Satellite image encryption using 2D standard map and advanced encryption standard with scrambling

Omar Benchikh[1], Youcef Bentoutou[2], Nasreddine Taleb[1]
[1]Communication Networks, Architecture and Multimedia Laboratory, Department of Electronics,
Djillali Liabes University of Sidi Bel Abbes, Sidi Bel Abbès, Algeria
[2]Satellite Development Center, Oran, Algeria

Article Info

Article history:

Received Jan 20, 2024
Revised May 27, 2024
Accepted Jun 4, 2024

Keywords:

Advanced encryption standard
Chaotic system
Image encryption
Satellite imagery
Scrambling

ABSTRACT

In today's world, the need for higher levels of security in storing and transferring data has become a key concern. It is essential to safeguard data from any potential information leaks to prevent threats that may compromise data confidentiality. Therefore, to protect critical and confidential satellite imagery, this paper proposes a novel encryption method based on the combination of image bands scrambling with chaos and the advanced encryption standard (AES). The proposed approach aims to enhance the security of satellite imagery while maintaining efficiency and robustness against various attacks. It possesses several appealing technical characteristics, notably a high level of security, a large key space, and resilience to single event upsets (SEUs) and transmission errors. To evaluate the performance of the proposed encryption technique, extensive experiments have been conducted by considering factors such as security level, resistance to SEUs, and computational efficiency. Our results demonstrate that the proposed method achieves a high level of security and a large key space, ensuring the confidentiality and integrity of satellite imagery data. Furthermore, the method exhibits resilience against SEUs and transmission errors, and offers efficient processing, making it suitable for real-world applications.

Corresponding Author:

Omar Benchikh
Communication Networks, Architecture and Multimedia Laboratory, Department of Electronics, Djillali Liabes University of Sidi Bel Abbes
Sidi Bel Abbes, Algeria
Email: omarb022@hotmail.com

1. INTRODUCTION

Nowadays, huge quantities of various types of digital data including text, image, and video are exchanged through different kinds of communication networks. Subject to possible high risks, such information must be protected and secured because it contains private and confidential data. In particular, earth observation satellites (EOS) and remote sensing (RS) are disrupted by random or intentional attacks on images. Since digital images are transmitted on different kinds of networks, their security becomes a necessity [1]. Referring to the US Computer Security Institute study [2], internal unauthorized file access accounts for 59% of threats, hence the need for efficient means to solve this problem and ensure the security of information systems. Among the security techniques employed, cryptography is the most widely used way to ensure the privacy, integrity or authentication of text and image data transmission processes and storage from unapproved users. This common technique, based on two functions called encryption and decryption, has found a great impact and became an interesting research theme in the area of information security

[3]–[5]. Furthermore, encryption is also used to ensure information transmission in communication networks. This task can be performed by using standard image encryption algorithms such as digital encryption standard (DES), international data encryption algorithm (IDEA), triple data encryption standard (3-DES), and advanced encryption standard (AES) [6]. However, DES and IDEA pose challenges due to their intricate nature and slow performance when tasked with encrypting large satellite image datasets. Moreover, both DES and 3-DES exhibit security vulnerabilities attributable to their limited key size. Among these encryption algorithms, AES is considered as a new generation of world encryption standard that was adopted by the National Institute of Standards and Technology (NIST) [7]. In the last two decades, AES has been most commonly used as an excellent choice for many critical applications seeking confidentiality and the secure exchange of information such as satellite imagery [8], [9]. These classical methods, while effective in certain contexts, may exhibit drawbacks when applied to large-size or bulky satellite image data.

In the past twenty years, chaotic maps have emerged as a viable tool for image encryption, thanks to their attractive characteristics such as pseudo-randomness, unpredictability, ergodicity, and sensitivity to initial conditions [10], [11]. Chaotic maps provide opportunities for developing novel image encryption methodologies or modifying conventional algorithms [12], [13]. A comprehensive review of recent studies on image data security and cryptographic analysis is presented in [8].

Existing cryptographic systems utilizing chaotic maps can be divided into two main categories: one-dimensional (1-D) and multi-dimensional (M-D) chaotic maps. Chaotic dynamics of certain 1-D chaotic maps like the Logistic and Sine maps are often deemed insufficiently secure due to inherent limitations stemming from the predictable nature of their simple orbits and the ability to forecast their control and initial parameters [14]. Consequently, classical 1-D chaotic maps are deemed unsuitable for image encryption. As a result, numerous endeavors have been undertaken to propose novel M-D chaotic maps to enable rapid and highly secure image encryption [15]. Compared to 1-D chaotic maps, these complex schemes exhibit greater unpredictability and superior chaotic behavior, rendering them more suitable for data encryption [13], [16]. However, the main limitations of M-D chaotic maps for image encryption include computational complexity, high dimensionality, and challenges in key management. Security analysis can be complex and may impact encryption performance and the overall security of the system.

In the context of image encryption, where the confidentiality and integrity of data are critical, the integration of AES with chaotic techniques holds particular significance [13], [17], [18]. In particular, satellite imagery often contains sensitive information related to national security, environmental monitoring, disaster management, and other applications, necessitating robust encryption mechanisms to protect against unauthorized access and tampering [19]–[21]. Recent developments in satellite image encryption have explored novel approaches that combine AES with chaotic techniques to achieve high security levels [13], [22], [23]. By incorporating chaotic dynamics into encryption algorithms, such as AES, researchers aim to introduce additional layers of randomness and complexity, making encrypted data more resistant to cryptographic attacks.

To increase the security level of AES, a combination of AES and chaos using Arnold's cat map to shuffle pixel values and Henon map to generate random sequences was proposed for satellite imagery encryption [22]. Another approach based on the combination of a customized version of the AES and the Arnold cat map to derive the encryption key was introduced in [24]. Similarly, A chaotic system with four dimensions was utilized to produce keys and enhance the AES standard [25]. Also, an adjusted AES cryptographic system featuring dynamic random keys derived from chaos synchronization was proposed in [18]. While these enhancements strengthen encryption keys, they come with a significant computational load, making them less suitable for processing large satellite images.

An implementation of chaos-AES combination was proposed to reduce the processing time and adhere to the time-sensitive requirements [8]. In this implementation, a correction strategy based on the properties of chaos theory is suggested to address the inherent limitations of the AES algorithm parameters [8]. Another efficient chaos-based encryption method was proposed to encrypt multispectral satellite images onboard Earth observation satellites [12]. The experimental results demonstrate that the proposed approach achieves a satisfactory level of security with minimal hardware complexity, power consumption, and computation time. However, the system may be susceptible to single event upsets (SEUs) induced by natural space radiation.

These encryption methods are inadequate for securing images onboard remote sensing satellites due to the avalanche effect, which is a crucial property in encryption where a small change in the input, such as a single bit, results in a significant change in the output. Furthermore, given that remote sensing satellites function within a challenging radiation environment, all onboard electronics, including encryption systems, are vulnerable to radiation-induced defects [26]. Consequently, there is a need for encryption techniques that achieve a compromise between computational efficiency, security strength, and suitability for encrypting large-scale satellite image data in a harsh radiation environment.

In this work, a novel encryption scheme, based on the use of chaos combined with an information scrambling process, is proposed to enhance the security level of AES. Firstly, the pixels of the various bands of the original satellite image undergo a meticulous scrambling operation. Subsequently, employing the 2D Standard map, the scrambled bands undergo the second step of encryption. Finally, the encryption process continues with the application of the AES algorithm based on the counter (CTR) mode. This method ensures comprehensive data security, demonstrating a structured and effective approach to safeguarding sensitive satellite imagery. Moreover, it achieves a balance between computational efficiency, security strength, and suitability for encrypting large-scale satellite image data within a harsh radiation environment.

The main contributions of this paper can be outlined as follows:

- We introduce a novel super-encryption technique that combines image scrambling, 2D standard map-based chaotic encryption, and CTR mode to bolster the security level of AES.
- We conduct a comprehensive performance evaluation and comparison of our proposed method against conventional image encryption approaches. Our findings demonstrate that the algorithm offers fast processing, high security, and robust resistance against brute-force, chosen and known plaintext, statistical, and differential attacks. The proposed algorithm is also tolerant to SEUs and transmission errors.

This paper is organized as follows: the theoretical principle of AES is presented in section 2, while the proposed technique is described in section 3. Detailed experimental results will be reported and discussed in section 4. Finally, a summary of the present work will be given in section 5.

2. BACKGROUND INFORMATION

2.1 AES description

Since the beginning of the 2000s, several chaotic encryption methods have been used to create confusion and diffusion properties for symmetric ciphers with the aim to ensure high level information security [27], [28]. Consequently, in an image encryption process, the confusion operation obscures pixel patterns within the image by randomly shuffling the positions of pixels. Therefore, the actual locations of those pixels are changed in the diffusion operation. Recently, the AES algorithm is strongly used as a symmetric key encryption standard. AES is also called “Rijndael algorithm” in reference to its designers Vincent Rijmen and Joan Daemen.

AES is a symmetric key block cipher, which encrypts information using an iteration process of transformation rounds called substitute bytes (SubBytes), shift rows (ShiftRows), mix columns (MixColumns) and add round key (AddRoundKey) [29]. Moreover, AES is a round-based encryption algorithm handling blocks of 128 bits and using keys of 128, 192 or 256 bits that set the number of rounds to 10, 12, or 14, respectively [7], [30] as shown in Figure 1. The block diagram of the AES encryption process is depicted in Figure 1(a), while Figure 1(b) represents the decryption process.

In an AES iteration process, we distinguish four transformations called layers where the round operation is the basic unit. Also, each round has a round key and transformation steps that generate data called States organized in 4×4 matrix of bytes array consisting of four rows and number of columns. In the encryption/decryption operations, the data and key blocks are processed through *Nr* rounds which are obtained from key size *K* of length *Nk.* On the other hand, let us note *Nc* the number of columns in a state matrix and which depends on the block size. Some variants of keys, blocks, and rounds are used and exhibited in Table 1.

Table 1. AES combinations [31]

AES type	Nk	Nc	Nr
128	4	4	10
192	6	4	12
256	8	4	14

AES operates such as a network of substitution and permutation where the four following basic transformations are performed as follows:

- SubBytes: In this transformation, each byte in a block is substituted by another from the substitution-box (S-box) according to a lookup table. A nonlinear substitution in the cipher is achieved using the S-box which is obtained from the chaotic map in Galois finite field GF(2^8) [32], [33].
- ShiftRows: In this step, the first row is unchanged and a circular permutation is applied to each of the last three block rows. Hence, each byte of a row is shifted to the left by one, two, and three for the second, the third and the fourth row, respectively.

- MixColumns: This transformation is a mixing operation which affects the columns where the four bytes of each column of the state are combined using a linear transformation.
- AddRoundKey: This step combines each byte of the state with the round key. For each round, a round key is generated from the initial key using the key schedule. The round key is added to each byte of the state by the eXclusive OR (XOR) function.

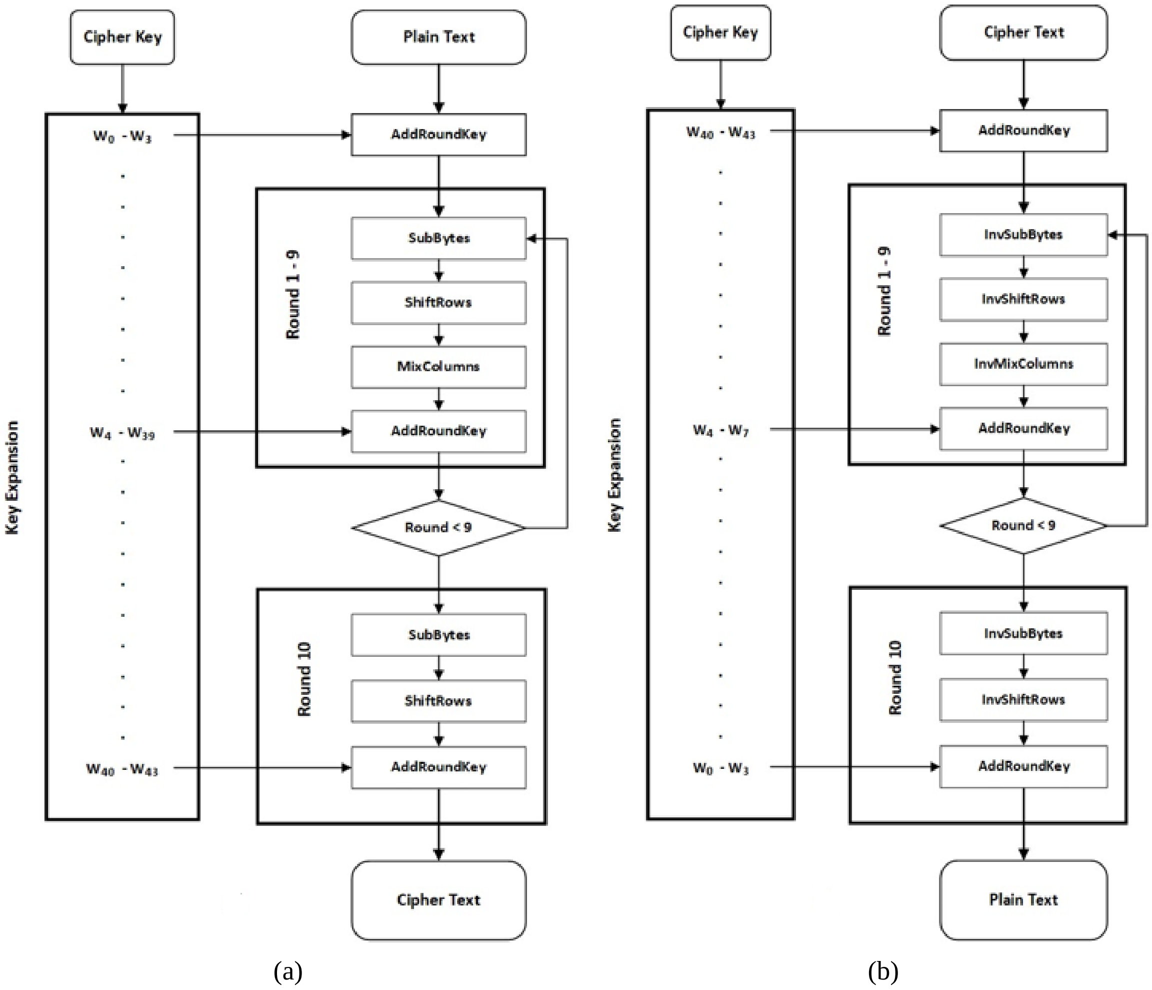


Figure 1. The architecture of AES (a) AES encryption process and (b) AES decryption process

Throughout the encryption process, data undergoes four transformations in each round, resulting in a substantial alteration of information. This property, known as the avalanche effect, significantly enhances the security of AES by ensuring that even a minor change in either the original image or the encryption key leads to about half of the image being modified. This effect causes slight modifications in pixel values to propagate and impact neighboring pixels and regions in a complex manner. However, in space applications where data storage and transmission are critical and often susceptible to various environmental factors such as radiation and electromagnetic interference, the avalanche effect can pose challenges. Bit upsets resulting from these factors can corrupt the original data, creating a noticeable difference between the original and decrypted images [13], [26]. Furthermore, AES is susceptible to cryptanalysis, including brute force attacks. Consequently, addressing these issues necessitates a more robust encryption technique that fulfills certain criteria for data confidentiality:

- Resilience against cryptanalysis by providing extremely high complexity through the simultaneous operations of image scrambling, chaotic encryption, and AES.
- Tolerance to SEUs by using the counter mode of AES to reduce error propagation during image encryption.

3. PROPOSED ALGORITHM

In this paper, inter and intra-band information scrambling is performed jointly with 2D standard map based chaotique encryption to improve the security level of satellite image encryption using AES. AES and 2D Standard map are used in the cryptosystem as very effective encryption mechanisms against computer attacks and data leakage. The detailed procedure and the block diagram of the proposed encryption algorithm are shown in Figure 2.

The proposed encryption process is carried out using the following steps:

Step 1: Perform inter and intra-band scrambling operation for the pixels of the different bands of the original satellite image.

Step 2: Encrypt the obtained scrambled bands using the 2D standard map.

Step 3: Utilize the AES-CTR algorithm to encrypt the acquired images.

The proposed encryption approach involves mixing pixels within and between bands of a satellite image to introduce confusion into the data. By dividing the clear image into layers and then manipulating the arrangement of pixels methodically, the algorithm aims to obscure the underlying information, making it harder for unauthorized users to decipher. Additionally, this encryption scheme utilizes a chaotic system based on the 2D standard map, which adds an extra layer of security. The chaotic behavior of the 2D Standard map system enhances the encryption process by introducing unpredictability and complexity. It helps in generating highly random sequences that are difficult to replicate, improving the resistance against various cryptographic attacks. Furthermore, to ensure robust security, the algorithm concludes with the application of AES-CTR encryption, a widely adopted and well-regarded encryption standard known for its strong cryptographic properties and widespread compatibility. The combination of inter- and intra-band pixel mixing, chaos based on the 2D standard map, and AES-CTR jointly contributes to establishing a robust and secure encryption mechanism.

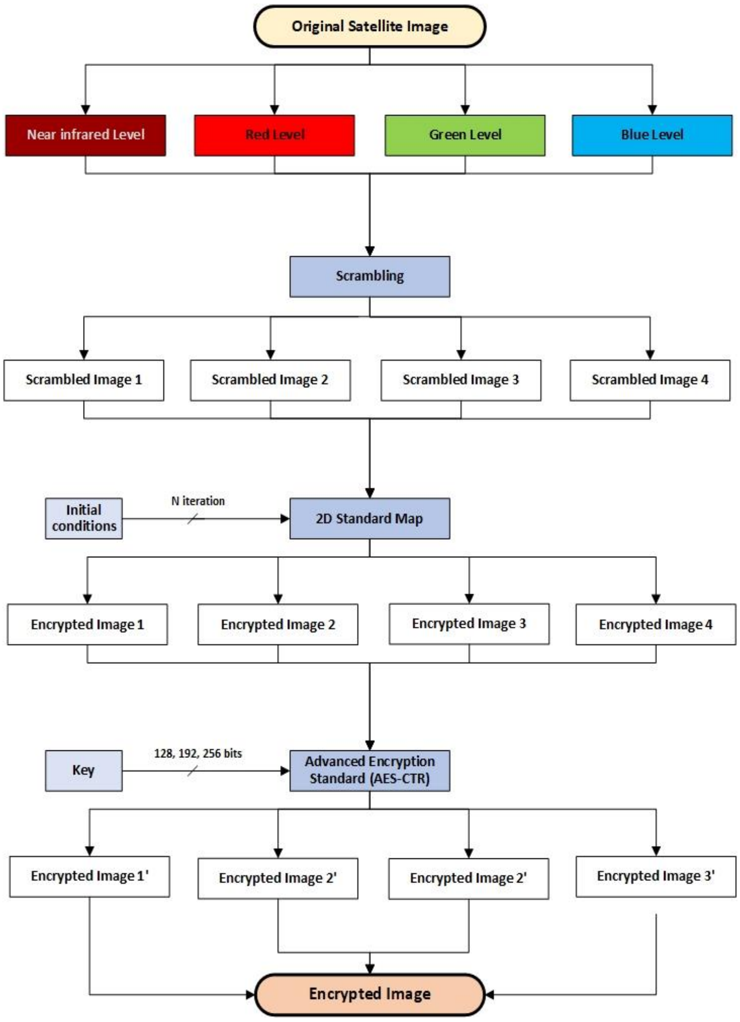


Figure 2. Flowchart of the proposed encryption algorithm

3.1. Step 1: Scrambling process

The initial encryption step in the proposed approach, prior to the application of the 2D standard map and AES, facilitates the mixing of pixels in a highly organized and rapid manner. This function transforms the different spectral bands of the plain image of size $[M \times N]$ to a vector of size $[M \times N \times P\ ]$, where P is the number of bands. Notably, this scrambling step enhances the confusion and diffusion properties of the overall encryption process. The pixels within these bands form the elements of the specified vector. Their positions are determined first by their chronological order. Subsequently, the order of the bands further organizes their placement. At the end of this process, the resulting vector will be transformed into P images of a size $[M \times N]$. Figure 3 shows an example of the principle of the scrambling process on an NRGB image of size [5×4]. The results of image scrambling are depicted in Figures 4(a)-(d), where Figure 4(a) and Figure 4(c) exhibit the original images. The effects of the scrambling process on these images are illustrated in Figure 4(b) and Figure 4(d), respectively.

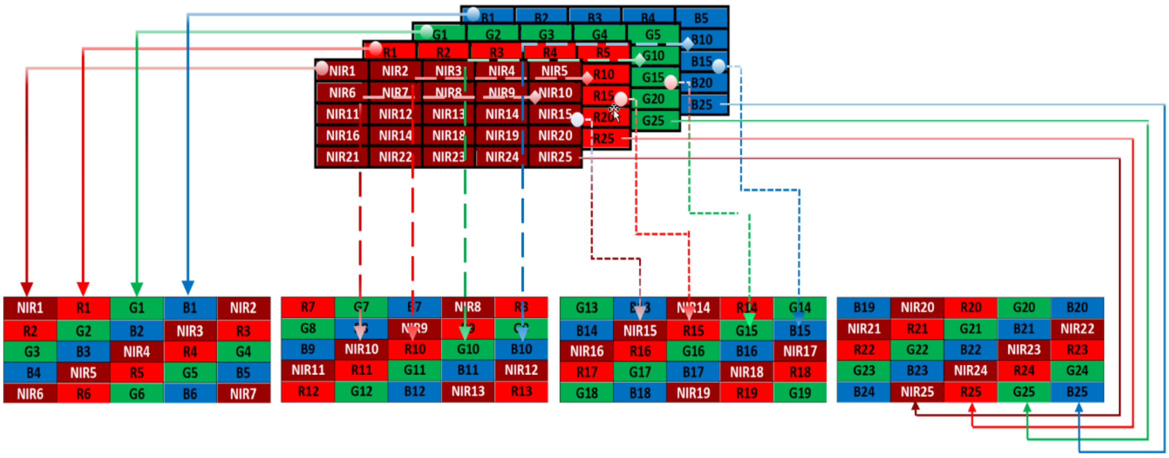
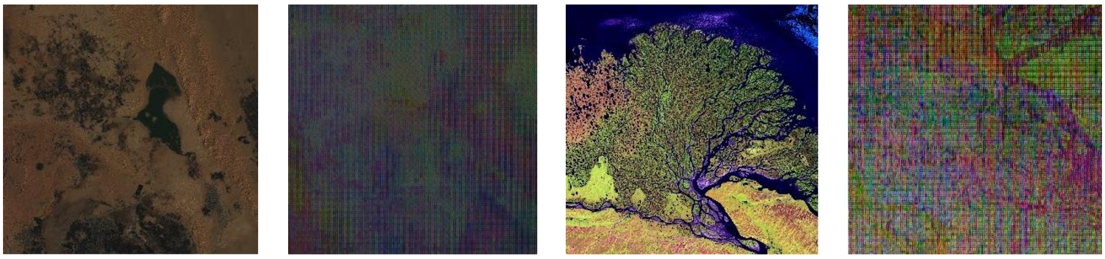


Figure 3. Example of NRGB image scrambling



(a) (b) (c) (d)

Figure 4. Results of the proposed scrambling process (a) Alsat-2 image of Ouargla (Algeria), (b) Alsat-2 image after applying the proposed scrambling process, (c) Lena Delta Reserve image, and (d) Lena Delta Reserve image after applying the proposed scrambling process

3.2. Step 2: Chaotic encryption of the scrambled bands

The 2D standard map can be utilized in image encryption as a chaotic mapping function to introduce randomness and complexity into the encryption process. It effectively disrupts pixel positions, enhancing security. This added complexity makes the encrypted image significantly different from the original.

The encryption process involves two key phases: permutation and diffusion.

- Permutation: During this phase, the image pixels undergo a random rearrangement. This step obscures the original pixel sequence in the encrypted image. Employing the 2D standard map function, which operates as a chaotic map, adds intricacy to this process. Chaotic maps are highly sensitive to initial conditions, making it challenging to predict their output even with known input. Consequently, reversing the permutation to recover the original image without the encryption key becomes exceedingly difficult.

- Diffusion: In this phase, pixel information is spread across the entire image, making individual pixel values indiscernible in the encrypted image. Utilizing the 2D standard map function, which serves as a nonlinear map, further complicates this stage. Nonlinear maps do not maintain original input-output relationships, making it difficult to deduce any single pixel's value solely from the encrypted image.

The combination of permutation and diffusion makes the 2D standard map function a secure and efficient way to encrypt images.

The 2D chaotic map known as the Standard map is defined as [34]:

$$\begin{bmatrix} x_{i+1} = \left(x_i + r_x + y_i + r_y\right) mod\, L \\ y_{i+1} = \left(y_i + r_y + K * sin \frac{{x_{i+1}}^N}{2\pi}\right) mod\, L \end{bmatrix} \tag{1}$$

where x_i and y_i represent the current positions in the phase space, and x_{i+1} and y_{i+1} represent the next positions after the map iteration. Parameter K is the strength of the nonlinearity of the system. For small values of K, the system exhibits regular motion, with periodic orbits that are confined to specific regions of the phase space. As K is increased, the orbits become more complex, and the system can manifest chaotic behavior, with trajectories that are sensitive to initial conditions. Note, r_x and r_y are two parameters that both vary from 0 to $L - 1$, and are used to shift the image in the horizontal and vertical directions [34]. Moreover, the parameter space of the 2D standard map exceeds that of the Cat map and Baker map, making it a favorable option for data encryption [34].

Within this section, the 2D standard map function is applied to the scrambled bands obtained after the application of the scrambling process. The encryption process involves specifying the desired number of rounds, denoted as n, and establishing the initial condition to initiate this operation. Each band obtained from the scrambling function must undergo this chaotic encryption process. Eventually, we obtain a set of P encrypted images, each with dimensions $[M \times N]$, as illustrated in Figure 2.

The application of the proposed chaotic map in this stage of image encryption can significantly enhance its security. This is because without knowledge of the precise control parameters and initial values, an unauthorized individual would be unable to predict the chaotic sequence generated by the system. In essence, the inherent chaotic behavior of this system introduces an additional security barrier, making it highly challenging for unauthorized parties to decipher encrypted images. Figure 5 shows the block diagram of the proposed chaotic image shuffling using the 2D standard map. Figures 6(a)-(d) illustrate the results of applying the proposed chaotic map to shuffle the scrambled images. Specifically, Figure 6(a) and Figure 6(c) exhibit the initial scrambled images, while Figure 6(b) and Figure 6(d) reveal the outcomes of encrypting these images using the chaotic 2D standard map, respectively.

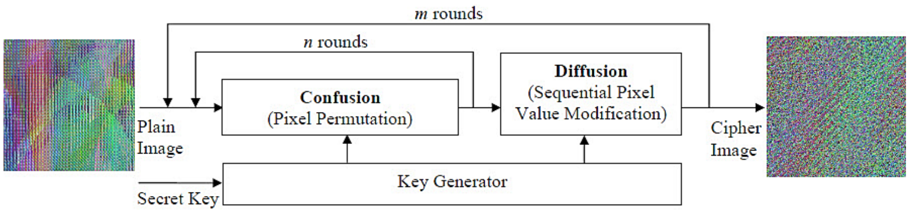
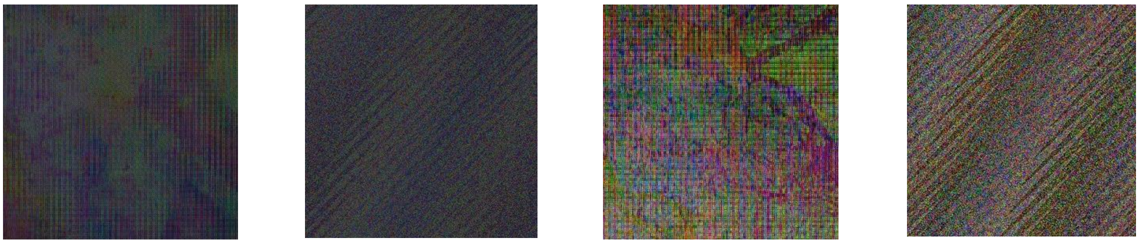


Figure 5. Block diagram of the proposed chaotic process based on 2D standard map



(a) (b) (c) (d)

Figure 6. Results of the application of chaotic encryption to two different images (a) Scrambled image of Alsat-2 image, (b) Alsat-2 image after 2D standard map function, (c) Scrambled image of Lena Delta Reserve, and (d) Lena Delta Reserve image after 2D standard map function

3.3. Step 3: AES-CTR encryption

AES in counter mode is a block cipher operation that utilizes a counter, initialized with a predetermined value, along with a nonce resembling the initial vector, to generate a key stream. The generated key stream is subsequently combined with the plaintext through an XOR operation to produce the ciphertext.

CTR mode has several advantages over other block cipher modes of operation. Firstly, it has the capability to overcome error propagation [21]. Secondly, it does not necessitate padding plaintext to match the block size of the cipher. Additionally, each plaintext block's encryption is independent of the encryption of previous blocks, enabling highly parallelizable architecture [21]. Overall, CTR mode is the preferred choice for block ciphers, offering efficiency, versatility, and high optimization for both hardware and software implementations across various platforms.

In the last stage of our proposed algorithm, an initial vector (IV) is concatenated with a 32-bit counter value to generate the keystream for encryption. This process uses AES encryption with a secret key of 256 bits. Each block of the keystream is fixed at a length of 256 bits. Figure 7 illustrates the principle of the CTR mode. It should be noted that the size of the generated keystream is equivalent to that of the original plain image. Afterward, images obtained through chaotic encryption will be processed through AES encryption using CTR mode and a single shared key, as depicted in the diagram presented in Figure 2. The final output of this encryption stage is a cipher image of size $[M \times N \times P]$ containing P bands. Figures 8(a)-(d) illustrates the results of the application of AES-CTR encryption on the shuffled images obtained from step 2 of the proposed encryption scheme. The original shuffled images are presented in Figures 8(a) and 8(c), whereas the final encrypted forms of these images are depicted in Figures 8(b) and 8(d).

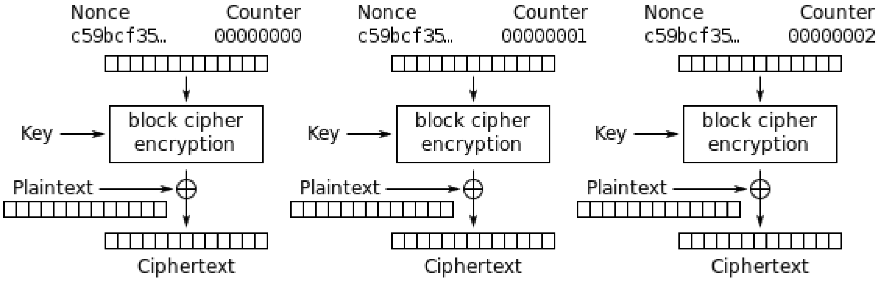


Figure 7. Counter (CTR) mode encryption

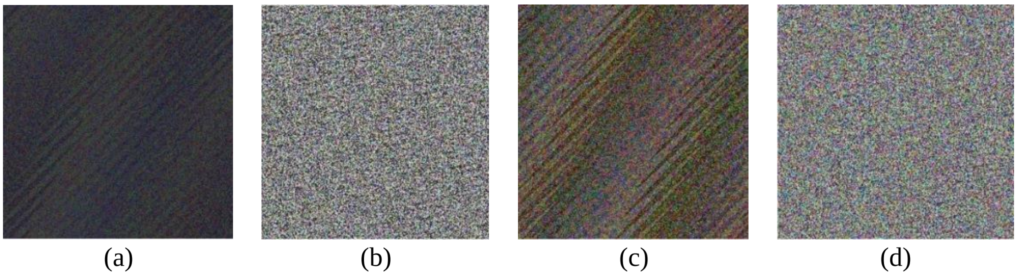


Figure 8. Results of the application of AES to two different images (a) ciphered Alsat-2 image, (b) Alsat-2 image after AES encryption, (c) ciphered Lena Delta Reserve image, (d) Lena Delta Reserve image after AES encryption

3.4. The decryption process

Given that the suggested encryption scheme is symmetric, the deciphering procedure utilizes an identical encryption key (chaos and AES key) and an IV to decrypt the ciphered image. Consequently, this results in the generation of an indistinguishable permutation key and keystream.

- At the beginning of the decryption process, AES is used in conjunction with a secret key to generate a keystream based on the same concatenated initial vector and counter value. The encrypted image needs to be fragmented into P images, and each image will undergo the standard AES decryption process using the confidential key.

- The next step involves a procedure that enables the restoration of the shuffled images obtained by utilizing the reverse of the disorderly permutation. Initially, the decryption process generates the key through 2D standard's mapping, incorporating the preselected count of iterations utilized during the encryption process, thereby initiating the decryption operation. The recipient merely requires the initial parameters and can obtain the corresponding encryption key using these values.
- In the third stage, the intermingled pixels across P images are subsequently reorganized based on their sequential orders, constructing the bands of the unencrypted image.
- Ultimately, the aforementioned P layers above are reassembled into a $[M \times N \times P]$ pixel array in sequence, and the resulting image is the decrypted image. The decryption of the ciphered image is completed.

The results of encrypting and decrypting different satellite images by using the proposed method are shown in Figures 9 to 11. On the left, Figure 9(a), Figure 10(a), and Figure 11(a) display three distinct original images. The central images, Figure 9(b), Figure 10(b), and Figure 11(b), present the encryption results obtained using the proposed algorithm. On the right, Figure 9(c), Figure 10(c), and Figure 11(c) illustrate the corresponding decryption results.

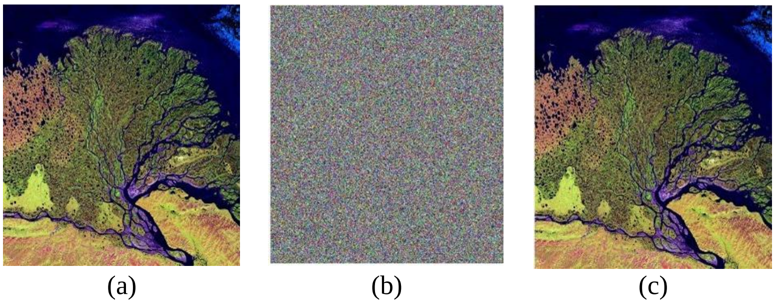


Figure 9. Lena Delta Reserve© USGS EROS Data Center-NASA (a) plain (original) RGB image, (b) encrypted image, and (c) decrypted RGB image

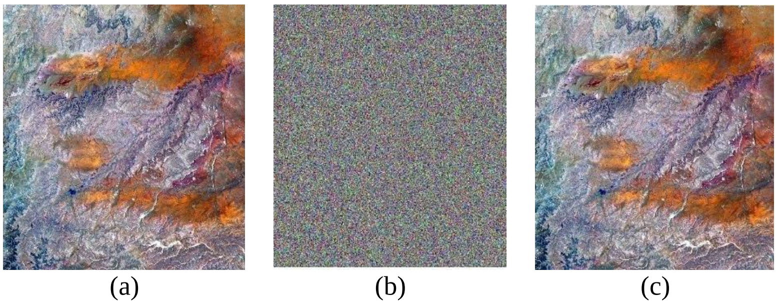


Figure 10. Sculpting a Basin, Iraq’s Ga’ara Depression, Landsat 8 - OLI © NASA (a) plain (original) RGB image, (b) encrypted image, and (c) decrypted RGB image

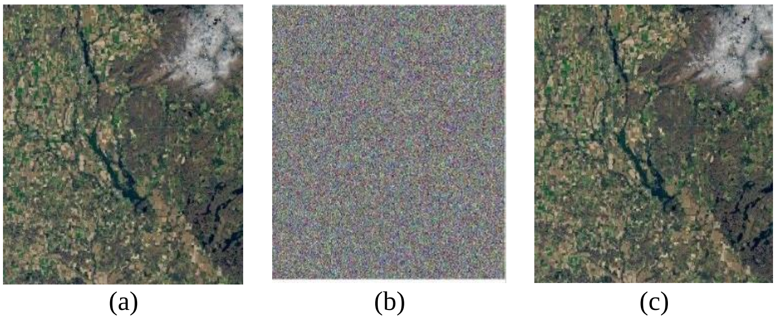


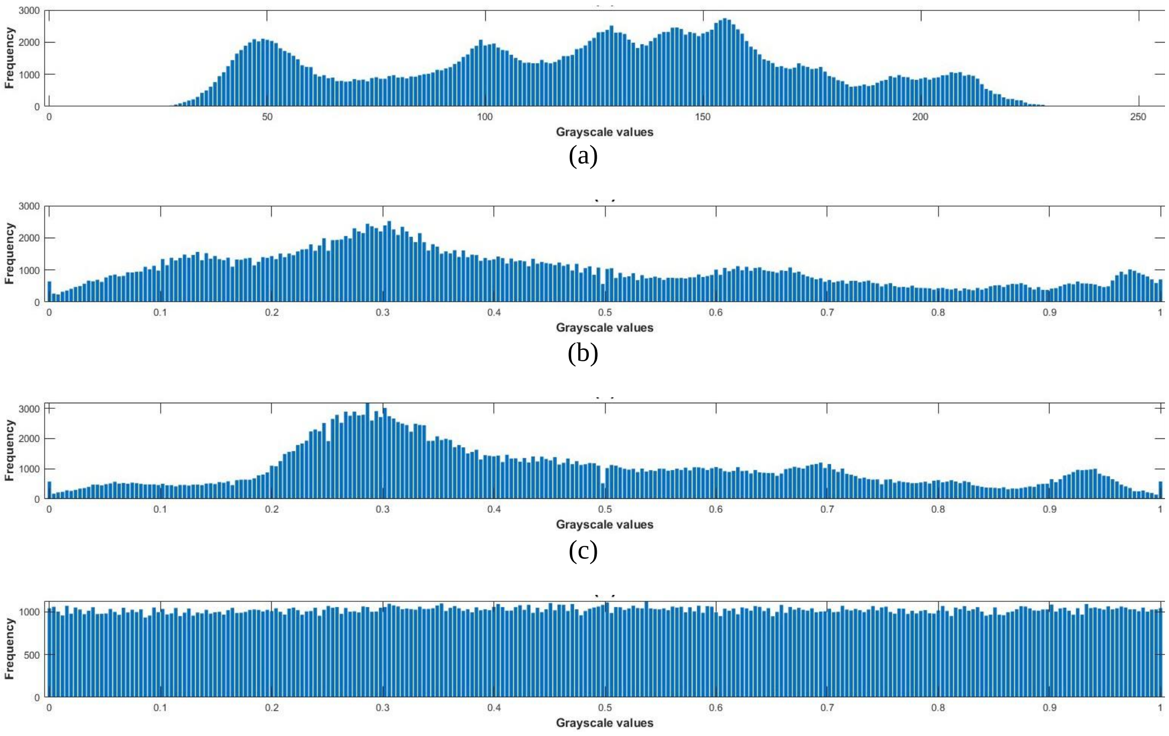
Figure 11. Sand Rush in Wisconsin © Landsat 8 - OLI_NASA (a) plain (original) RGB image, (b) encrypted image, and (c) decrypted RGB image

4. RESULTS AND DISCUSSION

The simulation tests were performed on a computer featuring an Intel® Core™ i7-5700HQ processor (Quad-Core 2.7 GHz) and 12 GB DDR3-RAM operating at 1600 MHz. The system was running Windows 10 (64-bit). The implementation was carried out using the MATLAB programming language. Tests were performed on various images, including "Lena image", and several satellite images "Lena Delta Reserve © USGS EROS Data Center-NASA", "Sculpting a Basin, Iraq's Ga'ara Depression, Landsat 8 - OLI © NASA", and "Sand Rush in Wisconsin © Landsat 8 - OLI_NASA", with sizes of 512×512, 3100×3100, 4627×4627, and 2848×2848, respectively.

4.1. Histogram analysis

Using the proposed algorithm, the histogram analysis was performed on several encrypted images as shown in Figure 12. The original image's histogram in Figure 12(a) serves as a baseline for comparison. Figure 12(b) illustrates the histogram after the initial scrambling step. Figure 12(c) shows the histogram after applying the 2D standard map. Finally, Figure 12(d) presents the histogram of the final encrypted image obtained after applying AES-CTR. As evident from the displayed figures the frequency distributions of the ciphered images exhibit a uniform characteristic. Therefore, the experimental results indicate that our proposed encryption process is well-suited to guarantee highly secure and reliable outcomes for satellite imagery. The uniform distribution of pixel values helps prevent statistical analysis and potential attacks.



(a)

(b)

(c)

(d)

Figure 12. Original image (Lena) and encrypted image histograms (a) Histogram of the original image, (b) Histogram of the scrambled image obtained after the application of the scrambling process (step 1), (c) Histogram of the encrypted image after the application of 2D standard map (step 2), and (d) Histogram of the final ciphered image using the proposed scheme (after applying AES-CTR)

4.2. Sensitivity analysis of the proposed algorithm

4.2.1. Differential attacks analysis

For image-based cryptosystems, security performance analysis should be carried out by optimizing two parameters: number of pixels change rate (NPCR) and unified average changing intensity (UACI), which are widely used to analyze the cipher's resistance to differential attacks [35]–[37]. NPCR refers to the percentage of pixels that change in the encrypted image when one pixel of the original (plain) image is modified. In contrast, UACI calculates the average difference in intensity between corresponding pixels in the plain and encrypted images. For a reliable cryptosystem against the known differential attacks, the recommended values of NPCR and UACI are typically as 99.61% and 33.46%, respectively [38].

To define NPCR and UACI, we consider ciphertext images as C_1 and C_2 with the same size, before and after a one-pixel change in a plaintext image, respectively. In this case, the pixel values at grid (i, j) are defined as $C_1(i, j)$ and $C_2(i, j)$ in C_1 and C_2, respectively. Thus, the corresponding bipolar array D can be calculated by (2).

$$D(i, j) = \begin{bmatrix} 0, if\ C_1(i, j) = C_2(i, j) \\ 1, if\ C_1(i, j) \neq C_2(i, j) \end{bmatrix} \tag{2}$$

NPCR can be computed using (3):

$$N(C_1, C_2) = \sum_{i,j} \frac{D(i,j)}{T} 100\% \tag{3}$$

where T indicates the total number of pixels in the ciphertext. On the other hand, UACI can be calculated using (4):

$$U(C_1, C_2) = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{F.T} 100\% \tag{4}$$

where F denotes represents the maximum pixel value compatible with the format of ciphertext image. The simulation of the previous (3) and (4) led to the test results which are summarized in Table 2.

In Table 2 we considered two encrypted images with the same key and a single bit change in the plaintext image. As shown in Table 2, the computed NPCR and UACI results closely approximate their respective theoretical values: 99.61% and 34.46%. These results confirm that the proposed image encryption algorithm has strong sensitivity to plain image changes and hence can resist differential attack analysis.

Table 2. NPCR and UACI results for plain image sensitivity

Image	NPCR	UACI
Lena	99.6306005859375	33.4561
Lena Delta Reserve	99.5147807617188	33.4276
Sculpting a Basin, Iraq’s Ga’ara Depression	99.5846606445313	33.4475
Sand Rush in Wisconsin	99.4925740699157	33.3958

4.2.2. Key sensitivity analysis

In cryptography, a good encryption algorithm should be highly sensitive to tiny modifications of the key to withstand an exhaustive attack. This sensitivity is typically examined through two aspects:

a. Encryption: a minor change of the key on the same input data should produce a different cipher image.

For this purpose, we have encrypted the four images mentioned before with two slightly different AES 256 keys (Key1 and Key2), then an evaluation of the NPCR and UACI parameters is made to assess the susceptibility of the proposed encryption approach to the key.

Key1 = [208 **231** 33 254 159 25 70 136 237 238 39 247 233 118 193 35 101 218 188 227 155 9 198 217 157 175 171 90 149 245 251 8]

Key2 = [208 **230** 33 254 159 25 70 136 237 238 39 247 233 118 193 35 101 218 188 227 155 9 198 217 157 175 171 90 149 245 251 8]

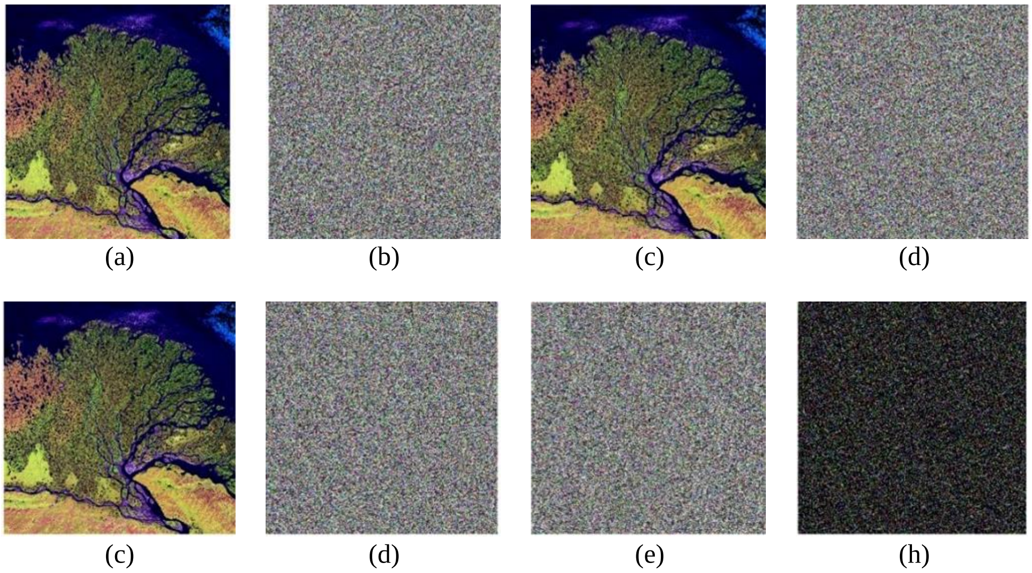
As shown in Table 3, the obtained results confirm NPCR and UACI values are close to 99.60% and 33.46%.

b. Decryption: any non-compliance with the encryption and decryption keys inevitably results in failure within the cryptographic system, leading to obscured deciphered images.

To check this aspect, we applied our algorithm using the same keys to encrypt the Lena Delta Reserve. The plain image of Figure 13(a) was first encrypted with Key1, resulting in the ciphered image shown in Figure 13(b). Subsequently, the ciphered image was decrypted using Key1, and the obtained decrypted image is shown in Figure 13(c). Next, we further encrypted the plain image with the second key (Key2). The resulting ciphered image is shown in Figure 13(d). We then used Key2 to decrypt the second ciphered image in Figure 13(d), resulting in the decrypted image shown in Figure 13(e). Similarly, this decrypted image resembles the original plain image. However, decrypting the images leads to different images from the plain image if the initial encryption key differs from the decryption key. Figures 13(f) and 13(g) show the deciphered images of image Figures 13(b) and 13(d) by using Key2 and Key1, respectively. These images confirm that the original information can only be restored with the correct key, highlighting the proposed method's extreme sensitivity to any slight key variation.

Table 3. NPCR and UACI results for key sensitivity

Image	NPCR	UACI
Lena	99.6106005859375	33.4216
Lena Delta Reserve	99.6000807617188	33.4578
Sculpting a Basin, Iraq’s Ga’ara Depression	99.4146606445313	33.3862
Sand Rush in Wisconsin	99.5355740699157	33.4126



(a) (b) (c) (d)

(c) (d) (e) (h)

Figure 13. Key sensitivity analysis: (a) the original Lena Delta Reserve image, (b) the encrypted image using key1, (c) the decrypted image from (b) using key1, (d) the encrypted image using key2, (e) the decrypted image from (d) using key2, (f) the decrypted image from (b) using key2, (g) the decrypted image from (d) using key1 (h) the difference image between (b) and (d)

4.2.3. Key space analysis

The size of the key space needs to be adequately extensive to withstand brute-force attacks. In the proposed encryption scheme, the secret keys encompass the AES key, which possesses a key space of 2^{256}, alongside the scrambling and chaos keys. The initial and control parameters of the used 2D standard map K, x_0, y_0, r_x and r_y constitute the chaos key. Since the parameters r_x and r_y vary from 0 to $L-1$, then each one has L possible values. L represents the highest intensity level (e.g.: $L = 255$ if the image pixels are coded using 8 bits and $L = 1023$ if the number of coding bits is 10). For the case of 8-bit coding, the two parameters r_x and r_y have 256 possible values each and the key space for these two parameters is $256 \times 256 = 2^{16}$. In this case, the computer's processing precision is set to 10^{-15} and the size of parameters K, x_0, y_0 is 52 bits. Consequently, the total key space for the chaotic system's parameters becomes $2^{16} \times 2^{52} \times 2^{52} \times 2^{52} = 2^{172}$.

The total key space of the proposed algorithm is $2^{256} \times 2^{172} = 2^{428}$, which largely exceeds 2^{100}. This vast key space provides robust protection against brute-force attacks. Accordingly, it ensures a high level of security.

4.3. Correlation coefficients analysis

In cryptography, correlation coefficient analysis [39] is a conventional technique for assessing similarity or dissimilarity between the original and encrypted images. The proposed image encryption scheme is assessed using the correlation coefficient between random variables x and y. Considering adjacent pixel values x and y as random variables, correlation coefficients are computed as (5):

$$r = \frac{cov(x,y)}{\sqrt{D(x).D(y)}} \tag{5}$$

where r is correlation coefficient; x, y is intensity values of chosen adjacent pixels; $cov(x, y)$ is covariance of x, y; $D(x)$ is variance of x; and $D(y)$ is variance of y.

Both $cov(x, y)$, $D(x)$ and $D(y)$ are calculated using their respective expressions as (6)-(8):

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \tag{6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \tag{7}$$

$$D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E(y))^2 \tag{8}$$

where N is number of adjacent pixel pairs in the plain and encrypted images. x_i and y_i are mathematically considered as two series with their corresponding means $E(x)$ and $E(y)$, respectively and expressed by (9) and (10):

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{9}$$

$$E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{10}$$

To check the correlation (horizontally, vertically, diagonally, and anti-diagonally) between the adjacent pixels of the plain image and those of the ciphered image, the correlation coefficients are determined utilizing (5), and the obtained results are summarized in Table 4. To accomplish this, we used four images as input: Lena, Lena Delta, Sculpting a Basin, Iraq's Ga'ara Depression, and Sand Rush in Wisconsin. Each image was subjected to three encryption experiments: using only the 2D standard map, using only AES, and lastly, employing our algorithm.

Table 4. Correlation coefficients of pixels in plain and cipher images

Images	Test	Algorithms	Correlation coefficient				
			Horizontal	Vertical	Diagonal	Anti-diagonal	Average
Lena	T_1	2D STD Map	0.001920	0.002099	0.002036	0.001176	0.001808
		AES-CTR	0.000776	0.001139	0.000581	0.007882	0.002594
		Proposed	**0.000068**	**0.000076**	**0.000181**	**0.000031**	**0.000243**
Lena Delta Reserve	T_1	2D STD Map	0.62791	0.62951	0.56136	0.87726	0.67401
		AES-CTR	**0.0004757**	0.021568	**0.0009027**	0.010358	0.0083261
		Proposed	0.0027112	**0.0006647**	0.0013403	**0.002285**	**0.0017503**
	T_2	2D STD Map	0.004309	0.0006207	0.001702	**0.000106**	0.001684
		AES-CTR	0.005022	0.0075562	0.003430	0.018989	0.008749
		Proposed	**0.001204**	**0.0001255**	**0.000383**	0.002866	**0.001144**
	T_3	2D STD Map	0.0039604	**0.0006230**	**5.3009e-05**	**0.0014537**	**0.0015225**
		AES-CTR	**0.0008493**	0.011719	0.0033124	0.01409	0.0074929
		Proposed	0.0046167	0.0019267	0.0010631	0.0032056	0.0027030
Sculpting a Basin, Iraq	T_1	2D STD Map	0.45591	0.45847	0.37094	0.83265	0.52949
		AES-CTR	0.017314	0.010482	0.0089327	0.0006947	0.009355
		Proposed	**0.0019682**	**0.0013057**	**0.0005234**	**1.1165e-05**	**0.000952**
	T_2	2D STD Map	0.0034801	0.0033211	0.012286	0.024194	0.01082
		AES-CTR	0.0131426	0.011949	**0.0073954**	0.0010647	0.008387
		Proposed	**0.0001748**	**0.0015572**	0.0084658	**0.0004967**	**0.002673**
	T_3	2D STD Map	0.0019221	0.0021067	**0.0007294**	0.0034544	**0.0020531**
		AES-CTR	0.0047796	0.0033896	0.0043567	0.014266	0.0066979
		Proposed	**0.0007446**	**0.0008999**	0.0013427	**0.0026373**	**0.0014061**
Sand Rush in Wisconsin	T_1	2D STD Map	0.30559	0.30918	0.2209	0.83094	0.41665
		AES-CTR	0.0095929	0.016175	0.029382	0.012609	0.01694
		Proposed	**0.0015861**	**0.011554**	**0.013131**	**0.0075847**	**0.0084641**
		2D STD Map	**0.0013397**	0.0028617	**0.0011548**	0.0078261	0.0032956
	T_2	AES-CTR	0.001792	0.0068657	0.0083733	0.0076681	0.0061748
		Proposed	0.004062	**0.0019855**	0.0058628	**0.0003535**	**0.0030659**
		2D STD Map	0.0054668	0.0004256	**0.0033708**	0.006466	0.0039323
	T_3	AES-CTR	0.0050823	0.0080286	0.018492	0.01273	0.011083
		Proposed	**0.0007681**	**1.3632e-05**	0.0055312	**0.0026489**	**0.0022404**

Note: T1: test with 5 iterations of 2D standard map; T2: test with 10 iterations of 2D standard map; T3: test with 20 iterations of 2D standard map; bold value represents the best result for each test; gray cell represents the best image result for all tests

Table 4 presents the statistical findings of the correlation coefficients for each image component. The outcomes reveal that the correlation coefficients for the encrypted images tend to approach 0, indicating the effectiveness of the encryption technique in reducing pixel correlation compared to using chaotic encryption or AES alone. Around 30% of the cipher images exhibit absolute correlation coefficients below 0.0005. Additionally, the ciphered test images demonstrate a minimum correlation value of 1.1165×10^{-5}.

Besides, to better visualize the change in correlation before and after encryption, a random selection of 10,000 adjacent pixel pairs was extracted from the ciphered image in all directions. Correlation distribution charts were then plotted for the original image and its encrypted versions along the horizontal, vertical, diagonal, and anti-diagonal directions. Figure 14 shows the correlation distribution of adjacent pixels. The columns from left to right show the input image and the ciphered images after each step of the proposed encryption namely Scrambling, 2D STD map, and AES, respectively.

By comparing the scatter plots of the plain and encrypted images, we observe a clear linear correlation in all directions between adjacent pixels in the original image. However, in the final encrypted image, the pixels are uniformly distributed and exhibit minimal correlation. This means that the pixel correlation in each direction has been almost completely eliminated.

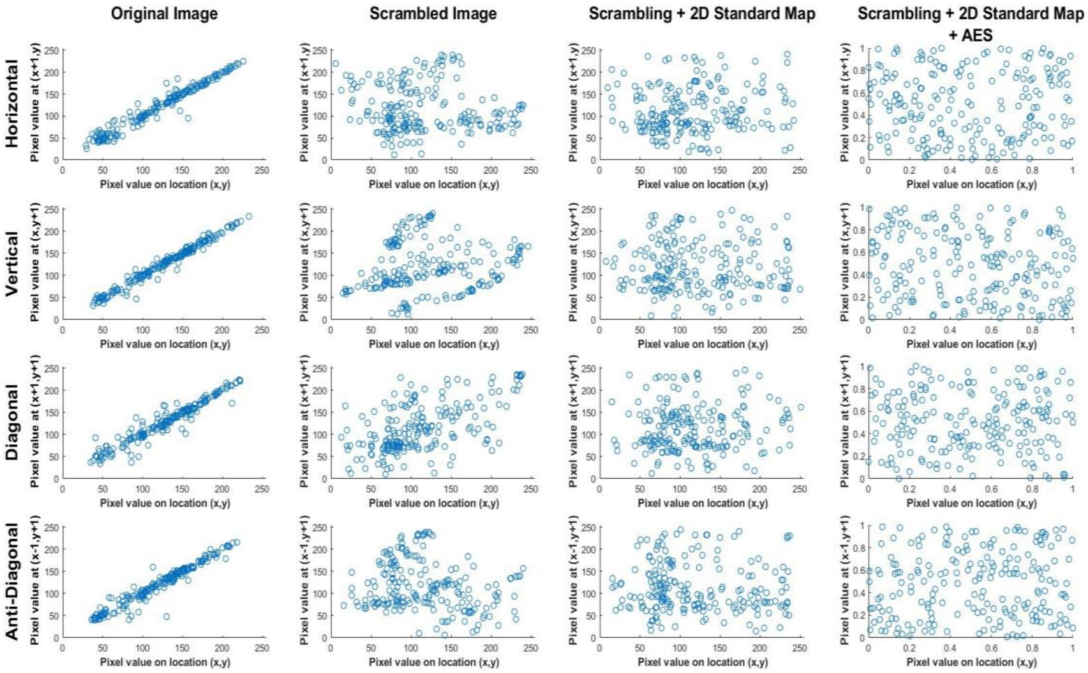


Figure 14. Pixel correlation distribution charts

4.4. The ability to withstand radiation-induced upsets and transmission errors

For satellite computer systems operating in harsh radiation environments, it is crucial to analyze the capability of the proposed algorithm to resist transmission errors and radiation-induced upsets. Radiation-induced errors, known as SEUs, primarily manifest as bit flips in satellite onboard computers. Additionally, satellite images are prone to transmission errors during their transfer to ground stations. Hence, it is imperative for the encryption algorithm utilized onboard to be resilient against both radiation-induced upsets and transmission errors [13], [26]. A proposed solution to mitigate data corruption due to SEUs and transmission errors involves combining the Hamming error detection and correction code with AES encryption [26]. This combined cryptosystem can identify and rectify double faults and single faults injected during data encryption. Understanding error propagation, in succeeding blocks affected by single-bit errors during encryption and transmission, is pivotal in selecting the appropriate fault detection and correction technique.

Thankfully, the proposed encryption scheme employing the AES-CTR mode meets this criterion effectively. In the event of a single SEU occurring during image scrambling or chaotic encryption, only one pixel of the entire image is affected, without propagating errors to other pixels. Within the AES-CTR encryption process, a single-bit error (SEU) occurring during keystream generation will only corrupt the corresponding ciphertext block (256 bits) upon decryption, with no errors spreading to subsequent blocks. This characteristic holds during transmission as well. A single-bit error affecting a pixel within a ciphertext block will only impact the corresponding decrypted pixel, with no error propagation to other pixels. The effect of error propagation and SEUs during transmission is demonstrated in Table 5. NPCR and UACI between two encrypted multispectral images are utilized to assess these impacts.

To analyze the impact of SEUs on AES encryption, a plain multispectral image of Alsat-2 is used along with two keystreams. One keystream is generated using a specific key and initialization vector (IV), while the other is intentionally altered by one bit at a random position to simulate an SEU occurring during keystream generation. These keystreams are subsequently utilized to generate two encrypted images, and the UACI and NPCR between the resulting ciphertext images are examined to determine the extent of changes. The impact of SEUs during image scrambling and chaotic encryption has been verified by injecting a random error during each process to generate a corrupted cipher image. Similarly, to evaluate the effects of transmission errors, the plain image is encrypted using the identical secret key and initialization vector (IV). Assuming a bit error rate of 10^{-6} for a typical low Earth orbit satellite transmission, errors (bit flips) are then injected at random pixel positions to produce the erroneous cipher image. The NPCR and UACI between the cipher images, obtained before and after error injection, are compared to assess transmission errors' impact as well as the effect of SEUs on the processes of image scrambling and chaotic encryption. The obtained UACI and NPCR values in Table 5 affirm that the encrypted images exhibit minimal differences, with SEUs affecting only one data block (26 pixels), and transmission errors do not propagate to the other image pixels. A total number of 13 pixels could be affected during the transmission of the Alsat-2 image multispectral image (4 bands of 1750×1750 pixels, each). Thus, the proposed encryption scheme demonstrates resilience against error propagation caused by SEUs and transmission errors.

Table 5. Effects of SEUs and transmission errors on Alsat-2 multispectral image (4 bands of 1750×1750 pixels, each)

Error Category		Number of affected pixels	NPCR	UACI
SEUs	Scrambling	1	8.16e-6	7.98e-8
	2D Standard Map	2	1.63e-5	6.38e-7
	AES-CTR	26	2.12e-4	2.65e-5
Transmission errors		13	1.06e-4	3.46e-6

4.5. Entropy

Usually, entropy is a measure of the randomness of a value as described in the literature [39], [40]. In information cryptosystems, entropy is used to quantify the amount of information contained in an image, usually in bits or bits/symbol. The entropy denoted by $H(m)$ of an image can be calculated using the following relation [41]:

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i)\, log_2\big(P(m_i)\big) \tag{11}$$

where $P(m_i)$ represents the probability of symbol m_i.

Ideally, for an 8-bit random image emitting 2^8 symbols with equal probability, H achieves its maximum value of 8. Thus, for encrypted satellite images, information entropy should be equal to the ideal value 8. The calculated information entropies are listed in Table 6. As demonstrated in Table 6, the computed information entropies of encrypted images are almost equal to the ideal value of 8. Therefore, the suggested method for image encryption is effective against the analysis based on information entropy.

Table 6. The calculated information entropies

Image	Original Image	Scrambling	Scrambling + 2D Standard Map	Encrypted image using proposed scheme
Lena	7.0087381088	7.4524782524	7.9684189808	7.9994867985
Lena Delta Reserve	7.0522700926	7.6002563699	7.9734236973	7.9997410604
Sculpting a Basin, Iraq	7.1239736813	7.4470071897	7.9682244176	7.9990379651
Sand Rush in Wisconsin	7.0454760535	7.5696391447	7.9750892917	7.9992744103

4.6. Time analysis

The execution speed is an essential parameter to evaluate the performance of an image encryption algorithm. For this reason, we analyzed the computation time of the encryption/decryption process. This analysis is based on the results presented in Table 7.

Table 7. Computation times of encryption/decryption algorithm

Image	Encryption process				Decryption process				All the process time (s)
	Scrambling	2D STD	AES	Total	Scrambling	2D STD	AES	Total	
Lena	0.0921	0.0921	19.973	20.1572	0.09528	0.0918	19.9889	20.1759	40.3331
Lena Delta	0.07944	0.0964	20.7857	20.9615	0.07808	0.0908	20.6357	20.8045	41.7661
Sand Rush	0.07929	0.0932	20.6325	20.8049	0.07299	0.0957	20.6547	20.8233	41.6283

4.7. Performance comparison and discussion

To assess the efficiency of the suggested encryption algorithm, a comprehensive comparison was carried out with various techniques, as depicted in Table 8. In order to substantiate this comparison, rigorous cryptographic assessment techniques, such as correlation coefficients, information entropy, NPCR, and UACI were meticulously employed to analyze a [512×512] Lena image. These metrics serve as reliable benchmarks for evaluating and contrasting the effectiveness of the proposed algorithm against other existing methods.

The analysis of correlation coefficients in Table 8 demonstrates the proposed algorithm's effectiveness. It consistently achieves the lowest and better correlation coefficient values across all axes, outperforming all listed references (horizontal, vertical and diagonal), indicating a significant reduction in correlation between neighboring pixels in the cipher image approaching almost zero. This demonstrates the algorithm's excellent performance against known attacks and its ability to eliminate the high correlation among pixels in the original image.

Additionally, the results indicate that the proposed algorithm's information entropy closely approximates the theoretical value of 8. The proposed scheme has the third highest entropy value among all the algorithms listed in Table 8 and reveals a more favorable random performance when compared to references [42]–[49]. This means that the proposed algorithm has stronger security and produces more random encrypted images, which makes it more difficult to attack the encrypted image using statistical methods.

Table 8. Performance comparison of the proposed algorithm vs. literature

Techniques		Correlation coefficient				NPCR	UACI	Entropy
	Algorithms	Horizontal	Vertical	Diagonal	Average			
1999	AES	0.001516	0.002648	0.006318	0.003494	99.55	33.41	7.9982
	Proposed T1	**0.000068**	0.000076	0.000181	0.0001083	99.61	33.41	7.9993
	Proposed T2	0.000094	**0.000001**	0.000221	**0.0001053**	99.59	33.55	7.9992
	Proposed T3	0.000745	**0.000001**	**0.000027**	0.0002576	99.63	33.42	7.9968
	Proposed T4	0.000121	0.000133	0.000076	0.00011	99.60	33.43	7.9981
2023	[49]	NA	NA	NA	0.0004	99.61	33.45	7.9994
	[50]	-0.00020	-0.00045	-0.00474	0,001796	99.63	33.03	7.9985
	[51]	0.00311	0.00266	-0.00188	0.00255	100	50.20	7.7043
	[42]	-0.0003	-0.0037	0.0020	0.002	99.64	33.49	7.9972
	[43]	0.0033	0.007	0.0027	0.004333	99.61	33.44	7.9991
	[45]	0.0019	0.0035	0.0008	0.002066	99.62	**33.46**	7.9959
2022	[52]	-0.00084	-0.0047	0.00008	0.001873	99.60	**33.46**	7.9993
	[53]	0.00182	0.00193	0.0023	0.002016	99.61	33.48	7.9993
	[54]	-0.0018	0.0001	0.0005	0.0008	99.61	33.45	7.9968
	[55]	NA	NA	NA	0.0003	99.61	33.48	NA
	[44]	-0.0059	-0.0064	0.0003	0.0042	99.62	33.04	7.997
2021	[56]	0.0004	0.0019	0.0012	0.001166	99.62	33.52	**7.9996**
	[57]	-0.0076	0.0004	0.0019	-0.001766	99.64	33.43	7.9993
2020	[58]	-0.00013	-0.00125	-0.00088	-0.000760	NA	NA	NA
2019	[24]	0.0027	0.0012	0.00031	0.001403	99.63	33.47	7.9974
	[13]	0.0004	0.0005	0.0003	0.0004	99.61	33.48	7.9994
2018	[59]	-0.0016	0.0012	0.0105	0.004433	99.62	**33.46**	NA
	[60]	0.0041	0.0031	0.0019	0.00303	99.62	33.48	7.9993
	[61]	-0.0045	-0.0001	0.0053	0.0033	99.59	33.42	7.9993
2017	[46]	-0.0042	0.0005	-0.0036	0.002766	99.61	33.49	7.9992
	[47]	-0.0230	0.0019	-0.0034	0.009433	99.62	33.51	7.9974
	[62]	0.001801	0.004798	0.002753	0.003117	NA	NA	NA
2015	[48]	0.0020	-0.0007	-0.0014	0.001366	99.65	33.48	7.9970

Note: N.A: not available; T1: test with 5 iterations of 2D standard map; T2: test with 10 iterations of 2D standard map; T3: test with 20 iterations of 2D standard map; T4: test with 30 iterations of 2D standard map; bold value represents the best result

Furthermore, to ensure a rigorous assessment, this study employs stringent methodology. A test image is selected, and a single pixel is randomly chosen for modification, specifically altering its least significant digit. This process is repeated multiple times, with iterations of 5, 10, 20, and 30 for the 2D Standard map function. Subsequently, the resulting encryption outputs are used to calculate NPCR and UACI values. The average values derived from these repeated tests are shown in Table 8. Regarding the NPCR parameter, our scheme attains the second highest average value, closely approaching 99.6184%. In the same context, through a comparative analysis with the anticipated results of other studies, it is validated that the proposed algorithm outperforms the majority of methods in terms of both the theoretical and the mean value of UACI, showcasing its superior performance exhibiting the capacity to deliver sufficient security, even in the face of intense differential attacks.

5. CONCLUSION

In this paper, a refined encryption algorithm based on the combination of the 2D Standard Map and AES with a scrambling process is proposed with the aim of securing confidential data in satellite imagery. The proposed algorithm was successfully implemented, and detailed experimental results were presented and discussed to perform security performance analysis. The combination of image scrambling and chaotic encryption has been utilized to enhance the security of the cryptosystem while retaining the benefits of the AES-CTR mode. Security assessments indicate that the proposed approach offers a broader key space and increased sensitivity to the secret key. Experimental findings demonstrate that the proposed algorithm outperforms both the classical AES-CTR and certain recent chaotic cryptosystems in performance. In fact, improved scrambling has been attained with a notable increase in execution speed. Additionally, the proposed scheme exhibits robustness against SEUs and transmission errors. Also, the experimental results show that the proposed cryptosystem can resist differential, statistical, and plain image attacks. Thus, the proposed approach is indeed suitable to ensure highly secure and reliable results for satellite imagery.

ACKNOWLEDGEMENTS

The authors are thankful to the entire research team of the laboratory “Communication Networks, Architecture and Multimedia Laboratory (RCAM), Department of Electronics, Djillali Liabes University, Sidi Bel Abbes, Algeria”. This work was supported by the Algerian Directorate General for Scientific Research and Technological Development (DGRSDT).

REFERENCES

[1] R. A. Williamson, “Remote sensing and transportation security,” *Space Policy*, 2002.

[2] D. Chen, D. Qing, and D. Wang, “AES key expansion algorithm based on 2D logistic mapping,” in *2012 Fifth International Workshop on Chaos-fractals Theories and Applications*, Oct. 2012, pp. 207–211, doi: 10.1109/IWCFTA.2012.81.

[3] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004, doi: 10.1016/j.chaos.2003.12.022.

[4] Y. Q. Zhang and X. Y. Wang, “A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice,” *Information Sciences*, vol. 273, pp. 329–351, Jul. 2014, doi: 10.1016/j.ins.2014.02.156.

[5] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, May 2014, doi: 10.1016/j.optlaseng.2013.12.003.

[6] N. Sklavos, “Book review: stallings, W. cryptography and network security: principles and practice,” *Information Security Journal: A Global Perspective*, vol. 23, no. 1–2, pp. 49–50, Jan. 2014, doi: 10.1080/19393555.2014.900834.

[7] M. J. Dworkin *et al.*, “Advanced encryption standard (AES),” Federal Information Processing Standards (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, May 2023. doi: 10.6028/NIST.FIPS.197-upd1.

[8] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, “Image encryption techniques: a comprehensive review,” *Multimedia Tools and Applications*, Jan. 2024, doi: 10.1007/s11042-023-17896-0.

[9] S. Liu, C. Guo, and J. T. Sheridan, “A review of optical image encryption techniques,” *Optics and Laser Technology*, vol. 57, pp. 327–342, Apr. 2014, doi: 10.1016/j.optlastec.2013.05.023.

[10] B. Zhang and L. Liu, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” *Mathematics*, vol. 11, no. 11, Jun. 2023, doi: 10.3390/math11112585.

[11] L. Gupta, P. Jaiswal, I. Lather, R. Agarwal, and A. Thakur, “Image encryption using chaotic maps: state of the art,” *2023 3rd International Conference on Intelligent Technologies (CONIT)*, Hubli, India, 2023, pp. 1-8, doi: 10.1109/CONIT59222.2023.10205829.

[12] E. H. Bensikaddour, Y. Bentoutou, and N. Taleb, “Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher,” *Journal of King Saud University - Computer and Information Sciences*, vol. 32, no. 1, pp. 50–56, Jan. 2020, doi: 10.1016/j.jksuci.2018.05.002.

[13] Y. Bentoutou, E. H. Bensikaddour, N. Taleb, and N. Bounoua, “An improved image encryption algorithm for satellite applications,” *Advances in Space Research*, vol. 66, no. 1, pp. 176–192, Jul. 2020, doi: 10.1016/j.asr.2019.09.027.

[14] Z. Hua, B. Zhou, and Y. Zhou, “Sine-transform-based chaotic system with FPGA implementation,” *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2557–2566, Mar. 2018, doi: 10.1109/TIE.2017.2736515.

[15] A. A. Arab, M. J. B. Rostami, and B. Ghavami, “An image encryption algorithm using the combination of chaotic maps,” *Optik*, vol. 261, Jul. 2022, doi: 10.1016/j.ijleo.2022.169122.

[16] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, “An image encryption algorithm based on compound homogeneous hyper-chaotic system,” *Nonlinear Dynamics*, vol. 89, no. 1, pp. 61–79, Mar. 2017, doi: 10.1007/s11071-017-3436-y.

[17] J. Zheng and Q. Zeng, “An image encryption algorithm using a dynamic S-box and chaotic maps,” *Applied Intelligence*, vol. 52, no. 13, pp. 15703–15717, Mar. 2022, doi: 10.1007/s10489-022-03174-3.

[18] C.-H. Lin, G.-H. Hu, C.-Y. Chan, and J.-J. Yan, “Chaos-based synchronized dynamic keys and their application to image encryption with an improved AES algorithm,” *Applied Sciences*, vol. 11, no. 3, Feb. 2021, doi: 10.3390/app11031329.

[19] D. E. Goumidi and F. Hachouf, “Modified confusion-diffusion based satellite image cipher using chaotic standard, logistic and sine maps,” in *2010 2nd European Workshop on Visual Information Processing (EUVIP)*, Jul. 2010, pp. 204–209, doi: 10.1109/EUVIP.2010.5699118.

[20] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, “Chaos-based secure satellite imagery cryptosystem,” *Computers and Mathematics with Applications*, vol. 60, no. 2, pp. 326–337, Jul. 2010, doi: 10.1016/j.camwa.2009.12.033.

[21] E.-H. Bensikaddour, Y. Bentoutou, and N. Taleb, “Satellite image encryption method based on AES-CTR algorithm and GEFFE generator,” in *2017 8th International Conference on Recent Advances in Space Technologies (RAST)*, Jun. 2017, pp. 247–252, doi: 10.1109/RAST.2017.8002953.

[22] F. T. B. Muhaya, “Chaotic and AES cryptosystem for satellite imagery,” *Telecommunication Systems*, vol. 52, no. 2, pp. 573–581, Jun. 2013, doi: 10.1007/s11235-011-9462-z.

[23] F. Bin Muhaya, M. Usama, and M. K. Khan, “Modified AES using chaotic key generator for satellite imagery encryption,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5754 LNCS, Springer Berlin Heidelberg, 2009, pp. 1014–1024.

[24] A. Arab, M. J. Rostami, and B. Ghavami, “An image encryption method based on chaos system and AES algorithm,” *Journal of Supercomputing*, vol. 75, no. 10, pp. 6663–6682, May 2019, doi: 10.1007/s11227-019-02878-7.

[25] C. H. Yang and Y. S. Chien, “FPGA implementation and design of a hybrid chaos-AES color image encryption algorithm,” *Symmetry*, vol. 12, no. 2, Jan. 2020, doi: 10.3390/sym12020189.

[26] R. Banu and T. Vladimirova, “Fault-tolerant encryption for space applications,” *IEEE Transactions on Aerospace and Electronic Systems*, vol. 45, no. 1, pp. 266–279, Jan. 2009, doi: 10.1109/TAES.2009.4805278.

[27] K. W. Wong, S. W. Ho, and C. K. Yung, “A chaotic cryptography scheme for generating short ciphertext,” *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 310, no. 1, pp. 67–73, Apr. 2003, doi: 10.1016/S0375-9601(03)00259-7.

[28] N. K. Pareek, V. Patidar, and K. K. Sud, “Discrete chaotic cryptography using external key,” *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 309, no. 1–2, pp. 75–82, Mar. 2003, doi: 10.1016/S0375-9601(03)00122-1.

[29] H. Mestiri, N. Benhadjyoussef, M. Machhout, and R. Tourki, “An FPGA implementation of the AES with fault detection countermeasure,” in *2013 International Conference on Control, Decision and Information Technologies (CoDIT)*, May 2013, pp. 264–270, doi: 10.1109/CoDIT.2013.6689555.

[30] M. McLoone and J. V. McCanny, “Rijndael FPGA implementation utilizing look-up tables,” in *IEEE Workshop on Signal Processing Systems, SiPS: Design and Implementation*, 2001, pp. 349–360, doi: 10.1109/sips.2001.957363.

[31] N. Floissac and Y. L’Hyver, “From AES-128 to AES-192 and AES-256, how to adapt differential fault analysis attacks on key expansion,” in *2011 Workshop on Fault Diagnosis and Tolerance in Cryptography*, Sep. 2011, pp. 43–53, doi: 10.1109/FDTC.2011.15.

[32] J. Daemen and V. Rijmen, “The block cipher Rijndael,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 1820, Springer Berlin Heidelberg, 2000, pp. 277–284.

[33] B. Sunar, “A euclidean algorithm for normal bases,” *Acta Applicandae Mathematicae*, vol. 93, no. 1–3, pp. 57–74, Aug. 2006, doi: 10.1007/s10440-006-9048-z.

[34] S. Lian, J. Sun, and Z. Wang, “A block cipher based on a suitable use of the chaotic standard map,” *Chaos, Solitons and Fractals*, vol. 26, no. 1, pp. 117–129, Oct. 2005, doi: 10.1016/j.chaos.2004.11.096.

[35] L. Li, “Image encryption algorithm based on hyperchaos and DNA coding,” *IET Image Processing*, vol. 18, no. 3, pp. 627–649, Nov. 2024, doi: 10.1049/ipr2.12974.

[36] G. dong Li and L. le Wang, “Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform,” *Visual Computer*, vol. 35, no. 9, pp. 1267–1277, Jul. 2019, doi: 10.1007/s00371-018-1574-y.

[37] Y. Mao, G. Chen, and S. Lian, “A novel fast image encryption scheme based on 3D chaotic baker maps,” *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 14, no. 10, pp. 3613–3624, Oct. 2004, doi: 10.1142/S021812740401151X.

[38] H. Khanzadi, M. Eshghi, and S. E. Borujeni, “Image encryption using random bit sequence based on chaotic maps,” *Arabian Journal for Science and Engineering*, vol. 39, no. 2, pp. 1039–1047, Sep. 2014, doi: 10.1007/s13369-013-0713-z.

[39] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.

[40] Claude E. Shannon, "Coding theorems for a discrete source with a fidelity criterion Institute of Radio Engineers, International Convention Record, vol. 7, 1959," in *Claude E. Shannon: Collected Papers*, IEEE, 1993, pp. 325-350, doi: 10.1109/9780470544242.ch21.

[41] T. Xiang, X. Liao, G. Tang, Y. Chen, and K. W. Wong, “A novel block cryptosystem based on iterating a chaotic map,” *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 349, no. 1–4, pp. 109–115, Jan. 2006, doi: 10.1016/j.physleta.2005.02.083.

[42] M. Maazouz, A. Toubal, B. Bengherbia, O. Houhou, and N. Batel, “FPGA implementation of a chaos-based image encryption algorithm,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 9926–9941, Nov. 2022, doi: 10.1016/j.jksuci.2021.12.022.

[43] Z. A. Abduljabbar *et al.*, “Provably secure and fast color image encryption algorithm based on S-boxes and hyperchaotic map,” *IEEE Access*, vol. 10, pp. 26257–26270, 2022, doi: 10.1109/ACCESS.2022.3151174.

[44] W. J. Jun and T. S. Fun, “A new image encryption algorithm based on single S-box and dynamic encryption step,” *IEEE Access*, vol. 9, pp. 120596–120612, 2021, doi: 10.1109/ACCESS.2021.3108789.

[45] T. S. Ali and R. Ali, “A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box,” *Multimedia Tools and Applications*, vol. 81, no. 15, pp. 20585–20609, Mar. 2022, doi: 10.1007/s11042-022-12268-6.

[46] W. Zhang, H. Yu, Y. L. Zhao, and Z. L. Zhu, “Image encryption based on three-dimensional bit matrix permutation,” *Signal Processing*, vol. 118, pp. 36–50, Jan. 2016, doi: 10.1016/j.sigpro.2015.06.008.

[47] L. Xu, Z. Li, J. Li, and W. Hua, “A novel bit-level image encryption algorithm based on chaotic maps,” *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, Mar. 2016, doi: 10.1016/j.optlaseng.2015.09.007.

[48] X. Y. Wang, Y. Q. Zhang, and X. M. Bao, “A novel chaotic image encryption scheme using DNA sequence operations,” *Optics and Lasers in Engineering*, vol. 73, pp. 53–61, Oct. 2015, doi: 10.1016/j.optlaseng.2015.03.022.

[49] M. Alawida, “A novel chaos-based permutation for image encryption,” *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 6, Jun. 2023, doi: 10.1016/j.jksuci.2023.101595.

[50] H. R. Shakir, S. A. Mehdi, and A. A. Hattab, “A new four-dimensional hyper-chaotic system for image encryption,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1744–1756, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1744-1756.

[51] A. A. Rashid and K. A. Hussein, “Image encryption algorithm based on the density and 6D logistic map,” *International Journal of Electrical and Computer Engineering*, vol. 13, no. 2, pp. 1903–1913, Apr. 2023, doi: 10.11591/ijece.v13i2.pp1903-1913.

[52] Z. Zhang, J. Tang, F. Zhang, H. Ni, J. Chen, and Z. Huang, “Color image encryption using 2D sine-cosine coupling map,” *IEEE Access*, vol. 10, pp. 67669–67685, 2022, doi: 10.1109/ACCESS.2022.3185229.

[53] J. Arif *et al.*, “A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution,” *IEEE Access*, vol. 10, pp. 12966–12982, 2022, doi: 10.1109/ACCESS.2022.3146792.

[54] X. Wang, Y. Su, H. Zhang, and C. Zou, “A new hybrid image encryption algorithm based on Gray code transformation and snake-like diffusion,” *Visual Computer*, vol. 38, no. 11, pp. 3831–3852, Jul. 2022, doi: 10.1007/s00371-021-02224-0.

[55] M. Alawida, J. Sen Teh, A. Mehmood, A. Shoufan, and W. H. Alshoura, “A chaos-based block cipher based on an enhanced logistic map and simultaneous confusion-diffusion operations,” *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 8136–8151, Nov. 2022, doi: 10.1016/j.jksuci.2022.07.025.

[56] X. Qian, Q. Yang, Q. Li, Q. Liu, Y. Wu, and W. Wang, “A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box,” *IEEE Access*, vol. 9, pp. 61334–61345, 2021, doi: 10.1109/ACCESS.2021.3073514.

[57] M. Z. Talhaoui, X. Wang, and M. A. Midoun, “A new one-dimensional cosine polynomial chaotic map and its use in image encryption,” *Visual Computer*, vol. 37, no. 3, pp. 541–551, Mar. 2021, doi: 10.1007/s00371-020-01822-8.

[58] A. Mansouri and X. Wang, “Image encryption using shuffled Arnold map and multiple values manipulations,” *Visual Computer*, vol. 37, no. 1, pp. 189–200, Jan. 2021, doi: 10.1007/s00371-020-01791-y.

[59] X. Q. Fu, B. C. Liu, Y. Y. Xie, W. Li, and Y. Liu, “Image encryption-then-transmission using DNA encryption algorithm and the double chaos,” *IEEE Photonics Journal*, vol. 10, no. 3, pp. 1–15, Jun. 2018, doi: 10.1109/JPHOT.2018.2827165.

[60] F. Sbiaa, S. Kotel, M. Zeghid, R. Tourki, M. MacHhout, and A. Baganne, “High-level implementation of a chaotic and AES based crypto-system,” *Journal of Circuits, Systems and Computers*, vol. 26, no. 7, Mar. 2017, doi: 10.1142/S0218126617501225.

[61] C. Li, G. Luo, K. Qin, and C. Li, “An image encryption scheme based on chaotic tent map,” *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, Aug. 2017, doi: 10.1007/s11071-016-3030-8.

[62] L. Wang, H. Song, and P. Liu, “A novel hybrid color image encryption algorithm using two complex chaotic systems,” *Optics and Lasers in Engineering*, vol. 77, pp. 118–125, Feb. 2016, doi: 10.1016/j.optlaseng.2015.07.015.

BIOGRAPHIES OF AUTHORS

Omar Benchikh is a Ph.D. student at Djillali Liabés University, Algeria. In 2011, he obtained his bachelor's degree in computer engineering from the Faculty of Engineering Sciences, University Djillali Liabés of Sidi Bel Abbes. In 2013, he graduated with a master's degree in computer engineering from the Faculty of Technology at the same university. His main research interests include image cryptosystems and image processing. He can be contacted at email: omarb022@hotmail.com.

Youcef Bentoutou received his engineer, magister, and doctorate degrees in electrical engineering from the University of Sidi Bel Abbes (Algeria) in 1997, 2000, and 2004 respectively. He is currently a research director of systems architecture and signal processing at the Satellite Development Center of the Algerian Space Agency. Dr. Bentoutou received the 2009 TWAS-AAS-Microsoft award for young scientists for his contributions to the fields of pattern recognition and information processing. His principal research interests are in the fields of remote sensing, satellite onboard data handling, and space radiation environment and effects analysis and mitigation. He can be contacted at email: bentoutou@asal.dz.

Nasreddine Taleb received an M.S. degree in computer engineering from Boston University, an Elect-Eng. degree from Northeastern University, and a Ph.D. degree in electrical engineering from Djillali Liabes University, Sidi Bel Abbes, Algeria. He is currently a professor at the faculty of electrical and engineering, Djillali Liabes University, where he has been teaching since 1990 and where he is also the director of the “Communication networks, architecture, and multimedia” research laboratory. His principal research interests are in the fields of digital signal and image processing, image analysis, medical and satellite image applications, and advanced architectures for implementation of DSP/DIP applications. He can be contacted at email: ne_taleb@yahoo.com.