IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 3 May 2024, accepted 20 July 2024, date of publication 1 August 2024, date of current version 20 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3436627

RESEARCH ARTICLE

Revolutionizing Image Encryption: Introducing the Beta Wavelet Map and DNA Coding Paradigm

AMANI FALLAH[1], MONIA HAMDI[2], NAZIK ALTURKI[3], OUMAIMA SAIDANI[3], AND MOURAD ZAIED[1]

[1]Research Team in Intelligent Machines, National School of Engineers of Gabes, University of Gabes, Gabes 6029, Tunisia
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

Corresponding author: Nazik Alturki (namalturki@pnu.edu.sa)

This work was supported by the Princess Nourah Bint Abdulrahman University Researchers Supporting Project, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia, under Grant PNURSP2024R333.

ABSTRACT In this groundbreaking study, we introduce a novel and highly advanced approach to image encryption, harnessing the power of chaotic Beta wavelet sequences and DNA coding. Unlike conventional methods, our methodology not only involves the generation of three intricate chaotic beta wavelet sequences but also integrates DNA coding with an XOR operation, ensuring an unprecedented level of security for the encrypted data. The strength of our work lies in the meticulous application of Beta Discrete Wavelet Transform (DWT) to encrypt images in the wavelet domain, adding an extra layer of complexity to the encryption process. This paper not only presents a cutting-edge solution for image security but also establishes a new paradigm in the field of encryption by seamlessly merging chaos theory, DNA coding, and wavelet transforms. The results showcase unparalleled strength in safeguarding sensitive information, making our methodology a pioneering contribution to the realm of image encryption.

INDEX TERMS Image encryption, Beta wavelet, Beta wavelet chaotic map, DNA coding.

I. INTRODUCTION

As we navigate through the contemporary digital landscape, the prolific generation of data has facilitated the widespread dissemination of images across critical domains such as healthcare, defense, military, e-commerce, social media, and IoT devices. Nonetheless, the vast expanse of the Internet introduces a myriad of cyber threats, posing challenges to the security and privacy of image data. Consequently, safeguarding images against unauthorized access or tampering becomes paramount. In pursuit of this objective, numerous researchers have proposed diverse encryption techniques, consistently demonstrating their efficacy. However, these cryptographic methods have undergone extensive cryptanalysis, an ongoing area of exploration [1], [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

Within the realm of cryptography, chaotic cryptography stands out as a field that harnesses the dynamic behaviors exhibited by chaotic systems, making it a formidable choice for encrypting images. These behaviors encompass sensitivity to initial conditions, ergodicity, and unpredictability [3]. By capitalizing on these properties, secure encryption algorithms can be crafted. Presently, there is a notable emphasis on investigating image encryption technology using chaotic systems. Recent studies involve intricate shuffling of images using chaotic maps. In works such as [6], [7], and [8], authors introduce chaotic encryption schemes, integrating chaotic maps with compressive sensing, Hadamard transformation, and sparse coding.

The utilization of the logistic map in encryption techniques has been prevalent due to its simplicity and effectiveness, as evidenced in studies like [9], [10], and [11]. However, researchers acknowledge its drawbacks, such as a small key

size and suboptimal security [12], [13]. Consequently, new chaotic maps, like those developed in [14] and [15], offer improved security and enhanced performance.

Another avenue for encrypting images involves leveraging wavelet analysis, a widely employed tool across various fields of study [16], [17], [18]. Wavelets can analyze an image at different resolutions, capturing both its frequency and spatial characteristics. The Discrete Wavelet Transform (DWT) subdivides an image into sub-bands representing different levels and orientations of detail [19]. Encryption algorithms can then be applied to these sub-bands, enhancing the security features of encryption methods in the wavelet domain. These schemes prove resilient against attacks and allow for targeted encryption of specific frequency bands or regions of interest [20], [24].

In recent years, DNA coding has attracted attention as a powerful technique for image encryption, drawing inspiration from biological systems. This approach consists of converting an image into a DNA sequence, to which encryption algorithms are applied. The inherent complexity of DNA structures ensures security [25], [26].

An increasing number of DNA-based image encryption techniques are being developed as a result of the high degree of parallelism and large volume storage of DNA. An encryption method based on chaotic systems and DNA was proposed by Chai et al. [41]. Zhang et al. encrypted pictures using DNA coding and quantum chaotic mapping [42]. Yet, there are several drawbacks to encryption techniques based on chaotic systems and DNA. They are not immune to chosen-plaintext attacks, for instance [4], [5].

In our image encryption methodology, we leverage the advantages of a unified parameterizable mathematical function, the Beta function, through the use of its derivatives to generate new chaotic maps and wavelets. This approach forms an ideal foundation for robust encryption. The parameterizability of the Beta function allows for the generation of an infinite number of wavelets and associated chaotic maps. Considering that a single chaotic map typically generates the encryption key, this approach appears more robust than known chaotic encryption algorithms. Additionally, we incorporate DNA coding to provide a second layer of security.

The subsequent sections of this paper are organized as follows: Section II is dedicated to the related works pertaining to our approach. Section III introduces the preliminary aspects, while Section IV presents the new chaotic Beta Wavelet Maps family. Following that, Section V is reserved to present the proposed encryption method. Section VI offers a presentation of the experimental results and the performance analysis, and the concluding remarks are presented in Section VII.

II. RELATED WORKS

Image encryption serves the crucial purpose of protecting image data against unauthorized access and tampering. This process entails transforming the image into another visual representation that is indecipherable and unpredictable, only to be decoded by authorized individuals [20]. Image encryption methods fall into two main categories: spatial domain methods, which directly manipulate the image values, and transform domain methods, which initially convert the image into a different domain before executing encryption operations on the transformed coefficients [21], [22], [23].

Among the transform domain methods, one widely employed approach involves the use of wavelet transform. This technique decomposes the image into sub-bands with varying resolutions and frequencies, offering benefits such as resolution analysis, precise localization, and straightforward implementation [27]. To enhance security and complexity in image encryption, the wavelet transform can be combined with systems exhibiting properties like sensitivity to conditions, ergodicity, and randomness [13]. Chaotic systems, for instance, can generate random sequences for encrypting wavelet coefficients or scrambling pixel arrangements within the image.

In recent years, numerous image encryption techniques leveraging wavelet transform and chaotic systems have been proposed [27], [28]. For example, Liu and Ko introduced a technique involving encryption and wavelet transform for processing images in the context of planar design [27]. Mao et al. contributed an algorithm combining a chaotic map with an optimized lifting wavelet transform for encrypting images [29]. Other proposals include Zhang et al.'s image encryption algorithm based on 2D rotational wavelet transform and chaos transform [30], and El Latif et al.'s method involving AES coding of wavelet coefficients along with maps [31]. The literature also reports various image encryption techniques employing both chaotic maps and wavelet transforms [28], [32], including comprehensive surveys evaluating the advantages and disadvantages of existing chaos-based image encryption methods [28].

Moreover, there are approaches using metaheuristic optimizers that offer robust optimization by employing different chaotic maps [33]. Hybrid schemes, such as one combining three distinct chaotic maps to enhance security [34], have been proposed. In this context, we present a novel image encryption approach utilizing the Beta wavelet transform and Beta chaotic wavelet maps. The flexibility of the Beta function allows for the generation of different Beta wavelets by adjusting their parameters [35]. Additionally, a Beta wavelet chaotic map, derived from the same wavelet, exhibits diverse dynamic behaviors, coupled with high sensitivity to initial conditions and parameters.

III. PRELIMINARIES

A. WAVELET FUNCTION

The wavelet function, denoted as $\psi(t)$, is a fundamental element in wavelet analysis. The wavelet has two basic properties: translation and dilation. Translation, or shifting,

is represented by the parameter b in the translated wavelet $\psi_{a,b}(t)$:

$$\psi_{a,b}(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right)$$

Dilation, or scaling, adjusts the width of the wavelet and is controlled by the scale factor a in the dilated wavelet $\psi_a(t)$

$$\psi_a(t) = \frac{1}{\sqrt{a}}\psi\left(\frac{t}{a}\right)$$

Here, $\psi(t)$ is the original wavelet function. The scaling parameter a influences the frequency content, with higher values corresponding to smoother, lower-frequency wavelets, and lower values to more oscillating, higher-frequency wavelets. This function is crucial for continuous wavelet transform (CWT) or discrete wavelet transforms (DWT), which enable signal analysis at different scales and locations in time. Wavelet analysis finds applications in signal processing, image processing, search, and various fields, including data analytics, where it proves valuable for capturing frequency and time information.

B. DISCRETE WAVELET TRANSFORM

The discrete wavelet transform (DWT) is an image processing technique that decomposes image I into four subbands, with different frequency and spatial characteristics. This decomposition is achieved using two filters the high pass filter h and the low pass filter g. These filters separate the image into components of frequency (LL) which represents the intensity and high frequency (LH, HL, HH) which capture the horizontal, vertical and diagonal edges of the image. The LL component can be further decomposed using the filters to create a structure of wavelet coefficients. To reconstruct the image we can reverse this process by employing two synthesis filters that are essentially inverse versions of the analysis filters. This reconstruction method is known as Inverse Discrete Wavelet Transform (IDWT). In the provided figure you can observe a one-level DWT applied to image I.

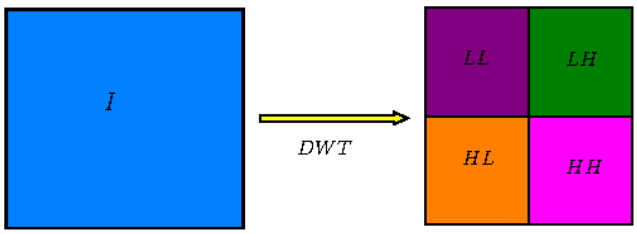

FIGURE 1. Histograms of decrypted images.

C. BETA WAVELET

The Beta Wavelet (BW) constitutes a group of wavelets obtained through the Beta function under specific conditions. In contrast to alternative wavelet structures, the generation of BW is contingent upon appropriately chosen parameters of the Beta function, namely p, q, x_0, and x_1. The mathematical expression for the Beta distribution is outlined as follows [35], [36], [37], [38]:

$$\beta(x; p, q, x_0, x_1) = \begin{cases} \left(\frac{x-x_0}{x_c-x_0}\right)^p \left(\frac{x_1-x}{x_1-x_c}\right)^q & x \in [x_0, x_1] \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where $x, p, q, x_0, x_1 \in \mathbb{R}$, with $p, q > 0, x_0 < x_1$, and $x_c = \frac{px_1+qx_0}{p+q}$

Beta distribution at the boundary of interval $[x_0, x_1]$ equals zero, that is $\beta(x_0) = \beta(x_1) = 0$.

Beta distribution at the centroid, x_c, equals 1, that is $\beta(x_c) = 1$.

Evaluation of the derivative of the Beta function (Beta1) with respect to x at x_0, x_1 or x_c equals zero. That is, knowing that:

$$\frac{d\beta(x)}{dx} = \frac{px_1 + qx_0 - (p+q)x}{(x-x_0)(x_1-x)}\beta(x) \quad (2)$$

The second derivative of the Beta function (Beta2) is given as follows:

$$\frac{d^2\beta(x)}{dx^2} = \beta(x)A(x) \quad (3)$$

where

$$A(x) = \frac{1}{(x-x_0)(x_1-x)} \left[\frac{1}{(x_1-x)} - \frac{1}{(x-x_0)} - (p+q)(x+1) + px_1 + px_0\right] \quad (4)$$

The Beta function derivatives are the fundamental component of Beta wavelets. The Beta function, however, adopts several wavelet shapes depending on the derivative order when $(n > 0)$ and the choice of the parameters p, q, x_0 and x_1. For example, Fig. 2 depicts the Beta function, its first derivative and its second derivative forms, with $p = q = 3$, $x_0 = -2$ and $x_1 = 2$

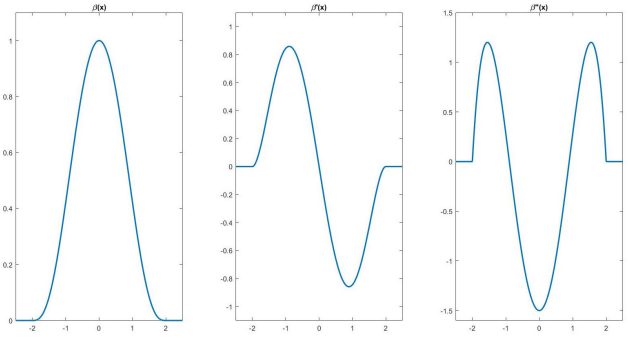

FIGURE 2. Beta function and its first and second derivatives.

D. DISCRETE BETA WAVELET FILTERS

As the DWT is not performed by the wavelet itself, but by a low-pass filter (h) and a high-pass filter (g) derived from it, a synthesis algorithm of these filters based on Orthogonal

multiresolution analysis has been developed in [35]. By interpolating scaling functions like Beta wavelet, multi-resolution can be produced that simplifies the estimation of wavelet filter coefficients. Consider the compact support wavelet in the range $[-N/2, N/2]$, which is denoted as follows:

$$\psi(\frac{N}{2}) = 2\sum_{\mathrm{k=-N}}^{\mathrm{N}} \mathrm{g_k}\phi\left(2\frac{\mathrm{N}}{2} - \mathrm{k}\right) = 2(g_N\phi(2N) + g_{N+1}\phi(2N-1) + \ldots + g_{N-1}\phi(1) + g_N\phi(0) \tag{5}$$

Let's define the interpolation scaling function as described in the following:

$$\phi(k) = \begin{cases} 1 & \text{if } k = 0 \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

Consequently, Eq.5 will be simplified as follows:

$$\psi\left(\frac{\mathrm{N}}{2}\right) = 2g \tag{7}$$

From Eq.7, filter coefficients g_N, can be calculated as the following:

$$g_N = \frac{\psi(\frac{\mathrm{N}}{2})}{2} \tag{8}$$

In general, the same method can be used to compute the other coefficients that constitute filter g as follows:

$$g_k = \frac{\psi(\frac{\mathrm{k}}{2})}{2} \tag{9}$$

Finally, if the evaluated wavelet is orthogonal, the filter is a quadrature mirror one and g is obtained by the following equation:

$$g_n = (-1)^n h_{1-n} \tag{10}$$

E. DNA CODING

DNA coding and decoding of images involves converting an image into a DNA sequence and vice. The coding process can be broken down into three steps.

Firstly the image is converted into binary format. Then each pair of bits, in the representation is mapped to a specific nucleotide, such as adenine (A) thymine (T) cytosine (C) or guanine (G). This mapping can follow for example '11','00','10','01' mapped to 'A','T','C','G' rule or any other one that satisfies Watson Crick complementarity [39]. These rules are shown in Table 1. This results in a nucleotide matrix.

In the next step the nucleotide matrix is transformed into a vector by concatenating its rows or columns. At this stage various operations based on the mathematical characteristics of DNA molecules can be applied for encryption purposes. These operations may include Xoring, addition or other methods that provide a desired level of security.

To decrypt and decode the DNA sequence back into an image the reverse process used during encryption is applied to the encrypted sequence. The resulting sequence is converted back, into a DNA matrix. Then transformed into a matrix using the inverse mapping rule of encryption stage. Finally this binary matrix is converted back into an image.

TABLE 1. DNA coding rules.

Rule	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
C	01	10	00	11	00	11	01	10
G	10	01	11	00	11	00	10	01

IV. A NEW CHAOTIC BETA WAVELET MAPS FAMILY

In this study, we present an innovative image encryption approach using chaotic Beta wavelet maps derived from Beta wavelet functions commonly used in image processing tasks such as compression, denoising, watermarking, and others. Chaotic wavelet Beta maps serve as a striking example demonstrating how simple nonlinear dynamical equations can lead to complex and chaotic behavior. The mathematical representation of the Beta wavelet map is formulated as follows:

$$x_{n+1} = k \cdot \psi(x_n, x_0, x_1, p, q, d, t) \tag{11}$$

where ψ is a Beta wavelet and $p = b_1 * a + c_1$ and $q = b_2 * a + c_2$

b_1 and b_2 are the appropriately selected constants, where k is the Beta map's amplitude and a is the bifurcation parameter. d and t represent respectively the dilation and the translation parameters of the wavelet function ψ. While the equation governing the Beta map is inherently simple, adjustments to its parameters yield new chaotic maps characterized by unique shapes. These maps not only exhibit robust chaotic dynamics, but also offer improved pseudo-random chaotic sequences, a diverse set of bifurcation parameters, and a variety of the other control parameters. Consequently, the application of these chaotic maps in encryption techniques increases their effectiveness and strengthens them against a wide range of potential attacks.

Varying the parameters of the Beta wavelet gives several possibilities for Beta wavelet chaotic maps. Fig. 3,4,5, and 6 shows a sample of the chaotic map that was produced.

V. PROPOSED IMAGE ENCRYPTION METHOD

The proposed encryption method is divided into three stages. The first involves generating three chaotic Beta wavelet sequences and Beta wavelet filters. In the second stage, DNA coding is applied to the first generated chaotic sequence and the original image, followed by an XOR operation between them. The final stage is dedicated to encrypt the image in the wavelet domain, where a Beta DWT is performed on the image resulting from the second stage. Subsequently, a scrambling of the four sub-bands is applied using the second chaotic sequence, followed by a second XOR operation between the approximation sub-band and the third chaotic

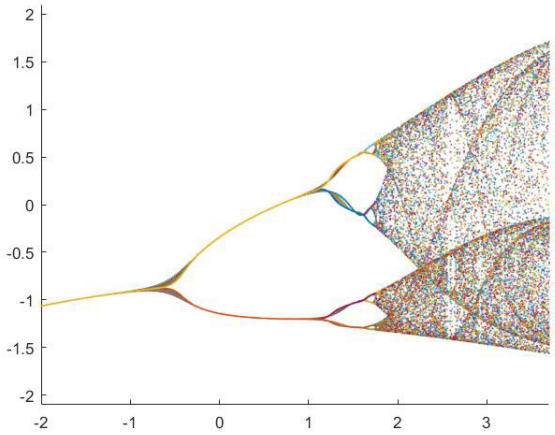

FIGURE 3. Beta1$_1$ wavelet map with $a = [-3.5 : 4]$, $x_0 = -4$, $x_1 = 4$, $k = 2.2$, $b_1 = 1$, $b_2 = 1$, $c_1 = 4$, $c_2 = 8$, $d = 1$, and $t = 0$.

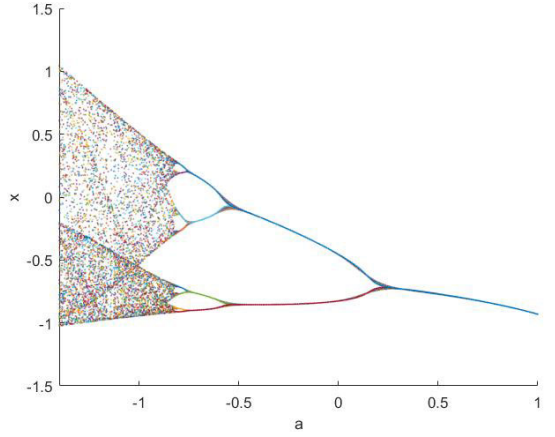

FIGURE 4. Beta1$_2$ wavelet map with $a = [-1.4 : 1.1]$, $x_0 = -2.05$, $x_1 = 3.05$, $k = 1.1$, $b_1 = -1$, $b_2 = -1$, $c_1 = 2$, $c_2 = 8$, $d = 1$, and $t = 0$.

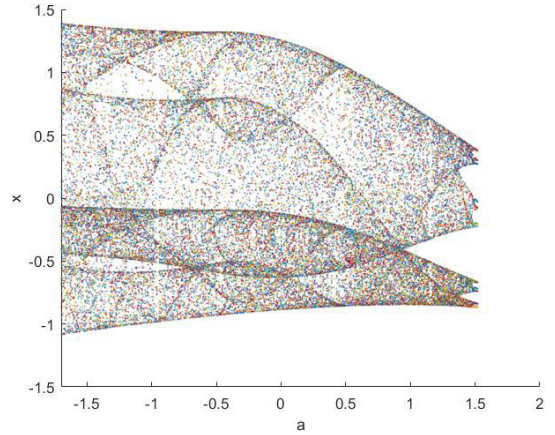

FIGURE 5. Beta1$_3$ wavelet map with $a = [-1.7 : 1.52]$, $x_0 = -2$, $x_1 = 3$, $k = 1.17$, $b_1 = -1$, $b_2 = -1$, $c_1 = 3$, $c_2 = 7$, $d = 0.8$, and $t = 0$.

sequence. Then the encrypted image is obtained by applying a Beta IDWT.

Part I: Key Definition and Beta Wavelet Chaotic Sequences, and filters Wavelet Generation

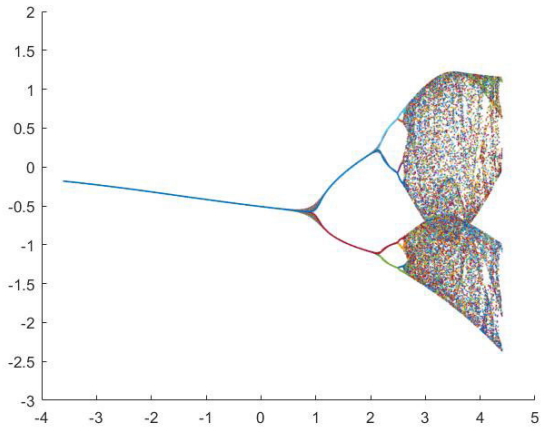

FIGURE 6. Beta2$_2$ wavelet map with $a = [-3.6 : 4.4]$, $x_0 = -4$, $x_1 = 4$, $k = 1.9$, $b_1 = 0.9$, $b_2 = 0.44$, $c_1 = 4$, $c_2 = 9$, $d = 1$, and $t = 0$.

- **Step 1:**
- Using three Beta wavelet maps Beta_wavelet_map1, Beta_wavelet_map2, and Beta_wavelet_map3) generate three chaotic sequences using three initial condition values. Thus, the encryption key is composed of the parameters of the maps: $(x_0^1, x_1^1, a^1, b_1^1, c_1^1, b_2^1, c_2^1, k^1, d^1, t^1;\quad x_0^2, x_1^2, a^2, b_1^2, c_1^2, b_2^2, c_2^2, k^2, d^2, t^2;\quad x_0^3, x_1^3, a^3, b_1^3, c_1^3, b_2^3, c_2^3, k^3, d^3, t^3)$, the three initial condition values, and two DNA rules used in encoding/decoding DNA stages.
- **Step 2:** Utilize the parameters $(x_0^1, x_1^1, a^1, b_1^1, c_1^1, b_2^1, c_2^1, k^1, d^1, t^1)$ of Beta_wavelet_map1 to generate low-pass h and high-pass g Beta wavelet filters.

Part II: DNA Coding and Encryption

- **Step 1:** Beta_wavelet_map1 sequence DNA coding
  - Reshape the sequence from Beta_wavelet_map1 to align with the dimensions of the image I to be encrypted.
  - Convert the chaotic sequence values to an 8-bit binary representation.
  - Convert the binary representation of the chaotic sequence to a DNA sequence by applying a predefined DNA rule (rule1). The resulting DNA sequence is denoted as Beta_wavelet_map1_DNA.
- **Step 2:** Original image DNA coding
  - Convert each pixel value of the original image (I) to its 8-bit binary representation.
  - Map the binary representation of each pixel to a DNA sequence using a second DNA rule (rule2). The resulting DNA sequence is denoted as I_DNA.
- **Step 3:** XOR Operation
  - Perform a XOR operation between the DNA sequences Beta_wavelet_map1_DNA and I_DNA to obtain a sequence, denoted as I_DNA_XORed.
  - Map I_DNA_XORed sequences back to binary using rule2.

– Convert the binary representations back to decimal values to obtain image DNA_fingerprint_I.

Part III: Encryption in the wavelet domain

- **Step 1:** Apply a 2D Beta DWT using h and g Beta wavelet filters generated in Part I to DNA_fingerprint_I. The result is LL, LH, HL, and HH sub-bands.
- **Step 2:** 2D Scrambling
  - Apply a Shuffling process to all sub-bands values using Algorithm 1 and Beta_wavelet_map2 sequence.
  - XOR the Shuffled LL sub-band with Beta_wavelet_map3 sequence to obtain LL_1.
  - Xor pixel(i-1) with pixel(i) of LL_1.
- **Step 3:** Reconstruct the image using the inverse 2D Beta DWT.

The decryption process of the algorithm can be seen as the inverse of the encryption process.

Algorithm 1 Image Shuffling Process

Inputs: I – image to be Shuffled, x – Beta wavelet chaotic sequence
Output: *IShuffled* – Shuffled image

$[row, col] = \text{size}(I)$
$k = 1$
$x\_sorted = \text{sort}(x)$
$N1_1 = \text{length}(x)$
for $i = 1$ to $N1_1$ **do**
  for $j = 1$ to $N1_1$ **do**
    if $(x\_sorted(i) == x(j))$ **then**
      $Shuffling\_mat(1, k) = j$
      $k = k + 1$
    end if
  end for
end for
$I\_1D = (I(:))'$
for $i = 1$ to $N1_1$ **do**
  $I\_shuffle(i) = I\_1D(Shuffling\_mat(i))$
end for
$len = 1$
for $i = 1$ to row **do**
  for $j = 1$ to col **do**
    $Shuffled(i, j) = I\_shuffle(1, len)$
    $len = len + 1$
  end for
end for

VI. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

To highlight the strength of our suggested method when faced with types of attacks we carried out a series of experiments, we conducted multiple tests: statistical analysis, differential attack tests, and Information Entropy Analysis. These tests were performed on grayscale images from the USC-SIPI Image Dataset used as plain text.

A. HISTOGRAM ANALYSIS

The histogram of an image provides insights, into the distribution of gray values within the image. When encrypting an image it is ideal for the histogram of the encrypted version to be almost uniform or closely resemble uniformity. At the time it should noticeably differ from the histogram of the plaintext image. This difference is crucial because a balanced distribution of values makes it difficult for attackers to extract information through statistical attacks.

The histograms of a series of encrypted images, as well as the original images, with greatly varied contents, were calculated and examined. Original image, cipher image, and decrypted image histograms of the Cameraman, Barbara and the house are displayed in Fig. 7. A plain image's histogram is steeply sloped and has large spikes (see figure 7). The cipher image's histogram is displayed in Fig. 8; it is smooth, very flat, considerably different from that of the input images, and bears no statistical resemblance to the plain image, and as a result, offers no hint for using any statistical attack on the suggested image encryption procedure. In light of this, we draw the conclusion that ciphertext images are random-like by contrasting their histograms to plaintext images and the suggested approach is secure against the entropy attack.

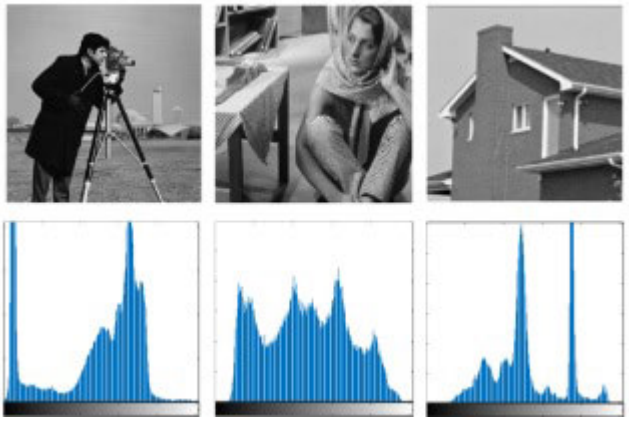

FIGURE 7. Respectively (from left to right): original images of 'Cameraman', 'Barbara', 'House', and their histograms.

B. INFORMATION ENTROPY ANALYSIS

Entropy of data is a measure that indicates the level of randomness and vulnerability, in an encryption method. Ideally the assessment of information entropy for an encrypted image should be close to 8 [40]. The Equation (12) is used to calculate the entropy. In this equation X is used to represent the test image. Each a_i represents a value of X. The notation $Pr(a_i)$ indicates the probability of X having the value a_i which shows how likely it is to select a pixel in X with that value. The highest possible value, The maximum of $H(a)$ is attained occurs when X follows an uniform distribution as shown in Equation (13). Additionally, G represents the number of

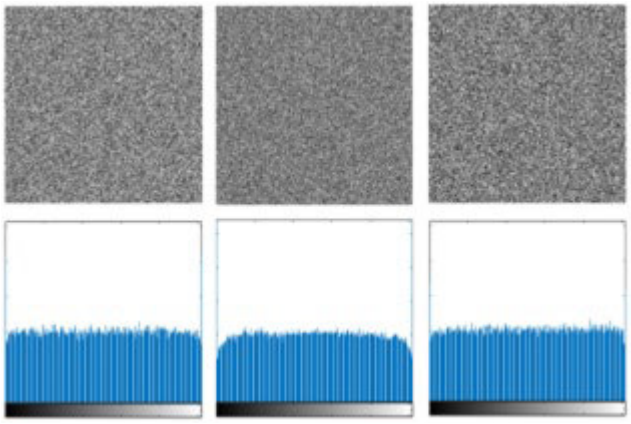

FIGURE 8. Respectively (from left to right): ciphered images of 'Cameraman', 'Barbara', 'House' and their histograms.

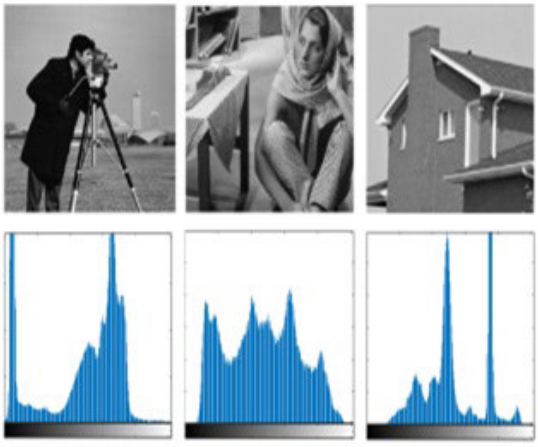

FIGURE 9. Respectively (from left to right): decrypted images of 'Cameraman', 'Barbara', 'House', and their histograms.

intensity levels associated with the image format.

$$H(a) = \sum_{i=1}^{n} Pr(a_i) \log_2 Pr(a_i) \tag{12}$$

$$Pr(A = a_i) = 1/G \tag{13}$$

For several ciphered images, the information entropy test was performed. The results summarized in Table 2 demonstrate that the encrypted images' entropies are extremely near to 8. Therefore, we can conclude that the entropy average of the suggested technique is 7.9971, which is significantly better than that of the methods in [39], [41], [43], and [44] and similar to that analyzed in [45]. As a result, the proposed encryption method is resistant to entropy assaults.

Image		Barbara	House	Peppers	Cameraman
Plain Image		7.5751	7.6269	7.5251	7.0097
Cipher image	Ref. [42]	7.9962	7.9970	7.9973	7.9972
	Ref. [44]	7.9970	7,9968	7.9971	7.9969
	Ref. [45]	7,9872	7.9860	7.9860	7.9890
	Ref. [46]	7.9965	7.9971	7.9970	79972
	Ref. [47]	7.9967	7.9973	7.9969	7.9973
	Our	7.9972	7.9972	7.9970	7.9971

C. NPCR AND UACI ANALYSIS

To determine the extent of change caused by a single pixel alteration in the simple image, we conducted various tests on plain images using the proposed algorithm, and in comparison to the algorithms in [43] and [45], we got good analyses. According to the comparison, our method has a NPCR average of 0.9962 and an UACI average of 0,334275 which are closer to 0.996094 and 0.334635 than NPCR and UACI averages in [43] and [45] (see Tables 2 and 3). The outcomes demonstrate that the proposed approach can withstand differential assault.

$$NPCR = \sum_{i=1}^{M} \sum_{j=1}^{N} D(i,j) \times \frac{\%100}{M \times N} \tag{14}$$

$$UACI = \left[\sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i,j) - C_2(i,j)|}{255} \right] \times \frac{\%100}{M \times N} \tag{15}$$

where C_1 or C_2's size is $M \times N$, respectively. The original images for the two cyphered images C_1 and C_2 are identical in size and only differ by one pixel. The pixels at coordinates (i, j) have $C_1(i, j)$ and $C_2(i, j)$ as values. The $D(i, j)$ is computed using $C_1(i, j)$ and $C_2(i, j)$.

$$D(i,j) = \begin{cases} 1, & \text{if } C_1(i,j) = C_2(i,j) \\ 0, & \text{otherwise} \end{cases} \tag{16}$$

TABLE 2. Test results of NPCR.

Image	Barbara	House	Peppers	Cameraman
Ref. [44]	0.9955	0.9961	-	-
Ref. [45]	0.9962	-	0.9961	-
Ref. [46]	0.9962	0.9959	-	-
Ref. [47]	0.9965	0.9968	0.9961	0.9964
Our	0.9963	0.9968	0.9961	0.9960

TABLE 3. Test results of UACI.

Image	Barbara	House	Peppers	Cameraman
Ref. [44]	0.3341	0.3339	-	-
Ref. [45]	0.2815	-	0.2919	-
Ref. [46]	0.3349	0.3347	-	-
Ref. [47]	0.3353	0.3339	0.3342	0.3350
Our	0.3344	0.3339	0.3341	0.3350

D. CORRELATION ANALYSIS

An original image has a high correlation on its horizontal, vertical and diagonal axes. This means that its adjacent pixels are highly interconnected. Whereas in an encrypted image, the correlation between adjacent pixels should be very low. To test the robustness of our encryption algorithm, we calculated the correlation $r_{x,y}$ of 2,000 randomly selected pairs of adjacent pixels (xi,yi) from the encrypted Barbara image.

Equation (17) is used to calculate the correlation. $\bar{x}$ and $\bar{y}$ represent the means of x and y. If the correlation value is close

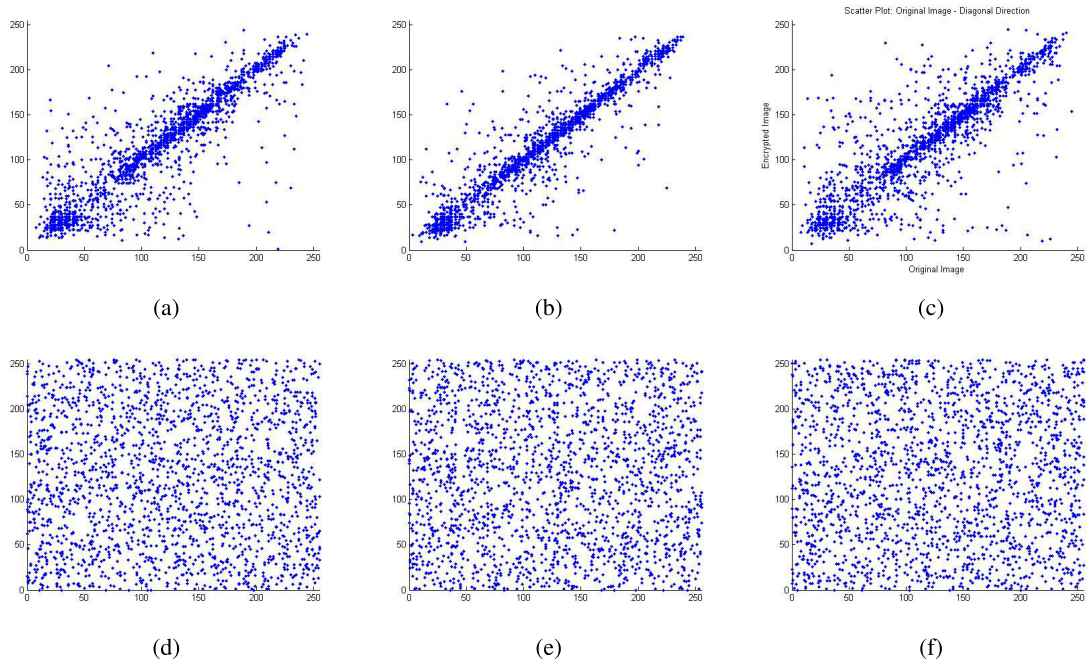

FIGURE 10. Correlation plots for the three directions of image Barbara: (a) plaintext horizontal, (b) plaintext vertical, (c) plaintext diagonal, (d) ciphertext horizontal, (e) ciphertext vertical and (f) ciphertext diagonal.

TABLE 4. Test results of correlation.

Image	Direction	Ref. [42]	Ref. [44]	Ref. [45]	Ref. [46]	Ref. [47]	Ours
Barbara	Horizontal	−0.0413	−0.0034	0.0051	0.0017	0.0021	0.0033
	Vertical	0.0135	0.0024	0.0212	−0.0133	−0.0114	−0.0125
	Diagonal	0.0075	0.0075	−0.0089	0.0173	0.0045	0.0438
House	Horizontal	0.0397	0.0077	−0.0063	0.0030	−0.0029	−0.0214
	Vertical	0.0327	0.0030	0.0035	0.0009	−0.0147	0.0456
	Diagonal	−0.0154	−0.0039	0.0103	0.0048	0.0086	−0.0192
Cameraman	Horizontal	0.0120	−0.0027	0.0047	−0.0037	−0.0051	−0.0560
	Vertical	−0.0478	0.0025	0.0018	−0.0019	−0.0017	−0.0240
	Diagonal	0.0354	0.0039	−0.0019	0.0034	−0.0051	0.0789
Peppers	Horizontal	−0.0654	0.0171	0.0028	0.0017	−0.0033	0.0991
	Vertical	−0.0259	0.0072	−0.0017	0.0091	0.0019	0.0234
	Diagonal	−0.0351	−0.0019	−0.0103	0.0056	−0.0088	0.0789

to 1, x and y have a high correlation, and if it's close to 0 their correlation is low.

$$r_{x,y} = \frac{\sum_{i=1}^{n} (x_i - \bar{x})\,(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n} (x_i - \bar{x})^2}\sqrt{\sum_{i=1}^{n} (y_i - \bar{y})^2}} \tag{17}$$

We repeated this test several times, calculated the mean correlations and compared them with the Refs. [39], [41], [43], [44], and [45] (see table 4). Fig. 10 shows the correlation of the Barbara image in three directions for both the plain image (a,b,c) and the encrypted image (d,e,f). We can notice that there is a strong correlation in each direction for the clear image, while the pixels are decorrelated for the ciphered image (d,e,f).

VII. CONCLUSION

In conclusion, our pioneering study presents a paradigm-shifting approach to image encryption, fusing the power of chaotic Beta wavelet sequences with innovative DNA coding techniques. The uniqueness of our methodology lies not only in the intricate generation of three chaotic Beta wavelet sequences but also in the integration of DNA coding through XOR operations, elevating the level of security to unprecedented heights.

The results obtained through rigorous testing demonstrate the unparalleled strength of our methodology in safeguarding sensitive information. This groundbreaking contribution sets a new standard in image encryption, showcasing the potential for a more secure and advanced future in data protection. As we pave the way for the evolution of encryption technologies, our approach stands as a beacon of innovation, marking a transformative milestone in the field of image security.

REFERENCES

[1] H. Wen and Y. Lin, "Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding," *Expert Syst. Appl.*, vol. 237, Mar. 2024, Art. no. 121514.

[2] R. Chen, L. Liu, and Z. Zhang, "Cryptanalysis on a permutation–rewriting–diffusion (PRD) structure image encryption scheme," *Multimedia Tools Appl.*, vol. 82, no. 3, pp. 4289–4317, Jan. 2023.

[3] D. Zou, T. Pei, G. Xi, and L. Wang, "Image encryption based on hyperchaotic system and improved zigzag diffusion method," *IEEE Access*, vol. 11, pp. 95396–95409, 2023.

[4] Y. Liu, J. Tang, and T. Xie, "Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map," *Opt. Laser Technol.*, vol. 60, pp. 111–115, Aug. 2014.

[5] Y. Dou, X. Liu, H. Fan, and M. Li, "Cryptanalysis of a DNA and chaos based image encryption algorithm," *Optik*, vol. 145, pp. 456–464, Sep. 2017.

[6] L. Huang, S. Cai, M. Xiao, and X. Xiong, "A simple chaotic map-based image encryption system using both plaintext related permutation and diffusion," *Entropy*, vol. 20, no. 7, p. 535, Jul. 2018.

[7] R. Ponuma and R. Amutha, "Image encryption using sparse coding and compressive sensing," *Multidimensional Syst. Signal Process.*, vol. 30, no. 4, pp. 1895–1909, Oct. 2019.

[8] S. N. Prajwalasimha, "Pseudo-Hadamard transformation-based image encryption scheme," in *Integrated Intelligent Computing, Communication and Security*. Cham, Switzerland: Springer, 2019, pp. 575–583.

[9] H. Çelik and N. Dogan, "A hybrid color image encryption method based on extended logistic map," *Multimedia Tools Appl.*, vol. 83, no. 5, pp. 12627–12650, Jul. 2023.

[10] D. R. I. M. Setiadi and N. Rijati, "An image encryption scheme combining 2D cascaded logistic map and permutation-substitution operations," *Computation*, vol. 11, no. 9, p. 178, Sep. 2023.

[11] D. Zareai, M. Balafar, and M. FeiziDerakhshi, "EGPIECLMAC: Efficient grayscale privacy image encryption with chaos logistics maps and Arnold cat," *Evolving Syst.*, vol. 14, no. 6, pp. 993–1023, Dec. 2023.

[12] M. Ausloos and M. Dirickx, *The Logistic Map and the Route To Chaos: From the Beginnings To Modern Applications*. Springer, 2006.

[13] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.

[14] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Secure image encryption scheme based on a new robust chaotic map and strong S-box," *Math. Comput. Simul.*, vol. 207, pp. 322–346, May 2023.

[15] S. Zhu, X. Deng, W. Zhang, and C. Zhu, "Image encryption scheme based on newly designed chaotic map and parallel DNA coding," *Mathematics*, vol. 11, no. 1, p. 231, Jan. 2023.

[16] H. Zhong and G. Li, "Multi-image encryption algorithm based on wavelet transform and 3D shuffling scrambling," *Multimedia Tools Appl.*, vol. 81, no. 17, pp. 24757–24776, Jul. 2022, doi: 10.1007/s11042-022-12479-x.

[17] H. R. Shakir, "An image encryption method based on selective AES coding of wavelet transform and chaotic pixel shuffling," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26073–26087, Sep. 2019, doi: 10.1007/s11042-019-07766-z.

[18] J. Wang, W. Liu, and S. Zhang, "Adaptive encryption of digital images based on lifting wavelet optimization," *Multimedia Tools Appl.*, vol. 79, nos. 13–14, pp. 9363–9386, Apr. 2020, doi: 10.1007/s11042-019-7704-3.

[19] B. Furht, "Discrete wavelet transform (DWT)," in *Encyclopedia of Multimedia*, 2008, p. 188, doi: 10.1007/978-0-387-78414-4-305.

[20] Z. Rim, E. Ridha, and Z. Mourad, "An improved partial image encryption scheme based on lifting wavelet transform, wide range beta chaotic map and Latin square," *Multimedia Tools Appl.*, vol. 80, no. 10, pp. 15173–15191, Apr. 2021.

[21] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. AbuTair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Int. J. Inf. Secur.*, vol. 21, no. 4, pp. 917–935, Aug. 2022, doi: 10.1007/s10207-022-00588-5.

[22] J. Khandelwal, V. K. Sharma, J. K. Raguru, and H. Goyal, "Recent trend of transform domain image steganography technique for secret sharing. Cyber warfare," *Security Space Research*, vol. 1, pp. 171–185, 2022, doi: 10.1007/978-3-031-15784-4-14.

[23] A. H. S. Abdelgader, R. A. Aboughalia, and O. A. S. Alkishriwo, "Combined image encryption and steganography algorithm in the spatial domain," 2018, *arXiv:1810.05263*.

[24] V. P. Khalane and U. S. Bhadade, "A parameterized halfband filterbank design for image encryption," in *Proc. IEEE 13th Int. Conf. Ind. Inf. Syst. (ICIIS)*, Dec. 2018, pp. 32–35.

[25] M. Uddin, F. Jahan, M. K. Islam, and M. Rakib Hassan, "A novel DNA-based key scrambling technique for image encryption," *Complex Intell. Syst.*, vol. 7, no. 6, pp. 3241–3258, Dec. 2021, doi: 10.1007/s40747-021-00515-6.

[26] Y. M. Afify, N. H. Sharkawy,W. Gad, and N. Badr, "A new dynamic DNA-coding model for gray-scale image encryption," *Complex Intell. Syst.*, vol. 10, no. 1, pp. 745–761, Feb. 2024, doi: 10.1007/s40747-023-01187-0.

[27] Y. Liu and Y. C. Ko, "Image processing method based on chaotic encryption and wavelet transform for planar design," *Adv. Math. Phys.*, vol. 2021, pp. 1–12, Oct. 2021.

[28] A. K. Singh and G. R. Sinha, "A survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *Multimedia Tools Appl.*, vol. 78, no. 9, pp. 11401–11446, 2019.

[29] N. Mao, X. Tong, M. Zhang, and Z. Wang, "Real-time image encryption algorithm based on combined chaotic map and optimized lifting wavelet transform," *J. Real-Time Image Process.*, vol. 20, no. 2, pp. 1–17, Apr. 2023.

[30] Y. Zhang, Y. Wang, and Y. Zhang, "Image encryption algorithm based on 2-D wavelet transform and chaos transform," *J. Ambient Intell. Hum Comput.*, vol. 1, pp. 1009–1020, Aug. 2022.

[31] A. A. A. El-Latif, A. El-Samie, and F. E. El-Rabaie, "Image encryption based on selective AES coding of wavelet coefficients and chaotic maps," *Multimedia Tools Appl.*, vol. 1, pp. 1469–1494, Sep. 2022.

[32] V. Thanikaiselvan, "Image encryption using integer wavelet transform, chaotic maps and DNA rules," in *Proc. Int. Conf. Electr., Electron., Commun., Comput., Optim. Techn. (ICEECCOT)*, Dec. 2018, pp. 1351–1357.

[33] S. M. Sameh, H. E.-D. Moustafa, E. H. AbdelHay, and M. M. Ata, "An effective chaotic maps image encryption based on metaheuristic optimizers," *J. Supercomput.*, vol. 80, no. 1, pp. 141–201, Jan. 2024.

[34] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools Appl.*, vol. 81, no. 18, pp. 25497–25518, Jul. 2022.

[35] A. C. Ben et al., "Synthesis and application to lossy image compression," *Adv. Eng. Softw.*, vol. 36, no. 7, pp. 459–474, 2005.

[36] O. Jemai, R. Ejbali, M. Zaied, and C. B. Amar, "A speech recognition system based on hybrid wavelet network including a fuzzy decision support system," in *SPIE Proc.*, Feb. 2015, pp. 1–28, doi: 10.1117/12.2180554.

[37] R. Ejbali, M. Zaied, and C. Ben Amar, "Multi-input multi-output beta wavelet network: Modeling of acoustic units for speech recognition," 2012, *arXiv:1211.2007*.

[38] A. El Adel, M. Zaied, and C. Ben Amar, "Learning wavelet networks based on multiresolution analysis: Application to images copy detection," in *Proc. Int. Conf. Commun., Comput. Control Appl. (CCCA)*, Hammamet, Tunisia, Mar. 2011, pp. 1–6, doi: 10.1109/CCCA.2011.6031444.

[39] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012.

[40] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 447–460, Feb. 2015.

[41] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, Jan. 2019.

[42] J. Zhang and D. Huo, "Image encryption algorithm based on quantum chaotic map and DNA coding," *Multimedia Tools Appl.*, vol. 78, no. 11, pp. 15605–15621, Jun. 2019.

[43] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools Appl.*, vol. 76, no. 5, pp. 6229–6245, Mar. 2017.

[44] J. Zhao, S. Wang, and L. Zhang, "Block image encryption algorithm based on novel chaos and DNA encoding," *Information*, vol. 14, no. 3, p. 150, Feb. 2023.

[45] J. Zheng and T. Bao, "An image encryption algorithm based on cascade chaotic map and DNA coding," *IET Image Process.*, vol. 17, no. 12, pp. 3510–3523, Oct. 2023, doi: 10.1049/ipr2.12882.

[46] S. Ahadpour, Y. Sadra, and Z. ArastehFard, "A novel chaotic encryption scheme based on pseudorandom bit padding," 2012, *arXiv:1201.1449*.

[47] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[48] A. Belazi, A. A. Abd El-Latif, A.-V. Diaconu, R. Rhouma, and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Opt. Lasers Eng.*, vol. 88, pp. 37–50, Jan. 2017.

AMANI FALLAH received the bachelor's degree in telecommunication and networks from the National School of Engineers, University of Gabes, Tunisia, in 2017. She is currently pursuing the Ph.D. degree. She is a Researcher, specializing in image processing with the Research Team in Intelligent Machines, National School of Engineers of Gabes, University of Gabes, Tunisia. In parallel, her doctoral studies, balancing her practical experience with her passion for academic research. This dual involvement allows her to enrich her perspective in the field of image security using chaotic approaches. Her recent work titled "Image encryption Based on Beta Discrete Wavelet Transform, New Beta Wavelet Chaotic Map, and Latin Square" were published in the proceedings of the 15th International Conference on Machine Vision (ICMV 2022). Her primary research focus is on image encryption, with a particular interest in chaotic methods. She is a Development Engineer with web development company.

MONIA HAMDI received the B.Eng. degree in information technology from Telecom SudParis, Paris-Saclay University, France, in 2008, the M.Sc. degree in telecommunications and networks from the Institut National Polytechnique, Toulouse, France, in 2008, and the Ph.D. degree in computer science from the University of Rennes 1, France, in 2012. From 2012 to 2017, she was an Assistant Professor with the Higher Institute of Computer Science and Multimedia, University of Gabes, Tunisia. From March 2015 to August 2015, she was a Visiting Researcher with the Department of Science and Technology, Linköping University, Sweden. She is currently an Associate Professor with the College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Saudi Arabia. Her research interests include mobile communications, wireless sensor networks, edge computing, and blockchain.

NAZIK ALTURKI is currently an esteemed Researcher affiliated with the Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. With a deep passion for advancing the field of information systems, she has made significant contributions in areas, such as data management, decision support systems, and information security. Her expertise lies in the application of data analytics and machine learning techniques to extract meaningful insights from large datasets. She is also dedicated to exploring the challenges and opportunities presented by emerging technologies, including cloud computing, the Internet of Things (IoT), and blockchain. Her work has been published in prestigious journals and presented at international conferences, solidifying her reputation as a respected scholar. Furthermore, she actively participates as a reviewer for reputable academic journals, ensuring the high quality and rigor of scientific publications. Driven by her passion for research and her commitment to academic excellence, she continues to contribute to the field of information systems, making valuable contributions, that advance knowledge and drive innovation. Her research interests include leveraging technology to enhance organizational processes and improve decision-making efficiency.

OUMAIMA SAIDANI received the M.Sc. degree in computer sciences from Paris Dauphine University, France, and the Ph.D. degree in computer sciences from Paris 1-Panthéon Sorbonne University, France. She is currently an Assistant Professor with the Information Systems Department, College of Computer and Information Sciences (CCIS-IS), Princess Nourah Bint Abdulrahman University (PNU), Saudi Arabia. Her research interests include information systems engineering, business process engineering, process mining, context-aware computing, deep learning, and artificial intelligence.

MOURAD ZAIED received the Engineer degree in computer science from the National Engineering School of Monastir, Tunisia, and the master's degree in computer engineering and the Ph.D. and H.D.R. degrees in computer science from the National Engineering School of Sfax, Tunisia, in 2003, 2008, and 2013, respectively. He is a Full Professor of computer science with the National Engineering School of Gabes. He has been a part of academia for more than 20 years. He has devoted his career to pushing the boundaries of research in artificial intelligence and computer vision. He also brings valuable insights, to the realm of computer science with his research work. At the University of Gabes, he has founded and heads the Research Team on Intelligent Machines (RTIM) Laboratory, guiding a group of researchers in exploring studies in artificial intelligence, computer vision, and the IoT. He is well regarded for his research having published extensively in journals and conferences showcasing the influence of his scholarly endeavors. He has supervised many Ph.D. theses and contributed to several edited scientific books. His commitment to pushing the boundaries of computer science has been acknowledged with honors and prizes both at home and abroad. He is highly regarded in the community, due to his significant impact on academia dedication, research and teaching, and forward thinking approach. His leadership and groundbreaking studies are influencing the evolution of computer science and motivating aspiring scholars.