Ibn Al-Haitham Journal for Pure and Applied Sciences
Journal homepage: jih.uobaghdad.edu.iq
PISSN: 1609-4042, EISSN: 2521-3407
IHJPAS. 2026; 39(3)

Secured Blind Image Watermarking using DWT base with Mixing Random Generator of Lorenz Chaotic System and Geffe Algorithm

Hussein Noori Saadoon[1*] and **Ghadah Al-Khafaji**[2]
[1,2] Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq
*Corresponding Author.

Received: 23/January/2026
Accepted: 23/April/2026
Published: 20/July/2026
doi.org/10.30526/39.3.4433

Abstract

In the contemporary electronic era, the significance of safeguarding information has attained crucial proportions. The watermarking technique has been utilized in several contexts for multimedia copyright protection, as it is recognized as one of the most prevalent protective techniques. This paper is concerned with utilizing a secure blind watermarking system based on the frequency domain, along with the new approach that mixes between the Lorenz chaotic system and the Geffe algorithm as a random key generator, to improve the key's randomness for watermark encryption and thereby increase security. The process primarily involves transforming the cover color image into the YCbCr color model and subsequently applying the Discrete Wavelet Transform (DWT) to the Y channel, where the embedding occurs in the high-high (HH) sub-band at four designated locations. The performance of the watermarking system was evaluated on a miscellaneous dataset with ten natural images/hosts of square size 512 x 512 pixels, along with a 64 x 64 binary watermark image. The measures are based on the Normalized Cross-Correlation (NCC), Bit Error Rate (BER), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index Metric (SSIM). The results of the proposed system showed its superiority against prevalent attacks, including noise augmentation attacks, image enhancement assaults, geometric transformation attacks, and JPEG compression attacks. The system demonstrated high NCC values and acceptable imperceptibility.

Keywords: Copyright, DWT, Lorenz system, Geffe algorithm, Encryption, Watermark.

1. Introduction

The emergence of digital communication technologies in contemporary times has rendered information security essential for information and communication technology. There have been severe copyright infringement difficulties brought about as a result of the rapid growth of the Internet, which has made it easier than ever before to disseminate information [1,2]. These issues include unauthorized copying and distribution of digital works, as well as illegal efforts to manipulate digital works. As a result, the protection of intellectual property becomes extremely significant in order to enhance the safety of information that is stored on the internet. The infringement of images is widely considered to be the most prevalent type of infringement concern. Infringement of an image will have a significant effect on the entity that has the copyright. Therefore, protecting digital images from unauthorized access is an essential matter that must be addressed in order to guarantee the secure growth of the information society. Within the realm of multimedia copyright protection, the watermarking approach has been utilized in a variety of contexts due to its status as one of the most extensively utilized protection mechanisms. Image, text, audio, and video information are all protected by this technique, which is a common information-embedding technology, and it plays a crucial role in this process[3-5]. Digital watermarking is a derivative of a method called steganography, which has existed for decades. In digital image watermarking, a sequence of bits is implanted into a

multimedia object to establish ownership of the object. The primary aim of digital watermarking is to ensure the protection of copyright for digital content. The primary concern of the image watermarking technique is that the embedded watermark should not compromise the quality of the host image, and it must remain as inconspicuous as possible. The characteristic of the watermark's invisibility is referred to as imperceptibility, while the effectiveness of embedding the watermark into the host image is termed robustness [6,7]. Digital watermarking techniques can be classified into two categories based on their operational domain. Spatial domain watermarking is a method in which the embedding process involves direct modification of pixel values. The other approach is frequency domain watermarking; watermarks can be embedded in image transform coefficients. The watermarked image is reconstructed via inverse transformation. Fast Fourier Transform (FFT) and Discrete Cosine Transform (DCT) are common frequency domain watermarking transformation methods. Image watermark embedding using DCT techniques resists compression assaults. It is not very resistant to geometric modifications like rotations and translations. Thus, DCT frequency domain watermarking is limited. The prominent transformation employed in the multiresolution domain is the DWT. Superior resilience and imperceptibility are observed in this technique. This is because its time/frequency decomposition is more similar to theoretical models of the human visual system than previous methods [8,9].

This paper presents a notable development in chaos-based watermarking techniques. The proposed system facilitates the concealment of an encrypted watermark within an image by using a randomly generated key derived from the Lorenz chaotic system combined with the Geffe algorithm. The suggested system employs DWT in the transformation domain, hence enhancing its overall efficacy.

This is a description of the paper's composition. The second section covers related works, the third section explains materials and methods, the fourth section delineates experimental results and analysis, and section 5 ultimately presents the conclusion.

2. Related Works

The frequency domain watermarking enhances robustness by converting the image into frequency coefficients through a transformation technique. A new color image adaptive watermarking method using DWT, Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD) was developed by [10]. Researchers encrypt the watermark image with Lorenz hyperchaotic mapping to increase security. Calculate the Bhattacharyya distance between the cover image and the watermark image to determine the embedding factor, then use alpha blending to embed the watermark image into the Y component of the YCbCr color space to make the algorithm more imperceptible. Experimental results show that the method's average the Peak Signal-to-Noise Ratio (PSNR) is 45.9382 dB and the Structural Similarity Index Measure (SSIM) is 0.9986. Extensive experimental results and comparative analysis show that the approach finds a balance between imperceptibility, robustness, and embedding capability. Its vulnerability to geometric attacks, computational usage, and semi-blind extraction should be improved. [11] examined two frequency-domain blind watermarking systems and used a fractional-order chaotic PRNG for watermark encryption. The cover image is converted to YCbCr and frequency transformed using DCT and DWT on the Y channel. The DCT and DWT mid-frequency band and HH band coefficients receive the encrypted watermark. The fractional-order Lorenz system doubles the encryption key size and prevents brute-force assault. The offered methods use the statistical properties of the embedding medium to identify the hidden watermark by testing the PRNG and watermarking systems for imperceptibility and robustness. Noisy attacks, picture augmentation, and geometric manipulation are investigated. The Pseudo-Random Number Generator (PRNG) shows system factor sensitivity, while the watermarking techniques show excellent imperceptibility and robustness. The Quaternion Discrete Fourier Transform (QDFT) and Tensor Decomposition (TD) are used in [12] approach. QDFT is applied to non-

overlapping portions of the cover image. A third-order tensor is formed from QDFT's three imaginary frequency components. Tucker decomposition yields a core tensor from the third-order tensor. An upgraded odd–even quantization approach adds a watermark to the core tensor. The watermark extraction phase also corrects geometric distortion using pseudo-Zernike moments and a Multiple Output Least Squares Support Vector Regression (MLS–SVR) network model. The method distributes the watermark throughout a color image's three RGB channels using their intrinsic correlations. The experimental results show that the proposed approach defeats each color channel exchange assault with higher fidelity and robustness against standard image-processing and geometry attacks. In [13] use an orthogonal moment as an image feature descriptor and present a rotation correction method that can handle any order and repetition. A quantization-based color image watermarking methodology that increases the conventional approach's rotation attack resistance is developed to demonstrate the method's extended usefulness. Experimental results show that the calibration algorithm is ubiquitous and accurate. The suggested rotation angle estimates model mean square error rose from 0.042 to 0.018 and mean absolute error from 0.065 to 0.032. This update has made color picture watermarking techniques more resistant to geometric attacks; the quantization watermarking process's normalized correlation coefficient, formerly sensitive to rotation attacks, now stays above 0.9. A synopsis of the aforementioned works is provided in **Table 1**. This paper presents a significant advance in secure blind watermarking techniques. The suggested system facilitates the concealment of an encrypted binary watermark within a color image by applying DWT. It enhances the digital image watermarking system that uses the DWT based on the Lorenz system mixed with the Geffe algorithm.

Table 1. A brief analysis of related work

Author	Technique used	Advantages	Limitations
AbdElHaleem SH, Abd-El-Hafiz SK, Radwan AG[11]	DCT, DWT	1- Efficient and Simple Extraction Process 2- Offering enhanced security with watermark encryption	1- The study compares with several current efforts but does not compare with hybrid transform methods.
Dong Y, Yan R, Zhang Q, Wu X[10]	DCT, DWT, SVD	1- Embedding strength is dynamically computed utilizing Bhattacharyya distance, circumventing static values that may compromise resilience. 2- Significant embedding capacity	1- Limited robustness to geometric attacks 2- High computational complexity
Li L, Bai R, Lu J, Zhang S, Chang CC[12]	QDFT, TD	1- Intelligent embedding position 2- A significant advantage is its robustness against "channel exchange attacks" (e.g., interchanging the red and blue channels).	1- The technique incurs significant computing costs. 2- The system lacks resilience to cropping attacks.
Yang Y, Jiang M, Feng X, Lu C, Chen Y, Zhou S, *et al.*[13]	QDCT, SVD	1-Improved Security through the Utilization of an Innovative Chaos System for Chaotic Encryption 2- Utilizes (QDCT) to concurrently process RGB channels, enhancing security and watermark resilience.	1- Computationally demanding owing to moment computations and QDCT transformations. 2- Insufficient robustness to affine transformations and histogram equalization.

3. Materials and Methods

This section presents a review of backgrounds concentrating on aspects relevant to the subjects of this paper: the fractional-order Lorenz system, the Geffe algorithm generator, and the proposed system's method, which will be discussed in detail below.

Chaos, defined as the inherent unpredictability or randomness in a defined system's behavior, is characterized by quasi-random movements that appear irregular within complex natural systems such as the atmosphere or the heartbeat. A chaotic system can provide a substantial quantity of pseudo-random high-security keys due to its extensive period and significant randomness of the

chaotic signal; however, this is not assured. The most appealing characteristic of chaos is its extreme sensitivity to initial conditions, signifying that two proximate trajectories originating from similar initial states diverge exponentially as time approaches infinity [14]. In addition, stream cipher is a paramount contemporary encryption technique frequently employed in communications. The majority of stream coding systems comprise a collection of shift recorders utilizing a Linear Feedback Shift Register. Each shift recorder comprises a series of hoppers (flip-flops), referred to as stages. The quantity of these steps is dictated by the length and complexity of the shift recorder. A crucial concept emerges: Linear Equivalence [15,16].

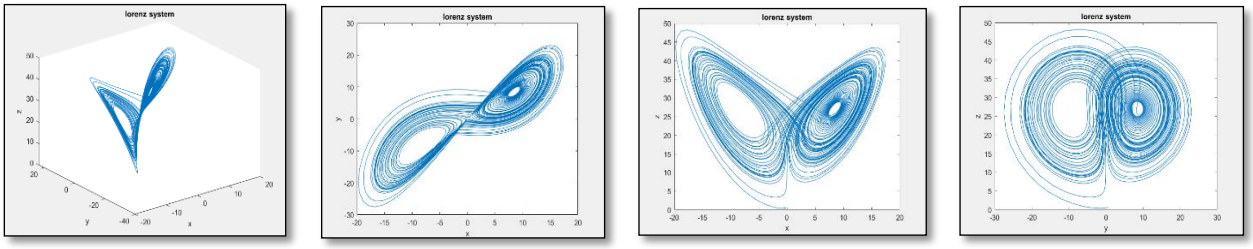
3.1. Fractional-Order Lorenz System

Numerous researchers exploit iteration functions for chaotic sequences; in other words, they use a certain ordinary differential equation as a chaotic sequence with designated parameters. Lorenz (1963) suggested three coupled ordinary differential equations characterized by three parameters: σ, ρ, and β, described as follows [16,17]:

$$\frac{dx}{dt} = \sigma\,(y - x)$$
$$\frac{dy}{dt} = \rho x - y - xz \qquad \textbf{(1)}$$
$$\frac{dz}{dt} = xy - \beta z$$

x, y, and z represent initial variables, while σ = 10, ρ = 28, and β = 8/3 denotes control parameters known as the Prandtl number, Rayleigh number, and direction ratio, respectively.

Figure 1, illustrates the chaotic attractors generated by the Lorenz system (LS). The figure demonstrates a significant differentiation among the three variables (x, y and z), highlighting their non-periodic characteristics and unpredictability. Moreover, the system's dynamic trajectory exhibits a three-dimensional double-helix configuration [18].



(a) 3d Lorenz system (b) x-y (c) x-z (d) y-z

Figure 1. Attractor projection of Lorenz system. (a) 3d system (b) x-y plane, (c) x-z plane, (d) y-z plane

3.2. Geffe Generator

The Geffe Generator is a stream cipher technique based on linear feedback shift registers (LFSR) that integrates three LFSRs of varying lengths that are substantially prime [19]. The Geffe Generator was proposed by P.R. Geffe in 1973, it comprises three LFSRs: two serves as input multiplexers, while one functions as a controller [20]. The Geffe Generator configuration is shown clearly in **Figure 2**, where the output of the LFSR (1, 2, 3) is denoted sequentially as (x1, x2, x3) [21].

$$keystream = (x_1 \wedge x_2) \oplus ((\neg x_2) \wedge x_3) \qquad \textbf{(2)}$$

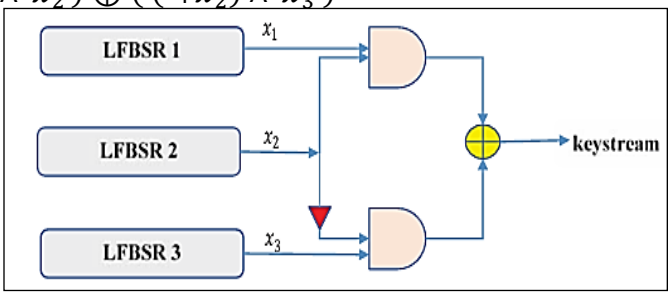


Figure 2. The generator of Geffe (20)

3.3. The Proposed Key Generator

This sub-section will address the proposed method for generating a binary random key, which will be used to encrypt the watermark image prior to its embedding in the host image according to the following steps:

Step 1: Solve the 3D chaotic Lorenz system using **Equation (1)** with initial values (x_0, y_0, z_0) to generate random sequences $X = \{x_1, x_2, x_3,\ldots, x_n\}$,Y = $\{y_1, y_2, y_3,\ldots, y_n\}$, and Z = $\{z_1, z_2, z_3, \ldots, z_n\}$, while utilizing a temporal value (t) to determine the quantity of chaotically generated random values; additionally, employ the Runge-Kutta method for the solution of the system.

Step 2: After solving the 3D chaotic Lorenz system, three vectors—X, Y, and Z—are generated to resolve any discrepancies present in these vectors. Each vector (X, Y, and Z) is normalized using these equations:

$$X_{new} = (X - \min(X))/(\max(X) - \min(X))),$$
$$Y_{new} = (Y - \min(Y))/(\max(Y) - \min(Y))), \quad \textbf{(3)}$$
$$Z_{new} = (Z - \min(Z))/(\max(Z) - \min(Z))).$$

Where min(X), max(X), min(Y), max(Y), min(Z), and max(Z) represent the minimum and maximum values of each respective vector, with, Y_{new}, and Z_{new} denoting the newly normalized vectors.

Step 3: Each value resultant from the above step should be converted to either 0 or 1 binary values with scale factor (*Sf*) as:

$$X_c = floor\,(X_{new} \times Sf) mod\ 2,$$
$$Y_c = floor\,(Y_{new} \times Sf) mod\ 2, \quad \textbf{(4)}$$
$$Z_c = floor\,(Z_{new} \times Sf) mod\ 2.$$

Where X_c, Y_c, and the vectors of binary values.

Step 4: Apply the Geffe generator using **Equation (4)** into **Equation (2)** to obtain the random sequence (*SK*).

Step 5: If the resulting random sequence (*SK*) successfully passes a minimum of 12 NIST tests, it can be used as a random binary key. However, if the sequence fails to meet the criteria, the entire process is initiated anew with new initial values.

3.4. Watermarking System Based on DWT

This section provides a concise explanation of the DWT, discusses watermarking systems, and elucidates the procedures for embedding and extracting watermark bits.

3.4.1. Discrete Wavelet Transform

DWT is a hierarchical or multi-resolution image transformation, simply decomposed and concentrating energy at low frequencies while revealing edges in the high-frequency sub-bands [22]. Haar basis is the most utilized one, due to its simplicity and efficiency, that yields four coefficients (quadrants): diagonal sub-band (HH), horizontal sub-band (HL), approximation sub-band (LL), and vertical sub-band (LH), where HH sub-bands exhibit sensitivity to the texture and edge details of the image; nevertheless, they are also comparatively susceptible to assaults, while the HL sub-band is utilized for image enhancement, as it contains horizontal high-frequency and vertical low-frequency information. On the other hand, the LH sub-band integrates the attributes of horizontal low frequency and vertical high frequency, making it appropriate for recognizing edges. Lastly, the LL segment constitutes the primary characteristic of image [10,23]. **Figure 3** illustrates two deterioration stages inside DWT. The HH sub-band is the better contender for concealing information because the energy stored in it is low (11). For an image of dimensions m× n, the DWT and IDWT coefficients can be calculated using [24]:

If $Z_W$is even:

$$L_i = \frac{I_{2i} + I_{2i+1}}{\sqrt{2}}, i = 0 \ldots\ldots (Z/2) - 1$$
$$H_i = \frac{I_{2i} - I_{2i+1}}{\sqrt{2}}, \ i = 0 \ldots\ldots (Z_W/2) - 1 \quad \textbf{(5)}$$

If Z_W is odd:

$$L_i = \frac{I_{2i} + I_{2i+1}}{\sqrt{2}}, i = 0 \ldots\ldots (Z_W - 1/2) - 1$$
$$H_i = \frac{I_{2i} - I_{2i+1}}{\sqrt{2}}, i = 0 \ldots\ldots (Z_W - 1\ /2) - 1 \quad \textbf{(6)}$$
$$L_{(z+1)/2} = \sqrt{2}\ (Z_W\ - 1)$$
$$H_{(Z_W+1)/2} = 0$$

Let $Z_W$be the data size of an input sequence (I_i), where i ranges from 0 to Z_W-1. L_i and $H_i$denote the low pass filter and high pass filter, respectively.

If Z_W is even:

$$I_{2i} = \frac{L_i + H_i}{\sqrt{2}}, i = 0 \ldots\ldots (Z_W/2) - 1$$
$$I_{2i+1} = \frac{L_i - H_i}{\sqrt{2}}, \ i = 0 \ldots\ldots (Z_W/2) - 1 \quad \textbf{(7)}$$

If Z_W is odd:

$$I_{2i} = \frac{L_i + H_i}{\sqrt{2}}, i = 0 \ldots\ldots (Z_W - 1)/2$$
$$I_{2i+1} = \frac{L_i - H_i}{\sqrt{2}}, i = 0 \ldots\ldots (Z_W - 1)/2 \quad \textbf{(8)}$$
$$I_{z-1} = \sqrt{2L_{(Z_W+1)/2}}$$

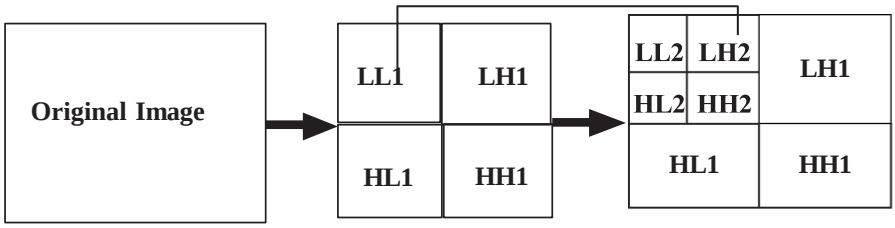


Figure 3. 2-Level DWT Decomposition [24]

3.4.2. Encryption and Decryption Processes

The encryption is applied to the watermark image to further strengthen the system's security. The random key obtained is used to encrypt the watermark image before it is embedded in the cover image. By using the bit XOR operator with (4096 bits) from the random sequence, equal to the size of the watermark, the value of each pixel is modified to complete the encryption process. The decryption process is executed in an identical manner.

3.4.3. Embedding and Extraction System

The DWT system consists of two essential stages: embedding and extraction. Each of these two stages comprises multiple steps. The embedding unit aims to incorporate watermark information within the DWT, rendering the watermark difficult to illicitly extract. In the embedding stage, the HH band is partitioned into distinct, non-overlapping blocks of dimensions 4 × 4. Each block conceals one bit of the encrypted watermark image. In each block, two coefficients are selected for modification: specifically, coefficients (1,1) and (1,2). The modification of the DWT coefficients commences with the computation of the mean of the two neighboring coefficients, Ci = C (1, 1) and C (1, 2), using [11]:

$$\mu = \frac{1}{2} \sum_{i=1}^{2} C_i \quad \textbf{(9)}$$

After that, the value of each coefficient is adjusted to C_m by utilizing the:

$$C_m = \begin{cases} (C_i - \mu) + \varphi, & W = 1 \\ (C_i - \mu) - \varphi, & W = 0' \end{cases} \quad \textbf{(10)}$$

where C_m denotes the modified coefficient value, φ signifies the embedding strength, and W indicates the watermark bit.

3.4.3.1. Proposed Embedding Stage

The embedding stage consists of several steps; these steps are essential for generating the watermarked image. **Figure 4** illustrates the block diagram of the embedding stage.

Step 1: Choose the binary watermark image of size (64 x 64) pixels, and encrypt it in the same manner discussed in subsection 3.2.1 before embedding it in the host image.

Step 2: Use a color square image of size (512 x 512) pixels as host and convert it to the YCbCr color model.

Step 3: Use the Y band, then apply the 2D DWT transform for each block using **Equations (5)** and **(6)**. Subsequently, exploit the HH sub-band and partition it into 4x4 pixel non-overlapping blocks; the quantity of blocks matches the number of pixels in the encrypted watermark image.

Step 4: Convert the encrypted watermark image into a vector format to embed each pixel into each individual block of the HH sub-band blocks.

Step 5: Specify the value of the embedding strength.

Step 6: Modifying the HH sub-band coefficients for each block, the quantity of coefficients to be altered has been specified as four, as shown in **Figure 5**, by calculating the mean value using the **Equation (9)** but with the four adjacent coefficients. Thereafter, the value of each coefficient will be modified using **Equation (10)**.

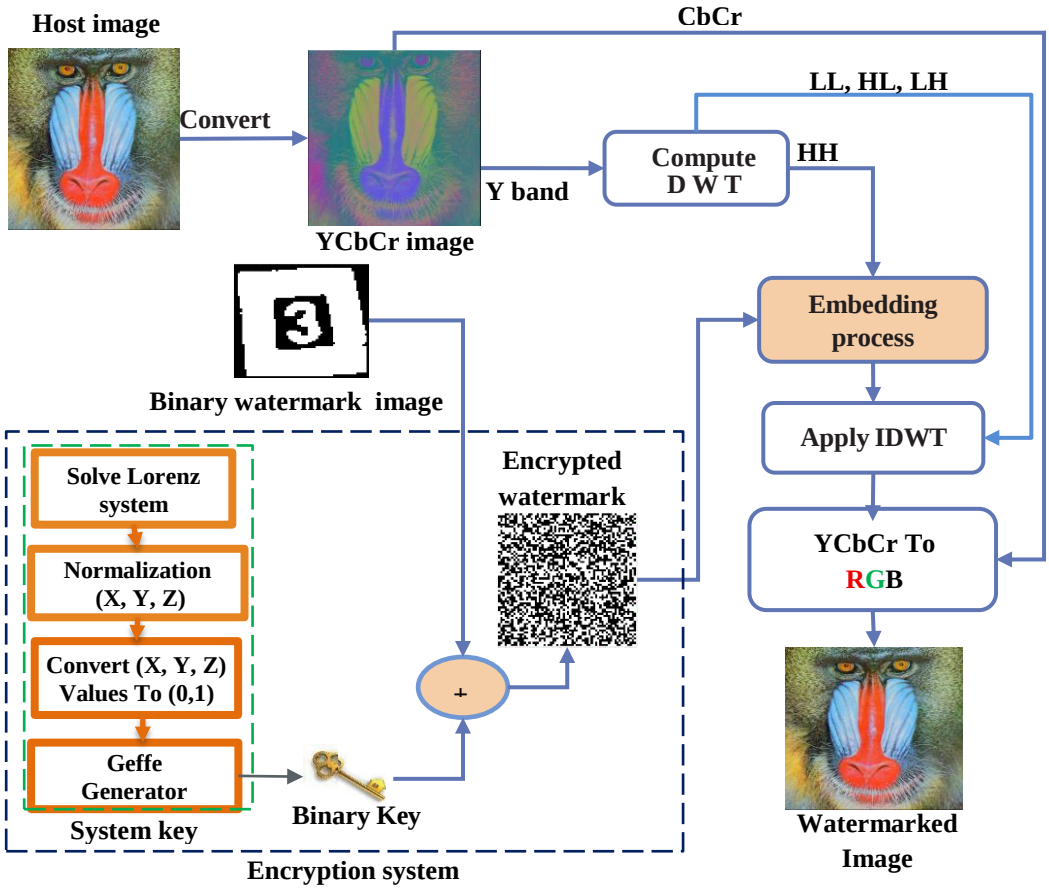


Figure 4. Block diagram of proposed watermarking embedding system

(1,1)	(1,2)		
(2,1)			
(3,1)			

Figure 5. Example of 4x4 block frequency for the HH sub-band

Step 7: Upon embedding the watermark, the IDWT transformations are performed as in **Equations (7)** and **(8)** on each modified block to convert the current block values from the frequency domain to the spatial domain. The new Y band is subsequently reconstructed.
Step 8: Combine the new Y band with the associated CbCr bands and transform it into the RGB color space to produce the watermarked image.

3.4.3.2. Proposed Extraction Stage

The extraction process adopted here is of blind base, as illustrated in **Figure 6**, relying solely on the watermarked image. The extraction stage comprises numerous steps outlined below:
Step 1: Select the watermarked image and transform it into the YCbCr color model.
Step 2: Apply the 2D DWT transform according to **Equations (5)** and **(6)** for the Y band, then use the HH sub-band that divides it into 4x4 non-overlapping blocks. Thereafter, calculate the mean (μ) value for four adjacent coefficients of each block.
Step 3: To extract the encrypted watermark image, check the mean value (μ). If (μ >= 0) then ($W = 1$), ($W = 0$).
Step 4: Finally, decrypt the extracted encrypted watermark image using the *SK* binary random key to retrieve the original watermark image.

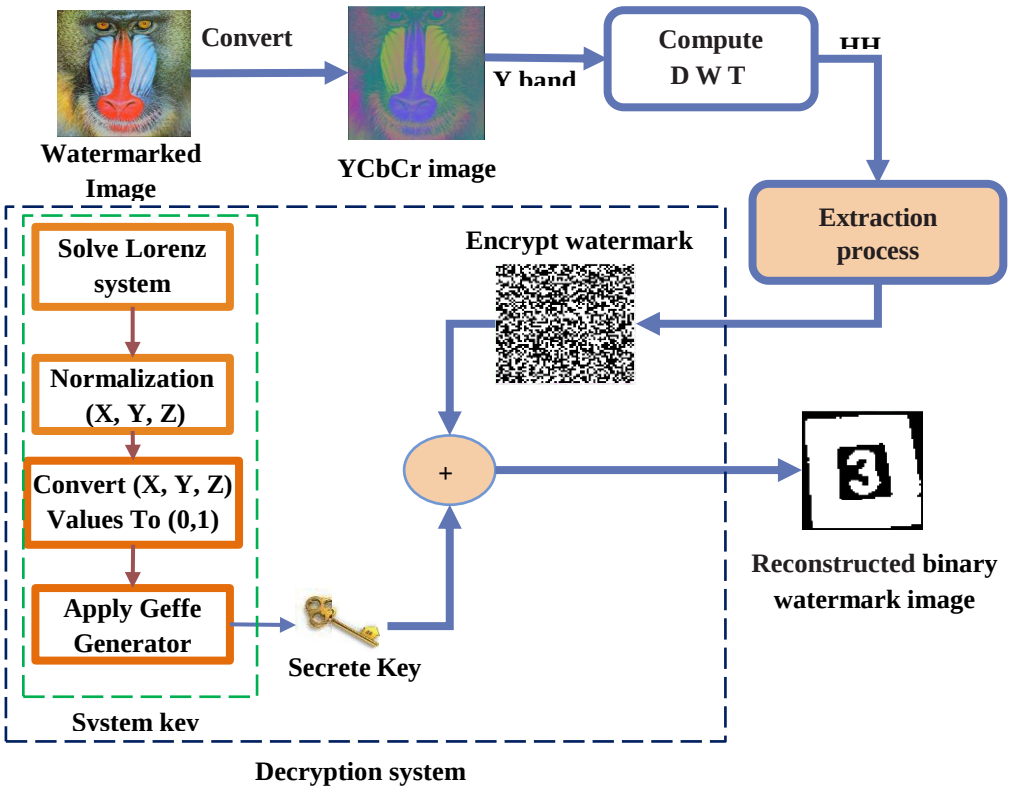


Figure 6. Block Diagram of DWT watermarking extraction system.

4. Experimental Results and Analysis

The proposed watermarking system is executed using the MATLAB application version (R2020b). The trials were conducted using the Windows 10 operating system (64-bit) on an Intel Core i7 CPU with 8 GB RAM. The suggested system utilized five color standard square images of sizes 512x512 pixels from the Miscellaneous dataset,ordered as Lena, Pepper, Baboon, Airplane, House, along with a watermark image represented as a binary square image of 64 x 64 pixels.

4.1. Key Generator

This subsection illustrates the performance of the proposed random key generator with the initial value (-0.6, 0.6, 0.6) by testing standard Lorenz system parameters (σ = 10, ρ = 28, and β = 8/3), a temporal value (t = 74) by testing, and a scale factor ($Sf = 10^7$) by testing to produce a random key sequence. The proposed method has been evaluated based on the SP800-22 test suite, adopted by the NIST to validate the characteristics of the generated key. This evaluation subjects a keystream sequence of 1,000,000 bits produced by the proposed keystream generator to testing. **Table 2** presents the outcomes of these tests alongside comparisons with [11]. All P-values surpass the significance threshold of α = 1%.

Table 2. NIST tests for the key generation with comparison results

Test No.	Statistical Test Name	Proposed		(11)	
		P-VALUE	Result	P-VALUE	Result
1	Frequency	0.649828	Pass	0.275709	Pass
2	Block Frequency	0.362904	Pass	0.637119	Pass
3	Cumulative Sums	0.668954	Pass	0.403400	Pass
4	Runs	0.038098	Pass	0.213309	Pass
5	Longest Run	0.170235	Pass	0.350485	Pass
6	Rank	0.918771	Pass	0.035174	Pass
7	FFT	0.180314	Pass	0.162606	Pass
8	Non-Overlapping Template	0.529464	Pass	0.313904	Pass
9	Overlapping Template	0.274729	Pass	0.025193	Pass
10	Universal	0.792958	Pass	0.739918	Pass
11	Approximate Entropy	0.111061	Pass	0.122325	Pass
12	Random Excursions	0.531433	Pass	0.350733	Pass
13	Random Excursions Variant	0.456168	Pass	0.453015	Pass
14	Serial	0.296137	Pass	0.105661	Pass
15	Linear Complexity	0.966294	Pass	0.637119	Pass

4.2. Watermarking System

The DWT system tests the concept of embedding a binary logo in a color image using SSIM and PSNR metrics to determine how embedding affects image quality. The brightness component (Y) of the original and watermarked images is used to calculate these measures; all the tests are conducted on the proposed system using an embedding strength value (φ = 12) because it provides a satisfactory balance between high robustness and imperceptibility.

The results of SSIM and PSNR are shown in **Table 3**, the experimental results for the five color images demonstrate an acceptable level of imperceptibility according to the defined criteria. Therefore, the embedding of the watermark image did not degrade the quality of the host images.

Table 3. Imperceptibility evaluation metrics for DWT watermarking system

Cover image	PSNR	SSIM
Lena	42.2875	0.9381
Peppers	41.6194	0.9449
Baboon	41.5169	0.9757
Airplane	41.8551	0.9357
House	42.0064	0.9415

The proposed system is tested for extracting watermarks from the watermarked images. These tests retrieve the watermark information from both non-attacked and attacked watermarked images that have undergone several types of attacks. Firstly, a watermark extraction test was conducted on all watermarked images without any attacks. The watermark was extracted without damage or loss. The NCC and BER metrics for all evaluations without attacks were 1 and 0. Secondly, several tests were performed to extract the watermark from the watermarked images, and the results of each attack were assessed following the images' exposure to various attacks. These attacks involve modifications to image processing, namely: Salt and Pepper Noise (SPN) with a density of 0.01, Gaussian Noise (GN) with a mean of 0 and a standard deviation of 0.01, Histogram Equalization (HE), and sharpening.

Furthermore, prior to watermark extraction, the image is compressed with JPEG at a 90-quality factor as a type of attack. Additionally, geometric attacks are discussed, including cropping and rotation. In the cropping attack, 25% of the image is removed from the top-left corner. In the rotation attack, the image is rotated anticlockwise by three degrees: 1°, 10°, and 75°. **Tables 4** and **5** demonstrate the effect of these attacks on the values of the **NCC** and **BER** metrics of the extracted watermark.

Table 4. DWT system robustness evaluation metrics with several attacks

Cover images	Attack type	SPN	JPEG	GE
Lena	**NCC**	0.9625	1	0.9591
	BER	5.2490	0	5.7129
Pepper	**NCC**	0.9677	0.9929	0.9553
	BER	4.5166	1.0010	6.2256
Baboon	**NCC**	0.9618	0.9984	0.9620
	BER	5.3467	0.2197	5.3223
Airplane	**NCC**	0.9666	0.9531	0.9632
	BER	4.6631	6.5674	5.1514
House	**NCC**	0.9669	0.9368	0.9637
	BER	4.6387	8.7646	5.0781

Table 5. DWT system robustness evaluation metrics with more attacks

Attack type		HE	Sharpening	Cropping	Rotation		
					1°	**10°**	**75°**
Lena	**NCC**	1	1	0.9085	0.9923	0.9705	0.9603
	BER	0	0	12.5977	1.0986	4.3213	5.6885
Pepper	**NCC**	1	1	0.9085	0.9941	0.9707	0.9604
	BER	0	0	12.5977	0.8301	4.2969	5.6641
Baboon	**NCC**	0.9998	1	0.9085	0.9680	0.9519	0.9371
	BER	0.0244	0	12.5977	4.4678	6.8848	8.8623
Airplane	**NCC**	1	1	0.9085	0.9893	0.9692	0.9589
	BER	0	0	12.5977	1.5137	4.5166	5.8838
House	**NCC**	1	1	0.9085	0.9870	0.9689	0.9569
	BER	0	0	12.5977	1.8311	4.5410	6.1523

The tested images show a great BER for all attacks except the cropping attack, which maintains 12.5%. The HE attack delivers a trivial BER of less than 0.025% for the Baboon image and zero for the other images, proving the system's robustness. The suggested approach accurately recognizes the watermark image in sharpening attacks, with a BER of 0% across all images. Thus, this attack cannot penetrate the system. The rotation attack shows that increasing the rotation angle increases BER. BER remains low, with a 75° rotation BER of less than 8.87%. Thus, the proposed system resists rotating attacks. Based on the Lena image, several embedding strength values were utilized to evaluate SPN and GN assaults. **Figure 7** shows results.

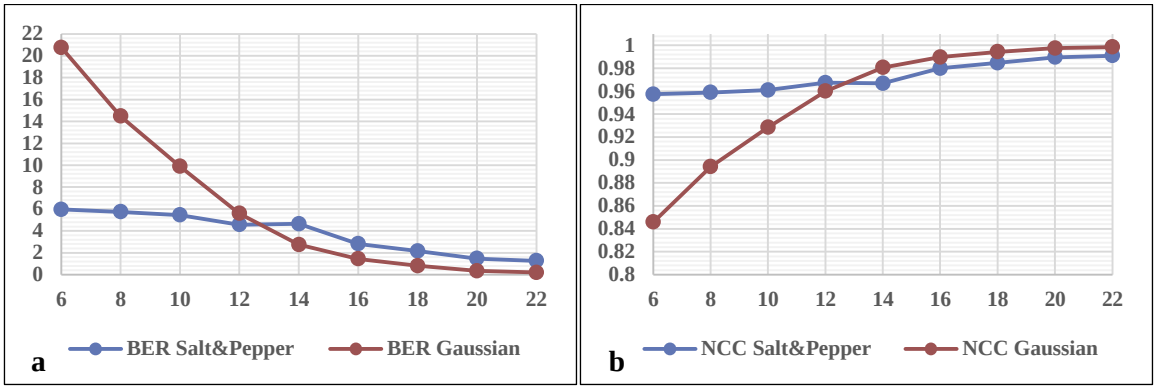


Figure 7. The evaluation results of the DWT system for additional attacks and varying (φ) values applied to the Lena image: (a) BER, (b) NCC

Table 6 compares the proposed watermarking system's imperceptibility against other approaches using φ = 12 and PSNR and SSIM for five cover images. **Table 7** shows the proposed watermarking system's robustness compared to other watermarking methods using NCC and BER over the Baboon image.

Table 6. Comparison of the proposed DWT system (φ = 12) with the existing techniques in the field of imperceptibility

Cover image	(12)		(11)		(13)		Proposed DWT system	
	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM	PSNR	SSIM
Lena	40.413	-	41.2756	0.9013	-	-	42.1883	0.9286
Pepper	-	-	41.0975	0.9315	40.1566	49.7744	42.0723	0.9280
Baboon	41.549	-	39.9675	0.9763	40.2324	46.9510	42.5441	0.9387
Airplane	42.562	-	41.3388	0.8167	40.0846	46.2803	42.6018	0.9282
House	40.993	-	41.2165	0.8542	-	-	42.4466	0.9305

Table 7. Comparison of the proposed DWT system (φ = 12) with the existing techniques in the field of robustness with the baboon image

Attack type	(10)		(11)		Proposed system	
	NCC	BER	NCC	BER	NCC	BER
Sharpening	0.8958	0.2576	1	0	1	0
Gaussian	-	-	0.9119	0.0576	0.9620	0.0532
Rotation 10°	0.8715	0.2979	0.9096	0.0551	0.9519	0.0688
JPEG (90)	0.9966	0.0661	0.9795	0.0129	0.9984	0.0021
Cropping	-	-	0.8226	0.1220	0.9085	0.1259
Histogram	-	-	0.9996	0.0002	0.9998	0.0002

5. Conclusion

The frequency-domain blind watermarking method in this study uses the Lorenz system and Geffe algorithm to encrypt the watermark. The Discrete Wavelet Transform is applied to the Y channel after the host picture is converted to YCbCr. The encrypted watermark is then incorporated into the DWT HH band coefficients. The embedded media's statistics reveal the hidden watermark. It was shown that watermarking is highly effective in the frequency domain via the Discrete Wavelet Transform (DWT), with the HH band being an excellent option for concealing information due to its low energy content. The suggested system resists image attacks well. Additionally, it resists geometric deformation, JPEG compression, and supplemental image enhancement attacks. The suggested method is more secure since the watermark is encrypted, and the mixed Lorenz system and Geffe algorithm increase the randomness of the key used in watermark encryption.

Conflict of Interest

There is no conflict to disclose.

Funding

No funding

References

1. Begum M, Uddin MS. Digital image watermarking techniques: A review. Information (Basel). 2020;11(2):110. https://doi.org/10.3390/info11020110
2. Fu H, Zhao X, He X. Improving anticompression robustness of JPEG adaptive steganography based on robustness measurement and DCT block selection. Secur Commun Netw. 2021;2021:9153468. https://doi.org/10.1155/2021/9153468
3. Naem SAS, Hameed SM. Digital watermarking techniques, challenges, and applications: A review. Mesopotamian J Cyber Secur. 2025;5(2):453–476. https://doi.org/10.58496/MJCS/2025/028
4. Singh B, Hathwal RP. Tamper detection technique for text images based on vowels and Unicode zero length characters. Wirel Pers Commun. 2023;132(4):2421–2436. https://doi.org/10.1007/s11277-023-10724-6
5. Hummadia TN, Hassan NF. Survey of recent video watermarking techniques. Eng Technol J. 2021;39(1B):165–174. https://doi.org/10.30684/etj.v39i1B.1950
6. Peng J, Abd El-Atty B, Khalifa HS, Abd El-Latif AA. Image watermarking algorithm based on quaternion and chaotic Lorenz system. In: Proc 11th Int Conf Digit Image Process (ICDIP 2019). Bellingham (WA): SPIE; 2019. p. 81. https://doi.org/10.1117/12.2539753
7. Singh B, Kasana G. A review of digital watermarking techniques: Current trends, challenges and opportunities. Web Intell. 2024;22(4):523–553. https://doi.org/10.3233/WEB-230280
8. Panyavaraporn J, Horkaew P. Wavelet-based digital image watermarking by using Lorenz chaotic signal localization. J Inf Process Syst. 2019;15(1):169–180. https://doi.org/10.3745/JIPS.03.0109
9. Li Q, Wang X, Pei Q. Compression domain reversible robust watermarking based on multilayer embedding. Secur Commun Netw. 2022;2022:4542705. https://doi.org/10.1155/2022/4542705
10. Dong Y, Yan R, Zhang Q, Wu X. A hybrid domain color image watermarking scheme based on hyperchaotic mapping. Mathematics. 2024;12(12):1859. https://doi.org/10.3390/math12121859
11. AbdElHaleem SH, Abd-El-Hafiz SK, Radwan AG. Secure blind watermarking using fractional-order Lorenz system in the frequency domain. AEU Int J Electron Commun. 2023;173:154998. https://doi.org/10.1016/j.aeue.2023.154998
12. Li L, Bai R, Lu J, Zhang S, Chang CC. A watermarking scheme for color image using quaternion discrete Fourier transform and tensor decomposition. Appl Sci. 2021;11(11):5006. https://doi.org/10.3390/app11115006
13. Yang Y, Jiang M, Feng X, Lu C, Chen Y, Zhou S, et al. Rotation correction algorithm based on polar harmonic Fourier moments and optimization of color image security quantization watermarking scheme. IEEE Photonics J. 2024;16(5). https://doi.org/10.1109/JPHOT.2024.3443345.
14. Udham Singh K, Singhal A. Color image watermarking based on LU factorization, logistic and Lorenz chaotic maps. Int J Adv Res Comput Sci. 2017;8(5). www.ijarcs.info
15. Jassim SA, Farhan AK, Radie AH. Using a hybrid pseudorandom number generator for cryptography in the Internet of Things. In: Proc 4th Int Iraqi Conf Eng Technol Their Appl (IICETA 2021). Piscataway (NJ): IEEE; 2021. p. 264–269. https://doi.org/10.1109/IICETA51758.2021.9717775
16. Kumar D, Joshi AB, Singh S. A novel encryption scheme for securing biometric templates based on 2D discrete wavelet transform and 3D Lorenz-chaotic system. Results Opt. 2021;5:100146. https://doi.org/10.1016/j.rio.2021.100146
17. Zhang B, Liu L. Chaos-based image encryption: Review, application, and challenges. Mathematics. 2023;11(11):2585. https://doi.org/10.3390/math11112585
18. Salim A, Mohammed KA, Jasem FM, Sagheer AM. Image steganography technique based on Lorenz chaotic system and Bloom filter. Int J Comput Digit Syst. 2024;16(1):851–859. https://doi.org/10.12785/ijcds/160161
19. Handayani F, Adiati NPR. Analysis of Geffe generator LFSR properties on the application of algebraic attack. In: AIP Conf Proc. 2019. https://doi.org/10.1063/1.5132456

20. Mahdi K, Salwa H, Baawi S, Kamil B, Qar H, Qar IT. An image watermarking technique proposed based on discrete cosine transformation and pseudo-random generator. J Educ Pure Sci Univ Thi-Qar. 2021;11(1):108–118. https://doi.org/10.32792/utq.jceps.11.01.12
21. Hattab AA, Saieed AH. Developing the complexity and security of the Twofish algorithm through a new key scheduling design. Iraqi J Sci. 2023;64(11):5923–5939. https://doi.org/10.24996/ijs.2023.64.11.37
22. Latif IH, Abdulredha SH, Hassan SKA. Discrete wavelet transform-based image processing: A review. Al-Nahrain J Sci. 2024;27(3):109–125. https://doi.org/10.22401/ANJS.27.3.13
23. Abdulrida R, A-Monem ME, Jaber AM. Quantum image watermarking based on wavelet and geometric transformation. Iraqi J Sci. 2020;61(1):153–163. https://doi.org/10.24996/ijs.2020.61.1.17
24. Li Q, Zhang W, Wu Z, Dai Y, Liu Y. An efficient multi-level 2D DWT architecture for parallel tile block processing with integrated quantization modules. Electron. 2024;13(23):4668. https://doi.org/10.3390/electronics13234668