Vokasi Unesa Bulletin of Engineering, Technology and Applied Science (VUBETA)
https://journal.unesa.ac.id/index.php/vubeta
Vol. 3, No. 2, 2026, pp. 330~343 DOI: 10.26740/vubeta.v3i2.44096
ISSN: 3064-0768

Biomedical Colors Images Watermarking Scheme Based on LSB, Henon Map and ECKBA

Noura Alexendre[1*], Fotsing Kuetche[1], Welba Colince[2], Simo Thierry[1], Ntsama Eloundou Pascal[3]
[1]Department of Physics, Faculty of Sciences, University of Ngaoundéré, Ngaoundéré, Cameroon
[2]Department of Fundamental Sciences, National Advanced School of Mines and Petroleum Industries, University of Maroua, Maroua, Cameroon
[3]Department of Physics, National Teaching School of Bertoua, University of Bertoua, Bertoua, Cameroon

Article Info

Article history:

Received July 14, 2025
Revised February 15, 2026
Accepted March 10, 2026

Keywords:

Biomedical Image
LSB Watermarking
Henon map
Enhanced Chaotic Key-Based

ABSTRACT

With rapid digitalization in healthcare, biomedical images like X-rays, CT, MRI, and ultrasound scans are routinely transmitted, stored, and shared across hospital networks and telemedicine platforms. Ensuring data security, authenticity, and patient privacy during this process is a major challenge. Unauthorized access, modification, or duplication of images can result in diagnostic errors, legal issues, and loss of patient trust. Researchers have developed algorithms for image watermarking (embedding copyright or authentication information) and image encryption (scrambling data to protect it) to address these concerns. In this article, we present an algorithm that combines watermarking with encryption to enhance security and ensure confidentiality for medical images. Our approach centers on a blind hybrid watermarking technique. 'Blind' means the original image is not needed to extract the watermark, and 'hybrid' refers to combining techniques. This method specifically uses LSB (Least Significant Bit) embedding with a text image as the watermark. For encryption, chaotic sequences generated by the Henon map (a mathematical system used to generate pseudo-random numbers) power selective encryption, while the Enhanced 1D Chaotic Key Based Algorithm (ECKBA) is used for image encryption. The main advantage is our method's ability to generate a large space of encryption keys, critical for resisting brute-force attacks. Experimental and planned results demonstrate the robustness of our algorithm against common attacks and its watermark's invisibility to the human eye.

1. INTRODUCTION

As healthcare systems become increasingly digitized, digital information systems such as hospital information systems (HIS), picture archiving and communication systems (PACS), and electronic medical record (EMR) systems play a crucial role [1][4]. Compared to analog (non-digital) data, digital medical data offers significant advantages, including efficient compression (reducing file size for streamlined storage and sharing), transmission (enabling electronic data transfer), and image enhancement (improving visual quality through digital tools). Nevertheless, current transmission methods may allow unauthorized interception or alteration of sensitive medical data over public networks, such as the Internet, especially in telemedicine contexts. Therefore, implementing robust security measures in clinical information systems is essential. Digital watermarking—the imperceptible embedding of supplemental information into host signals (such as images, audio, or video)—has emerged as a promising approach to securing multimedia data. Applied in medical settings, watermarked images can remain compliant with the DICOM (Digital Imaging and Communications in Medicine) format [2][3], the standard for handling, storing, and transmitting medical images, and the embedded security information can persist even if the image format changes. Additionally, the watermark's subtlety makes it more challenging for unauthorized parties to detect or compromise the hidden information. Due to these benefits, researchers have adopted watermarking techniques in medical data [4]–[10].

For example, Zhou et al. presented a watermarking method for verifying the authenticity and integrity of digital mammography images. They embedded a digital envelope in the image using the least significant

*Corresponding Author
Email: nouraalexendre@gmail.com

bit (LSB) [11]. Mousavi et al. [12] provided an extensive survey, outlining the potential of watermarking for confidentiality and integrity in medical imaging. Sujatha [13] introduced a blind watermarking technique based on discrete wavelet transform (DWT) decomposition for image authentication. Earlier work by Puech et al. [14] demonstrated that robust watermarking algorithms, when combined with AES encryption, can effectively safeguard the confidentiality and integrity of medical images. Gokcen et al. [15] proposed a robust chaotic digital image watermarking scheme based on redundant discrete wavelet transform (RDWT) and singular value decomposition (SVD).

Welba et al. [16][17] have integrated watermarking strategies to securely embed patient data in biomedical images. Several studies [18]–[21] have further enhanced performance by exploiting various transformations. Methods such as wavelet, empirical mode decomposition, and discrete cosine transform (DCT) have improved embedding capacity and robustness [22]–[25].

Several researchers have proposed data protection techniques based on watermarking and encryption for digital imaging and communication in medicine, including partial encryption methods [26]. In [27], a coding algorithm was proposed to determine selective blocks for regular embedding. In [28], a scheme integrating modular arithmetic and chaos theory was introduced for image encryption and decryption. Benoraira et al. proposed a blind watermarking scheme that embeds bits differentially into two DCT-transformed sub-vectors of the LL sub-band in the DWT. This achieves robust extraction without threshold setting [5][6][29][30]. Bao and Wang embed color watermark bits into mid-frequency DCT coefficients in the Radon transform domain. A geometric correction mechanism resists rotation, scaling, and cropping [31]. Liu and Li extract feature vectors via DWT and DFT and secure the watermark using a logistic chaotic map before embedding. This approach provides strong robustness against geometric and signal-processing attacks [32]. Li et al. fuse accelerated-KAZE feature extraction with DCT, perceptual hashing, and chaotic scrambling. This enables zero-watermarking that is highly resistant to a wide range of attacks [33].

According to the scientific studies listed above, image watermarking provides authentication and allows the confidential insertion of personal and essential information. In the medical field, combining image watermarking and encryption is paramount, as this addresses key security requirements, including authentication and confidentiality. Additionally, robustness against attacks, algorithm reversibility, speed, and strong integration capacity are essential features for the successful transmission of medical images via transmission channels. Our algorithm meets all these needs.

2. METHOD

2.1. Least Significant Bit (LSB) Watermarking

Least Significant Bit (LSB) watermarking is a simple and widely used technique for invisible digital watermarking. In this method, each 8-bit pixel's least significant bit—the bit with the smallest value in the binary representation of the pixel's color—is replaced by a bit from the watermark. Changes to the least significant bit result in minimal changes to pixel intensity (brightness or color value). As a result, the embedded watermark is often imperceptible to the human visual system. This is especially true in regions of high texture or visual complexity; such areas have many details or variations in color and intensity [34][35]. Information can be embedded directly into every pixel, or preferentially in busy regions where small modifications are less noticeable [36]. Despite its low computational complexity and ease of implementation, LSB insertion is inherently vulnerable to noise (random changes during storage or transmission). It is also susceptible to compression (reducing file size by discarding data) and cropping attacks (removal of image parts). These vulnerabilities have driven researchers to develop enhanced, adaptive methods and hybrid schemes. Such methods combine LSB modifications with transform-domain techniques (like embedding information after transforming the image into the frequency domain) to improve robustness [37].

2.2. The Enhanced Chaotic Key-Based Algorithm (ECKBA)

The Enhanced Chaotic Key-Based Algorithm (ECKBA) enhances the original CKBA by incorporating a more robust chaotic map and expanding the key size to 128 bits. It also applies substitution and permutation steps to strengthen resistance against differential cryptanalysis [38][39]. The algorithm employs CBC mode to bolster security while sustaining efficient performance for multimedia encryption.

Let I be an $M \times N$ image with b-byte pixel values, where a pixel value is denoted by I(i),$0 \leq i < M \times N \times b$, scanned in the raster order. Let Cμ be a one-dimensional chaotic map—a mathematical function that exhibits unpredictable behavior—characterized by a real coefficient μ, which is determined by normalizing a 32-bit integer $\mu I32$ to fit within the chaotic interval. Let x (0), the initial value for Cμ, be set by normalizing a 32-bit integer $xI32$ to a value within the range defined for Cμ. For any n-bit binary segment x, let l(x) represent its least significant (lower) half and h(x) its most significant (upper) half. In addition, we define an S-box transformation σr, where an S-box (substitution box) is a basic cryptographic component that performs substitution operations on input data. and its inverse $\sigma_r^{(-1)}$as follows:

$$\sigma_r(x,y) = \begin{cases} x \oplus y & if\ r\ is\ even \\ x + y\ mod\ 256, & if\ r\ odd \end{cases} \quad (1)$$

$$\sigma_r^{-1}(x,y) = \begin{cases} x \oplus y, & if\ r\ is\ even \\ x - y\ mod\ 256, & if\ r\ odd \end{cases} \quad (2)$$

where x and y are two bytes.

The ECKBA encryption and decryption schemes are implemented by Algorithms 1 and 2, respectively. In the algorithm, we use the following notation: if if x_{I32} denotes a 32-bit integer variable, then x denotes its normalized floating-point representation corresponding to the relevant real interval, and vice versa.

The Enhanced CKBA (ECKBA) encryption algorithm processes an image by first initializing chaotic parameters and cipher-block chaining with a 128-bit key. It then generates pseudo-random sequences from a piecewise linear chaotic map (PWLCM) to derive substitution keys and permutation indices. Each pixel is XORed with the previous cipher-block, implementing cipher-block chaining. Multiple rounds of substitution use an S-box, and permutation uses a P-box. Chaotic sequences control these transformations to enhance security and resist cryptanalysis.

Conversely, the ECKBA decryption algorithm reverses this process by first initializing the same parameters as in encryption, then performing inverse transformations in reverse order. It starts by applying the inverse permutation and inverse substitution using the inverse S-box, guided by the same chaotic sequences used in encryption. Finally, it XORs each pixel with the previous cipher block to undo the cipher block chaining, thereby reconstructing the original plaintext image.

ENCRYPTION ALGORITHM
Data: An M × N × b plain-image I, 128-bit key k, and the number of rounds r.
Result: An M × N × b cipher-image I'.
begin
  x(r/4 - 1)$_{I32}$ ← l(l(k)); α$_{I32}$ ← h(l(k))
  y(r/2 - 1)$_{I32}$ ← l(h(k)); β$_{I32}$ ← h(h(k))
  I'(-1) ← 0
  for i = 0 to r/4 - 1 do
    z(i) ← 0
  end
  for i = 0 to MNb - 1 do
    if i = 0 mod r then
      if i > 0 then
        for j = 0 to r/4 - 1 do
          t ← i - r + 4j
          z(j)$_{I32}$ ← I'(t) || I'(t+1) || I'(t+2) || I'(t+3)
        end
      end
      for j = 0 to r/4 - 1 do
        x(j) ← Cα(x(j - 1 mod r/4))
        x(j) ← x(j) + z(j) mod 1
        c(4j) ← l(l(x(j)$_{I32}$))
        c(4j+1) ← l(h(x(j)$_{I32}$))
        c(4j+2) ← h(l(x(j)$_{I32}$))
        c(4j+3) ← h(h(x(j)$_{I32}$))
      end
      for j = 0 to r/2 - 1 do
        y(j) ← Cβ(y(j - 1 mod r/2))
        z(j) ← x(j) + z(j mod r/4) mod 1
        d(2j) ← l(y(j)$_{I32}$) mod 8!
        d(2j+1) ← h(y(j)$_{I32}$) mod 8!
      end
    end
    I'(i) ← I(i) ⊕ I'(i - 1)
    for j = 0 to r - 1 do
      I'(i) ← σ$_j$(I'(i), c(i + j mod r))
      I'(i) ← π$_{d(4j+ij\ mod\ 8!)}$(I'(i))
    end
  end
end

DECRYPTION ALGORITHM
Data: An M × N × b plain-image I, 128-bit key k, and the number of rounds r.
Result: An M × N × b cipher-image I'.
begin
  x(r/4 - 1)$_{I32}$ ← l(l(k)); α$_{I32}$ ← h(l(k))
  y(r/2 - 1)$_{I32}$ ← l(h(k)); β$_{I32}$ ← h(h(k))
  I(-1) ← 0
  for i = 0 to r/4 - 1 do
    z(i) ← 0
  end
  for i = 0 to MNb - 1 do
    if i = 0 mod r then
      if i > 0 then
        for j = 0 to r/4 - 1 do
          t ← i - r + 4j
          z(j)$_{I32}$ ← I(t) || I(t+1) || I(t+2) || I(t+3)
        end
      end
      for j = 0 to r/4 - 1 do
        x(j) ← Cα(x(j - 1 mod r/4))
        x(j) ← x(j) + z(j) mod 1
        c(4j) ← l(l(x(j)$_{I32}$))
        c(4j+1) ← l(h(x(j)$_{I32}$))
        c(4j+2) ← h(l(x(j)$_{I32}$))
        c(4j+3) ← h(h(x(j)$_{I32}$))
      end
      for j = 0 to r/2 - 1 do
        y(j) ← Cβ(y(j - 1 mod r/2))
        z(j) ← x(j) + z(j mod r/4) mod 1
        d(2j) ← l(y(j)$_{I32}$) mod 8!
        d(2j+1) ← h(y(j)$_{I32}$) mod 8!
      end
    end
    I'(i) ← I(i)
    for j = 0 to r - 1 do
      I'(i) ← π$^{-1}_{d(i+j\ mod\ 8!)}$(I'(i))
      I'(i) ← σ$_j^{-1}$(I'(i), c(i + j mod r))
    end
    I'(i) ← I'(i) ⊕ I(i - 1)
  end
end

Chaotic permutation and substitution methods

The ECKBA [40] encryption algorithm, presented in Figure 1, transforms an image I using a substitution (S) and a bit-permutation (P) network controlled by a PWLCM chaotic map. The algorithm performs r rounds of the SP-network on each pixel. The next iteration i+1 of the chaotic map is perturbed using the previous cipher block C_i.

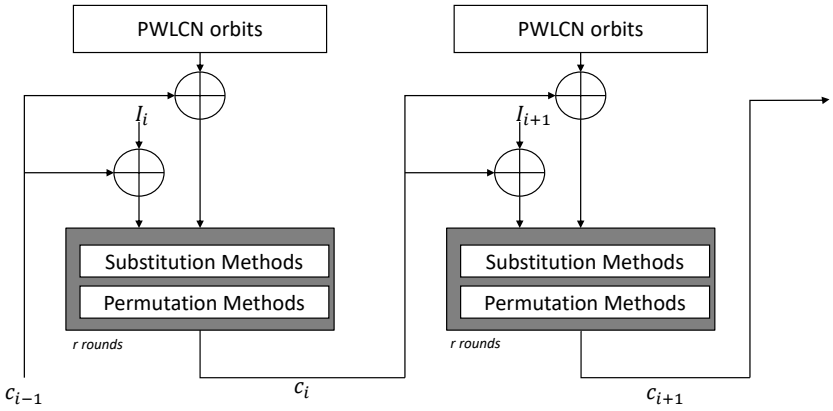


Figure 1. The ECKBA encryption algorithm

2.3. Henon Map

The Henon map is a two-dimensional nonlinear discrete chaotic system widely used in the study of image encryption due to its sensitivity to initial conditions, unpredictability, and ergodic properties, which align well with the requirements for secure encryption algorithms [41][42]. It is defined mathematically as:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 - y_n \\ y_{n+1} = bx_n \end{cases} \quad (3)$$

where n represents the iteration number, x and y are the iteration values, and a and b are control parameters.

The parameters a and b are typically constrained within the ranges a ∈ [0,1.4] and b ∈ [0.2,0.314], ensuring chaotic behavior under specific values such as a=1.4 and b=0.31. In image encryption applications, these parameters are often fine-tuned; for instance, in the proposed algorithm, a=1.399 and b=0.314 are selected to optimize the chaotic dynamics for secure encryption. Fig. 2 shows images of the Henon map for different parameter values. In our proposed algorithm, we set a = 1.399 and b = 0.314.

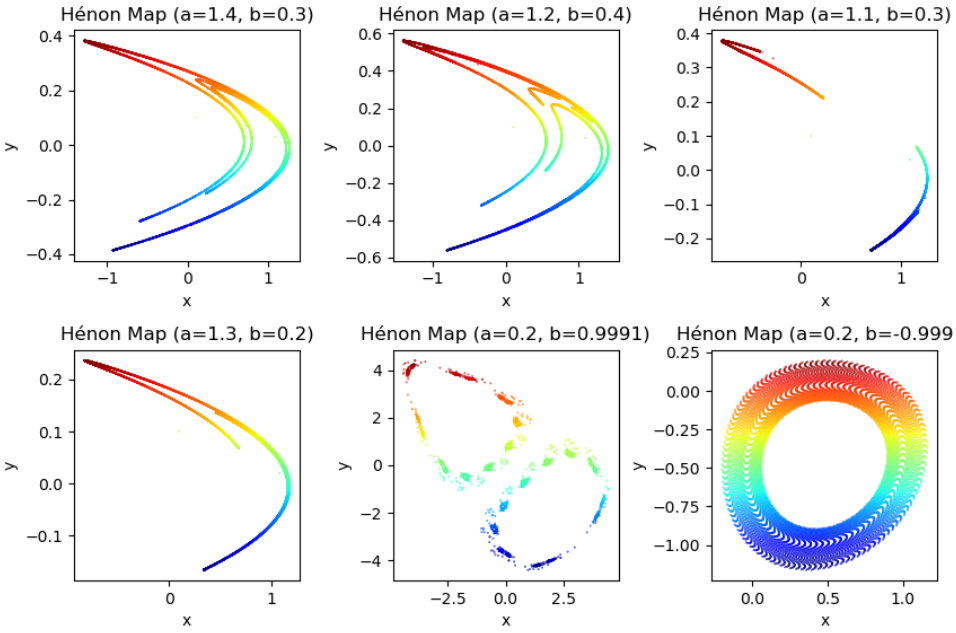


Figure 2. Images of Henon map

3. PROPOSED METHOD

Figure 3 shows the proposed scheme for biomedical images encryption.

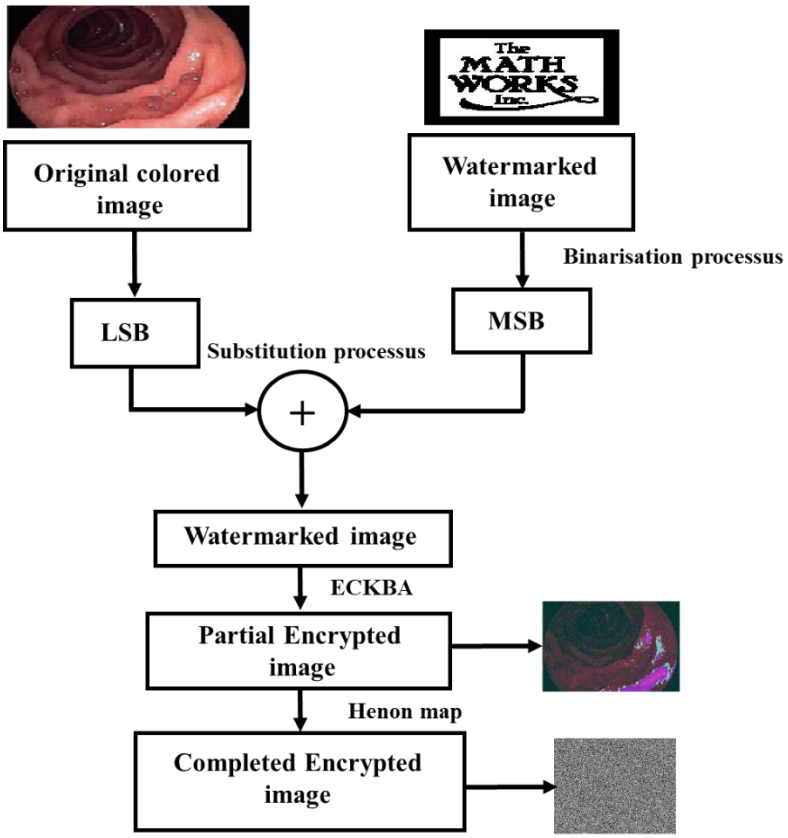


Figure 3. Proposed Method

3.1. Watermarks Embedding

Figure 4 presents the watermarks embedding algorithm:

Step 1: Extract the feature vector $VF(j)$ using $DTCWT - DCT$ transform on the original image $Oi(i,j)$, using the feature extraction method above

Step 2 : generate binary henon sequences $Key_n(i,j)$ with the following operations:

$$Key_n(i,j) = VF(j) \oplus BW_n(i,j) \quad (4)$$

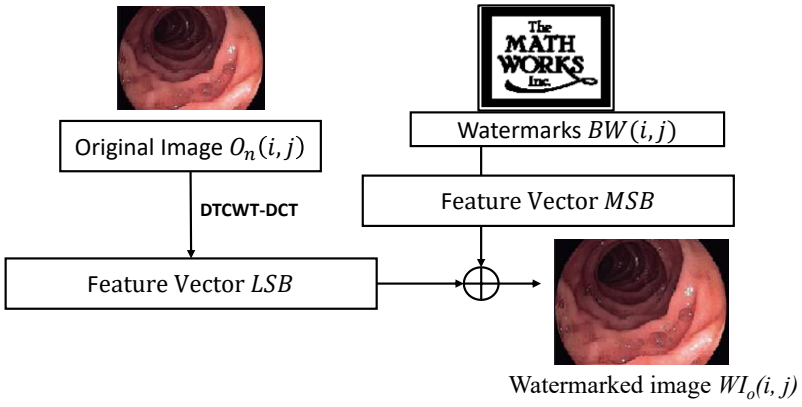


Figure 4. Watermarks embedding algorithm

3.2. Watermarks Extraction

Figure 5 presents the watermarks extraction algorithm:

Step 5: Apply the same operation as step 3 to tested image $Oi'(i,j)$ to get a feature vector $VF'(j)$
Step 6: Extract the watermarks $BW_{n'}(i,j)$ via the following operate:

$$BW_{n'}(i,j) = Key_n(i,j) \oplus VF'(j) \quad (5)$$

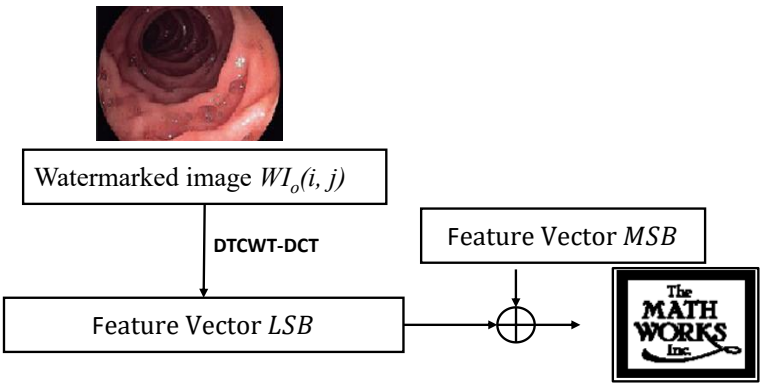


Figure 5. Watermarks Extraction algorithm

4. RESULTS AND DISCUSSION

4.1. Tests of Imperceptibility

a) Peak-Signal-To-Noise-Ratio (PSNR) and Normalized Correlation (NC

The peak signal-to-noise ratio (PSNR) is a measure of the ratio of the maximum signal power to the noise affecting its quality [43][44]. In the context of images, it is often used to evaluate the quality of a compressed or modified image relative to the original image. It is also used to assess the degree of similarity between the original and watermarked images. A high PSNR indicates high image quality. The formula for calculating the PSNR between two images is as follows:

$$psnr = 10log_{10}\left(\frac{max^2}{MSE}\right) \quad (6)$$

MSE (Mean Squared Error) represents the average error between the original and watermarked images; the lower the MSE, the better the imperceptibility.
The higher the PSNR, the better the quality (and therefore the imperceptibility). Typical acceptable value: > 35 dB.

Normalized Correlation (NC) is a widely used measure in image watermarking, particularly for assessing the fidelity of the extracted watermark to the inserted watermark. It ranges from 0 (no correlation) to 1 (perfect correlation) and measures the similarity and difference between the original and extracted watermarks. Generally, an NC score between 1 and 0.7 is acceptable.

$$NC = \frac{\sum_{i=0}^{n} Or_{watermark} \times Ex_{watermark}}{(\sum_{i=0}^{n} Or_{watermark} \times \sum_{i=0}^{n} Ex_{watermark})^{\frac{1}{2}}} \quad (7)$$

$Or_{watermark}$ is original watermark, $Ex_{watermark}$ is extracted watermark is number of pixels in watermark.

b) Bit Error Ratio (BER)

The bit error ratio (BER) is used to measure the ratio between the number of bits received in error and the total number of bits received [45]. The BER measures the accuracy of the extracted watermark bits, and is calculated as follows:

$$BER = \frac{N\prime}{N} \quad (8)$$

where N' indicates the total number of embedded watermark bits and N represents the number of bits that are erroneous when extracting the watermark. Therefore, when all watermark information is correctly extracted, the BER is 0.

c) Structural similarity index measurement (SSIM)

The Structural Similarity Index Measure (SSIM) was introduced by [46] to quantify the structural similarity between two images. Unlike MSE and PSNR, which do not account for image structure and

measure absolute errors, SSIM is based on luminance, contrast, and changes in structural information. The key idea behind this measure is that pixels are highly correlated, especially when they are spatially close [8]. The SSIM metric is defined by:

$$SSIM = \frac{(2\mu_{x_r}\mu_{x_g}+C_1)(2\sigma_{x_r x_g}+C_2)}{(\mu_{x_r}^2+\mu_{x_g}^2+C_1)(\sigma_{x_r}^2+\sigma_{x_g}^2+C_2)} \quad (9)$$

where μ_{x_r} et μ_{x_g} represent the mean values of the pixels in the original image x_r and the watermarked image x_g, respectively. Consequently, σxr and σxg are the standard deviations of x_r e x_g. Furthermore, $\sigma_{x_r x_g}$denotes the covariance between the two images, while C_1 and C_2 are constants defined to avoid instability. Table 1 presents the PSNR value. We observe that PSNR improves as the scale coefficient decreases. From this table, it is clear that the PSNR values are very high, indicating that our watermarking method maintains high-quality watermarking images.

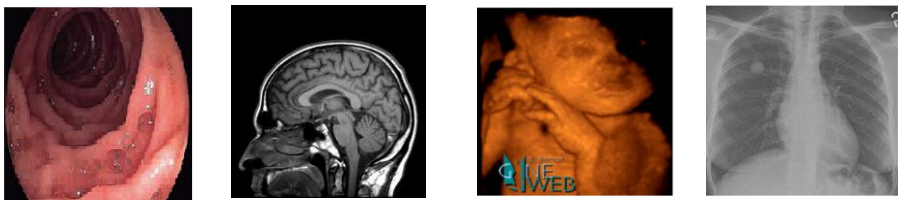
Table 1. PSNR obtained values

Images	*MSE*	*PSNR*	NC	BER
Image 1	0.73	$PSNR = 57.45$	0.932	0.991
Image 2	0.45	$PSNR = 54.01$	0.966	0.985
Image 3	0.54	$PSNR = 58.32$	0.973	0.998
Image 4	0.34	$PSNR = 51.44$	0.967	0.962

Test results for our scheme are compared with those of other researchers' schemes working in the same domain.

(a) **(b)** **(c)** **(d)** **(e)**

Figure 6. (a) : original Image1, (b) : Original Image 2, (c) : original Image 3,d) : Original Image4, e) : Watermark Image.



a) Watermarked image 1 $PSNR = 57,45$

b) Watermarked image 2 $PSNR = 54,01$

c) Watermarked image 3 $PSNR = 58,32$

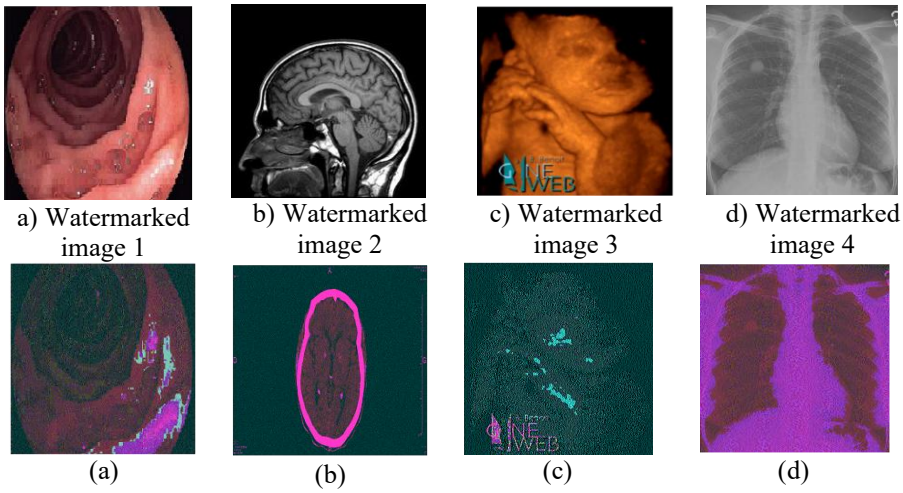
d) Watermarked image 4 $PSNR = 51,44$

Figure 7. (a) Watermarked Image1, (b) Watermarked, Image2, c) Watermarked Image3, (d) Watermarked Image4.

Figure 7 and Table 2 show the results under different scale factors. The PSNR results in our case are superior to 50, indicating the robustness and imperceptibility of the proposed scheme.

Table 2. Comparison of proposed scheme with some works

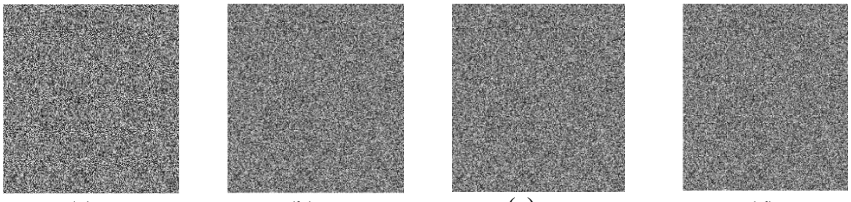
geometrical Attacks	Intensity of Attacks	Aditi Zear et al.[47] NC1	Rohit Thanki et al. [48] NC2	Xiaochen Yuan et al. [49] NC3	Amit Kumar Singh et al. [50] NC4	Proposed Algorithm NC	BER
Rotation (clockwise)	10° 20° 40°	0.21 0.17 0.10	0.85 0.92 0.95	0.86 0.84 0.80	0.85 0.82 0.53	0.91 0.92 0.89	0.0067
Scaling	0.4 0.8 2.0	0.39 0.54 0.92	0.52 0.61 0.91	0.59 0.63 0.74	0.93 0.99 0.99	0.98 0.98 1.00	0.0078
Down Translation	8% 15% 20%	0.73 0.66 0.54	0.80 0.69 0.63	0.86 0.77 0.61	0.90 0.79 0.71	0.99 0.90 0.77	0.0068
Left Translation	3% 5% 8%	0.77 0.74 0.70	0.88 0.84 0.72	0.90 0.83 0.66	0.91 0.81 0.77	0.96 0.95 0.89	0.00756
Cropping	12% 23% 35%	0.76 0.21 0.03	0.95 0.92 0.33	0.97 0.92 0.02	0.88 0.64 0.14	1.00 1.00 0.64	0.00743



a) Watermarked image 1 b) Watermarked image 2 c) Watermarked image 3 d) Watermarked image 4

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

Figure 8. a) Image1 partially encrypted b), Image2 partially encrypted c), Image partially encrypted 3 ,d) Image4 partially encrypted)



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

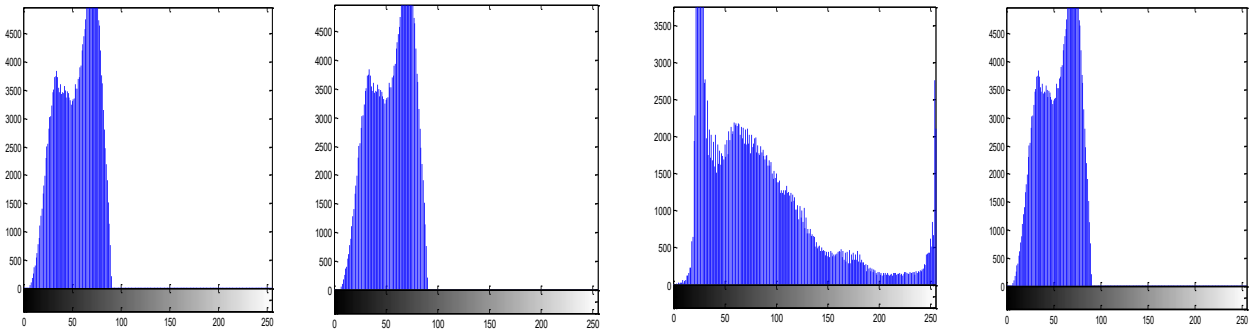
Figure 9. Encrypted image Image1 a), Encrypted image Image2 b), Encrypted image Image3 c) Encrypted image Image4.

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

Figure 10. a) Mark1 extracted (NC=0.992), b) Mark2 extracted (NC=0.988), c) Mark3 extracted (NC=0.976), d) Mark extracted (NC=0.996).

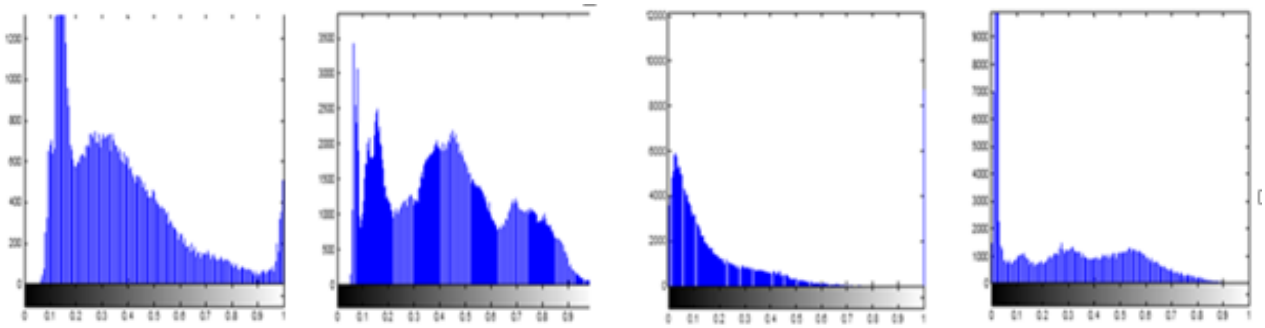
Histogram-based analysis

The histogram is one of the security analysis elements of a cryptographic algorithm. It provides information on the statistical properties of the encrypted image. The histogram of an encrypted image shows the distribution of its pixels. When the image is perfectly encrypted, the histogram is uniform (i.e., the pixel distribution is uniform). The figures below show the histograms of the four test images (image1, image2, image3, image4).



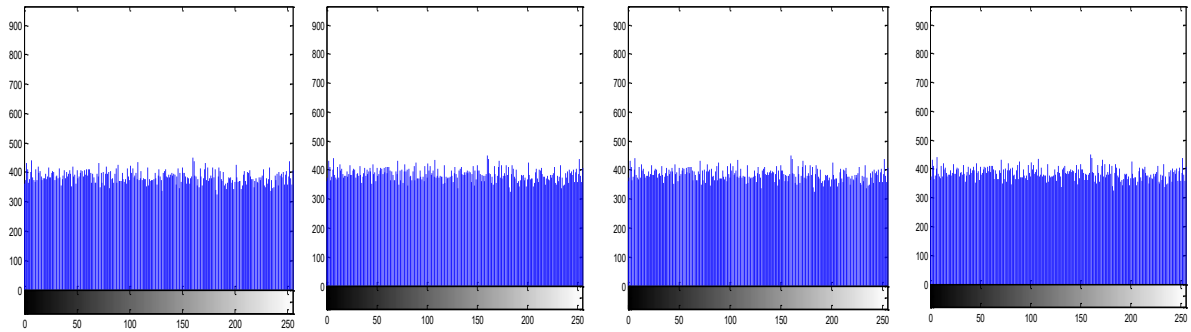
(a) (b) (c) (d)

Figure 10. a) Histogram Image1 partially encrypted b) Histogram Image2 partially encrypted c) Histogram Image3 encrypted partially d) Histogram Image4 partially encrypted



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

Figure 11. a) Original histogram Image1, b) Original histogram Image2, c) Original histogram Image3, d) Histogram of original image4



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

Figure 12. a) Histogram of the coded image Image1, b) Histogram of the coded image Image2, c) Histogram of the coded image Image3, d) Histogram of the coded image Image4

3.4. Security Analysis, key sensitivity Test

3.6. Correlation Coefficient Analysis

Correlation coefficients play an essential role in assessing the security of an encryption algorithm, particularly when processing encrypted images or sensitive data. Here's a clear explanation of their definition, importance, and interpretation. The correlation coefficient (often Pearson's) measures the degree of linear dependence between two variables. Its value ranges from -1 to +1:

- +1: perfectly positive correlation.
- 0: no correlation.
- -1: perfectly negative correlation.

In a cryptographic context, it is generally used to measure the correlation between neighboring pixels (or neighboring bits) before and after encryption. The correlation coefficients are also calculated by following the formula:

$$cov(n,m) = E\big(n - E(n)\big)\big(m - E(m)\big) \tag{8}$$

$$r_{nm} = \frac{cov(n,m)}{\big(\sqrt{D(n)}\big)(\sqrt{D(m)})} \tag{9}$$

where n and m are intensities values of two adjacent pixels, r_{nm} is the correlation coefficient. $cov(n,m)$, $E(n)$ and $D(n)$ are given as follows

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

$$D(n) = \frac{1}{N}\sum_{i=1}^{N}\big(n_i - E(n)\big)^2 \tag{11}$$

$$cov(n,m) = \frac{1}{N}\big(n_i - E(n)\big)\big(m_i - E(m)\big) \tag{12}$$

Table 3 below shows the correlation coefficients of the four test images calculated

Table 3. Correlation coefficients of tested images

	Direction		
Images	Horizontal	Vertical	Diagonal
Image1	−0008	00019	0004
Image2	00021	00012	00028
Image3	00064	−0013	00069
Image4	00044	00033	0072

Figure 14 and 15 present the correlation coefficients between neighboring pixels for the original and encrypted images, respectively.

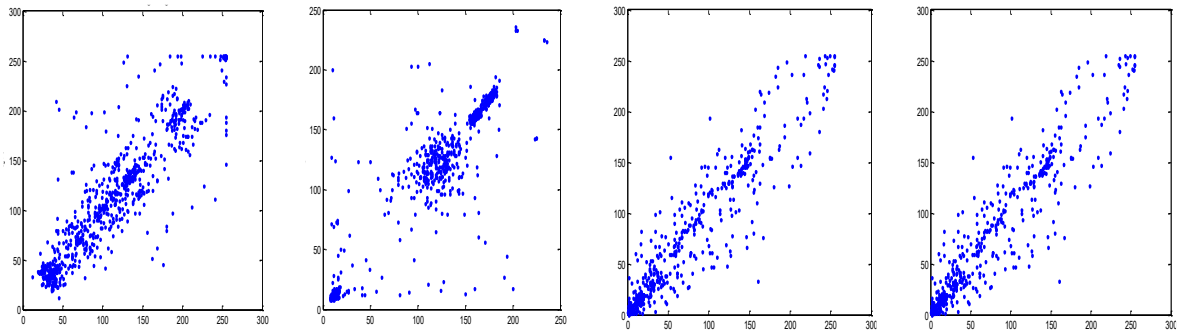


Figure 13. a) Correlation original image1, b) Correlation original image2, c) Correlation original image3, d) Correlation original image4

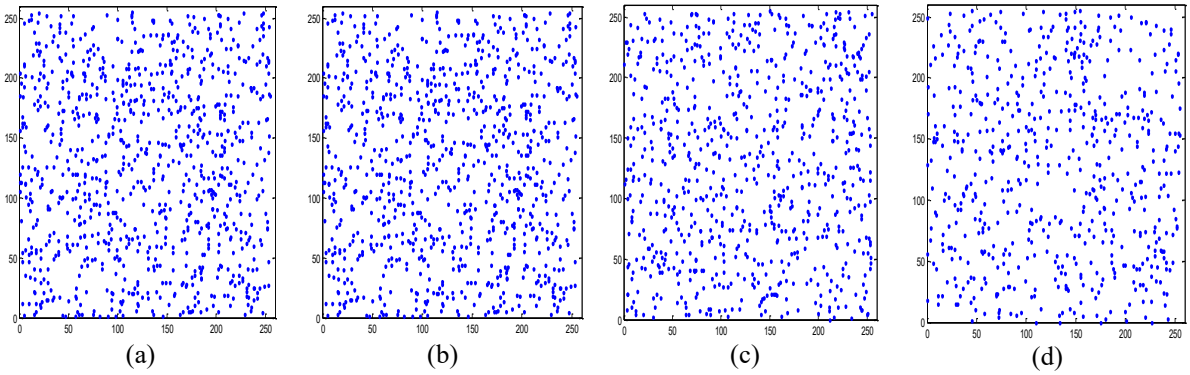


Figure 14. a) Correlation of encrypted watermarked image1, b) Correlation of encrypted watermarked image2, c) Correlation of encrypted watermarked image3, d) Correlation of encrypted watermarked image4.

It is noteworthy that in Figure 14, the pixels are concentrated in a specific area, resulting in a high correlation. The former situation is highly desirable in cryptography, as it allows us to conclude that the encryption algorithm is very robust.

3.7. Differential Analysis

Differential analysis in image encryption is a method of assessing the robustness of an encryption algorithm against attacks in which an attacker attempts to deduce the key or encryption scheme by observing the effects of small modifications on the original image. Number of Pixels Change Rate (NPCR) measures the percentage of pixels that change between two encrypted images, when only one pixel has changed in the original image. The Unified Average Changing Intensity (UACI) measures the average intensity change between two coded images.

$$\text{NPCR} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{L} D_j}{H \times L} \qquad \text{ith} \quad D_{i;j} = \begin{cases} 1 & if\ I_{o1} \neq I_{O2} \\ 0 & if\ I_{o1} = I_{o2} \end{cases}$$

$$\text{UACI} = \frac{1}{H \times L}\sum_{i=1}^{H}\sum_{j=1}^{L}\frac{I_{o1(i,j)} - I_{o2(i,j)}}{2^8 - 1} \times 100\%$$

Table 4 presents the values obtained after testing the original images.

Table 4. Obtained values of NPCR and UACI

Images	NPCR(%)	UACI(%)
Encrypted image 1	97.56%	41.04%
Encrypted image 2	98.55%	42.34%
Encrypted image 3	98.33%	43.56%
Encrypted image 4	99.37%	43.02%

In the above table. It is worth noting the values of the encryption tests. acting on the NPCR. They are around 95% to 99%. while the UACI values are above 40%. These results denote the robustness and confidentiality of the encryption process developed.

5. CONCLUSION AND LIMITATION

In this article, we have proposed a color watermarking scheme for biomedical images. integrating LSB embedding. Henon map. and ECKBA encryption. This proposed algorithm consists of two main phases: the first is blind watermarking, which involves applying the LSB substitution algorithm. The second step is to encrypt the watermarked image using the Henon map. ECKBA algorithm using initial conditions. generate a number of iterations and a chaos parameter. The proposed method. offers a secure. imperceptible. and a lightweight solution for protecting sensitive medical data. The use of chaotic systems ensures high security and key sensitivity, while LSB minimizes visual distortion. crucial for diagnostic accuracy in biomedical images. This hybrid approach effectively balances robustness against attacks. low computational complexity. and high watermark capacity. making it highly suitable for secure medical image transmission and telemedicine applications. The experimental results, in particular, the PSNR. NC calculations for the watermarking stage and the encryption key sensitivity and security tests. Provide ample proof of the confidentiality and robustness of the developed method.

REFERENCES

[1] R. Jawad and R. Jawad, "Comparison Feed Forward Back Propagation Networks (FFBPNs) with Support Vector Machine (SVM) for Diagnosis Skin Cancer Based on Images," *Vokasi Unesa Bull. Eng. Technol. Appl. Sci.*, vol. 2, no. 2, pp. 127–135, 2025. https://doi.org/10.26740/vubeta.v2i2.36117.

[2] Q. Su, X. Zhang, and H. Wang, "A Blind Color Image Watermarking Algorithm Combined Spatial Domain And Svd," *Int. J. Intell. Syst.*, vol. 37, no. 8, pp. 4747–4771, 2022. https://doi.org/10.1002/int.22738.

[3] S. Chen, Q. Su, Y. Sun, and X. Zhang, "A Blind Color Image Watermarking Algorithm Using The Energy Concentration Principle Of Hadamard Matrix," *Optik*, vol. 249, p. 168231, 2022. https://doi.org/10.1016/j.ijleo.2021.168231.

[4] E. Gul, "A Blind Robust Color Image Watermarking Method Based On Discrete Wavelet Transform And Discrete Cosine Transform Using Grayscale Watermark Image," *Concurr. Comput. Pract. Exp.*, vol. 34, no. 22, p. e6884, 2022. https://doi.org/10.1002/cpe.6884.

[5] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, "A Dwt Based Watermarking Approach For Medical Image Protection," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 2, pp. 2931–2938, 2021. https://doi.org/10.1007/s12652-020-02450-9.

[6] M. Begum, J. Ferdush, and M. S. Uddin, "A Hybrid Robust Watermarking System Based On Discrete Cosine Transform, Discrete Wavelet Transform, And Singular Value Decomposition," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5856–5867, 2022. https://doi.org/10.1016/j.jksuci.2021.07.012.

[7] Y. Luo *et al.*, "A Multi-Scale Image Watermarking Based On Integer Wavelet Transform And Singular Value Decomposition," *Expert Syst. Appl.*, vol. 168, p. 114272, 2021. https://doi.org/10.1016/j.eswa.2020.114272.

[8] Q. Su, G. Wang, X. Zhang, G. Lv, and B. Chen, "A New Algorithm Of Blind Color Image Watermarking Based On Lu Decomposition," *Multidimens. Syst. Signal Process.*, vol. 29, pp. 1055–1074, 2018. https://doi.org/10.1007/s11045-017-0487-7.

[9] P. T. Nha and T. M. Thanh, "A Novel Image Watermarking Scheme Using Lu Decomposition," *2021 RIVF International Conference on Computing and Communication Technologies (RIVF)*, IEEE, pp. 1–6, 2021. https://doi.org/10.1109/RIVF51545.2021.9642085.

[10] S. P. Maity and M. K. Kundu, "DHT Domain Digital Watermarking With Low Loss In Image Informations," *AEU - Int. J. Electron. Commun.*, vol. 64, no. 3, pp. 243–257, 2010. https://doi.org/10.1016/j.aeue.2008.10.004.

[11] X. Zhou, S. A. Lou, and H. K. Huang, "Authenticity And Integrity Of Digital Mammographic Images," *Medical Imaging 1999: PACS Design and Evaluation: Engineering and Clinical Issues*, SPIE, pp. 138–144, 1999. https://doi.org/10.1117/12.352736.

[12] S. M. Mousavi, A. Naghsh, and S. Abu-Bakar, "Watermarking Techniques Used In Medical Images: A Survey," *J. Digit. Imaging*, vol. 27, no. 6, pp. 714–729, 2014. https://doi.org/10.1007/s10278-014-9700-5.

[13] S. S.s and M. Sathik, "A Novel DWT Based Blind Watermarking for Image Authentication," *Int. J. Netw. Secur.*, vol. 14, Jul. 2012.

[14] W. Puech, M. Dumas, J. C. Borie, and M. Puech, "Tatouage D'images Cryptées Pour L'aide Au Télédiagnostic," in *Actes de Colloques. 18th Colloque Traitement du Signal et des Images, GRETSI*, Toulouse, France, 2001.

[15] G. Cetinel and Ll. Cerkezi, "Robust Chaotic Digital Image Watermarking Scheme Based On RDWT And SVD," *Int. J. Image Graph. Signal Process.*, vol. 8, no. 8, p. 58. https://doi.org/10.5815/ijigsp.2016.08.08

[16] C. Welba, S. Thiery, N. Alexendre, and N. P. Eloundou, "Exploitation Of Second- And Fourth-Order PDEs To Improve Lossy Compression Of Noisy Images," *Phys. Scr.*, vol. 98, p. 045025, 2023. https://doi.org/10.1088/1402-4896/acc2f1.

[17] C. Welba *et al.*, "Josephson Junction Model: FPGA Implementation and Chaos-Based Encryption of sEMG Signal through Image Encryption Technique," *Complexity*, 2022. https://doi.org/10.1155/2022/4510236.

[18] W. Alomoush *et al.*, "Improved Security Of Medical Images Using DWT–SVD Watermarking Mechanisms Based On Firefly Photinus Search Algorithm," *Discov. Appl. Sci.*, vol. 6, no. 7, p. 366, Jul. 2024. https://doi.org/10.1007/s42452-024-06066-y.

[19] X. Kang, Y. Chen, F. Zhao, and G. Lin, "Multi-Dimensional Particle Swarm Optimization For Robust Blind Image Watermarking Using Intertwining Logistic Map And Hybrid Domain," *Soft Comput.*, vol. 24, no. 14, pp. 10561–10584, 2020. https://doi.org/10.1007/s00500-019-04563-6.

[20] M. Begum *et al.*, "Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition for Enhanced Imperceptibility and Robustness," *Algorithms*, vol. 17, no. 1, Art. no. 1, 2024. https://doi.org/10.3390/a17010032.

[21] Laxmanika and P. K. Singh, "Robust And Imperceptible Image Watermarking Technique Based On SVD, DCT, BEMD And PSO In Wavelet Domain," *Multimed. Tools Appl.*, vol. 81, no. 16, pp. 22001–22026, 2022. https://doi.org/10.1007/s11042-021-11246-8.

[22] A. Benoraira, K. Benmahammed, and N. Boucenna, "Blind Image Watermarking Technique Based On Differential Embedding In DWT And DCT Domains," *EURASIP J. Adv. Signal Process.*, vol. 2015, no. 1, p. 55, 2015. https://doi.org/10.1186/s13634-015-0239-5.

[23] H. Wang, Z. Yuan, S. Chen, and Q. Su, "Embedding Color Watermark Image To Color Host Image Based On 2d-Dct," *Optik*, 2023. https://doi.org/10.1016/j.ijleo.2023.170585.

[24] K. Fares, A. Khaldi, K. Redouane, and E. Salah, "DCT & DWT Based Watermarking Scheme For Medical Information Security," *Biomed. Signal Process. Control*, vol. 66, p. 102403, 2021. https://doi.org/10.1016/j.bspc.2020.102403.

[25] P. Khare and V. K. Srivastava, "A Reliable And Secure Image Watermarking Algorithm Using Homomorphic Transform In Dwt Domain," *Multidimens. Syst. Signal Process.*, vol. 32, pp. 131–160, 2021. https://doi.org/10.1007/s11045-020-00732-1.

[26] S. Thierry, N. Alexendre, and N. Pascal, "New Approach To Estimation Threshold Parameter Of The Anisotropic Diffusion Intended For Reduction Of Noise," vol. 67, Apr. 2020.
[27] N. Alexendre, N. E. Pascal, and B. Laurent, "Non-Blind Image Watermarking Scheme Using Bi-Dimensional Empirical Mode Decomposition, DWT, DCT and fuzzy set," *Glob. J. Eng. Sci. Res.*, vol. 4, no. 5, 2017. https://doi.org/10.5281/zenodo.581047.
[28] N. Alexendre, N. E. Pascal, and B. Laurent, "Non-Blind Wavelet Packet Watermarking Scheme Using Radon Transform," *Adv. Comput. Sci. Eng.*, vol. 15, no. 1/2, p. 41, 2015. https://doi.org/10.17654/CS015120041.
[29] E. Gul and A. N. Toprak, "Contourlet And Discrete Cosine Transform Based Quality Guaranteed Robust Image Watermarking Method Using Artificial Bee Colony Algorithm," *Expert Syst. Appl.*, vol. 212, p. 118730, 2023. https://doi.org/10.1016/j.eswa.2022.118730.
[30] A. Zear and P. K. Singh, "Secure And Robust Color Image Dual Watermarking Based On Lwt-Dct-Svd," *Multimed. Tools Appl.*, vol. 81, no. 19, pp. 26721–26738, 2022. https://doi.org/10.1007/s11042-020-10472-w.
[31] B. Bao and Y. Wang, "A Robust Blind Color Watermarking Algorithm Based On The Radon-DCT Transform," *Multimed. Tools Appl.*, vol. 83, no. 24, pp. 64663–64682, 2024. https://doi.org/10.1007/s11042-023-17875-5.
[32] Y. L. Liu and J. B. Li, "DWT-DFT and Logistic Map Based Watermarking Algorithm for Medical Image," *Appl. Mech. Mater.*, vol. 380–384, pp. 4124–4127, 2013. https://doi.org/10.4028/www.scientific.net/AMM.380-384.4124.
[33] D. Li, Y. Chen, J. Li, L. Cao, U. A. Bhatti, and P. Zhang, "Robust Watermarking Algorithm For Medical Images Based On Accelerated-KAZE Discrete Cosine Transform," *IET Biom.*, vol. 11, no. 6, pp. 534–546, 2022. https://doi.org/10.1049/bme2.12102.
[34] I. J. Cox, M. L. Miller, and J. A. Bloom, "Digital Watermarking and Steganography," Morgan Kaufmann, 2002. https://doi.org/10.1016/B978-155860714-9/50009-2.
[35] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding-A Survey," *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999. https://doi.org/10.1109/5.771065.
[36] M. Kharrazi, H. T. Sencar, and N. Memon, "Image-Adaptive Watermarking In The Spatial Domain," *IEEE Trans. Image Process.*, vol. 13, no. 5, pp. 710–722, 2004.
[37] G. Bhatnagar and N. Rao, "Digital Watermarking Using LSB and Transform Domain Techniques," in *Proceedings of the International Conference on Digital Image Processing*, IEEE, 2007, pp. 450–455.
[38] N. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Chaos Solitons Fractals*, vol. 25, no. 3, pp. 775–784, 2006. https://doi.org/10.1016/j.chaos.2005.06.020.
[39] E. Yavuz, R. Yazıcı, M. C. Kasapbaşi, and E. Yamaç, "Enhanced Chaotic Key-Based Algorithm For Low-Entropy Image Encryption," *2014 22nd Signal Processing and Communications Applications Conference (SIU)*, pp. 385–388, 2014. https://doi.org/10.1109/SIU.2014.6830246.
[40] D. Socek, Shujun Li, S. S. Magliveras, and B. Furht, "Short Paper: Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption," *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, Athens, Greece: IEEE, pp. 406–407, 2025. https://doi.org/10.1109/SECURECOMM.2005.39.
[41] S. Kanwal *et al.*, "An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices," *Sensors*, vol. 22, no. 12, p. 4359, 2022. https://doi.org/10.3390/s22124359.
[42] J. Wu, X. Liao, and B. Yang, "Image Encryption Using 2D Hénon-Sine Map And DNA Approach," *Signal Process.*, vol. 153, pp. 11–23, 2018. https://doi.org/10.1016/j.sigpro.2018.06.008.
[43] G. Liu, H. Wang, and C. Miao, "A Three-Dimensional Text Image Watermarking Model Based On Multilayer Overlapping Of Extracted Two-Dimensional Information," *Inf. Process. Manag.*, vol. 60, no. 1, p. 103122, 2023. https://doi.org/10.1016/j.ipm.2022.103122.
[44] H. Cao, F. Hu, Y. Sun, S. Chen, and Q. Su, "Robust And Reversible Color Image Watermarking Based On Dft In The Spatial Domain," *Optik*, vol. 262, p. 169319, 2022. https://doi.org/10.1016/j.ijleo.2022.169319.
[45] P. Singh *et al.*, "Ensuring Integrity And Security Of Medical Image Transmission In Iomt Using Highly Imperceptible And Robust Watermarking Approach," *Sci. Rep.*, vol. 15, no. 1, p. 26058, 2025. https://doi.org/10.1038/s41598-025-11023-9.
[46] Zhou Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image Quality Assessment: From Error Visibility To Structural Similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004. https://doi.org/10.1109/TIP.2003.819861.
[47] A. Zear, A. K. Singh, and P. Kumar, "A Proposed Secure Multiple Watermarking Technique Based On DWT, DCT And SVD For Application In Medicine," *Multimed. Tools Appl.*, vol. 77, no. 4, pp. 4863–4882, 2018. https://doi.org/10.1007/s11042-016-3862-8.
[48] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "An Efficient Medical Image Watermarking Scheme Based on FDCuT–DCT," *Eng. Sci. Technol. Int. J.*, vol. 20, no. 4, pp. 1366–1379, 2017. https://doi.org/10.1016/j.jestch.2017.06.001.
[49] X.-C. Yuan and M. Li, "Local Multi-Watermarking Method Based On Robust And Adaptive Feature Extraction," *Signal Process.*, vol. 149, pp. 103–117, 2018. https://doi.org/10.1016/j.sigpro.2018.03.007.
[50] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Multiple Watermarking On Medical Images Using Selective Discrete Wavelet Transform Coefficients," *J. Med. Imaging Health Inform.*, vol. 5, no. 3, pp. 607–614, 2015. https://doi.org/10.1166/jmihi.2015.1432.

BIOGRAPHIES OF AUTHORS

Noura Alexendre is a researcher in Applied Artificial Intelligence with a focus on health. He holds a PhD in Electronics. Automatics. and Computer Science and he is lecturer at the Department of Physics at the University of Ngaoundere. Cameroon. He received his BSc in Electronics. Electrotechnics. and Automation from the Faculty of Science. University of Ngaoundere. in 2005. He later obtained his M.Eng in the same field and institution in 2009. His research interests are primarily focused on signal processing and image watermarking. He can be contacted via email at: nouraalaxendre@gmail.com.

Fotsing Kuetche is a researcher in Applied Artificial Intelligence with a focus on health and energy applications. He holds a PhD in Electronics, Automatics and Computer Science and published several scientific papers in this domain. Following his PhD, he expanded his work to include deep learning applications in photovoltaic fault diagnosis and now aims to develop AI systems suitable for resource-constrained environments, especially in African contexts. He can be contacted via email at Fotsing.fk@gmail.com