined as follows:

$$H = -\sum p(i) * log p(i) \qquad (12)$$

p(i) is the probability of a pixel's intensity level appearing. i=0,1,2, N. N is the maximum level of intensity of a pixel. For interferograms the maximum level of intensity is between [-π, + π]. As shown in [Table 6], the entropy of the two OFB-CTR modes of the AES-256 can reach 2.3238; it is a very good value close to the ideal entropy of such a type of image. This means that the pixels of the encrypted interferogram are statistically independent of each other.

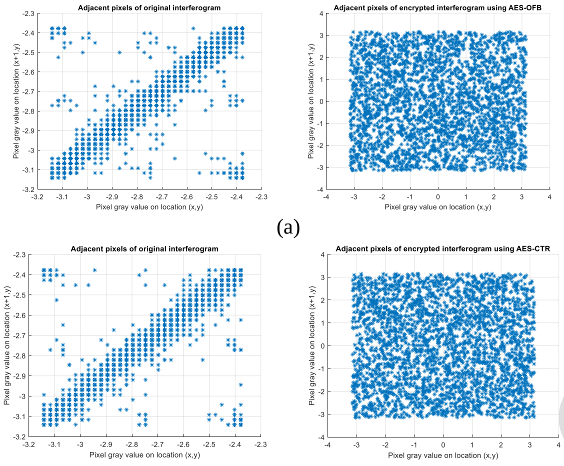
Table 6. Entropies for the two operating modes of the AES-256

Interferogram	Entropy	
	AES-256-OFB	AES-256-CTR
Int 1	2.3238	2.2797

From [Table 6] it is clear that the maximum entropy is recorded in the OFB mode.

7.3. Analysis of the correlation coefficients between the original and encrypted interferogram

Another method for evaluating the quality of cipher interferogram by the two modes (AES-256-OFB, AES-256-CTR), is to measure the correlation factor between adjacent pixels. In [Figure 9], each point on the X-axis represents a pixel value between -π and + π. The Y axis shows the value of the adjacent pixel on the X-axis [25]. It is easy to note that the values of the adjacent pixels in the original interferogram are strongly correlated in the two modes (AES-256-OFB, AES-256-CTR), while the values of the adjacent pixels in the encrypted interferogram are not correlated as shown in [Figure 9a], and [Figure 9b].



(a)

(b)

Figure 9. Correlation for the original interferogram and figures for the two modes. (a) AES-256-OFB modes (b) AES-256-CTR modes

Another important factor that shows the overall correlation between adjacent pixels in an image, horizontally, vertically, or diagonally, is the correlation coefficient. It is the measure of the extent and direction of the linear combination of two pixels. If two pixels are closely linked to a stronger association, the correlation coefficient is close to 1 or -1. On the other hand, if the coefficient is close to 0, two pixels are not linked and cannot be predicted. The correlation coefficient is calculated as follows [8]:

$$r = \frac{cov(x, y)}{\sqrt{D(x) * D(y)}} \qquad (13)$$

Where:
r: correlation coefficient.
x, y: pixel intensity values.
cov (x, y), D (x) and *D (y)* are calculated as follows:

$$D(x) = D(y) = \frac{1}{N}\sum_{i=1}^{N}(x(i) - E(x))^2 \qquad (14)$$

$$cov(x) = \frac{1}{N}\sum_{i=1}^{N}\big(x(i) - E(x)\big) - (y(i) - E(y)) \qquad (15)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(x(i)) \qquad (16)$$

The correlation coefficient r is expressed between -1 and +1, where:
If r = -1; means that the encrypted image is the reverse of the original image,

If -1 <r <0 (Negative correlation) indicates a negative relationship between the pixels.
r = 0; indicates no correlation between the pixels.
0 <r ≤ 1 (positive correlation) indicates a positive relationship between the pixels.

We must remember that images, in our work, are in SAR interferogram.

Table 7. Correlation coefficients for the two interferograms

Correlation coefficients	Interferogram Int 1		
	Original	AES-256-OFB	AES-256-CTR
Horizontal	1	0.0103	0.0079
Vertical	1	0.0085	0.0076
Diagonal	1	0.0303	0.0808

From [Table 7] on the way that the correlation coefficient indicates a positive relationship between the pixels for the two modes (AES-256-OFB and AES-256-CTR).

7.4. Encryption speed

The encryption speed is calculated by taking the ratio of the number of pixels (bytes) in the interferogram to the time taken for encryption, indicated by [Table 8]. The tests were carried out using Matlab-2016 in a 2.00 GHz Intel Core 2 Duo processor with the Windows-10 operating system.

Table 8. Encryption speed for tow mode of AES-256

Interferogram	Encryption speed bit/s	
	AES-256-OFB	AES-256-CTR
Int 1	904.7758	751.0725

7.5. Encryption execution time

[Table 9] tells us, the execution time required for each mode to encrypt the original InSAR interferogram.See that the AES-256-OFB mode executes in 18.3195 seconds, which is a faster execution time than that of the AES-256-CTR mode.

Table 9. Encryption execution time

Advanced Encryption Standard (AES) Encryption Modes	Execution time (s)
AES-256-OFB	18.3195
AES-256-CTR	24.3193

8. Conclusion

The work done in this article is based on the evaluation of the quality of an interferogram from an InSAR system, which is a type of satellite image, decrypted and encrypted by a cryptosystem based on the AES-256 algorithm and RSA, using two encryption modes AES-256-OFB, and AES-256-CTR. To analyze the quality of the interferogram encrypted and decrypted by the AES-256 algorithm, several evaluation metrics were used. In practice, subjective assessment is usually too cumbersome, time consuming and very costly. And to avoid all this, for our work, we have chosen objective methods a measure of the degradation in terms of quadratic mean error (MSE), the measure of PSNR which is considered until today as a criterion of quality assessment most used in image processing, which is a qualitative measure which sometimes requires a subjective assessment of degradation. Therefore, we use methods that reflect human evaluation well such as SSIM which is based on the assumption that the human visual system is strongly influenced by the structures presented in a scene. These methods are based on the measurement thus the degradation of the structures between two images namely degraded and original, in our work the original interferogram and that deciphered. Other methods are used such as Statistical Analysis comprising the analysis of encrypted interferogram histograms, entropy and the correlation coefficient between the adjacent pixels for the two operating modes of the AES-256.

From all this we can see that the two modes (AES-256-OFB, and AES-256-CTR) give a deciphered interferogram identical to the original, which means that the interferogram recovered after encryption operation with (AES-256 -OFB, and AES-256-CTR) is identical to the original. Knowing that the OFB mode and according to the literature is useful in satellites since it minimizes the number of on-board circuits, which is crucial, while for the CTR mode which is recommended by the CCSDS for the encryption of telemetry (TM) and the remote controls (TC).

References

[1] Bensikaddour. E, “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,” Ph.D. dissertation in Sciences, pp.6-37 **(2019)**

[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] P. A, Rosen. S, Hensley. I. R, Joughin. F. K, Li. S, N. Madsen, E. Rodriguez, R. M, Goldstein, “Synthetic aperture radar interferometry,” IEEE Proceedings, vol.88, no.3, pp.333-382, **(2000)**

[4] Bamlery.R, and Hartl. P, “Synthetic aperture radar interferometry Synthetic aperture radar interferometry, Inverse Problems,” vol.14, pp.1-54, **(1998)**

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

[6] FIPS Publication 197, “Advanced Encryption Standard (AES),” National Institute of Standards and Technology, US Department of Commerce, **(2001)**

[7] Dumont. R, “Cryptographie et Sécurité informatique,” Notes de cours, Université de Liège Faculté des Sciences Appliqués, pp.63-68, **(2010)**

[8] Rivest. R., Shamir. A, and Adleman. L, “A method for obtaining digital signatures and public-key cryptosystems,” communications of the ACM, vol.21, no.2, pp.120-126, **(1978)**

[9] Douglas. R.Stinson, “Cryptography: Theory and practice (7th ed.) ,” Chapman & Hall/ CRC, **(2005)**

[10] Peng. J, You. M, Yang. Z, and Jin. S, “Research on a block encryption cipher based on chaotic dynamical system,” Publisher: IEEE, Third International Conference on Natural Computation, Haikou, China, Aug 24-27, **(2007)**

[11] Sharing Earth Observation Resources.https://directory.eoportal.org/web/eoportal/satellite-missions, **(2018)**

[12] Pahal. R, Kumar, Vikas, “Efficient Implementation of AES,” International Journal of Advanced Research in Computer Science and Software Engineering, vol.3, no.7, **(2013)**

[13] Fathi, E.A.S., H Ahmed, Elashry, I.F., Shahieen, M.H., Faragallah, O.S. Image Encryption A Communication Perspective (1st ed.). Boca Raton [Florida]: CRC Press, **(2013).**DOI:10.1201/b16309

[14] Nigel. P, Smart. Rijmen. V, Gierlichs. B, Paterson. K.G, Stam. M, Warinschi. B, Watson. G, “Algorithms key size and parameters,” report 2014. European Union Agency for Network and Information Security (ENISA), **(2014)**.

[15] Bensikaddoura. E, Bentoutoua.Y, and Talebb. N, “Satellite Image Encryption Method Based On AES-CTR algorithm and GEFFE generator,” Publisher: IEEE, 8th International Conference on Recent Advances in Space Technologies (RAST), Istanbul, Turkey, 19-22 June, **(2017)**

[16] Dumas. J-G, Roch. J-L, Tannier. É, and Varrette. S, “Théorie des codes compression, cryptage, correction,”, Dunod, Paris, pp.38-41, **(2007)**

[17] Stavroulakis. P, and Stamp. M, “Handbook of information and communication security,” Springer Science & Business Media, pp.569-608, **(2010)**

[18] Burr. W. E, “Selecting the advanced encryption standard,” IEEE Security & Privacy, vol.1, no.2, pp.43-52, **(2003)**

[19] CCSDS. 350.9-G-1, “Ccsds cryptographic algorithms,” blue book, **(2019)**

[20] Preethi. M, Nithya. M, “Study and performance of RSA algorithm,” International Journal of Computer Science and Mobile Computing, vol.2, no. 6, pp. 126-139, **(2013)**

[21] Ahmed seghir. Z, “Evaluation de la qualité d’image,” Doctoral thesis, Université de Mentouri, Constantine, Algerie, **(2012)**

[22] Wang. Z, Bovik. A.C, Sheikh. H. R, and Simocelli. E. P, “Image quality asssessment:From error measurement to structural similarity,” IEEE Trans. Image Processing, vol.13, no.4, pp.600-612, **(2004)**

[23] 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 taylor and francis Group, New York, pp.33-34, **(2013)**

[24] Patila. P, Narayankarb. P, Narayan. D.G, Meena. S.M, “A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish,” Published by Elsevier B.V, International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015, Nagpur, India, **(2016)**

[25] Mansour. I, Chalhoub. G, and Bakhache. B, “Evaluation of a fast-symmetric cryptographic algorithm,” IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, June 25-27, **(2012)**