Multimedia Tools and Applications (2023) 82:20497–20516
https://doi.org/10.1007/s11042-022-14301-0

A novel steganographic technique for medical image using SVM and IWT

Partha Chowdhuri[1] · **Pabitra Pal**[2] · **Tapas Si**[3]

Received: 25 May 2022 / Revised: 11 November 2022 / Accepted: 10 December 2022 /
Published online: 6 January 2023

Abstract

This study presents an efficient authentication scheme for digital image steganography on medical images benefiting from the combination of both techniques: Support Vector Machine (SVM) and Integer Wavelet Transform (IWT). We use two different strategies in this paper, where SVM is used first to separate the Region of Interest (ROI) from Non-Region of Interest (NROI) in the medical image. Then IWT is applied to embed secret information within the NROI part of the medical image (Cover Image). Moreover, we have applied a circular array and a shared secret key to enhance the robustness of the proposed scheme. The research looked into the various experimental analyses to establish the acceptability of the existing scheme. The simulation is performed to measure the imperceptibility using Peak Signal to Noise Ratio (PSNR) and to test the robustness using the Structural Similarity Index Measure (SSIM). The experimental result shows good imperceptibility with a PSNR of 64 dB and better robustness with a SSIM of 0.96 for the proposed steganographic scheme.

Keywords Steganography · Integer wavelet transform · Support vector machine · Circular array · ROI & NROI · Medical image

Partha Chowdhuri and Tapas Si contributed equally to this work.

✉ Pabitra Pal
pabipaltra@gmail.com

Partha Chowdhuri
prc.email@gmail.com

Tapas Si
shritapassi.ai@gmail.com

[1] Computer Science, Vidyasagar University, Vidyasagar University Road, Paschim Medinipur, 721102, West Bengal, India

[2] Department of Computer Applications, Maulana Abul Kalam Azad University of Technology, Simhat, Haringhata, 741249, West Bengal, India

[3] Department of Computer Science and Engineering, Bankura Unnayani Institute of Engineering, Pohabagan, Bankura, 722146, West Bengal, India

1 Introduction

The pandemic of COVID-19 has emphasised the significance of the Internet and multimedia technology. We are becoming more agnostic to internet communication technologies as we share private information such as health information, bank details, credit card data, or family pictures via the internet in our daily lives. Nowadays, sharing this personal or commercial information over the internet is a high risk activity. Unauthorized use, tampering, and copy-right violations may happen very easily as the information is transmitted over an untrusted digital platform. Authentication and confidentiality are very much needed to defend against unauthorised access and usage. So users need a trustworthy platform or application through which they can easily share their personal information without any doubt. In this scenario, a joint venture of steganography and machine learning may provide an efficient and effective solution. In the existing steganographic model, the embedding position remain same in each and every image used as cover. It does not depend on a type of the image we are using. But in the proposed model, the embedding position depends on the type of the image. With the help of machine learning, it finds the non region of interest (NROI) and embeds the secret information there. It not only makes the embedding process dynamic but also ensures that the region of interest of every image remain unchanged even after embedding secret bits in the image. In this study, we proposed a robust steganographic scheme using Support Vector Machine (SVM) and Integer Wavelet Transform (IWT) to improve security and robustness while maintaining authenticity and data integrity.

Medical images are more typical than any other ordinary images since they store a patient's valuable information for diagnosis purposes. Such images need more security and confidentiality as total diagnosis depends on it. In tele-medicine applications, the transmission of medical images via an open channel demands strong security and copy-right protection. So we always have to take care of these images while embedding the secret information into them. To do so, a medical image is classified into two regions; an important part of the medical image used for diagnosis purposes is known as the Region of Interest (ROI), and the rest of the image, which is not so essential, is known as the Non Region of Interest (NROI). A small mis-classification may cause big trouble in extracting essential information of the patient. In statistical learning theory, SVM is a new class of machine learning method that can be used as an image classifier. Applying SVM in the transform domain for medical image watermarking is still an open area of research.

Steganography in medical images can be performed in three stages. The first stage can be described as the classification of NROI and ROI; the second stage is stego embedding in the host image in the transform domain; and the last stage is the extraction of embedded information. The machine learning algorithm named SVM is being used, which is widely used for classification problems. On the other hand, the transform domain methods such as Singular Value Decomposition (SVD), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Integer Wavelet Transform (IWT) are robust against various attacks in the embedding and extraction processes. However, among all these schemes, the IWT has the special property that it can transform the pixel values into some integer values, which might be very useful for designing a reversible steganographic model.

In the proposed model, a double layer of security is introduced to ensure the robustness of embedded data. The embedded data is scrambled using a unique key. The transform domain based hybrid steganographic technique is applied to embed the scrambled data into the IWT coefficients of the host image. The proposed scheme exploits the reversibility feature of IWT and the randomization property of the circular array.

The main motivations of this work are as follows:

- Identifying the least important portion of a medical image for embedding secret information.
- Increasing the embedding capacity of the medical image with a minimal degradation of the cover image.
- From the literature survey, it has been found that a very few number of researchers have developed a steganographic scheme in the cryptographic point of view. Also, there exist some security loop-hole in the state-of-the-art methods. Therefore, development of a high security steganographic scheme in the medical image application is still a demanding research area.

The major contributions of this article are as follows:

- Detecting the NROI and ROI portion of a medical image using machine learning model.
- Embedding secret patient information in the NROI section to protect the important portion of the image.
- Using Circular Array to embed multiple secret bits by changing one pixel in the original medical image to enhance the imperceptibility of the cover image.
- Provide a double layer security by using a secret key (κ) along with the circular array.

The rest of the paper is structured in the following manner: A literature survey has been done in Section 2. Section 3 describes some preliminary information. The developed stego embedding and extraction algorithms are defined in Section 4. Section 5 describes the experimental results of the proposed model and the performance comparisons with some state-of-the-art techniques. Finally, discussion and conclusions are drawn in the Sections 6 and 7 respectively.

1.1 Abbreviations

The abbreviations used in this article have been tabulated in the Table 1.

2 Literature review

In 2021, Rasha [21] analyzed a Medical Image Watermarking (MIW) method for image authentication and integrity verification. The current Medical Image Authentication (MIA) methods emphasise the need to achieve robustness against unintended attacks (i.e., image noise and image compression), which are inescapable attacks; hence, the new MIA methods should validate their resilience against these attacks. However, because of the nature of colour images, the MIW and MIA schemes created for monochrome images cannot be easily transferred to colour medical images, providing a fresh challenge for future study in this area. In 2022, Meng et al. [12] proposed a new data hiding scheme using encrypted images based on IWT and chaotic systems. The IWT transform was employed in this approach to divide the carrier image into wavelet components, and the chaotic system was utilised to create location sequences, encryption sequences, and scrambling sequences for data concealment and image encryption. The hidden information was concealed in the diagonal element using the position sequence, and the approximate component was encrypted using the encryption and scrambling sequences, generating the final encrypted image. A solution to the issue of pixel loss in the reconstruction phase was given after the wavelet component

Table 1 Abbreviations with their descriptions

Abbr	Description	Abbr	Description
I	Cover Image	ROI	Region of Interest
SI	Stego Image	NROI	Non Region of Interest
W	logo Image	SVM	Support Vector Machine
B_w	Secret bit stream	IWT	Integer Wavelet Transform
CA	Circular Array	κ	Shared Secret Key
Arr_r^{pos}	ROI pixel positions	Arr_r^{pix}	ROI pixel values
Arr_{nr}^{pos}	NROI pixel positions	Arr_{nr}^{pix}	NROI pixel values
MIW	Medical Image Watermarking	MIA	Medical Image Authentication
DCT	Discrete Cosine Transform	DWT	Discrete Wavelet Transform
PTB	Pixel to Block	SVD	Singular Value Decomposition
SS	Spread Spectrum		

was encrypted. For varying degrees of security, the key required to decode the image and extract the hidden message was separated into two portions. The approach of encrypting images after data concealment increased the security and maximal payload of the solution. In 2020, Sabbane et al. [17] suggested a new image watermarking scheme using polynomial decomposition. From the experimental results, they achieved good perceptibility, i.e., 61.66 dB PSNR with NCC value of 1. When compared to state-of-the-art techniques, experimental findings show that the suggested approach achieves a good balance in terms of watermark invisibility and robustness. In 2020, Zhang et al. [27] analyzed various research challenges on medical image confidentiality. In 2021, An and Liu [1] proposed a medical image segmentation algorithm based on a deep learning model. A multi-level boundary-aware RUNet segmentation model is proposed in this research. A U-Net-based segmentation network and a multi-level border detection network comprise the network structure. It is capable of resolving the issue of border location. Simultaneously, in order to address the issue of deep learning network architectures' poor adaptation to medical imagery, this research recommends including a novel interactive self-attention module into deep learning models. In 2017, Thanki et al. [22] proposed a medical image watermarking scheme in the transform domain. They proposed a blind medical picture watermarking system based on the Fast Discrete Curvelet Transform (FDCuT) and DCT. FDCuT is used on a medical image to get the frequency coefficients of its curvelet decomposition. Block wise DCT is used to extract the high frequency curvelet coefficients of the medical image to get distinct frequency coefficients. In 2017, Singh et al. [18] presented an imperceptible watermarking system to address the security issue of medical fundus images for tele-ophthalmology applications and computer aided automated diagnosis of retinal diseases. In 2017, Parah [14] suggested a reversible data hiding technique in medical image applications. The Pixel to Block (PTB) conversion technique has been used as an effective and computationally efficient alternative to interpolation for the cover image generation to ensure reversibility of medical images. They proposed a new image interpolation based scheme, [15] to get a high

payload data hiding system for medical image applications. In 2017, Rai et al. [16] proposed a SVM based watermarking scheme where they achieved better robustness and imperceptibility with an SSIM of more than 0.50 and a PSNR of more than 35 dB. In 2004, Ganic et al. [3] suggested a robust image watermarking scheme where they embedded the data in all frequency domains of DWT and SVD. In 2022, Vulli et al. [25] used Fast AI framework along with the 1-cycle policy to diagnose and detect metastases from whole slide images. They achieved more accuracy than the others existing models used for the same. Karakus and Avci [8] proposed a new optimized steganographic scheme by making of the pixel similarity. Their experimental results show that their scheme can achieve an average PSNR value of 66.5 which is reasonable better than the other existing scheme. In 2023, Yadav et al. [26] developed a efficient steganographic scheme for secure communication framework where the information are concealed using heuristic approach. They also used the machine learning scheme to make the scheme more efficient. In 2022, Garg et al. [4] developed a steganographic algorithm to encapsulate the content of secret image in the style information of the host image using Neural Style Transfer (NST) algorithm. Here, they uses discriminator loss for optimization to achieve an accuracy of 50% without noise, and 35% with noise. Mehta et al. [11] proposed a Blind image steganography scheme which resistant against JPEG compression attack. Their scheme can survive under JPEG compression attack for any quality factor range from 10 to 90. In 2022, Song et al. [19] proposed a robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain where they achieved stronger anti-detection capability.

Some researchers have proposed a steganographic model using SVM and Spread Spectrum (SS). In such schemes, SVM has been used for classification of ROI and NROI in medical images, whereas Spread Spectrum has been used for embedding and extraction of patient information. However, embedding has been done in the spatial domain and no attacks have been performed on the proposed model. Here, a new steganographic technique has been proposed for medical images using a supervised machine learning algorithm. The secret information is inserted unsymmetrically within the cover image. The scheme is robust against various attacks since embedding has been performed in the transform domain.

3 Prerequisite

In this research, a steganographic scheme using SVM and IWT has been proposed. This section will go over the related background of SVM, IWT, and Circular Array.

3.1 Support vector machine (SVM)

In statistical learning theory, SVM is a new class of supervised machine learning method, which can be used for regression and mostly for classification problems. In this classification algorithm, each data item is plotted as a point in an n-dimensional feature space of items with the value of a particular coordinate. Then a classification is performed to distinguish two classes by finding the best hyperplane as depicted in Fig. 1.

Here, margin defines the utmost breadth of two parallel lines to the hyperplane, which does not contain any data points within the parallel slabs; the data points nearby the separating hyperplane are named as support vectors. Support vector points lie on the edge of the slab. The data points in the positive category are shown by squares, and the data points in the negative category are shown by circles. The classification of ROI and NROI regions in medical images is an important procedure for embedding the secret information in non-essential

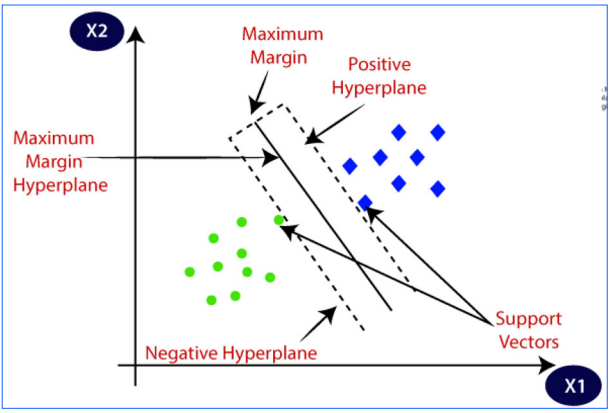


Fig. 1 Schematic diagram of the hyperplane classification in SVM

portions. It can be overcome by using SVM as a classifier, which avoids any distortion to the diagnosis part of the image. So, such a classification technique can ameliorate the schematic steganographic methodology.

3.2 Integer wavelet transform (IWT)

Integer Wavelet Transform (IWT) is an advanced method that is often used for compression, image processing, and steganography, among other things. In digital image steganography techniques, IWT has its own importance due to its favourable spatial localization and multi-resolution properties. Its multi-resolution property reveals several details of an image. The Wavelet function partitions the data into distinct frequency components. Discontinuities and sharp spikes of a signal can be studied in IWT, which shows its advantage over traditional transform methods. In single level, two-dimensional IWT, decomposes the signal or image into four non-overlapping coefficient bands, known as LL, LH, HL, and HH bands, where LL represents approximation coefficients and LH, HL, and HH represent detail orientations such as horizontal, vertical, and diagonal components, respectively, of the two-dimensional signal. The approximation coefficient (LL) of the first level can be furthermore separated into another four LL, LH, HL, and HH sub-bands. This process can be repeated up to the desired number of levels. Inverse IWT is used to reassemble the sub-bands to construct the original image (Fig. 2).

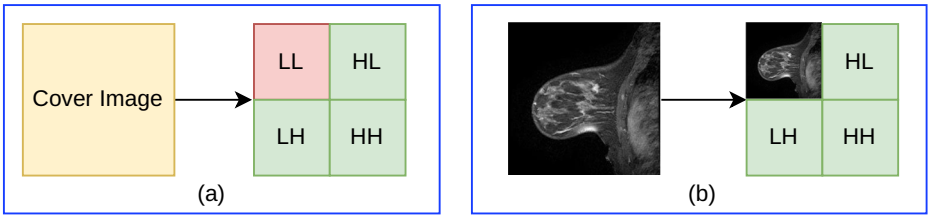


Fig. 2 IWT decomposition of an image

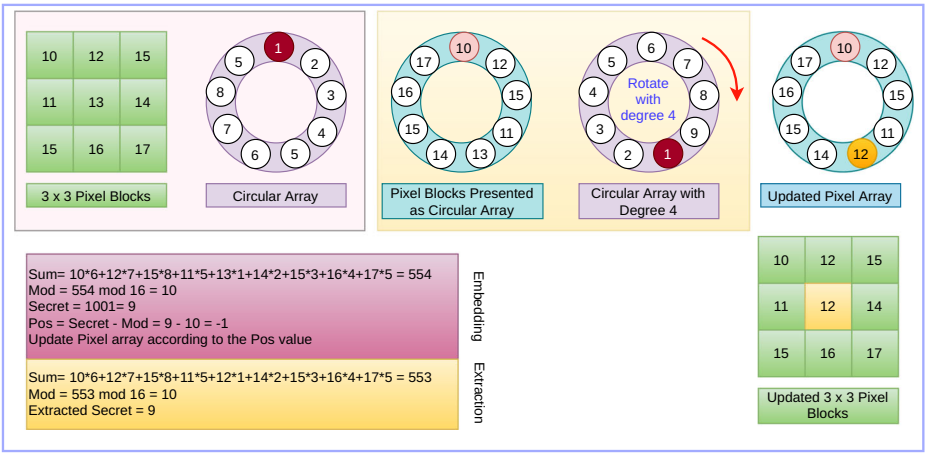


Fig. 3 Circular array formation

3.3 Circular array

The concept of data hiding using a weighted matrix was first suggested by Tseng et al. [24]. The scheme is able to hide $\lfloor log(2^{mn} + 1) \rfloor$ bits information by changing at most two bits in a block of size $2mn$ of the cover image. The concept of circular array, used in this proposed work, is an inspiration from this weighted matrix. But, instead of a matrix, an array is considered here. The array is circular in shape as the index of the elements can be changed by rotating the elements, either clockwise or anticlockwise. In order to hide k secret bits, the array must contain all the values from $(0\ to\ 2^{k-1} + 1)$. If any position in the array is left, the positions can be filled by any of these values (Fig. 3). Now a new value, v is generated by the following equation:

4 Proposed steganographic scheme

The proposed scheme has been classified into three sub-sections, Image classification 4.1, Information Embedding 4.2 and Information Extraction 4.3.

4.1 Image classification

In this classification stage of the proposed model, the pixels of the medical host image are characterised into ROI and NROI to perform embedding. In an SVM classification model, the labelled predictor data is used to build a trained model. To find adequate predictive precision, various SVM kernel functions are available, which require the parameters to be set for better accuracy. After training the model, it is cross-validated using the test data set. For instance, the host medical image is partitioned into two parts: ROI and NROI. The trained SVM model utilises the available dataset to manage its related parameters, i.e., weight vector and bias, which are mainly used to reduce the mis-classification between ROI and NROI. ROI is basically used for diagnosis purposes, whereas NROI does not have more significance. Therefore, a small mis-classification in the selection of ROI & NROI can cause big trouble in diagnosis.

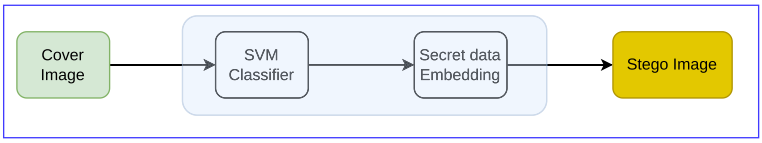


Fig. 4 Two phase diagram of steganographic scheme

The schematic diagram of the proposed model shown in Fig. 4. Here, a model has been created after performing the training of the SVM algorithm using breast MRI dataset. The SVM model predicts the ROI and NROI regions of the host medical image. The pixels lies in the NROI regions are selected for embedding secret data without affecting the pixels in the ROI region. The detailed embedding procedure has been discussed in Section 4.2.

4.2 Information embedding

The embedding scheme of the proposed scheme has been described in this section. Initially, a colour cover image of size $(M \times N)$ has been considered as an input image. In the previous section, the detection of ROI and NORI parts of an image using SVM has been discussed. These ROI and NORI pixel positions are stored in two different arrays, say, Arr_r^{pos} and Arr_{nr}^{pos} and the pixel values are stored in two different arrays, say Arr_r^{pix} and Arr_{nr}^{pix} respectively. Here, only the NROI part is of major concern for embedding. Now, the cover image is separated into three RGB colour components (Fig. 5). Then, IWT is applied to each colour block to get IWT_R, IWT_G and IWT_B coefficients blocks of different colors. Then, the red component (IWT_R) is considered first for the steganographic process. Now, any shared secret key (κ) is considered and a 512 bit string is generated from κ using the standard SHA-512 hashing algorithm. Henceforth, the stego bit stream (B_w) is generated from the logo (W). Moreover, a circular array is used to embed the stego information (B_w) within the (IWT_R) block with the help of κ. Basically, the shared secret key, κ is used to select the direction of the rotation of the circular array. The circular array is rotated

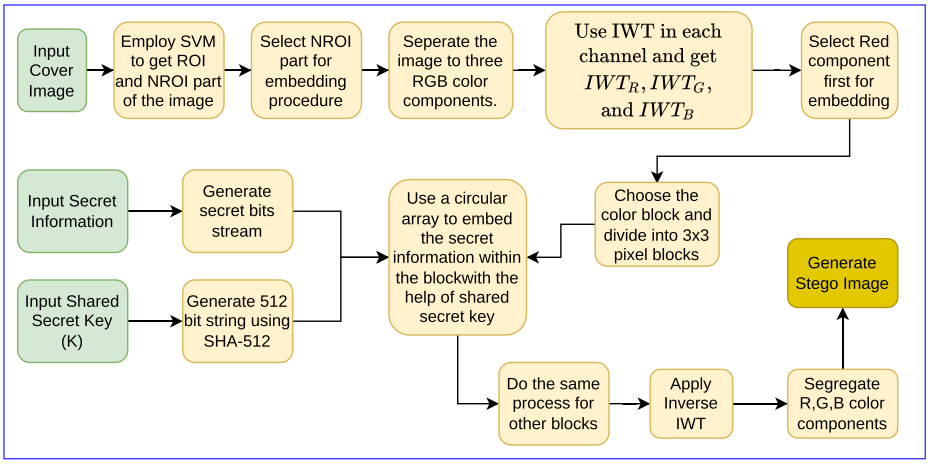


Fig. 5 Block diagram of the steganographic scheme

clockwise if the κ bit is 0 and anti-clockwise if the κ bit is 1. For each operation, four (4) stego bits are embedded within nine (9) pixels of IWT_R. This process will carry forward for the other two colour components, IWT_G and IWT_B. In this way, all the secret bits are embedded within the NROI part of the cover image. After that, inverse IWT is applied to all the three colour component coefficients to get the pixel value in the image format. Finally, all the R, G, and B colour components are merged to generate the stego image (SI).

Require: Cover Image (I), Secret Information (W), Circular Array (CA), Secret Key (κ)
Ensure: Stego image (SI)

Process the image I using SVM to separate ROI and NROI regions.
Select the pixels lies in the NROI regions into the pixel matrix (M).
IWT is applied to the pixel matrix M and the coefficients lies in the NROI are selected for embedding
A set of 3×3 coefficient blocks are created from the selected coefficients
The secret information is converted to a binary stream WS
The secret key κ into a binary stream of 512 bits (key)using SHA-512 algorithm
▷ Process this for RED, GREEN, and BLUE components
for $layer$ in (0, 1, 2) **do**
▷ Process for each pixel block
    for $block$ in $layer$ **do**
        Arrange the coefficients of the $block$ as a circular array
        Take 1 bits from the key and check
        if (key == 1) **then**
            rotate the CA clockwise
        else
            rotate the CA anticlockwise
        end if
        Entry-wise multiplication of $block$ and CA is done
        The pos value is calculated
        The pixel value at position pos of $block$ is changed after embedding 4 bits data from the binary data of the secret information W
    end for
end for
All the $blocks$ are then converted to 3×3 coefficient matrix
The matrices are joined to get the changed IWT coefficient matrix
The coefficient matrix is converted to pixel matrix using IIWT
The secret image W is generated from the pixel matrix

Algorithm 1 Embedding Algorithm.

In the proposed model, a double layer of security is introduced to ensure the robustness of embedded data. In the double layer of security, the first layer of security is the shared secret key (κ) and second layer of security is the circular array whose elements can be chosen by the user of their own.

4.3 Information extraction

The extraction process of the secret bits has been described in this section. At first, the stego image (SI) of size ($M \times N$) is taken as an input. ROI and NROI parts of the stego image are then separated using SVM as described in Section 3.1. Now these ROI and NROI pixel positions are stored in two different arrays say, $Arr_r^{pos'}$ and $Arr_{nr}^{pos'}$ and the pixel values are stored in two separate arrays say $Arr_r^{pix'}$ and $Arr_{nr}^{pix'}$ respectively. Here only the NROI part of the image is our major concern, as only this portion contains the hidden information bits. Now the image is separated into R, G, and B colour components. Then, the IWT is applied to each colour component to get coefficient matrices IWT'_R, IWT'_G and IWT'_B. The red component (IWT'_R) is then considered first for extraction. The shared secret key (κ) that was used during the embedding process is now chosen, and a 512 bit string is generated from it using the standard SHA-512 hashing algorithm. This shared secret key, κ is used to select the direction of the rotation of the circular array at the time of embedding. The same rule is followed during the extraction process. The circular array considered during embedding is used to extract the stego bits from the (IWT'_R) block and store them within B'_w using κ. So, for each operation, four (4) secret bits are extracted from the nine (9) pixels of IWT'_R. This process is carried out for two other colour coefficient blocks, IWT'_G and IWT'_B. After that, an inverse IWT is applied to the coefficient blocks of all the three colour components to get the pixel value in the image format. Then, all the R, G, and B colour components are merged to generate the cover image (I). Finally, the extracted secret bits are appended to generate the original logo image.

5 Experimental results and comparisons

For subjective and objective assessment of the performance of steganographic systems, many approaches and metrics are available. In general, objective analysis corresponds to performance benchmarks that do not require the presence of the examiner, and these tests may be carried out according to certain guidelines. The detailed descriptions are described in the following subsections.

5.1 PC configurations

The segmentation method is implemented with an environment having Intel ® Core™ i7-9700K @3.60 GHz, 64 GB RAM, Windows 10 Professional 64-bit Operating System, MATLAB 2018b Software.

For the experiment of watermarking, an Intel ® Core™ i7-8565U CPU @1.80 GHz processor, 4 GB, 500 GB SDD, DDR3 Memory, Matlab version 20b, and JAVA 8 software are used.

5.2 Dataset description

The proposed method is applied to Sagittal T2-weighted fat-suppressed Dynamic Contrast-Enhanced Magnetic Resonance Imaging (DCE-MRI) of the breast collected from The Cancer Genome Atlas Breast Invasive Carcinoma Collection (TCGA-BRCA) [2, 10, 23]

Table 2 Performance of the various segmentation approaches

Approaches	TP	TN	FP	FN
SVM	**92.40**	**99.40**	0.60	**7.6**
KNN	23.73	99.95	0.05	76.27
Naive Bayes	90.02	98.36	1.64	9.98

in The Cancer Imaging Archive (TCIA).[1] The size of the images is (256 × 256). For the experiment, 500 DCE-MRI slices of 50 women patients are used.

5.3 Experimental analysis:

The SVM was trained with 400 MR images and tested with 100 MR images. These 100 images are considered as the cover image and a gray-scale image of size (165 × 165) as the logo image. Here, breast lesional regions are the ROIs and other regions are the NROIs. A standard dataset is considered with 10 images of size (256 × 256) as cover image and a gray-scale image of size (165 × 165) as logo image for reporting the results.

The radial basis function (RBF) is used as kernel function for SVM. For a comparative study of lesion prediction, K-nearest neighbor (KNN) algorithm with 5 neighbors and Naive Bayes classifier are applied to the same dataset and prediction results in terms of true positive rate (TP), true negative rate (TN), false positive rate (FP), and false negative rate (FN) are reported in Table 2. From this table, it is observed that SVM has better predicted the lesions in MR images than KNN and Naive Bayes.

Figure 6 shows some of the original images and their corresponding lesional images after applying SVM.

5.4 Capacity:

Capacity is another significant aspect in medical image steganography that should be considered when evaluating the overall effectiveness of the proposed approach. It is the amount of information encoded in the host image, represented in bits per pixel (BPP) units. Table 3 shows that the capacity (in BPP) achieved with our technique is 0.44 bpp. The capacity can be calculated by using the (1).

$$\text{Capacity} = \frac{\text{Total number of bits that can be embedded}}{\text{Total number of pixels in the image}} BPP \tag{1}$$

5.5 Visual quality measures:

The following performance metrics are used to measure the visual quality of a steganography system.

[1] https://wiki.cancerimagingarchive.net/display/Public/TCGA-BRCA

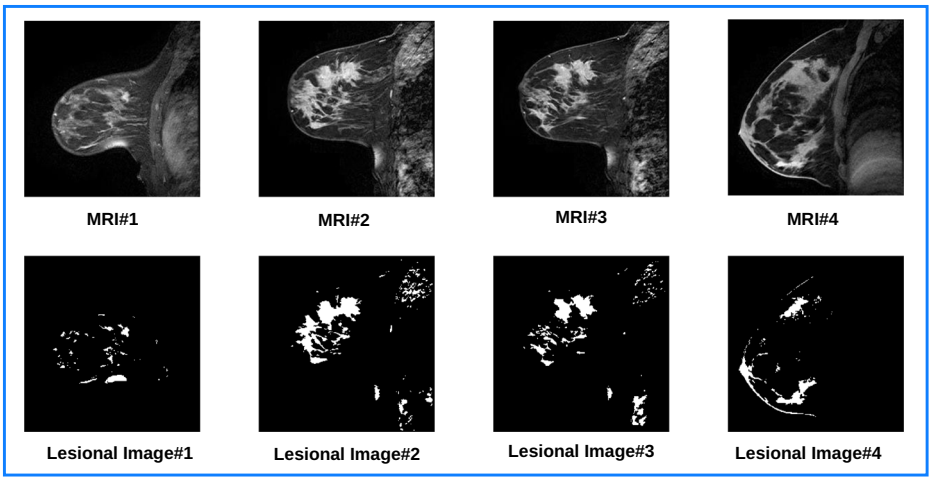


Fig. 6 Original and their corresponding lesional images

5.5.1 Peak signal to noise ratio (PSNR)

The PSNR (Peak Signal to Noise Ratio) is used to assess the image deterioration induced by inclusion of the secret image within the cover image. It is expressed by the (2).

$$\text{PSNR} = 10 * \log_{10} \frac{255^2}{\text{MSE}} \tag{2}$$

Where the Mean Square Error (MSE), it is defined as (3)

$$\text{MSE} = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{I(i, j) - SI(i, j)}{m \times n} \tag{3}$$

Where, $I(i, j)$ and $SI(i, j)$ are the pixel intensities of original and stego images of size $(m \times n)$ respectively.

Table 3 Cover image with NROI and ROI pixel value with payload

Image	Pixel	NROI	ROI	Block	EC	Payload
Breast#1	65536	64688	848	7187	28748	0.44
Breast#2	65536	61690	3846	6854	27416	0.42
Breast#3	65536	62731	2805	6970	27880	0.43
Breast#4	65536	65491	45	7276	29104	0.44
Breast#5	65536	65489	47	7276	29104	0.44
Breast#6	65536	65422	114	7269	29076	0.44
Breast#7	65536	65253	283	7250	29000	0.44
Breast#8	65536	65255	281	7250	29000	0.44
Breast#9	65536	63516	2020	7057	28228	0.43
Breast#10	65536	64763	773	7195	28780	0.44

5.5.2 Structural similarity index measure (SSIM):

In addition to PSNR, SSIM is applied to evaluate the degree to which the host image (I) and the stego image (SI) can be distinguished from one another. SSIM calculates the degree of resemblance between two images by comparing three different parameters: luminance, contrast, and structure. The SSIM of I and SI is defined as given in (4).

$$SSIM(I, SI) = \alpha(I, SI)\beta(I, SI)\gamma(I, SI) \tag{4}$$

where,

$$\alpha(I, SI) = \frac{2\delta_I\delta_{SI} + c_1}{\delta_I^2 + \delta_{SI}^2 + c_1} \tag{5}$$

$$\alpha(I, SI) = \frac{2\sigma_I\sigma_{SI} + c_2}{\sigma_I^2 + \sigma_{SI}^2 + c_2} \tag{6}$$

$$\gamma(I, SI) = \frac{\sigma_{I.SI} + c_3}{\sigma_I + \sigma_{SI} + c_3} \tag{7}$$

where, δ_I and δ_{SI} represent the luminance of the respective images. If the luminance of both images is the same, i.e., $delta_I = deltaSI$, the maximum value of $alpha$ is one. Similarly, if the contrast of both images is the same, the maximum value of β is also 1. whereas the structural comparison i.e., γ measures the correlation coefficients between the host and stego images. Here, σ_I and σ_{SI} represent the standard deviation, and $\sigma_{T.SI}$ represents the covariance factors of host and stego images.

5.6 Robustness analysis

5.6.1 Bit error rate (BER)

Bit Error Rate (BER) is used to measure the robustness of the analysis between the original secret (W) and extracted secret (W') images with a size ($m \times n$). BER is expressed using (8):

$$BER = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i, j) \otimes W'(i, j)}{m \times n} \tag{8}$$

5.6.2 Normalized correlation coefficients (NCC)

The Normalized Correlation Coefficients (NCC) metric assesses the robustness of the steganoghaphic scheme. It calculates the correlation coefficients between the retrieved secret (W') and the original one (W) that was initially placed. The NCC is expressed as the (9):

$$MSE = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W'(i, j) - W(i, j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i, j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W'(i, j)^2}} \tag{9}$$

The NCC value is defined on the interval [0, 1] with unity as the ideal value.

From the Table 3 one can easily find out that the considered cover image is of size (256×256), which means there are a total 65, 536 data points used for the classification purpose

Table 4 Tabular representation of various metrics

Image	Pixels	PSNR	Capacity	Payload	SSIM	NCC
Breast#1	65536	64.93	28748	0.44	0.9771	0.9991
Breast#2	65536	63.12	27416	0.42	0.9802	0.9989
Breast#3	65536	62.08	27880	0.43	0.9712	0.9991
Breast#4	65536	63.81	29104	0.44	0.9606	0.9996
Breast#5	65536	64.82	29104	0.44	0.9694	0.9992
Breast#6	65536	63.86	29076	0.44	0.9604	0.9997
Breast#7	65536	62.88	29000	0.44	0.9637	0.9991
Breast#8	65536	63.88	29000	0.44	0.9637	0.9997
Breast#9	65536	62.04	28228	0.43	0.9797	0.9999
Breast#10	65536	61.91	28780	0.44	0.9753	0.9994

using SVM model. In Table 3 it is seen that from the total 10 images, the minimum number of NROI pixel values is 61,690 for image "Lesional Image#2". Moreover, the payload for the gray scale image will be in the range of $0.42-0.44$ bpp, whereas the embedding capacity of our proposed scheme is in the range of 27,416 bits to 29,104 bits. The Table 4 represents the experimental results of PSNR, Capacity, Payload, SSIM and NCC. For any standard image processing experiment, an image with a PSNR value greater than 30 dB is considered a good quality image. From the Table 4 it is clear that the PSNR for the proposed scheme is approx 64 dB. That means the stego image is undetectable to the human visual system.

Moreover, to justify the robustness of the proposed scheme, we have found the experimental results on Structure Similarity Index Measurement (SSIM) and NCC. The average SSIM and NCC results for the ten images are approximately 98% and 99%, respectively, which is very acceptable to demonstrate robustness. Our proposed algorithm provides a good trade-off among imperceptibility, embedding capacity, and robustness.

Table 5 Comparison of the proposed scheme

Scheme	PSNR	SSIM
Thanki et al. [22]	50.3600	0.9575
Parah et al. [14]	46.3698	0.9933
Singh et al. [18]	48 .7200	NA
Parah et al. [15]	46.5122	0.9932
Sabbane et al. [17]	61.7769	0.9997
Muhuri et al. [13]	35.6865	0.9282
Subhedar et al. [20]	45.248	0.976
Jeevitha et al. [6]	49.536	NA
Kadhim et al. [7]	51.4018	0.9993
Ghosal at al. [5]	38.45	NA
Kumar et al. [9]	44.84	0.9646
Proposed Scheme	64	0.9998

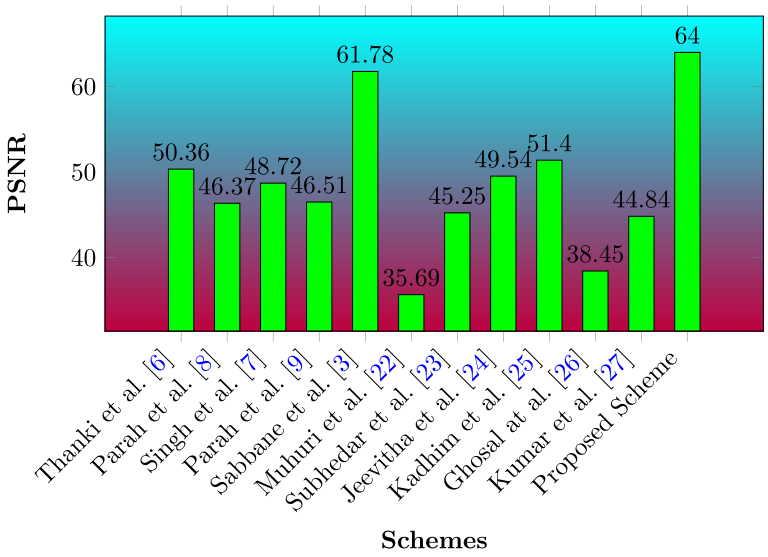


Fig. 7 PSNR comparison graph

The proposed technique is compared with some recent state-of-the-art methods shown in Table 5. The comparison is based on PSNR and SSIM. From the table, it is clear that the PSNR is better in the proposed scheme as compared to the listed methods. The better SSIM value also proves the robustness of the proposed scheme.

The graphical representation of the proposed results is depicted in Figs. 7 and 8. The graphical bar graphs also represent the superiority of the proposed scheme in terms of imperceptibility and robustness.

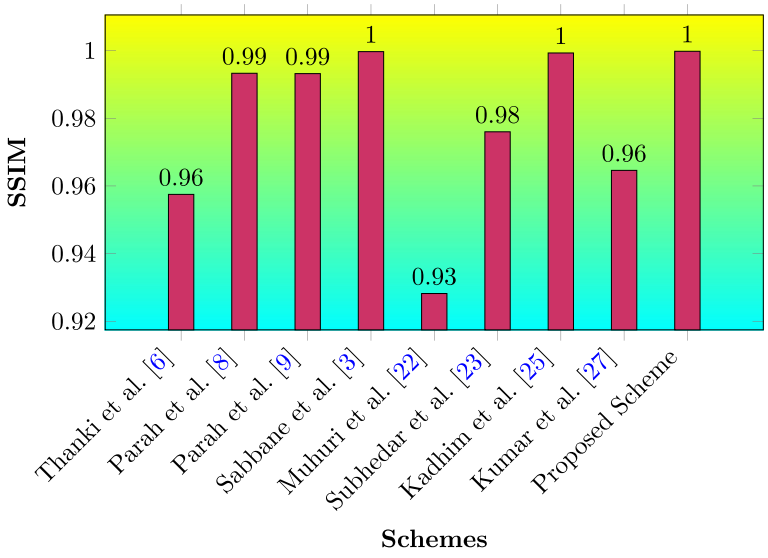


Fig. 8 SSIM comparison graph

Table 6 Comparison results for various scaling factor

Images	Original	Different scaling factor (in Percentage)			
		10	20	40	80
Breast#1.png	64.93	55.808	50.451	46.143	40.754
Breast#2.png	63.12	56.051	50.718	46.344	40.438
Breast#3.png	62.08	55.543	50.303	46.073	40.419
Breast#4.png	63.81	55.378	49.132	46.555	40.725
Breast#5.png	64.82	55.398	50.134	46.301	40.382
Breast#6.png	63.86	56.936	50.751	46.392	40.983
Breast#7.png	62.88	56.987	50.084	46.632	40.892
Breast#8.png	63.88	56.971	50.621	46.569	40.961
Breast#9.png	62.04	56.448	49.077	46.841	40.642
Breast#10.png	61.91	56.258	50.871	46.952	40.915
Average	63.333	56.1778	50.214	46.480	40.7111

We have also tested our model in some attacking scenario to test the robustness of the scheme against the attacks as well as to check the imperceptibility of the image. Table 6 depicts the PSNR difference in various scaling factors. We have considered ten breast images with scaling factors of 10%, 20%, 40% and 80%. In general, the average PSNR value for the original image is 63.33 dB. But for the scaling factors of 10%, 20%, 40% and 80% the average PSNR values become 56.1778 dB, 50.214 dB, 46.480 dB, and 40.7111 dB, respectively, which means that the stego image can still be undetectable to the human visual system.

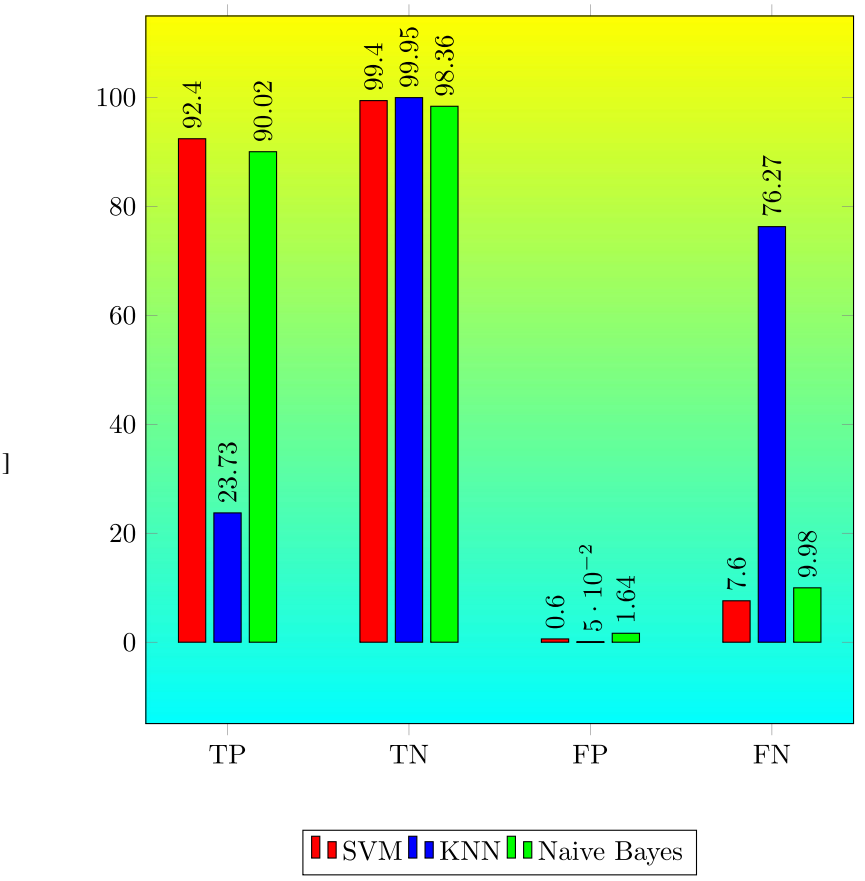
We have also applied various attacking scenarios like Salt & Paper Noise, Cropping, Filtering, Gaussian Noise, JPEG Compression, Histogram Equalization, and Rotation (90 degree), and the results are shown in Table 7. From the tabulated results, it is clear that the PSNR value for the extracted stego image is more than 30 dB for all the cases except JPEG compression and rotation, which means that the secret logo image can not be easily detectable by the HVS system. Hence, it can be concluded that the imperceptibility can still be exists after attacking by the salt and pepper noise and Gaussian noise but in case of jpeg compression (40%), our scheme cannot show reasonable imperceptibility. Again in terms of robustness which is measured by NCC, our scheme exhibits a fairly good results after

Table 7 Comparison results in attacking scenario

Attacks/noise	PSNR (Secret)	NCC	SSIM
Salt and paper noise	35.45	0.7294	0.6992
Cropping	36.51	0.7638	0.6407
Filtering	36.49	0.7614	0.6956
Gaussian noise	37.58	0.7599	0.6922
JPEG compresion (40%)	21.56	0.6136	0.5536
Histogram equilization	37.91	0.7283	0.6255
Rotate (90)	19.23	0.6042	0.5638

Table 8 Statistical test: SD and CC

Image	SD	CC	
	Cover	Stego	Cover vs Stego
MRI#1	128.5813	128.6647	0.9993
MRI#2	125.4325	125.6534	0.9994
MRI#3	125.2653	125.5346	0.9982
MRI#4	128.2543	128.6696	0.9923
MRI#5	128.3425	128.7756	0.9839
MRI#6	125.2142	126.2653	0.9974
MRI#7	124.2653	125.6447	0.9853
MRI#8	125.6993	126.6677	0.9838
MRI#9	125.3393	126.2347	0.9939
MRI#10	128.6254	128.7786	0.9918



]

Fig. 9 Bar chart to represent the performances of various approaches over 256 × 256 images

attacking by salt and pepper noise and Gaussian noise whereas the robustness will degrade in a bit in case of jpeg compression.

5.7 Statistical test

The Table 8 shows the statistical results in terms of standard deviation (SD) and correlation coefficients (CC). From the tabulated results, it is clear that CC results between cover image and stego images are near about to unity which conforms the acceptability of the proposed model (Fig. 9).

6 Discussion

In this study, we proposed a robust steganographic scheme using Support Vector Machine (SVM) and Integer Wavelet Transform (IWT) to improve security and robustness while maintaining authenticity and data integrity in the medical image. From the literature survey, it has been found that a very few number of researchers [8, 12, 14, 17] have developed a steganographic scheme in the field of biomedical imaging. Also, there exist some security loop-hole in the state-of-the-art methods. Therefore, development a high security steganographic scheme in the medical image application is still a demanding research area. Moreover, increasing the embedding capacity with a minimal degradation of the medical image is another challenging task. So, to embed the secret information in the proper location i.e., NROI region instead of ROI region is more justifiable.

Medical images contain very sensitive information about the patient. This information should not be compromised in any circumstance. The proposed scheme can be used to hide the sensitive patient information into the medical image to ensure confidentiality. This way the overhead of paperwork to record the patient information can be reduced.

The only limitation of the proposed work is that the SVM classifier model can under perform when the dataset is very large. So before training the model, we need to precisely choose the medical image dataset to ensure that the target classes are not overlapping.

7 Conclusion

In the healthcare industry, medical images or diagnostic information are transmitted from one place to another using wired or wireless medium. Therefore, the transmission of such information requires more security.

In this study, we have proposed a robust steganographic scheme using SVM and IWT to improve security and robustness while maintaining authenticity and data integrity. SVM is used to classify the breast MRI into the ROIs and NROIs and prediction performance is compared with KNN and Naive Bayes classifier. The SVM performs better prediction than other algorithms.

The proposed model ensures imperceptibility and robustness of medical images against attacks like salt and pepper noise, Gaussian noise, and jpeg compression. When SVM and double-layer security are used together, they make the proposed model stronger against several attacks on image processing. The secret message is embedded in the NROI portion of the medical image. The NROI portion varies from image to image depending upon the type of the medical image. As the NROI section or the embedding positions are not predefined for

every image, it is very difficult for any attacker to extract the valuable patient's information embedded in the form of secret information.

The outcomes from this experiment prove the high imperceptibility and better robustness of the proposed steganographic scheme. Here, the average SSIM value is 0.9802, payload is 0.44 bpp, and the PSNR value is 64 dB (approx), which is more than the acceptable value. The results of the proposed embedding method ensure some potential applications of the proposed scheme in tele-medicine. However, the proposed model has high initial computation complexity due to the SVM model building, which needs to be improved.

In the present study, we have used MR images. In the future, we intend to study the proposed model in other modalities of biomedical imaging such as Ultra-Sound (US), Computed Tomography (CT), Positron Emission Tomography (PET), etc. Furthermore, we intend to use Deep Learning (DL) models in place of SVM for the generation of NROIs from medical images in the future.

Author Contributions All authors contributed to the study conception and design, material preparation, data collection and analysis.

Funding The authors declare that no funds, grants, or other support were received during the preparation of this manuscript.

Data Availability Open Source

Declarations

Ethics approval and consent to participate Allowed

Consent for Publication Allowed

Conflict of Interests We declare that we do not have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

1. An FP, Je Liu (2021) Medical image segmentation algorithm based on multilayer boundary perception-self attention deep learning model. Multimed Tools Appl 80(10):15017–15039
2. Clark K, Vendt B, Smith K, Freymann J, Kirby J, Koppel P et al (2020) The cancer imaging archive: maintaining and operating a public information repository. Accessed December 2020
3. Ganic E, Eskicioglu AM (2004) Robust DWT-SVD domain image watermarking: embedding data in all frequencies. In: Proceedings of the 2004 workshop on multimedia and security, pp 166–174
4. Garg M, Ubhi JS, Aggarwal AK (2022) Neural style transfer for image steganography and destylization with supervised image to image translation. Multimed Tools Appl:1–18
5. Ghosal SK, Mandal JK, Sarkar R (2018) High payload image steganography based on Laplacian of Gaussian (LoG) edge detector. Multimed Tools Appl 77(23):30403–30418
6. Jeevitha S, Amutha Prabha N (2020) Effective payload and improved security using HMT Contourlet transform in medical image steganography. Health Technol 10(1):217–229
7. Kadhim IJ, Premaratne P, Vial PJ (2020) High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform. Cognit Syst Res 60:20–32
8. Karakus S, Avci E (2020) A new image steganography method with optimum pixel similarity for data hiding in medical images. Med Hypo 139:109691
9. Kumar V, Kumar D (2018) A modified DWT-based image steganography technique. Multimed Tools Appl 77(11):13279–13308
10. Lingle W, Erickson BJ, Zuley ML, Jarosz R, Bonaccio E, Filippini J et al (2020) Radiology Data from the cancer genome atlas breast invasive carcinoma collection [TCGA-BRCA]. Accessed December 2020
11. Mehta D, Bhatti D (2022) Blind image steganography algorithm development which resistant against JPEG compression attack. Multimed Tools Appl 81(1):459–479

12. Meng L, Liu L, Wang X, Tian G (2022) Reversible data hiding in encrypted images based on IWT and chaotic system. Multimed Tools Appl:1–29
13. Muhuri PK, Ashraf Z, Goel S (2020) A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. Appl Soft Comput 92:106257
14. Parah SA, Ahad F, Sheikh JA, Bhat GM (2017) Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J Biomed Inf 66:214–230
15. Parah SA, Ahad F, Sheikh JA, Loan NA, Bhat GM (2017) A new reversible and high capacity data hiding technique for E-healthcare applications. Multimed Tools Appl 76(3):3943–3975
16. Rai A, Singh HV (2017) SVM based robust watermarking for enhanced medical image security. Multimed Tools Appl 76(18):18605–18618
17. Sabbane F, Tairi H (2019) Medical image watermarking technique based on polynomial decomposition. Multimed Tools Appl 78(23):34129–34155
18. Singh A, Dutta MK (2017) Imperceptible watermarking for security of fundus images in tele-ophthalmology applications and computer-aided diagnosis of retina diseases. Int J Med Inf 108:110–124
19. Song X, Yang C, Han K, Ding S (2022) Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain. Multimed Tools Appl:1–20
20. Subhedar MS, Mankar VH (2019) Image steganography using contourlet transform and matrix decomposition techniques. Multimed Tools Appl 78(15):22155–22181
21. Thabit R (2021) Review of medical image authentication techniques and their recent trends. Multimed Tools Appl 80(9):13439–13473
22. Thanki R, Borra S, Dwivedi V, Borisagar K (2017) An efficient medical image watermarking scheme based on FDCuT–DCT. Eng Sci Technol Int J 20(4):1366–1379
23. The cancer imaging archive (2019) TCGA-BRCA. Accessed March 2019. https://wiki.cancerimagingarchive.net/display/Public/TCGA-BRCA
24. Tseng YC, Chen YY, Pan HK (2002) A secure data hiding scheme for binary images. IEEE Trans Commun 50(8):1227–1231
25. Vulli A, Srinivasu PN, Sashank MSK, Shafi J, Choi J, Ijaz MF (2022) Fine-tuned densenet-169 for breast cancer metastasis prediction using FastAI and 1-cycle policy. Sensors 22(8):2988
26. Yadav SK, Jha S, Sharma UK, Shrama S, Dixit P, Prakash S et al (2023) An efficient security technique using steganography and machine learning. In: Proceedings of the third international conference on information management and machine intelligence. Springer, pp 53–58
27. Zhang B, Rahmatullah B, Wang SL, Zaidan A, Zaidan B, Liu P (2020) A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations. Multimed Tools Appl:1–40