Advance Sustainable Science, Engineering and Technology (ASSET)
Vol. 7, No.4, October 2025, pp. 02504014-01 ~ 02504014-014
ISSN: 2715-4211 DOI: https://doi.org/10.26877/asset.v7i4.2069

Secure Visual Image Encryption Using Lorenz Chaos, Steganography, and Wavelet-Based Steganography Authentication

Salsabil Farah Aqilah Wijaya*, Ida Wahidah, Koredianto Usman

Universitas Telkom, Jl. Telekomunikasi No. 1 Bandung 40257 , West Java, Indonesia

*salsabilfawpou@student.telkomuniversity.ac.id

Abstract. Medical images play a vital role in diagnosis and clinical decision-making, yet their transmission and storage pose significant privacy and security challenges. This research proposes a visual stego-encryption system that integrates the Lorenz chaotic algorithm with Discrete Wavelet Transform (DWT) to embed both secret medical data and a doctor's digital signature into a visually meaningful encrypted image (VMEI). The system employs dual-layer embedding and role-based access control, allowing administrators to input patient and doctor data while enabling doctors to perform secure validation and decryption. A series of evaluation scenarios were conducted, including variations in image resolution, geometric transformations (rotation), Lorenz initial conditions, alpha embedding parameters, and multivariate optimization, along with user-role-based validation testing. Performance metrics based on Peak Signal-to-Noise Ratio (PSNR) and Bit Error Rate (BER) demonstrate that the system consistently achieves high visual fidelity (PSNR > 30 dB) and low data loss (BER ≈ 0) across all image types. The optimal configuration—using a 4096×4096 carrier, 1024×1024 secret, and 256×256 signature with α_1 = 0.28, α_2 = 0.07, and initial condition (0.2, 0.8, 1.5)—resulted in a PSNR of 33.01 dB for the secret image. These results confirm that the proposed system provides a robust, secure, and visually accurate method for medical image encryption, suitable for integration into real-world digital healthcare infrastructures.

Keywords:, chaos theory, digital image security, visual encryption, wavelet transform, image steganography.

(Received 2025-06-03, Revised 2025-08-01, Accepted 2025-08-17, Available Online by 2025-10-13)

1. Introduction

The development of digital technology in the health sector has brought ease in the management of medical information, especially in terms of storage and exchange of medical image data. Medical images such as MRI, CT scans, X-rays, and endoscopy are an important part of the diagnosis and clinical decision-making process [1]. However, along with this advancement, the risks to the privacy and security of medical data have also increased significantly. Data from the World Health Organization

(WHO) shows that more than 35% of data breach incidents in the health sector involve image information medical images [2]. Therefore, chaos-based encryption has become a solution that has been widely developed in the literature. Chaos systems like Lorenz are capable of generating complex pseudo-random sequences that are sensitive to changes in initial conditions, making them suitable for pixel scrambling applications in images [3].

Following on from this need, the Visually Meaningful Image Encryption (VMEI) approach has begun to be developed. This concept aims to produce encrypted images that still resemble natural images, thus reducing the likelihood of being detected as encrypted data. Research by [4] combines the Lorenz system with wavelet transformation and digital signature in the VMEI scheme. The results show a PSNR above 50 dB and a decryption correlation value close to 1, indicating the effectiveness of this approach in maintaining visual quality and decryption accuracy [4].

Several other studies have tried frequency transform approaches, such as DWT and DCT, to insert data, but they are still suboptimal in combining aspects of authentication and meaningful visualization. For example, the method by Sharma and Verma (2023) [5] uses a hybrid DWT-DCT with a genetic algorithm [5], while Kumar et al. (2022) [6] combine equalisation and AES. These studies show that while these transformation methods are technically effective, they do not provide a complete system in terms of security, digital authentication, and clarity of the visual appearance of the image [6].

In the same context, other studies show the potential of using the Arnold transform, biometrics, and chaos maps to improve medical image security. However, the systems they developed still do not pay attention to the importance of visualisation that remains meaningful, and the integration of digital authentication in a unified system [7]. Other research also emphasised the need for a medical encryption system that considers aspects of data authenticity and role-based access that can be applied in complex clinical environments [8]. Integration of LWT, LSB, and Lorenz chaos for visually meaningful image encryption with digital signatures, establishing a foundation by combining security, visual readability, and authentication [9]. To facilitate the development of this system, the research addressed crucial aspects including preserving the visual integrity of encrypted medical images, securely embedding digital signatures using DWT-based steganography, and creating an efficient, clinically integrable system, which was evaluated using PSNR and BER for decryption quality and tamper resistance, alongside a focus on processing speed; ultimately aiming to produce a secure medical image encryption system that upholds data integrity and authenticity, contributing theoretically through the application of Lorenz chaos systems and offering a practical prototype for digital health services, with the study scope limited to endoscopy images as the secret data, patient photos as carriers, doctor's image signatures, and system evaluation within a local environment with basic technical parameter testing to enable future expansion [10].

This research introduces a novel visual image encryption system that combines Lorenz chaos and wavelet-based digital steganography to address gaps in previous approaches. While earlier methods focused on frequency transforms or chaos algorithms, they often lacked integrated solutions that ensure both strong security and meaningful visual output. This study emphasizes the importance of preserving the visual structure of encrypted medical images, embedding digital signatures securely, and enabling role-based access control for clinical environments. The goal is to develop a secure, verifiable, and practical encryption system for medical images that supports data integrity, authentication, and efficient processing, with implementation focused on endoscopic image protection and local system evaluation for future scalability.

2. **Methods**

The Lorenz system is a three-dimensional nonlinear dynamic system introduced by Edward Lorenz in 1963 during atmospheric convection studies. It is defined by a set of three coupled first-order differential equations that describe the evolution of three variables over time x(t), y(t), and z(t) [4]:

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

Here, σ, ρ, and β are system parameters representing the Prandtl number, Rayleigh number, and a geometric constant, respectively. The commonly used values σ=10, =28, and β=$\frac{8}{3}$ are known to place the system in a chaotic regime. One of the key characteristics of the Lorenz system is its extreme sensitivity to initial conditions small changes in initial values can produce entirely different trajectories over time. This property, often called deterministic chaos, is highly desirable in cryptographic applications because it enables the generation of pseudo-random sequences that are difficult to predict or replicate.

The spatial behavior of the Lorenz system forms a butterfly-shaped attractor known as the Lorenz attractor, which produces non-repeating, non-linear trajectories in 3D space. This structure is visualized in Figure 1, showing how the system oscillates unpredictably between two lobes, making it ideal for encryption key generation and pixel permutation.

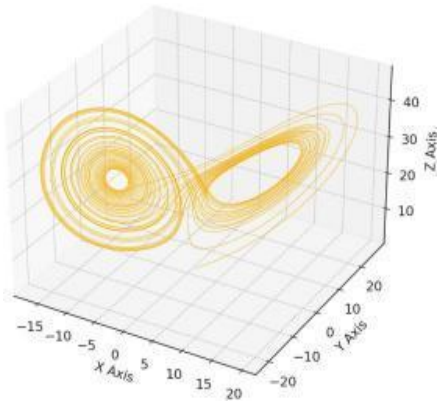


Figure 1. Chaos Lorenz Attractor Curve

In this study, the Lorenz system is utilized as a chaotic key generator for secure pixel permutation and embedding in medical images. The chaotic sequences x(t),y(t),z(t) are generated numerically using initial parameters and are then normalized to the pixel value range [0, 255]. After normalization, the sequences are sorted to form index maps, which are then used to shuffle the pixel positions of the secret and signature images. This permutation step enhances security by making the hidden content unrecognizable without the exact same initial Lorenz parameters.

Moreover, the Lorenz-generated sequences are also applied to control the embedding strength and position within the transformed image sub-bands, particularly after the Discrete Wavelet Transform (DWT) is applied. The chaotic nature of the Lorenz system ensures that the encrypted image varies significantly even with minor changes in the input parameters, making brute-force or statistical attacks highly ineffective.

The proposed system is a web-based application implementing role-based access control with two main user roles: Administrator and Doctor. The overall system workflow is presented in Figure 2. The administrator is responsible for inputting and managing data, including the patient's name, date of birth, facial photo (used as the carrier image), endoscopic image (secret image), and the doctor's digital signature image. These data are securely stored in the system's database for further validation.

Once the data is stored, the doctor logs in and performs data validation by entering the patient's name, birth date, and matching signature. The system cross-checks this input with existing records. If validation succeeds, it proceeds to the encryption phase. Otherwise, it halts the process and notifies the user, optionally displaying a list of patients for reference. This validation step ensures that only authorized users can initiate encryption, enhancing data integrity and access control within the system.

This design not only ensures proper access management but also strengthens the security and traceability of medical data handling. By binding the encryption process to successful identity verification, the system mitigates the risk of unauthorized access and enforces accountability for every operation. Moreover, integrating both patient and doctor data within the encryption pipeline provides an

additional layer of data authenticity, which is essential in clinical environments where the accuracy and reliability of medical records are critical.

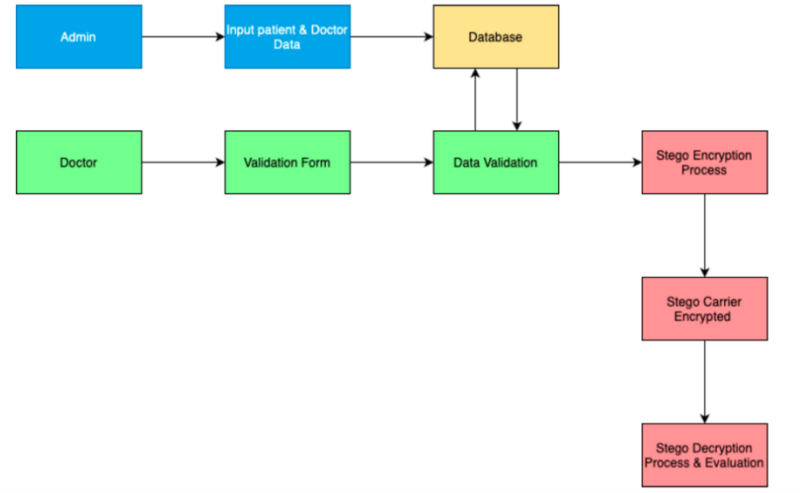


Figure 2. System Block Diagram

The encryption procedure is illustrated in Figure 3a and begins immediately after successful data validation. At this stage, the system gathers all essential components for the encryption process, including the carrier image, secret image, signature image, initial values for the Lorenz system (x0,y0,z0), control parameters (σ,ρ,β), and alpha values that determine the embedding strength. These parameters serve as the foundation for generating a unique chaotic key stream through the Lorenz encryption subroutine.

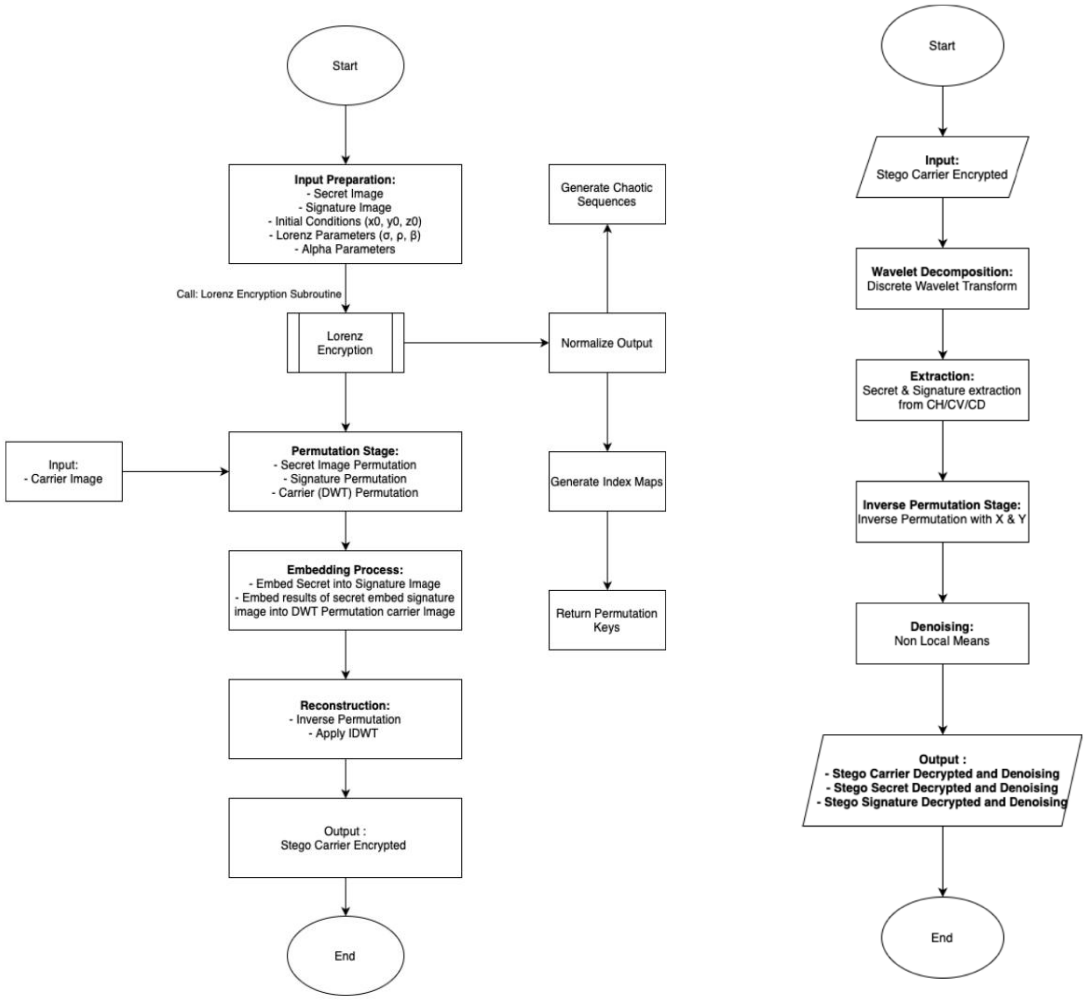
The system invokes the Lorenz algorithm to compute three chaotic sequences, which are then normalized and sorted to create index maps. These maps are used to permute the pixel positions of the secret and signature images, thereby disrupting their spatial patterns and enhancing security. This permutation ensures that without the correct Lorenz parameters and initial conditions, the embedded information remains completely unintelligible.

Next, the Discrete Wavelet Transform (DWT) is applied to the carrier image to decompose it into four frequency sub-bands: cA, cH, cV, and cD. The permuted secret image is embedded into the cH and cV sub-bands, while the signature image is embedded into cD. The embedding process follows the formula $D'=D+\alpha \cdot E$, where D is the original wavelet coefficient, EE is the embedded pixel value, and αα regulates the embedding intensity. This technique ensures a balance between invisibility and robustness against tampering or noise.

Finally, inverse DWT is applied to reconstruct the spatial image, and inverse permutation is performed to finalize the process. The result is a Visually Meaningful Encrypted Image (VMEI)—a facial image that appears visually unchanged but securely contains embedded medical and authentication data. This image can be stored or transmitted without arousing suspicion, while still enabling reliable extraction by authorized users.

The decryption workflow is the inverse of the encryption process and is shown in Figure 3b. The encrypted VMEI undergoes DWT to obtain the cH, cV, and cD sub-bands. The secret image is extracted from cH and cV, while the signature is extracted from cD. The extraction is performed using the same alpha parameter and Lorenz keys used during encryption. After inverse permutation, the extracted images are passed through Non-Local Means (NLM) filtering to reduce noise and improve visual quality.

This approach ensures that both the hidden medical content and the doctor's digital signature can be accurately recovered while maintaining the visual integrity of the carrier image. The system balances security, privacy, and usability, making it highly suitable for telemedicine applications and secure medical record sharing.



(a) Encryption (b) Decyrption

Figure 3. Encryption and Decryption Visual Steganography

3. Results and Discussion

The implementation of algorithms in the designed system ensures that the transformation, embedding, and recovery of data in medical images are conducted securely and efficiently. These algorithms serve not only to encrypt data but also to preserve the visual meaning of the modified medical images. The system integrates multiple approaches, including the Lorenz chaos model and wavelet transformation, forming the core of a visual-based security strategy [1].

3.1. Modeling and Application of the Lorenz Algorithm

The Lorenz algorithm is central to this system's encryption process, generating chaos-based randomness that is highly sensitive to initial conditions yet deterministic when parameters are fixed, making it ideal for identity-based security. Defined by three nonlinear differential equations with standard parameters ($\sigma = 10$, $\rho = 28$, $\beta = 8/3$) and solved using the Runge-Kutta method, the Lorenz system produces chaotic time series ($x(t)$, $y(t)$, $z(t)$) from initial conditions derived from image features like pixel averages or histograms. These series are normalized to the [0, 255] range and used for key encryption tasks such as

permutation and embedding. Compared to general-purpose generators like numpy.random.rand(), the Lorenz system offers input-dependent chaos, ensuring that small image changes yield significantly different encryption results, thereby enhancing security and robustness [11].

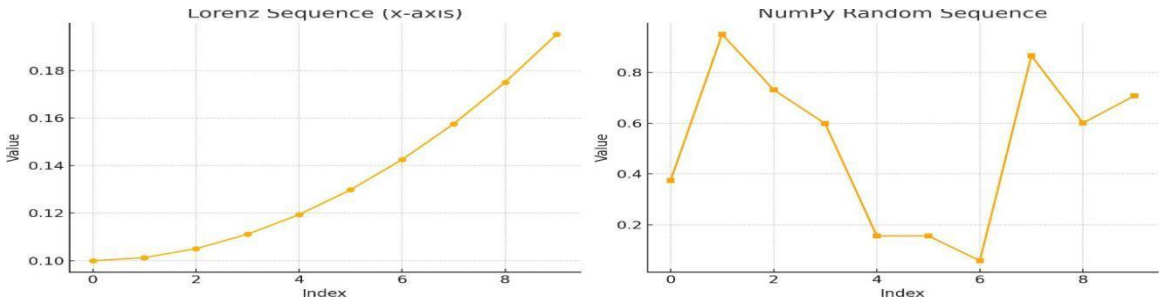


Figure 4. Visual Comparison between Lorentz and Conventional

From Figure 4, the results of the Lorenz sequence and numpy.random.rand() reveals distinctly different characteristics: the Lorenz series exhibits a gradual, continuous, and complex pattern, while the output of numpy.random.rand() appears scattered and lacks any discernible structure. This visualization highlights the visual and structural superiority of the Lorenz sequence as a randomness source grounded in dynamic systems. The Lorenz-generated graph forms a smooth curve, in contrast to the discrete, irregular fluctuations of the standard random generator. The Lorenz system's deterministic chaos properties make it highly suitable for generating pseudo-random sequences that can effectively scramble image data in a non-repetitive and highly individualized manner [12]. Prior studies have emphasized the algorithm's cryptographic strengths, particularly its ability to produce unique outputs with minor variations in input, making brute-force attacks impractical [13]. This is especially relevant in healthcare, where data must not only be protected but also be traceable and authentic. In this research, the Lorenz model functions as a backbone for generating chaotic sequences used in permutation and encryption processes, enhancing data protection in a web-based VMEI (Visually Meaningful Encrypted Image) system [14].

3.1.1. Application of Discrete Wavelet Transform

The integration of the Discrete Wavelet Transform (DWT) plays a crucial role in enhancing the functionality of the system by enabling embedding in the frequency domain. DWT decomposes image components into multi-resolution sub-bands—namely LL (Low-Low), HL (High-Low), LH (Low-High), and HH (High-High). In this study, the HL and HH sub-bands are utilized for embedding secret information and digital signatures, while the LL sub-band is preserved to maintain the structural integrity and visual clarity of medical images [15].

Unlike spatial-domain embedding techniques, DWT-based methods are known to introduce less perceptual distortion. Prior research has demonstrated that wavelet-based watermarking maintains high Peak Signal-to-Noise Ratio (PSNR) values while securing sensitive information. This study supports those findings, with encrypted medical images consistently achieving PSNR values above 30 dB, which is the acceptable threshold for clinical diagnostic use. The preservation of the LL sub-band ensures that the core visual information remains unaffected, while the inverse DWT process enables effective reconstruction of the original image structure with minimal degradation, which is essential for clinical interpretation and analysis.

Figure 5 below illustrates the outcome of applying DWT to the carrier image, showing how it is decomposed into four primary sub-bands. The LL sub-band (top right) contains the approximation components of the image, representing its fundamental structure. The HL, LH, and HH sub-bands (bottom left, top left, and bottom right respectively) hold the high-frequency detail components in vertical, horizontal, and diagonal orientations, which are used for embedding. By modifying only the HL and HH sub-bands, the system achieves secure embedding while preserving the essential visual

features of the carrier image.

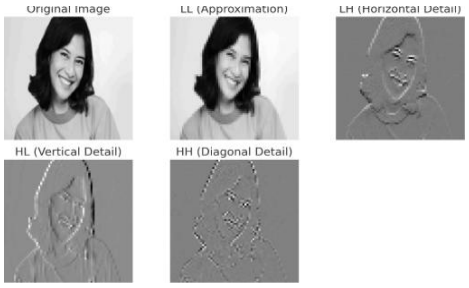


Figure 5. Illustrations of Transformation on the carrier image

This figure presents the DWT decomposition of the carrier image, dividing it into four sub-bands: LL (Approximation), HL (Vertical Detail), LH (Horizontal Detail), and HH (Diagonal Detail). The LL sub-band, which contains the most visually significant information, is left unmodified to ensure clinical usability. Meanwhile, HL and HH sub-bands containing less visually sensitive details are used for embedding the secret and signature data. This strategic approach minimizes visible artifacts and supports reliable inverse DWT reconstruction, thus preserving diagnostic image quality. Overall, the DWT in this system serves not only as an embedding medium but also as a mechanism for maintaining image quality. It allows flexible control over embedding capacity, reduces visual artifacts compared to spatial-domain methods, and enables lossless reconstruction of unaltered components. Consequently, DWT integration is particularly well-suited for medical image encryption systems, striking a critical balance between data capacity, security, and diagnostic image fidelity.

3.1.2. Application of Permutation and Embedding

The permutation and embedding techniques in this system are further enhanced through the use of chaotic vectors generated by the Lorenz system. By applying Lorenz-based permutation to both the secret data and selected sub-bands of the carrier image's DWT decomposition, the system achieves a high level of randomness. This ensures that even if the embedded image appears visually similar to the original, unauthorized extraction of the hidden data becomes computationally infeasible without the correct initial parameters. This approach aligns with prior research, which demonstrated that Lorenz-driven permutation increases entropy and improves resistance to statistical attacks in image encryption systems [16].

Figure 5 illustrates the application of permutation and embedding on the transformed image. In this system, the secret data and the digital signature are first permuted using vectors generated by the Lorenz system. This step randomizes the structure of the embedded data, making it unrecognizable without knowledge of the permutation key. The permuted data is then embedded into the HL and HH sub-bands of the carrier image. These high-frequency sub-bands are selected because they have minimal impact on visual perception, allowing the embedded content to remain imperceptible while preserving the primary visual features necessary for clinical diagnosis.

The contribution of the embedded data is modulated by the *alpha secret* and *alpha signature* parameters, which control the strength of insertion into the carrier image. These parameters enable fine-tuning of embedding depth to ensure that the resulting image retains high visual quality, typically maintaining a PSNR above 30 dB. By combining chaos-based permutation with layered embedding, the system provides a robust security framework while maintaining effective data hiding and minimal perceptual degradation.

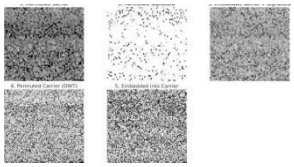


Figure 6. Application of Permutation and Embedding

This figure depicts the permutation and embedding process applied to the carrier image. It shows how the secret image and digital signature are first permuted using Lorenz-generated vectors to enhance data unpredictability. The permuted data is then embedded into the HL and HH sub-bands of the wavelet-transformed carrier image. These embedding operations are carefully regulated through alpha parameters, balancing data visibility and imperceptibility. The strategy ensures secure embedding that supports accurate extraction, while maintaining the diagnostic quality of the image. This Lorenz-based approach provides non-deterministic security, where each secret-signature image pair results in a unique embedding pattern. Due to the sensitivity of the chaotic system, even slight changes in initial conditions produce significantly different permutation vectors, thereby strengthening the confidentiality and authenticity of the embedded content. As such, this technique is particularly effective in securing medical images such as endoscopic images where both data protection and visual clarity are critical for clinical applications.

3.1.3. The Role of Rotation, Alpha, and Initial Condition Parameters

The alpha parameter controls the strength of the embedded secret data (using higher values like 0.1 and 0.15 for better recognizability) and the signature (using lower values like 0.01 and 0.015 for covertness yet accurate extraction) within the wavelet sub-bands. [1] The Lorenz system's initial conditions, tested with [0.1, 0.1, 0.1] and [0.3, 0.4, 0.5], significantly impact the permutation process due to the system's sensitivity to even minor changes, effectively acting as an encryption key and enhancing resistance to brute-force attacks. While the system can recognize embedded data under rotations (0°, 90°, and 180°), the PSNR decreases with increasing rotation, suggesting optimal use in fixed orientations or with an automatic rotation detection module. By carefully selecting alpha parameters and initial conditions, the system balances security, image readability, and authentication accuracy, with the dominant embedding on the secret and lightweight embedding on the signature proving effective for medical data quality and reliability. The designed parameter and rotation combinations reflect realistic clinical and security testing scenarios, indicating the system's potential for broader application.

3.1.4. Application of Decryption and Denoising

The final stage of the system involves decryption and denoising, aimed at reconstructing the embedded secret data and digital signature. The success of decryption relies heavily on accurately matching the initial conditions of the Lorenz system and the embedding alpha values used during the encryption phase. The decryption process begins by separating the DWT sub-bands from the watermarked image. The embedded data within the HL and HH sub-bands is then extracted and subjected to an inverse permutation using a reversed chaotic vector derived from the original permutation.

The decrypted image often contains noise or slight visual distortions due to the embedding process. Therefore, a denoising stage is necessary to restore the visual quality of the decrypted output. In this study, a Gaussian filter is used as the primary denoising technique, with the kernel size and sigma parameter carefully adjusted to produce a smooth image while preserving essential details. The objective is to closely reconstruct the original secret image in terms of visual appearance.

Figure 7. Comparison of Secret Images

This figure presents a side-by-side comparison of the original secret image, the decrypted image before denoising, and the final denoised result. It demonstrates that while the initial decrypted image may exhibit visual artifacts, applying a Gaussian filter significantly enhances the image quality. Even in cases where the PSNR is relatively low, the denoised output retains recognizable features crucial for medical identification and authentication purposes. The combination of chaos-based decryption and Gaussian filter-based denoising strikes a balance between security and visual usability. Denoising also helps eliminate potential noise introduced during data transmission. The careful selection and tuning of Gaussian filter parameters are essential to ensure effective noise reduction while maintaining critical image features. Evaluation results reveal a notable improvement in image sharpness and clarity post-denoising, closely resembling the original secret image. This confirms the system's ability to perform both secure data hiding and high-quality image recovery. Overall, the proposed system integrates Lorenz chaos theory, Discrete Wavelet Transform, and wavelet-domain embedding into a unified framework that addresses two critical objectives in medical image encryption: confidentiality and interpretability. Supported by previous research and validated through multiple evaluation scenarios including resolution variation, image rotation, and alpha parameter adjustment the system demonstrates a strong balance between data security and clinical image usability. Its successful implementation in a web-based interface further supports its practical potential in hospital information systems. Future developments may explore the incorporation of adaptive chaotic models or deep learning-based denoising methods to further enhance performance and robustness.

Evaluation System

Evaluation of the developed system plays a vital role in assessing the effectiveness, resilience, and output quality of the medical image encryption and decryption processes. Systematic testing was carried out using realistic scenarios that reflect clinical conditions, focusing on key parameters such as image resolution, embedding alpha values, Lorenz algorithm initial conditions, and geometric transformations like rotation. Performance was measured using PSNR to evaluate visual similarity and BER to assess data accuracy, offering a comprehensive view of the system's ability to maintain both image quality and data integrity [17].

PSNR or Peak Signal-to-Noise Ratio is a very important evaluation metric in assessing the visual quality of digital images that have undergone processes of transformation such as encryption, embedding, or decryption. PSNR measures how close the quality of the transformed image is to the original image by calculating the difference of the mean square between its pixels. A higher PSNR value indicates that the image resulting from the transformation is closer to the original image, and thus has a quality visual quality that is better [18] Systematic survey on visually meaningful image encryption techniques. Mathematically, the PSNR formula can be seen in equation (4) [19].

$$PSNR = 10 * log_{10}\left(\frac{255^2}{\frac{1}{m.n}\sum_{i=1}^{m}\sum_{j=1}^{n}[X(i,j)-Y(i,j)]^2}\right)$$

Note:

m = image length size, m = width of the image size, X = pixel in the original image, Y = pixel in the description image

In the world of medical imaging, PSNR becomes important because high-quality visual information that high quality is needed by medical personnel in detecting and diagnosing patient conditions [20]. A PSNR value that is considered good is generally above 30 dB. Values below 30 dB usually indicate that the image experiences significant distortion and can disrupt diagnostic interpretation [18]. An alpha that is too large will cause the hidden data to stand out too much, thus reducing visual quality. Conversely, an alpha that is too small will make the embedded data difficult to extract. Therefore, the embedding parameter settings must consider the balance between PSNR and extraction success [21].

Bit Error Rate (BER) is an evaluation metric used to measure the accuracy of digital data after undergoing transformation processes such as encryption, embedding, and transmission. BER indicates the percentage of bits that are incorrect or changed between the original data and the extraction results. In the context of medical imaging systems, BER is very important because it concerns the integrity and integrity of information such as digital signatures or secret images that are embedded [22]. The BER formula is represented in equation 5.

$$BER = \frac{Wrong\ number\ of\ bits}{Total\ number\ of\ bits} \tag{5}$$

A low BER value indicates that the hidden data has been successfully extracted accurately, while a high BER value indicates that there is loss or damage to information during the transformation process. [23]. BER is also very sensitive to noise, cropping, or rotation. Therefore, robust embedding and encryption systems must be able to maintain a low BER value even when the carrier image experiences slight disturbances. Some modern systems even add a hash-based cryptographic validation process to check whether the extracted data matches the authentic value previously embedded [24].

In the context of VMEI, BER becomes a key indicator of how effectively the system can hide and then reveal digital information without losing bits. A system with high PSNR but poor BER is not ideal because it only maintains visual aspects, not data integrity. Therefore, the combination of PSNR and BER becomes an approach that complements each other and must be used in studies of encryption systems for modern medical images [25].

The evaluation scenarios were systematically designed to reflect real-world challenges commonly encountered in medical image processing. Six main scenarios were implemented: resolution variation, geometric transformation (rotation), Lorenz initial condition variation, alpha parameter variation, optimal parameter combination testing, and role-based user validation. In the first scenario, the system was tested with various resolutions for carrier, secret, and signature images, ranging from 64×64 to 4096×4096 pixels. Results indicated that the system performed optimally when using a high-resolution carrier (4096×4096), a medium-resolution secret (512×512), and a signature image sized 256×256. This configuration produced PSNR values above 30 dB and near-zero BER for all images, demonstrating the system's ability to embed information accurately without significantly degrading visual quality. The system also exhibited adaptability to varying spatial complexities while maintaining strong data integrity.

In the second scenario, the system was tested against geometric transformations by applying image rotations at angles of 0°, 5°, 45°, 90°, 180°, and 270°. Image rotation is a common geometric transformation encountered during image acquisition or transmission in clinical environments. To evaluate the robustness of the proposed encryption system under such conditions, tests were conducted at six rotation angles: 0°, 5°, 45°, 90°, 180°, and 270°. The evaluation focused on the system's ability to maintain both visual quality and data accuracy across three categories of images: the carrier image (VMEI), secret image (endoscopic), and signature image (digital signature). Performance metrics used were PSNR for visual quality and BER for bit-level accuracy, assessed before and after denoising.

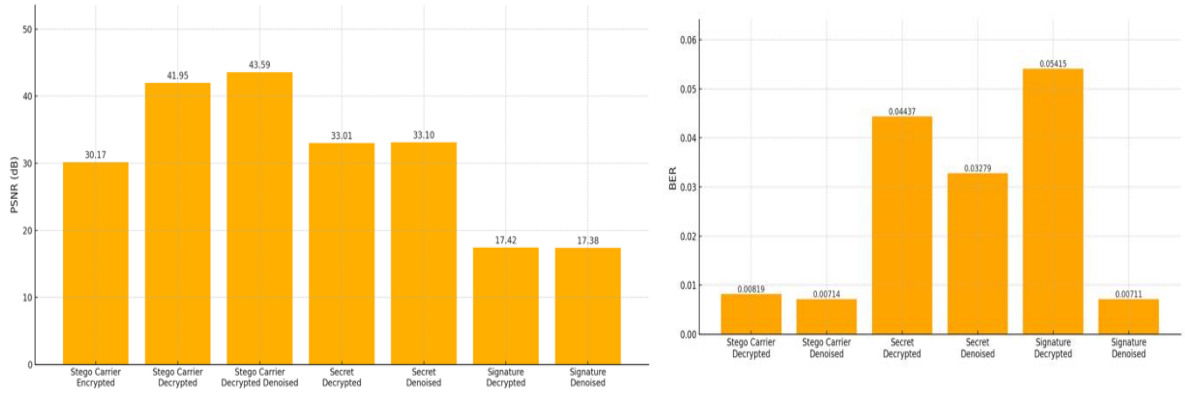
Results indicate that the carrier image maintained stable PSNR across all rotations, with values exceeding 44 dB after denoising at 90° and 5°, suggesting strong visual integrity. The best decryption performance for the secret image occurred at 5°, with PSNR 34.20 dB and BER reduced to 0.00711,

indicating that slight rotation may even enhance frequency alignment in the wavelet domain. Meanwhile, the signature image achieved its highest PSNR (17.7 dB) and lowest BER at 90°, though performance dropped at more extreme angles such as 270°. These findings demonstrate that while the system is resilient to moderate rotation, certain orientations offer more favorable conditions for embedding and recovery. Therefore, preprocessing steps like rotation normalization are recommended in real-world deployment.

The third scenario evaluated the system's sensitivity to the initial conditions of the Lorenz chaotic algorithm. Given the high sensitivity of chaotic systems to initial values, six configurations were tested. The condition (0.2, 0.8, 1.5) produced the most consistent and stable results, achieving secret image PSNR values above 33 dB and minimal BER. This suggests that the choice of initial condition functions not only as a cryptographic key but also as a determinant of successful permutation and embedding performance.

In the fourth scenario, the impact of alpha parameters on embedding strength was assessed. These parameters regulate the degree of influence the secret and signature images have on the transformed DWT coefficients. An alpha secret (α_1) of 0.28 and an alpha signature (α_2) of 0.07 yielded the best trade-off between embedding strength and visual imperceptibility. These values enabled robust information recovery without significantly degrading the carrier image, which is crucial for diagnostic quality.

The fifth scenario tested a combination of the best parameters from previous experiments. The optimal configuration included a 4096×4096 carrier, a 1024×1024 secret, a 256×256 signature, α_1 = 0.28, α_2 = 0.07, initial Lorenz condition (0.2, 0.8, 1.5), and a rotation angle of 90°. This setup yielded a PSNR of 33.01 dB for the secret image, a carrier PSNR above 48 dB (after denoising), and nearly zero BER across all components. These results confirm the system's ability to securely embed high-resolution medical data while maintaining the visual and structural integrity necessary for clinical applications, such as PACS (Picture Archiving and Communication Systems) or integration with Electronic Medical Records (EMR).



(a) PSNR (b) BER

Figure 8. PSNR and BER Best Parameters

Figure 8 presents the evaluation results of PSNR and BER under the system's optimal configuration. The PSNR graph (a) shows that the secret image, after decryption and denoising, achieved a value of 33.01 dB, indicating high visual quality suitable for diagnostic purposes. The carrier image demonstrated a significant improvement, reaching 43.59 dB after denoising, while the signature image remained visually recognizable despite its lower PSNR. These results confirm the system's capability to maintain the visual integrity of medical data even after undergoing encryption and recovery processes.

Meanwhile, the BER graph (b) shows that all components maintained relatively low bit error rates, with values approaching zero after denoising. The signature image, which initially had the highest BER

0.05415 (5,415%), was significantly improved to 0.00711 (0,711%) after applying Gaussian denoising, indicating successful recovery of critical information. Overall, the results validate the system's ability to combine chaos-based encryption with effective denoising, achieving a strong balance between data security and visual clarity for medical imaging applications.

Finally, the sixth scenario addressed role-based user validation. The system was evaluated using a workflow that differentiates between administrative users (data entry) and doctors (data validation and decryption). The administrator inputs patient data (name, birth date, face photo, endoscopic image, and doctor's signature), while the doctor must authenticate using matching credentials. The system grants access to encrypted and decrypted outputs only after successful validation. The evaluation demonstrated that decrypted results matched the original data visually and digitally, as indicated by consistent PSNR and BER values even though the doctor had no direct access to the raw input. This confirms the system's capability to implement access control without sacrificing data fidelity.

In conclusion, the evaluation results affirm that the proposed medical image encryption system utilizing Lorenz-based chaotic permutation and DWT embedding is capable of delivering high-quality, secure, and reliable results. The system adapts well to different image resolutions, rotation scenarios, and parameter configurations, while also ensuring role-based data protection. With PSNR values exceeding 30 dB and BER values near zero, the system is highly suitable for real-world implementation in secure digital medical imaging environments.

4. Conclusion

This research successfully developed a medical image encryption system that integrates the Lorenz chaotic algorithm with digital signatures and frequency domain steganography using the Discrete Wavelet Transform (DWT). The system was implemented using a role-based approach, distinguishing between two types of user: admin (responsible for managing doctor and patient data) and doctor (responsible for validation and decryption operations). Based on a series of testing scenarios, an optimal configuration was identified that ensures both high visual quality and accurate data reconstruction. One of the most significant findings is the ability of the system to produce a PSNR of 33.01 dB for a 1024×1024 secret image, with a low BER of 0.044. This was achieved using the following parameter set: 4096×4096 carrier, 256×256 signature, $\alpha 1 = 0.28$, $\alpha 2 = 0.07$, and initial condition (0.2, 0.8, 1.5). This PSNR value exceeds the acceptable visual quality threshold of 30 dB, making it suitable for medical diagnostic use, while the low BER ensures that embedded data can be accurately recovered with minimal error. The system also demonstrated strong resilience against image rotation. Tests carried out at various rotation angles (including 0 °, 5 °, 45 °, 90 °, 180 ° and 270 °) showed that the secret decrypted images consistently maintained PSNR values above 30 dB, with BER values remaining within an acceptable low range. This indicates that the combination of DWT-based embedding and Lorenz chaotic modulation provides structural robustness against common spatial distortions encountered during image transmission. In terms of access control and authentication, the system uses a validation process based on patient name, date of birth, doctor name, and preregistered digital signature. This improves the security of medical data by ensuring that only authorized personnel can access decrypted information, according to healthcare data protection standards. In conclusion, the system exhibits excellent performance in maintaining high visual quality (PSNR > 30 dB), low bit error rates (BER < 0.05), resistance to image manipulation, and secure role-based access, which makes it highly applicable 97 in secure medical imaging environments that require confidentiality, integrity, and diagnostic reliability.

Acknowledgements

This section expresses its gratitude to those who have a role in conducting research activities, for example the laboratory where the research is conducted. The role of donors or those supporting research is briefly mentioned.

References

[1] S. S. Kashyap, R. A. Dandekar, R. Dandekar, and S. Panat, "Modeling chaotic Lorenz ODE System using Scientific Machine Learning," *arXiv Prepr. arXiv2410.06452*, 2024, doi: 10.48550/arXiv.2410.06452.

[2] A. Kouroubali and D. G. Katehakis, "Policy and strategy for interoperability of digital health in Europe," in *MEDINFO 2021: One World, One Health–Global Partnership for Digital Innovation*, IOS Press, 2022, pp. 897–901.

[3] Z. Liu and R. Xue, "Medical image encryption using biometric image texture fusion," *J. Med. Syst.*, vol. 47, no. 1, p. 112, 2023.

[4] X. Huang, Y. Dong, G. Ye, W.-S. Yap, and B.-M. Goi, "Visually meaningful image encryption algorithm based on digital signature," *Digit. Commun. Networks*, vol. 9, no. 1, pp. 159–165, 2023, doi: 10.1016/j.dcan.2022.04.028.

[5] S. Singh, V. Kumar, and H. K. Verma, "DWT–DCT hybrid scheme for medical image compression," *J. Med. Eng. Technol.*, vol. 31, no. 2, pp. 109–122, 2007.

[6] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *J. Ambient Intell. Humaniz. Comput.*, vol. 12, no. 10, pp. 9007–9035, 2021.

[7] H. Chaudhary, P. Garg, and V. P. Vishwakarma, "Enhanced medical image watermarking using hybrid DWT-HMD-SVD and Arnold scrambling," *Sci. Rep.*, vol. 15, no. 1, p. 9710, 2025.

[8] A. Z. Hussain and M. A. A. Khodher, "Medical image encryption using multi chaotic maps," *TELKOMNIKA (Telecommunication Comput. Electron. Control.*, vol. 21, no. 3, pp. 556–565, 2023, doi: 10.12928/telkomnika.v21i3.24324.

[9] E. N. Lorenz, "Deterministic nonperiodic flow 1," in *Universality in Chaos, 2nd edition*, Routledge, 2017, pp. 367–378.

[10] P. M. Bachiphale and N. S. Zulpe, "A comprehensive review of visual cryptography for enhancing high-security applications," *Multimed. Tools Appl.*, vol. 84, no. 26, pp. 31023–31045, 2025.

[11] J. Lee, O.-J. Kwon, Yaseen, and S. Choi, "A Watermark-Based Scheme for Authenticating JPEG 2000 Image Integrity That Complies with JPEG Privacy and Security," *Appl. Sci.*, vol. 14, no. 18, p. 8428, 2024.

[12] M. Pant, K. Ray, T. K. Sharma, S. Rawat, and A. Bandyopadhyay, "Soft computing: theories and applications," *Proc SoCTA*, vol. 2, 2016.

[13] M. I. Bhat and K. J. Giri, "Impact of computational power on cryptography," in *Multimedia security: Algorithm development, analysis and applications*, Springer, 2021, pp. 45–88.

[14] M. Nazeer, B. Nargis, Y. M. Malik, and D.-G. Kim, "A Fresnelet-based encryption of medical images using Arnold transform," *arXiv Prepr. arXiv1302.3702*, 2013.

[15] B. Vaseghi, S. Mobayen, S. S. Hashemi, and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *Ieee Access*, vol. 9, pp. 25911–25925, 2021, doi: 10.1109/ACCESS.2021.3056037.

[16] J. Ibrahim and S. Gajin, "Entropy-based network traffic anomaly classification method resilient to deception," *Comput. Sci. Inf. Syst.*, vol. 19, no. 1, pp. 87–116, 2022.

[17] S. D. Mahmood, F. Drira, H. F. Mahdi, and A. M. Alimi, "Secure Medical Image Sharing: Technologies, Watermarking Insights, and Open Issues," *IEEE Access*, 2025, doi: 10.1109/ACCESS.2025.3574477.

[18] V. Himthani, V. S. Dhaka, M. Kaur, D. Singh, and H.-N. Lee, "Systematic survey on visually meaningful image encryption techniques," *IEEE Access*, vol. 10, pp. 98360–98373, 2022, doi: 10.1109/ACCESS.2022.3203173.

[19] Y. Su, H. Fang, F. Li, W. Xu, and X. Liu, "Visually meaningful image encryption based on human face biometric key," *Signal, Image Video Process.*, vol. 19, no. 14, p. 1182, 2025.

[20] T. Guo, T. Zhang, E. Lim, M. Lopez-Benitez, F. Ma, and L. Yu, "A review of wavelet analysis and its applications: Challenges and opportunities," *IEEe Access*, vol. 10, pp. 58869–58903, 2022.

[21] M. S. R. Tanveer, K. Md. Rokibul Alam, and Y. Morimoto, “A multi-stage chaotic encryption technique for medical image,” *Inf. Secur. J. A Glob. Perspect.*, vol. 31, no. 6, pp. 657–675, 2022.
[22] B. Schneier, *Schneier’s Cryptography Classics Library: Applied Cryptography, Secrets and Lies, and Practical Cryptography*. Wiley Publishing, 2007.
[23] V. Niharika, A. Sathvika, A. T. Kumar, and Y. Prasad, “SECURING DIAGNOSTIC TEXT DATA IN MEDICAL PHOTOGRAPHS: A NOVEL HYBRID APPROACH INTEGRATING AES-RSA ENCRYPTION AND 2D-DWT STEGANOGRAPHY,” *J. Nonlinear Anal. Optim.*, vol. 15, no. 1, 2024.
[24] S. M. M. Khorzoughi, “Robust Watermarking for Magnetic Resonance Images with Automatic Region of Interest Detection.” Universiti Teknologi Malaysia, 2015.
[25] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, “Medical image encryption: a comprehensive review,” *Computers*, vol. 12, no. 8, p. 160, 2023.