International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

COVERLESS IMAGE STEGANOGRAPHY FOR PATIENT DATA PROTECTION USING GABOR-DWT FEATURE HASHING

***Noor Alhuda Abbas Jasim[1], Suhad A. Ali[2], Majid Jabbar Jawad[3]**

Department of Computer Science, College of Science for Women, University of Babylon, Iraq

Email: [1] scw227.nour.alhda@student.uobabylon.edu.iq

[2] wsci.suhad.ahmed@uobabylon.edu.iq

[3] wsci.majid.jabbar@uobabylon.edu.iq

Abstract

Coverless information hiding has gained increasing interest due to its steganalysis resilience, but existing approaches have the limitation of low capacity and reliance on large datasets. In this approach, a successful coverless image steganography (CIS) technique is proposed with the aim of protecting patient information using one medical image without changing its content. The method has the following steps: Firstly, the confidential message is encrypted using XOR. and Arnold transform and divided into numerous pieces. Secondly, cover medical image is filtered using Gabor filters and Discrete Wavelet Transform (DWT) to yield robust features. Three, a hash table is formed using the resultant features. Four, each piece of the message is mapped to an index in the hash table. Fifth, the indexes are kept in an auxiliary file. Finally, the original image and the auxiliary file are transmitted to the receiver. Experimental outcomes show that the proposed CIS technique achieves zero Bit Error Rate (BER = 0) and 100% Recovery Correctness (RC) and is able to achieve high capacity along with immunity to common image processing attacks. Compared to previous techniques such as the technique employed in [22], which requires more than 550 medical images for scanning all alphanumeric characters, the new method functions as equally or even superior with a single medical image, a significant advancement in terms of efficiency, scalability, and usability.

Keywords: Coverless Image Steganography, Medical Images, Gabor Filters, DWT, Patient Data Security

1. Introduction

Similar to artificial intelligence, cloud computation, and wireless communication have advanced, IoMT, or the internet of medical things, has become a well-known application area. With the Internet and mobile connectivity, medical images the most crucial component of medical data are increasingly being transmitted and shared across various hospitals and research institutions worldwide in order to meet the demands of diagnosis and research. Private information and clinical data, including test results and diagnostic records, make up the majority of the medical data that was disclosed,in contrast to other industries. The two primary elements contributing to the increasing danger of medical data are the comparatively inadequate protection measures and the high value of medical data. Therefore, it is imperative

Received: August 03 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)
to improve the information security and privacy protection of medical images throughout transmission, storage, and use. Maintaining the privacy of personal information is crucial, and steganography has emerged as a preferable method for obtaining safeguarded data because to advancements in computer security. Steganography is the process of inserting secret data into another image, audio file, video, or communication with the intention of hiding it [1–3]. Every pixel of the cover image is concealed using an equal the quantity of secret bits in steganography techniques. The cover picture has an equivalent amount of embedding change. In contrast, each pixel in a digital image has intricate statistical relationships. Consequently, when changes are made to the cover image pixel with an identical number of bits, the picture quality is automatically reduced [6]. To overcome these issues, the steganography method has used difreerent adaptive embedding techniques. This method of adaptive embedding contains an arbitrary number of bits into every pixel in the cover picture. Because of this, most academics focused on adaptive solutions to make the steganography approach safer [7–11]. Changes performed during the embedding process have no effect on the edge pixels. Therefore, compared to smooth pixels, edge pixels can store more hidden bits. Metaheuristic algorithms are used to solve optimization problems in the majority of applications [12–15]. IoT-transmitted data via the Internet is used in the cloud to protect data. Complex encryption and decryption technologies give high data security. Data concealment is more advantageous than encryption and decryption alone [16, 17].

2. Related Works

To ensure confidentiality without compromising image quality, the need to transmit clinical information discreetly has led in recent years to the development of steganography techniques. Current steganography methods alter pixels to hide confidential data, thereby modifying their intensity, enabling a clear transformation and exposing the system to steganography analysis. To avoid these drawbacks, overlay steganography has been proposed as an attractive alternative, as it does not directly alter the overlay image itself.

Several researchers have conducted studies on some steganography methods based on image properties. Karim (2022) presented a robust wavelet hashing-based coverless image steganography technique. Without altering the images, the secret message is split up into binary segments and compared to pictures in a sizable database whose hash sequences precisely match. Steganalysis is thwarted and security is enhanced by this method. According to the experiments, there is limited resistance to JPEG compression and noise, but there is strong resilience against geometric attacks (rotation, scaling) and image processing (filtering, brightness). Eight bits per image is the maximum hiding capacity, indicating that capacity and robustness will need to be improved in future work [18]. Mangi (2023) suggested a coverless image steganography technique that maintains robustness while boosting hiding capacity. Cover images are split up into non-overlapping blocks, features are extracted using DWT, and hash sequences are created to match segments of secret messages. Without changing the cover image, extraction is guided by auxiliary data. The technique shows good normalized correlation (NC) and bit error rate (BER) performance, achieves high capacity, and withstands attacks such as JPEG compression, noise, filtering, and brightness changes. Future research attempts to improve security through auxiliary data encryption. [19]

Received: August 03 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

In 2024, the researchers used Generative Adversarial Networks (GAN) with attention vectors to offer a new technique for concealing information in photos. Important information is preserved in delicate areas of photos with this technique. Three different dataset types' brain tumors, glaucoma, and ovarian cancer were used to test the approach. Compared to previous techniques like SteganoGAN, HCISNet, and CSIS, the results show great accuracy; the new method can classify brain tumors with an accuracy of up to 96%. This technique allows for a small (less than 2%) decrease in embedding capacity while maintaining the quality of concealed images [20].

AlHamdani et al. (2025) proposed a coverless image steganography method based on deep learning to embed secret messages without altering the cover image. The approach uses ResNet50v2 to extract deep features from cover images, then applies Discrete Wavelet Transform (DWT) to generate binary hash sequences. Secret messages are embedded by matching segments with hash sequences stored in a hash table, and auxiliary data records the matching locations. The system achieves high accuracy in feature extraction, showing strong robustness against various noise attacks such as Gaussian noise, filtering, and salt-and-pepper noise, maintaining good Structural Similarity Index (SSIM), Bit Error Rate (BER), and Normalized Correlation (NC). Future work aims to enhance security by improving the encryption of auxiliary data.[21]

This paper introduces a new CIS technique that uses a single medical image to secure patient data. The method guarantees great robustness and precise message recovery without modifying the image by combining hash-based indexing, DWT, Arnold transform, and Gabor filters. This makes it appropriate for real-world healthcare applications.

3. Proposed system

To protect patient data privacy, this work proposes a coverless steganography technique based on features extracted using Gabor filters and DWT transform, without altering the original image. A hash table is created to aid in message encoding, and the Arnold transform is used to scramble the secret data. To retrieve the hidden message, the recipient uses the same reference image and file that the sender created as an auxiliary file. The system's two primary stages the sender and the receiver are depicted in Figure 1.

3.1 Processes on the Sender Side

Several actions are taken on the sender's end, as detailed in Algorithm (1.1):

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

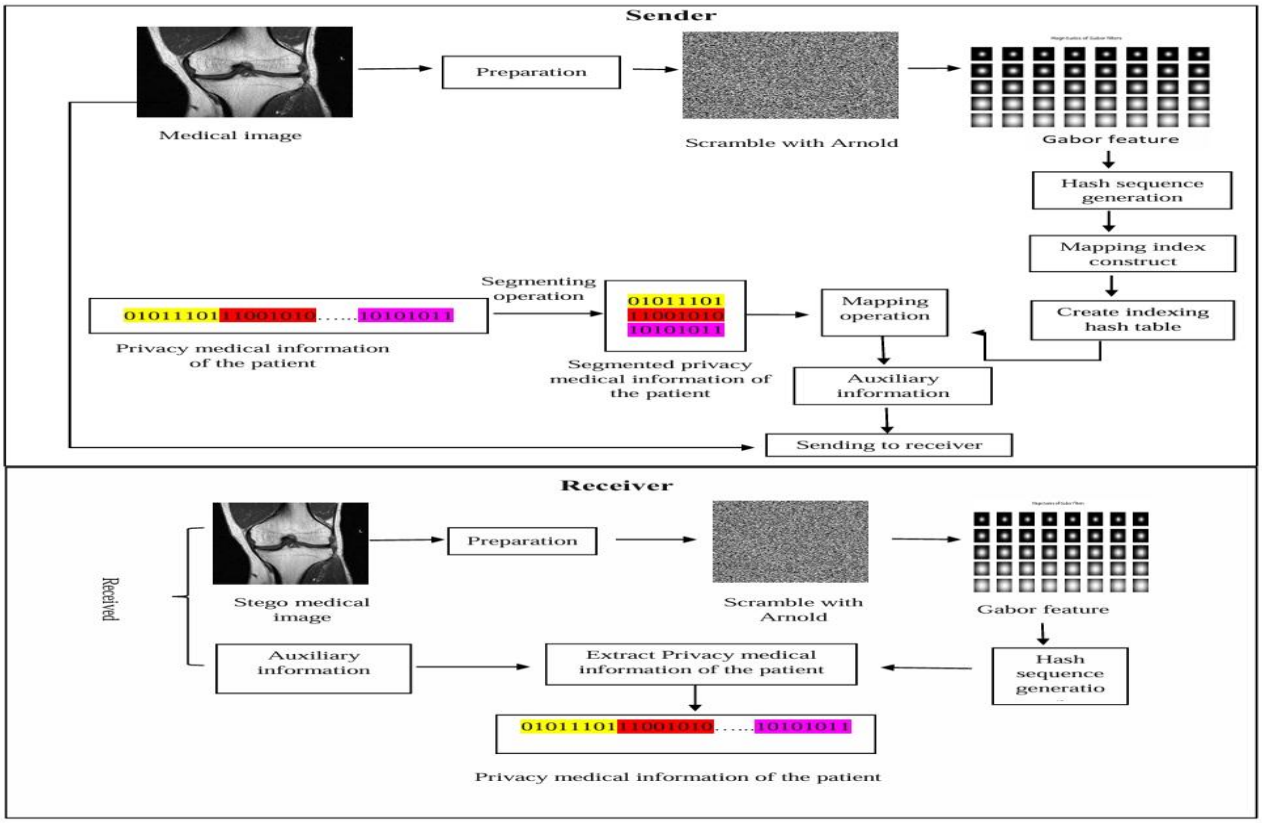


Figure 1: The suggested system's block diagram

Algorithm (1.1): The Sending Procedure

Input: Cover Image CI , Secret Data SD

Output: Stego Image SI. Auxiliary File AF

Begin

Split the secret data **SD** into segments of 8 bits each.

2. Use Arnold Transform to create a scrambled version of the cover image CI' using equation (1).

Apply **DWT** (Discrete Wavelet Transform) on CI' to break down the image into smaller frequency bands.

Apply **Gabor filters** on selected DWT components to extract feature responses from image blocks.

Generate **hash values** from the Gabor responses of each non-overlapping block using equation (2).

Build a **Hash Table** mapping each block to its corresponding hash value described in Section (4).

For each segment SD (i) of the secret data:
a. Map SD(i) to a block whose hash value corresponds to embed the data.
b. Save the block locations to the **Auxiliary File (AF)**.

Send **SI** and **AF** to the receiver.

End

Received: August 03 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Preparation of Medical Image

Applying the Arnold Transform to the input medical picture is the first step in the methodology. The scrambling mechanism offered by Arnold Transform reorganizes pixel locations, enhancing the image representation's resilience and security. This stage is essential for protecting sensitive patient data by obscuring the original image content prior to feature extraction. Conceal sensitive information in medical images such as CT, MRI scans, and X-rays have the following goals:

- Prevent visual access to sensitive information and alterations.
- Enhance security measures for feature-based encoding systems.

Given an image of dimension N×N , each pixel at position (x,y) is moved to a new location (x′,y′) as follows:

$$\text{Mod N} \quad \begin{bmatrix} x \\ y \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} x' \\ y' \end{bmatrix} \qquad (1)$$

Repeating the transform multiple times increases the scrambling level. The transform is **reversible**, so the original image can be recovered after decoding.

In addition to scrambling, the system employs a bitwise XOR operation to bind the secret message to image-derived data. After extracting features (e.g., using Gabor filters), and generating a binary hash representing stable image characteristics, each bit of the secret message is encrypted using the corresponding bit from the hash sequence.

2. Hash Sequence Generation

The proposed approach is systematic and follows a sequence. Medical images are first processed with a Discrete Wavelet Transform (DWT) to extract the low-frequency components which usually contain critical information regarding the medical image. The presence of important features is indicated by sudden changes in texture within these components. The low-frequency images are then processed with Gabor filters at multiple scales and orientations to capture texture details in various spatial directions. Block diagrams of the DWT-Gabor system are presented in Figure 2.

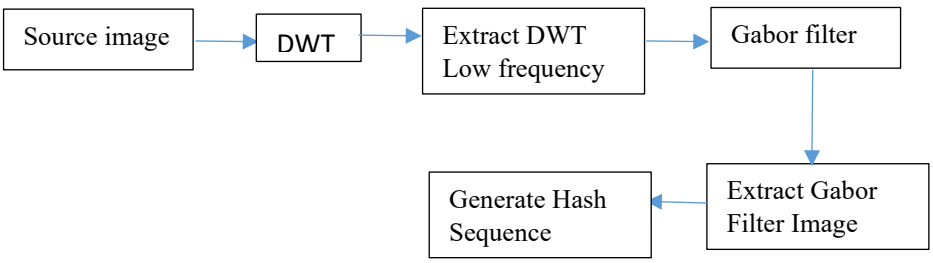


Figure 2: Block diagrams of the DWT-Gabor approach

Received: August 03 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

After Gabor filtering, the Gabor coefficients are converted into a fixed-length binary hash sequence. Equation (2) states that this is accomplished by applying a thresholding function based on the feature vector's mean value:

$$f(x) = \begin{cases} 0 & if\ x < mean(X) \\ 1 & if\ x \geq mean(X) \end{cases} \quad (2)$$

in where mean(X) is the mean of the input vector X and x is the input value.

3. Creating a Hash Table from Gabor Coefficients

Once the selected feature extraction approaches (e.g., Gabor filtering for Discrete Wavelet Transform (DWT)) are applied to the entire input image, one can derive a binary feature vector f(x). This vector includes the general structural and textural properties of the image, and does not segment the entire image to smaller blocks.

To achieve a higher embedding rate and derive a more robust solution, sliding window operation is conducted directly over the binary feature vector. Namely, an 8-byte window of fixed length is employed in order to produce all possible overlapping hash sequences by sliding the window one position at each shift over the vector. If the length of the feature vector is L, this procedure produces a number of L−7 overlapping 8-bit binary sequences.

Each 8-bit sequence is then:

- Interpreted as a binary hash
- Converted to decimal value (between 0 and 255)
- Related with the beginning of the feature vector

This data is maintained as a Hash Table (HT) and has the following three columns:

- The 8-bit binary hash sequence
- Its decimal value
- The position index within f(x)

This hash table is used as a pointer index in the message embedding stage. The hidden message is then chunked into 8-bit unit. Figure (3) shows steps for creating hash table.

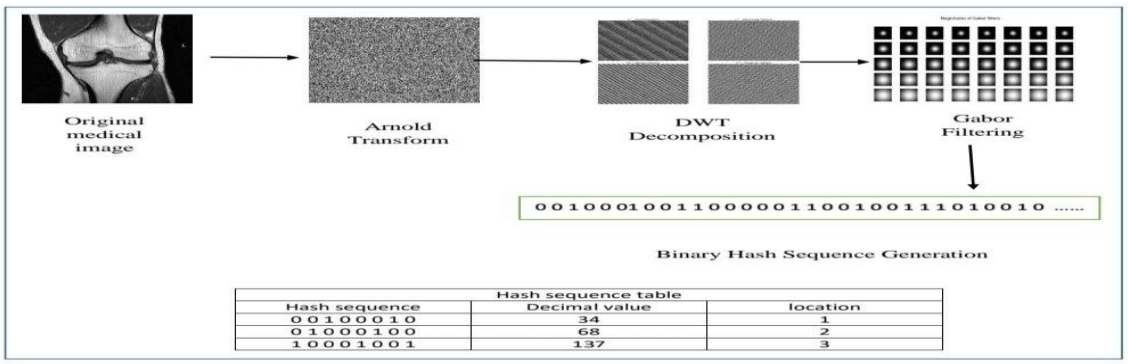


Figure 3: Generating Hash Sequenc Table from input image

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Building Indexing Hash Table for Efficient Embedding Process

In order to improve the speed of the embedding process, the embedding step is optimized by creating indexing hash table derived from the original hash table. The main function of this indexing table is to act as an inverted index. It allows the rapid retrieval of positions within the feature set which correspond to a given hash value. Specifically, each 8-bit hash (from 0 to 255) is uniquely associated with a list of indices in the relevant feature vectors in which the corresponding sequence appears. This change enhances the efficiency of the hash table by allowing the system to access it as if it were an index while supplying only the feature vectors and the segments of the message.

In the embedding phase, the confidential information is segmented into 0 and 1s binary of specific lengths. Each segment is then converted into decimal hash values. Matching feature positions are found for each hash value in the auxiliary index table. This approach avoids redundant comparisons and sequential scanning, thus embedding photomasks, especially in high-capacity situations, is remarkably faster. In addition, this design allows for flexible random, weighted voting, or stable feature ranking embedding strategies by narrowing down potential embedding location quickly.

Upon finishing the embedding process for all message segments and linking them to their corresponding hash entries, an auxiliary information file is created. This document lists in order the positions (indices) of the feature vectors that correspond to the hash values of the secret message. The image is not altered in any way meaning the medical image can be transmitted without any visual or statistical changes. This auxiliary file is essential for preserving both the confidentiality of the data as well as the integrity of the message. It is the only necessary side channel for reconstructing the secret message on the recipient's end by re-extracting the feature vector from the image and matching the positions listed in the auxiliary file. This approach keeps the system coverless while still ensuring security and efficient communication. By disassociating the image from the data and the data embedded within, there is much less risk of steganalysis, whether visual or statistical, and the scheme is appropriate for highly sensitive areas like the transmission of medical images.

As described earlier, Figure (4) depicts the flow of the described embedding processes. It demonstrates how secret information is embedded in images and retrieved through hashing, including data retrieval in an auxiliary table, and the ultimate mapping to predetermined feature positions. This figure also demonstrates how unnecessary element-wise comparisons are eliminated by the use of a table, thereby improving the entire embedding pipeline. From this phase, an auxiliary file matching the feature positions as the stego-key of message recovery is generated. Because the modification is not made on the cover image and only feature-derived positions are kept, the proposed method preserves the covert characteristic of the system while ensuring strong security, high capacity, and low computational effort.

Received: August 03 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

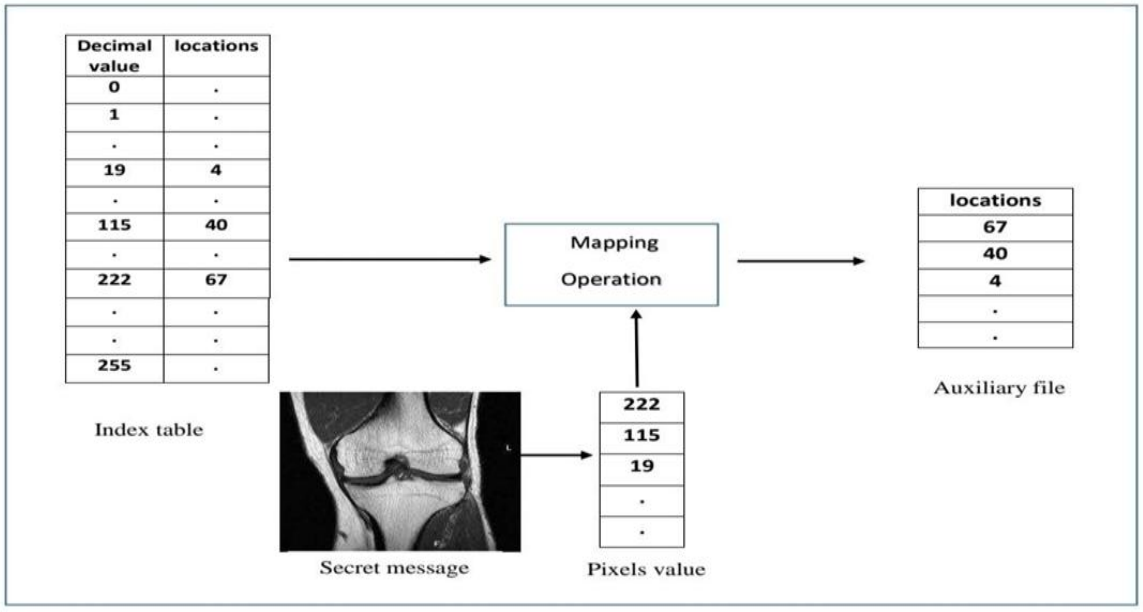


Figure 4: Embedding Operation

3.2 Extraction Process on the Receiver side

Several actions are taken on the receiver's end, as detailed in Algorithm (1.2) and Figure (5).

In the receiver's end, the extraction procedure initiates with receiving two critical components: the medical image untouched and the auxiliary information file. This auxiliary file's pivotal listing includes where feature vectors were stored in relation to the binary message segments during embedding phase procedures. Initially, the receiver executes feature extraction the same way as it was done during embedding for the image. This will reconstruct the global binary feature vector (x), usually done via Gabor filtering and Discrete Wavelet Transform (DWT). The integrity of the feature vector is crucial since it enables recovering the embedded data without any alteration to the image.

After feature vector reconstruction, the receiver accesses the auxiliary file to fetch the position indices of the fragments to be extracted. An 8-bit binary string is extracted from the position in the overlapping hash sequences of the feature vector for each index in the list. These sequences are processed to convert them to decimal which are then transformed into the binary segments of the secret message.

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Once all the segments have been processed, the segments are merged to retrieve the original

Algorithm (1.2): The Receiving Procedure

Input: Stego Image **SI** , Auxiliary File **AF** (contains only block locations)

Output: Reconstructed Secret Data **SD**

Begin

To produce the converted picture CI′, apply Arnold Transform to the received stego image SI using an equal number of iterations as during the sending phase.

Apply **Discrete Wavelet Transform (DWT)** on **CI′** to decompose it into sub-band components.

Apply **Gabor filters** on selected DWT sub-bands to extract local texture features from non-overlapping blocks.

Generate **hash values** for each block based on its Gabor features.

Construct a **Hash Table** that maps each block's location to its corresponding hash value.

Initialize an empty list for secret data **SD**.

For each location entry in the Auxiliary File **AF**:
a. Retrieve the corresponding block at the specified location.
b. Extract the **hash value** of that block.
c. Convert the hash value into its corresponding **8-bit ASCII character** (or symbol).
d. Append the character to the secret data **SD**.

Concatenate all retrieved characters to reconstruct the full secret message **SD**.

End

bit stream. This method of extraction has the following notable advantages:

- No detectable distortion: since the cover image is not modified, it is not necessary to seek out or undo any steganographic changes or distortion.
- Great endurance: because stable feature points are used, minor image variations or deteriorations can be tolerated by the system.
- Risk and privacy: since the message is masked solely within the geometric configuration and spacing of features and entails no overt modifications, the possibility of steganalysis suffers a considerably heightened risk.

In any case, the extraction method provided greatly assures the reliability and the security of the retrieval of the secret medical information with the transmitted image and the auxiliary

file designed for coverless, high capacity, and attack-resistant steganography.

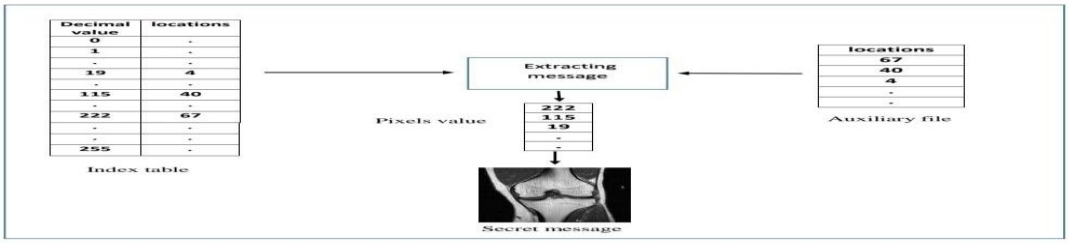


Figure 5: Extraction Operation

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

4. Results Analysis & Comparison

Extensive experiments were conducted on various standard medical images including brain MRI and chest X-ray and abdominal CT scans effectively. Images were picked from various public datasets and crudely resized uniformly 256×256 pixels for sake of visual consistency apparently as shown in Figure (6). Evaluation focused on system embedding capacity and bit error rate under various attacks with comparisons made against several conventional steganographic methods slowly.

Figure 6: Examples of medical images

4.1 Robustness Measures

To quantify this resilience, two evaluation metrics the Recovery Correctness (RC) and the Bit Error Rate (BER) are used. Error rate between original and extracted secret information is computed using Metric for bit error rate (BER).

BER is calculated as follows:

$$BER = \frac{N_{Errors}}{N_{Total}} \quad (3)$$

Where: N_{Errors} is the quantity of incorrectly received bits. N_{Total} is the overall quantity of bits sent.

The Recovery Correctness (RC) Metric is used to assess how accurately the secret message was recovered following a variety of attacks using image processing on the cover image. RC is computed as follows:

$$\text{RC} = \left(\frac{N_{correct}}{N_{total}}\right) * 100 \quad (4)$$

Where:

- $N_{correct}$: Number of correctly recovered characters (or bits).
- N_{total} : Total quantity of characters (or bits) in the original secret message.
- RC: Recovery Correctness, expressed as a percentage.

Bit Accuracy

Received: August 03 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Bit Accuracy tells you how many bits are the similar to both the first and current secret messages that was recovered. It gives a general idea of how well the binary data was kept. To find Bit Accuracy, do the following:

$$\text{Bit Accuracy} = \left(\frac{N_{correct\ Bits}}{N_{total\ Bits}}\right) \quad (5)$$

Where:

- $N_{correct\ Bits}$: Number of bits that match exactly between the original and recovered message.
- $N_{total\ Bits}$: Total number of bits in the original message.

Block Accuracy tells you how many characters (or symbols) in the original secret message match those in the recovered secret message. Each letter is seen as one "block." This is how to figure out Block Accuracy:

$$\text{Block Accuracy} = \left(\frac{N_{correct\ chars}}{N_{total\ chars}}\right) \quad (6)$$

Where:

- $N_{correct\ chars}$: Number of characters correctly recovered.
- $N_{total\ chars}$: Total number of characters in the original message.

4.2 Capacity Evaluation

To evaluate the data-hiding capacity of the proposed coverless image steganography (CIS) technique, we consider two distinct scenarios depending on whether or not repeated hash-to-symbol mapping is allowed.

Scenario 1: One-to-One Mapping (No Repetition of Position Assignment)

In this case, every symbol **s** of the secret message corresponds to a particular appearance of the hash of that symbol in the feature vector. That is, if the symbol s occurs **k** times in the message, then there must be **k** distinct positions **i** in the hash table where hash[i] = s.

Let:

L: Length of the binary feature vector extracted from the image (after DWT + Gabor filtering).

N=L−7: Number of 8-bit overlapping hash sequences.

U⊆[0,255]: Set of unique hash values present in the image.

Now, the maximum message length (in symbols) is:

$$\text{Capacity\_ unique} = N = L - 7 \quad (7)$$

If the symbol is 8 bits the total capacity (in bits) is:

$$\text{Capacity\_unique\_bits} = 8 \times (L - 7) \quad (8)$$

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This is useful when the position of the symbol is randomly arranged or used only one time, it brings the message to be traceable, and it provides conditions for methods like block voting or majority decoding.

Scenario 2: Fixed Mapping (Repeated Hash-to-Symbol Mapping)

In this case, every symbol of the message is mapped into a pre-determined fixed location in the hash table. That is, the hash value **s** is uniquely determined by a known position p_s with Hash(p_s) = s, and is used again for each occurrence of the symbol **s** in the message.

As a result:

- There are more available symbols than there are hash positions.
- The only constraint is that there should exist all the 256 hash values (0 to 255) at least once in the feature vector.

As a result, the theoretical embedding capacity is

$$\text{Capacity fixed} = \infty \tag{9}$$

$$\text{Capacity fixed bits} = 8 \times N_{symbols}$$

where $N_{symbols}$ is arbitrary

This allows for finite, and unbounded message length (bounded by external factors like auxiliary file size, or system memory), and is particularly well-suited for secure communication in practical applications involving medical image transmission over the Internet where symbol consistency needs to be maintained across sessions.

For example, if the input image with size 256×256 then

- DWT decomposition (1 level), LL subband size = 256/2×256/2=128×128=16,384 pixels
- After applying Gabor filtering, we compute a 1D feature vector from the filtered LL band. That feature vector length L = 16,384 values.

The computation of capacity into scenarios as follows:

Scenario 1: Unique Mapping (No Repeats)

Step 1: Compute number of 8-bit overlapping hashes:

$$N = L - 7 = 16384 - 7 = 16377 \text{ symbols}$$

Step 2: Compute total capacity in bits:

$$\text{Capacity\_unique\_bits} = 8 \times 16377 = 131016 \text{ bits} \approx 16 \text{ KB}$$

Scenario 2: Fixed Mapping (Allow Reuse)

If each symbol always maps to the **same fixed hash position**, and all 256 values from 0–255 appear at least once in the hash table:

- You can reuse each symbol's index infinitely.

Received: August 03 2025

International Journal of Applied Mathematics
Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

- Only your message length limits the capacity.

For example, to hide 100,000 symbols then

$$\text{Capacity\_fixed\_bits} = 8 \times 100000 = 800000 \text{ bits} = 100 \text{ kB}$$

Table 1 presents a comparative evaluation between the proposed coverless image steganography (CIS) method and the earlier approach by Tan et al. [22], focusing on the number of images required and the total embedding capacity.

Table 1: Proposed Method and Tan et al. [22] Comparison of Image Requirements and Total Capacity

Method	**# Images Required**	**Total Capacity (TC)**
Tan et al. [22]	550 images	62 characters (496 bits)
Proposed Method Unique (no reuse)	1 image (256×256)	16377 characters (131016 bits)
Proposed Method Fixed (reuse allowed)	1 image (256×256)	Unlimited

The Tan et al. [22] has a capacity of only 550 symbols for encoding 62 alphanumeric characters, resulting in encoding capacity of only 496 bits. This corresponds to around 0.9 bits per image, and is very inefficient for storage and downloading, especially in medical fields such as bandwidth-limited or real-time medical.

On the contrary, the proposed CIS method uses a solitary 256×256 medical image which, subjected to DWT and the Gabor filter for one time, yields reliable and dissimilar 8-bit hashes for every one of the 1024 non-overlapping blocks. This allows a full ASCII character (8 bits) to be represented per block, and hence a total of 16,377 characters (131,016 bits) capacity with no block re-use. This corresponds to **512×** higher capacity using **~550× fewer images**, demonstrating a significant gain in both embedding efficiency and resource utilization.

More importantly, in the fixed reuse situation, our method is able to reuse the block hashes to form the identical symbols, that is, arbitrarily large payload per image can be achieved theoretically for a given message length and redundancy level.

4.3 Performance under Attacks

The robustness of this coverless image steganography (CIS) method was further tested by common image processing attacks on the stego image. These attacks model real-world scenarios in transmission, compression and unauthorized modification. The system effectiveness against each class of attack was measured by two quantitative indicators, the Bit

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

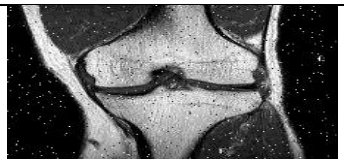
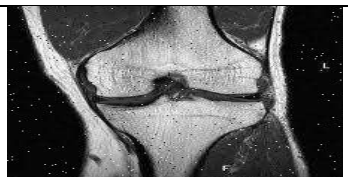
Error Rate (BER) and Recovery Correct Analysis (RC). Further, we present visual evidence of the attacked image to assist in qualitative analysis.

We define the Bit Error Rate (BER) as the fraction of recovered bits that are different from the embedded bits, and the Recovery Correctness (RC) as the number of symbols which were correctly recovered.

Results for this comparison are summarized in Table 2 for various types of affections such as JPEG compression, Gaussian noise, rotation, cropping, and resizing. Every row consists of the attack, attack parameter, the corresponding BER and RC value, and the visual representation of the attacked image.

The experiments shown in Table (2) clearly show the fact that the proposed scheme is able to possess low BER and high RC under some moderate level of distortion (e.g., JPEG compress ion quality ≥ 70% and Gaussian noise variance ≤ 0.01) specifically against the attacks.

Table 2: Robustness Evaluation of the Proposed Method under Various Image Attacks

Attack type	Attack Value / Parameters	BER (%)	RC (%)	Attacked Image
	0.01	0.125000	87.50%	
	0.005	0.093750	90.62%	
	0,001	0.000000	100.00%	

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

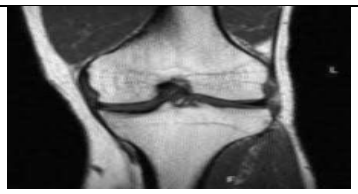
Noise from salt and pepper				
Speckle noise	0,01	0.000000	100.00%	
	0.005	0.000000	100.00%	
	0,001	0.000000	100.00%	
Gaussian noise	0.005	0.000000	100.00%	
	0.01	0.000000	100.00%	
	0,001	0.000000	100.00%	
				

Received: August 03 2025

International Journal of Applied Mathematics

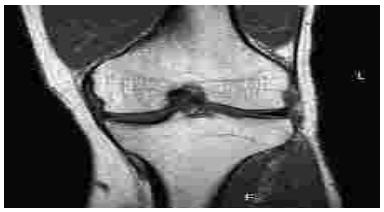
Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Medium filter	3*3	0.125000	87.50%	
Average filter	3*3	0.156250	84.38%	
Resizing	0.7	0.093750	90.62%	
Rotation	10°	0.093750	90.62%	
Cropping	10%	0.281250	71.88%	
translation	20*30	0.093750	90.62%	

Received: August 03 2025

Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

JPEG compression	Q=10	0.062500	93.75%	
	Q=90	0.000000	100.00%	

4.4 Comparative Analysis

In order to further prove the superiority of the proposed CIS method, a comparison experiment was performed with the DenseNet-based method developed by Tan et al. [22]. All the experiments performed in this section are conducted under the same attack scenarios for comparison, and Table 3 compares the two approaches in terms of Bit Accuracy, Block Accuracy and the Bit Error Rate (BER).

In this set of experiments, the same secret message “Za91” in [22] was used for fairness and consistency. The hidden message was well hidden and extracted with a single 256×256 medical image, a task that the walk method of [22] needed over 550 medical images to facilitate bout symbol representation and message reconstruction. This large performance gap demonstrates that the system we propose has better efficiency and scalability, especially in limited and expensive image resources transmission industry.

The method based on DenseNet in [22] has high storage and transmission requirements because it relies on a large image dataset. Instead, our method produces the invariant feature hashes using Gabor filtering and DWT, and overlapping, achieving strong robustness against the distortions.

Experimental results in Table 3 demonstrate that the proposed method achieves 0% BER and 100% RC in presence of the various types of image attacks such as JPEG compression (Quality Factor = 90), resizing, Gaussian noise and speckle noise. These results show the robustness of the system and confirm its practical feasibility as a secure high-capacity steganographic communication method.

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 3: Comparison of the Effects of Different Attack Types on Image Steganography Technique Performance

Attack type	**Attack Value / Parameters**	**Tan et al. [22]Bit Accuracy/Block Accuracy**	**Proposed system** **Bit Accuracy** **Block Accuracy**
Salt & Pepper Noise	σ =0.001	0.9955/0.9641	1.0000/ 1.0000
	σ =0.005	0.9941 /0.9501	0.906250 / 0.625000
	σ = 0.01	0.9938 /0.9454	0.875000 /0.625000
Speckle Noise	σ =0.001	0.9945 /0.9516	1.0000/ 1.0000
	σ =0.005	0.9938 /0.9454	1.0000 / 1.0000
	σ = 0.01	0.9932 /0.9407	1.0000 / 1.0000
Gaussian Noise	σ =0.001	0.9934/ 0.9423	1.0000 / 1.0000
	σ =0.005	0.9908 /0.9204	1.0000 / 1.0000
	σ = 0.01	0.9863 /0.8814	1.0000 / 1.0000
Median Filter	3×3	0.9922 /0.9329	0.875000 /0.750000
Mean Filter	3×3	0.9638 /0.7239	0.843750 /0.625000
JPEG Compression	Q = 10 Q=50	0.9936 /0.9423 0.9938 /0.9485	0.937500/0.750000 1.0000 / 1.0000
Rotation	10°	0.8851 / 0.2839	0.906250 /0.625000
Cropping (Edge)	10%	0.9853/ 0.8705	0.718750 /0.375000
Scaling	0.3	0.9825/ 0.8518	0.875000 /0.500000

Experiments showed that the proposed method was more robust against a range of attacks. It maintained 100% recovery correctness and high bit accuracy (≥ 1.0000) under Gaussian, speckle, and JPEG compression attacks, while [22] exhibited noticeable degradation, especially under rotation (block accuracy dropped to 0.2839). The proposed system maintained acceptable performance even in the face of filtering and geometric attacks, demonstrating its efficacy and suitability for real-world medical scenarios with limited resources and strict confidentiality requirements.

Received: August 03 2025

International Journal of Applied Mathematics

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

.Conclusion

In this paper, a robust and high payload CIS (coverless image steganography) method is presented in an efficient way to ensure good quality enhancement from the health care communication systems. This method is a fusion of techniques such as DWT, Gabor filtering, Arnold scrambling, and XOR-based encryption along with lightweight auxiliary hash file, to provide a secure embedding and extraction of the secret message without altering the cover image.

Extensive experimental results verify the method's robustness to a variety of frequent image-processing attacks, such as filtering, compression, geometric warping, and addition of noise. The system obtained bit level accuracy of 1.0000 and block level accuracy ≥ 0.5000 with BER = 0 on several difficult scenarios such as Gaussian and Speckle Noise cases and also with RC = 100%.

Furthermore, the proposed system provides a significant increased capacity of embedding up to (131016 bits) into single medical image. This surpasses existing methods, including Tan et al by a large margin. [22], which use more than 550 images to represent 62 characters, causing high overhead in transmission and storage. The experimental results in general validate the practical feasibility, good robustness, and high efficiency of our proposed method and thus establish it as a promising scheme for secure, scalable, and covert medical data transmission within the context of contemporary healthcare systems.

References

[1] K. A. Al-Afandy, O. S. Faragallah, A. ELmhalawy, E.-S. M. El Rabaie, and G. M. El-Banby, "High security data hiding using image cropping and LSB least significant bit steganography," in Proceedings of the 4th IEEE International Colloquium on Information Science and Technology (CiSt), pp. 400–404, IEEE, Tangier, Morocco, October 2016.

[2] A. Elhadad, S. Hamad, A. Khalifa, and A. Ghareeb, "High capacity information hiding for privacy protection in digital video files," Neural Computing & Applications, vol. 28, no. 1, pp. 91–95, 2017.

[3] S. Hamad, A. Khalifa, and A. Elhadad, "A blind high-capacity wavelet-based steganography technique for hiding images into other images," Advances in Electrical and Computer Engineering, vol. 14, no. 2, pp. 35–42, 2014.

[4] M. Hashim and M. Rahim, "Image steganography based on odd/even pixels distribution scheme and two parameters random function," Journal of theoretical and Applied Information Technology, vol. 95, no. 22, 2017.

[5] B. M. Krishna, C. Santhosh, S. Suman, and S. K. Shireen, "Systems, and computers, "evolvable hardware-based data security system using image steganography through dynamic partial reconfiguration," Journal of Circuits, Systems, and Computers, vol. 31, no. 1, Article ID 2250014, 2022.

Received: August 03 2025

Volume 38 No. 5s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[6] C. Qin, W. Zhang, F. Cao, X. Zhang, and C.-C. Chang, “Separable reversible data hiding in encrypted images via adaptive embedding strategy with block selection,” Signal Processing, vol. 153, pp. 109–122, 2018.

[7] Q. Li, X. Liao, G. Chen, and L. Ding, “A novel game-theoretic model for content-adaptive image steganography,” in Pro ceedings of the IEEE 37th International Conference on Dis tributed Computing Systems Workshops, pp. 232–237, ICDCSW, Atlanta, GA, USA, June 2017.

[8] D. B. Khadse and G. Swain, “Data hiding using quotient value differencing and remainder value substitution avoiding in correct extraction problem,” Sensing and Imaging, vol. 22, no. 1, pp. 1–21, 2021.

[9] R. Sonar and G. Swain, “A hybrid steganography technique based on RR, AQVD, and QVC,” Information Security Journal: A Global Perspective, pp. 1–20, 2022.

[10] R. Sonar and G. Swain, “Steganography based on quotient value differencing and pixel value correlation,” CAAI Transactions on Intelligence Technology, vol. 6, no. 4, pp. 504–519, 2021.

[11] G. Swain and A. Pradhan, “Image steganography using remainder replacement, adaptive QVD and QVC,” Wireless Personal Communications, vol. 123, no. 1, pp. 273–293, 2022.

[12] S. I. Nipanikar, V. Hima Deepthi, and N. Kulkarni, “A sparse representation based image steganography using particle swarm optimization and wavelet transform,” Alexandria Engineering Journal, vol. 57, no. 4, pp. 2343–2356, 2018.

[13] G. Swain, “Adaptive and non-adaptive PVD steganography using overlapped pixel blocks,” Arabian Journal for Science and Engineering, vol. 43, no. 12, pp. 7549–7562, 2018.

[14] G. Swain, “A data hiding technique by mixing MFPVD and LSB substitution in a pixel,” Information Technology and Control, vol. 47, no. 4, pp. 714–727, 2018.

[15] G. Swain, “Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function,” Optik, vol. 180, pp. 807 823, 2019.

[16] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, “SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images,” Measurement, vol. 139, pp. 426–437, 2019.

[17] E. S. B. Hureib and A. A. Gutub, “Enhancing medical data security via combining elliptic curve cryptography with 1-LSB and 2-LSB image steganography,” International J Comp Sci Network Security (IJCSNS), vol. 20, no. 12, pp. 232–241, 2020.

[18] Karim, Nadia A., Suhad A. Ali, and Majid Jabbar Jawad. "A coverless image steganography based on robust image wavelet hashing." TELKOMNIKA (Telecommunication Computing Electronics and Control) 20.6 (2022): 1317-1325.

Received: August 03 2025

Volume 38 No. 5s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[19] Mangi, Hadeel Talib, Suhad A. Ali, and Majid Jabbar Jawad. "Enhancing of coverless image steganography capacity based on image block features." TELKOMNIKA (Telecommunication Computing Electronics and Control) 21.6 (2023): 1364-1372.

[20] A. Virupakshappa, & D.S. Uplaonkar , " Deep learning-based coverless image steganography on medical images shared via cloud" , Engineering Proceedings, pp.59,176 , 18 2024 .

[21]AlHamdani, Teba Hassan, Suhad A. Ali, and Majid Jabbar Jawad. "Coverless Image Steganography Based on Machine Learning Techniques." Journal of Cybersecurity & Information Management 15.2 (2025).

[22]Tan, Yun, et al. "Privacy Protection for Medical Images Based on DenseNet and Coverless Steganography." Computers, Materials & Continua 64.3 (2020).

Received: August 03 2025