



# Security of medical images for telemedicine: a systematic review

Mahmoud Magdy<sup>1</sup> · Khalid M. Hosny<sup>2</sup> · Neveen I. Ghali<sup>1</sup> · Said Ghoniemy<sup>3</sup>

Received: 29 June 2021 / Revised: 23 December 2021 / Accepted: 3 January 2022 /  
Published online: 22 March 2022

© The Author(s) 2022

## Abstract

Recently, there has been a rapid growth in the utilization of medical images in telemedicine applications. The authors in this paper presented a detailed discussion of different types of medical images and the attacks that may affect medical image transmission. This survey paper summarizes existing medical data security approaches and the different challenges associated with them. An in-depth overview of security techniques, such as cryptography, steganography, and watermarking are introduced with a full survey of recent research. The objective of the paper is to summarize and assess the different algorithms of each approach based on different parameters such as PSNR, MSE, BER, and NC.

**Keywords** Medical images · Watermarking · Steganography · Cryptography · Attacks · Copyright

## 1 Introduction

Medical imaging like Magnetic Resonance Imaging (MRI), Computed Tomography (CT), X-rays, and ultrasound. Has an essential role in diagnosing a wide range of diseases. Rapid improvements have been made on the internet for sharing and transferring massive amounts of information. Especially for telemedicine services development like telesurgery, teleconsultation [43], and badly need for exchanging medical images between patients' doctors and scan centers. These medical data should be transmitted in a secure communication medium to protect patients' sensitive information during transmission of medical images; if the transmitted medical image [87] is captured and tempered [150] by the attacker will lead to a

---

✉ Khalid M. Hosny  
k\_hosny@yahoo.com

<sup>1</sup> Department of Digital Media Technology, Future University in Egypt (FUE), New Cairo, Egypt

<sup>2</sup> Department of Information Technology, Zagazig University, Zagazig 44519, Egypt

<sup>3</sup> Department of Computer systems, Faculty of Computer and Information Sciences, Ain Shams University, Cairo, Egypt

false diagnosis issue [145]. So, confidentiality and integrity [54] became a significant challenge in medical image transmission. So, more attention is needed to secure the medical images transferred over a public network. Standard techniques used in medical image security are cryptography, steganography, and watermarking.

As of late, every year, medical companies acknowledge extra medical imaging machinery and propose advanced devices and contemporary technologies that have become a revolution. Today, a broad scope of medical imaging technologies in the world of diagnosis, as listed in Fig. 1 helps physicians obtain high-quality images for more accurate disease diagnosis.

This medical information can be downloaded with no approval from the owner. These assets cause several different problems. For example, security, proof of ownership, and copyright protection. Sensitive images carry extensive important information and different features compared to standard images. Medical images have much more sensitive and essential information than any other digital image. Each pixel in the image can be necessary for the diagnosis process, and any deformation can result in a faulty diagnosis [44]. The most robust securing of these images affects an image to the extent that it can be ignored; this is different from insensitive imagery as the border of redundancy is very low. The embedding capacity in medical images is deficient. Because medical images have a specific nature, they consist of two sections called the region of interest (ROI) [139, 195] and the region of no interest (RONI). ROI is considered an important area as vulnerable and sensitive information is present, so pixels values are critical in the diagnosis process. Because of this, the ROI is not allowed to be modified. On the other hand, RONI, or more specifically the image's background, is the region that does not contain vital information [194].

Computer-aided diagnosis (CAD) becomes a powerful standard digital image processing tool for identifying common diseases from medical images as cancers. Role in this research area. In this research [117], the authors proposed an automatic system for identifying acute lymphoblastic leukemia by applying two steps to the medical images segmentation and feature extraction and classification. The first step is based on segmenting the white blood cells (WBCs). The second one extracts some essential features from the segmented part as statistical, shape, and geometrical. The extracted features are classified by applying various techniques to detect normal and abnormal cells. After applying the algorithm to the IDB dataset of microscopic images of blood, the experimental results demonstrate that the proposed algorithm classification accuracy rate = 97.45%.

Multi-label classification of X-ray images. Karar et al. [86] proposed a new CAD framework based on deep learning classifiers to enhance the diagnosis performance of suspected COVID-19 diseases from X-ray images. The authors utilized eleven convolutional neural networks, as Residual Neural Network (ResNet) and Visual Geometry Group Network (VGG). The experiment showed that ResNet50V2, Dense Neural Network (DenseNet169),

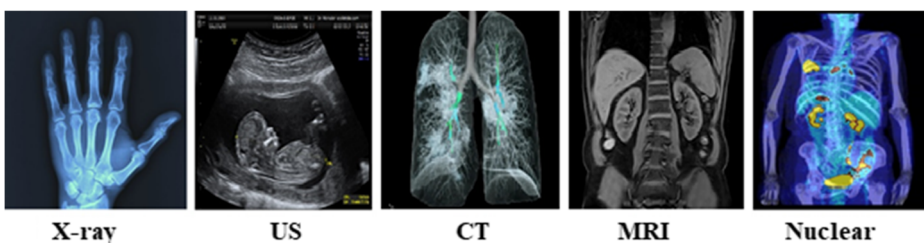


Fig. 1 Different Medical Imaging Modalities

and VGG16 models achieved the best detection accuracy of COVID-19. Hizukuri et al. [65] developed a computer-aided diagnosis (CAD) scheme on MRI (DCE-MRI) dataset by using a deep convolutional neural network (DCNN) with Bayesian optimization. The classification accuracy results of the proposed DCNN model are more significant than other conventional models that achieve high classification performance in diagnoses of masses in breast DCE-MRI images.

Forensic is considered one of the fields that need image security, not just securing images, identifying the existence of image modifications, and determining the manipulation operation applied to this data. This achievement is still a challenging problem. This paper [101] uses a convolutional neural network (CNN) model for detecting image operators in the forensics framework. Two CNN architecture is utilized to detect local noise evidence and tamper artifact evidence. The authors applied their framework to JPEG compressed images. The experimental results show that the proposed model has high detection accuracy and, in some cases, can determine the order of manipulation that previous works can't identify.

The term “biometrics” is derived from the Greek words “bio” (life) and “metrics” (to measure). Biometrics has been traced back thousands of years; one of the oldest examples is the human face. Biometric systems identify individuals based on unique features, such as fingerprints, voice, iris, face. Deep learning has a significant role in the security of biometric systems.

Biometric systems have become widely used across a large application scale for identity verification and payment authorization. Also plays an essential role in the medical image security field. A brief introduction of some security techniques that use biometrics is discussed below.

Shen et al. [157] proposed an encryption method passed on the human face biometric by generating the chaotic face phase mask (CFaPM). The medical image ROI has been encrypted using C-Means Clustering (FRFCM).

Shams et al. [180] proposed a real-time, invisible, and secured protection method based on biometric fingerprint, further used in the recognition process for allegation ownership. This technique achieved a higher level of robustness against various attacks. Dalila Cherifi et al. [8] proved that brain MRI could be used as Security Biometrics (Hidden Biometrics), which is considered as a very robust anti-spoofing form, based on the extracted features from the brain MR images form what is called “Brainprint,” or “Brain code,” which can be used as a signature for recognition purposes. As shown in Fig. 2, many kinds of attacks can affect medical images during transmission via eHealth networks. The definition of Attacks on secured images is different from normal attacks on any transmitted data. Attacks here are not to get information from ciphers but to pollute data and deform the secured media. These are classified into geometric attacks [132] like scaling, rotation, translation, cropping, and stretching. Signal processing attacks [104, 165] as histogram equalization (HE) [192], contrast adjustment (CA), gamma correction (GA), and adaptive histogram. On the other side, image filtering [200], such as median, average, and Sobel filters, are examples of denoising attacks. Additionally, image compression techniques are other kinds of signal processing attacks as JPEG compression. Some of these attacks are shown in Table 1.

Researchers present different data security techniques as cryptography and data hiding to guarantee data verification [171], as shown in Fig. 3. The data hiding [93] approach is classified into watermarking and steganography to load additional data into image pixels. In most of these techniques [99], the reconstruction phase's container image cannot be reconstructed due to the losses during the embedding or compression process.

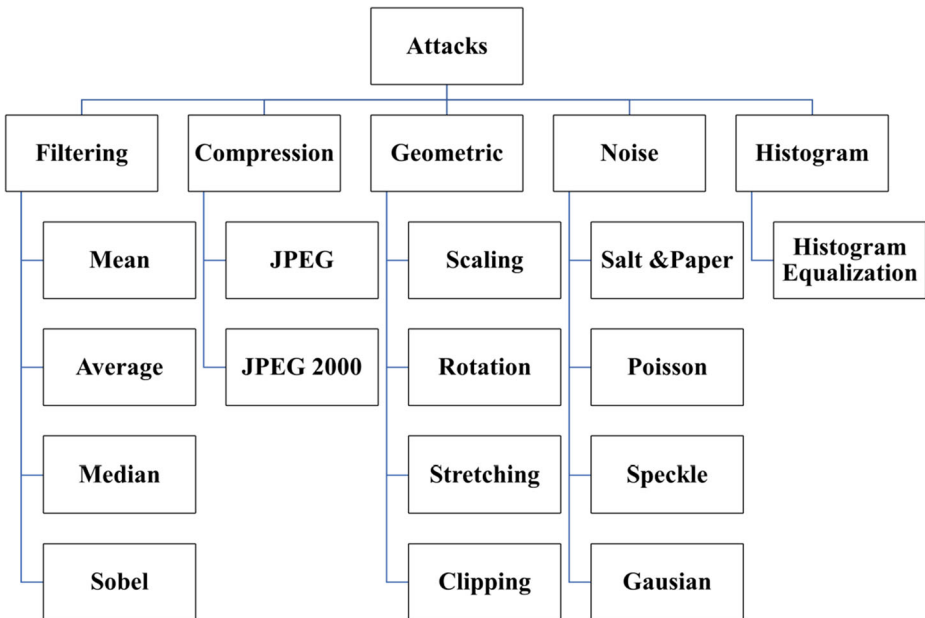


Fig. 2 Attacks


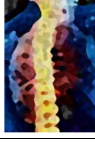
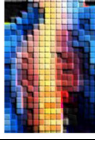

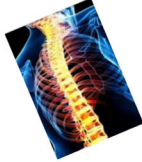




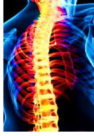
Medical image security has become an essential requirement for eHealth applications, including storage, retrieval, identity theft, and data management. For this reason, a lot of research work and surveys have been published to discuss medical data security approaches and copyright protection. These surveys focused only on one or two approaches, such as cryptography [37, 171], steganography [44, ], and watermarking [114, 162]. The surveys do not cover all approaches. This paper presents a study on these approaches, properties, techniques, and evaluation criteria.

The remainder of this paper is organized as follows: in section 2, we present recent cryptography techniques used in medical data security. In contrast, various techniques and types of steganography are discussed in section 3. Section 4 provides a detailed survey of recent image watermarking techniques, while performance measurement metrics and datasets are presented in sections 5 and 6. Finally, sections 7 and 8 discuss and conclude this paper.

## 2 Cryptography

Cryptography [191] targets secure the communication channel. It provides data encryption techniques so that only the person who has the decryption key can decode the encrypted message. It benefits in preventing any changes or updates by an assailant in the communication medium. It is accomplished using hash functions and a public-key cipher. Most cryptographic techniques, such as Blowfish, DES, AES, and RSA guarantee a maximum level of privacy. The hybridization of these methods is also used to accomplish maximum security. While these techniques are essential to encrypting text data, they are inefficient for image security since images have essential features, such as numerous redundancies and a potent correlation between neighboring pixels. Hence, images need an effective method to attain robust security

**Table 1** Image attacks

| <br>Original Image |                        |   |   |
|---|------------------------|---|---|
| Category  | Attack                 | Description   | Example   |
| <b>Denoising Attack [36]</b>  | Median Filter          | It is a non-linear filtering algorithm for noise removal  |    |
| <b>JPEG Compression [105]</b>   | JPEG Compression       | It is a famous method for digital images compression  |    |
|   | Scaling                | It is a linear transformation that enlarges or reduce images (scale up, scale down)             |    |
| <b>Geometric Attacks [104]</b>  | Rotation               | It is a circular movement of an image around a point  |    |
|   | Cropping               | It is the removal operation of unwanted areas from an image.                                    |   |
|   | Shearing               | It is a transformation by pushing one part of an image in one specific direction                |  |
| <b>Noise Attack [138]</b>   | Salt & peppers         | It is a type of noise in which some white and black pixels are added to images                  |  |
|   | Gaussian noise         | Is statistical noise which known as Gaussian distribution having a probability density function |  |
| <b>Image Processing Attack [154]</b>  | Histogram Equalization | It is an image processing operation for image contrast adjustment                               |  |

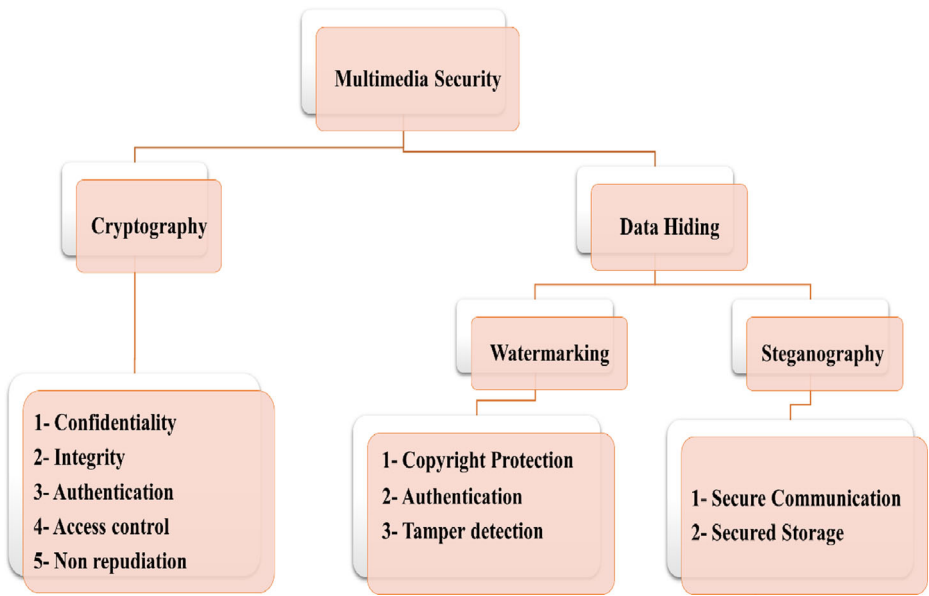


Fig. 3 Multimedia Security approaches

[10]. Cryptography [41] typically passes through two stages known as encryption and decryption, as presented below in Fig. 4. Encryption is a method to convert data to incomprehensible format by unlawful users using cryptographic algorithms to protect the data. The original image is transformed or encoded into an unreadable format using a secret key in the encryption stage. In decryption, the encoded image is decoded into the original image using the same key. The encrypted data is then transmitted through an unsecured channel towards the destination.

Stream cipher and block cipher are modes of encryption. When the data encoded is limited, stream ciphers are used. When the data size is large, they are chunked into blocks, and then encryption algorithms are applied, as presented below.

Different encryption techniques are proposed. Image encryption techniques can be categorized into the position-substitution-based algorithm, value transformation, and position permutation-based algorithm [37] or classified according to domain spatial and transform. In this survey, we are focused on domain classification, as shown below.

Therefore, medical image security is an essential responsibility. We need to achieve information or network security goals, such as confidentiality, integrity, and availability

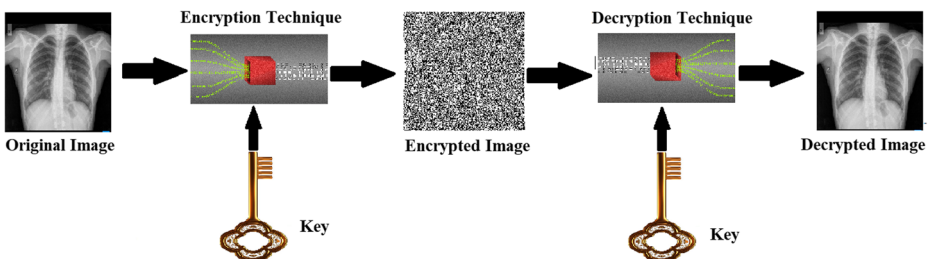


Fig. 4 General Cryptography (Encryption and Decryption) Scheme

(CIA). Confidentiality refers to information that is secure and not accessible to an unlawful person. Integrity means the accuracy of data. Availability refers to the information being accessible to the authorized personnel.

Network security is not acceptable for reliable information communication like audio, text, video, and digital images. The multimedia security scope is categorized into two parts, cryptography and information hiding algorithms. The information hiding methodologies are also classified into steganography and watermarking. As shown in Fig. 5, a large number of researches about medical image security have been proposed. A brief introduction of some cryptography techniques is discussed below.

## 2.1 Cryptography in spatial domain

### 2.1.1 Chaotic-based medical image security methodologies

Chaotic maps should be considered in the effective medium as they display a chaotic manner. This process means that any slight modification in primary conditions can generate violent change in outputs. Chaotic maps are widely used in security. The chaotic-based encryption method has many pros, such as sensibility to initial conditions, ergodicity, and necessity [88]. Therefore, chaotic maps are used on a large scale in different implementations. Some of the chaos-based encryption methods have been illustrated below.

Rajendran et al. [135] proposed a chaotic-based cryptographic architecture for medical images security during storage and transmission. At first, the key is generated by applying the chaotic map technique to the medical image. Secondly, both row-by-row and column-by-column confusion is executed. Furthermore, the diffusion process is performed using binary reverse and complement operation. Diffused images and chaotic key images are XORed. The proposed system security level is measured by applying different attacks. Simulation results indicate that the developed cryptosystem has to satisfy the requirements of IoT healthcare applications. Harshitha et al. [64] proposed an image encryption technique for medical images based on a chaotic logistic map and linear feedback shift register to generate pseudo-random sequences, then XORing these sequences to construct the key used for encryption generate cipher medical image data. The proposed scheme is robust to various attacks and secures many formats of medical images.

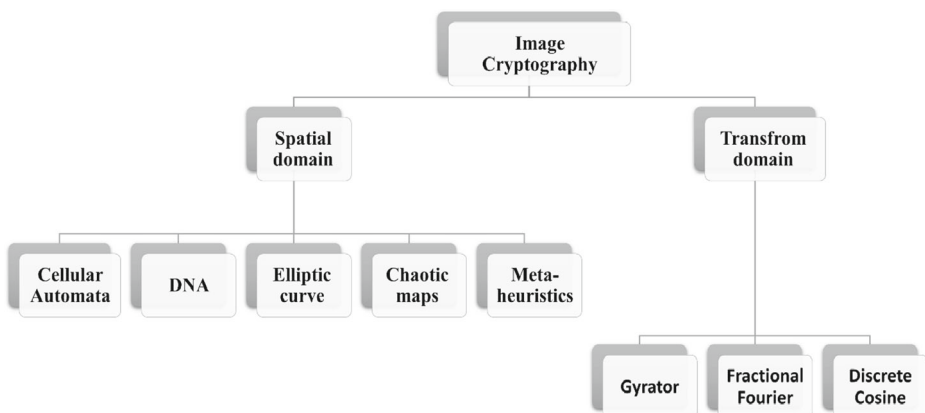


Fig. 5 Image Cryptography Domains

Pak and Huang [128] proposed a technique that cures the issue in a single chaotic map. In [84], the authors proposed a new image encryption algorithm for both gray and colored medical images, wherein the proposed algorithm surpassed other existing encryption methods.

### 2.1.2 Deoxyribonucleic acid (DNA)-based medical image encryption techniques

DNA technology began receiving significantly more attention a few years ago. Affected various fields, such as information science, medical systems, etc. DNA consists of a genetic code in which data is stored and converted to various genetic codes. Recently, a simulation environment has been designed based on DNA technology for biological experiments. This concept has been advanced in the expansion of DNA in the encryption field [197]. Massive storage, enormous parallelism, and low power exhaustion are the significant reasons for using DNA in the encryption of images [187]. Some DNA-based techniques are demonstrated in the following discussion.

Banu et al. [29] recommended a new medical image encryption technique for DICOM images based on Integer wavelet transform (IWT) and (DNA) sequences. Logistic map utilized for random keys generation. The results confirm that it is robust against various attacks. Mishra et al. [116] introduced a medical image security system using bit-level diffusion and DNA coding, also pseudo-randomly based on Logistic Sine utilized for key generation to make the secured image more robust. The experimentation proved that the original image could be recovered without any data distortion.

Guesmi et al. [58] introduced a hybrid cryptography model of hash algorithm SHA-2, chaotic map, and DNA masking for medical image security. Since the information entropy is an essential feature of randomness, the proposed approach works on improving entropy. So the theoretical analysis showed that the algorithm is robust against typical, statistical, and exhaustive attacks.

To overcome digital medical image threats, Ravichandran et al. [137] address an encryption technique to medical image security based on DNA hybrid with chaos and IWT. The technique consists of two stages diffusion and shuffling phases. The row and column of the image are shuffled circularly bitwise shifted to enhance the security against attacks, then the diffusion stage start based on DNA XOR. The proposed model was tested on 100 DICOM medical images to evaluate it against differential and statistical attacks, which showed that it overcame other techniques.

This paper [16] proposes a secure medical image encryption scheme based on DNA), chaotic maps, and hash functions (SHA-256 and MD5). The algorithm is applied in three stages: key generation, second rotation, and permutation, third DNA encoding-decoding. In the key generation stage, the key is generated based on original image metadata. Rotation and permutation applied on two MSB bits of the medical image To remove the black background. The third part is the DNA encoding-decoding utilized through the logistic map. Security analysis of the proposed scheme proved that the scheme is robust against common attacks. Furthermore, a large key space.

El-Shafai et al. [47] present efficient cryptosystem-based deoxyribonucleic acid (DNA) in addition to logistic chaos maps and piecewise linear chaotic maps. First, the secret key is generated using PWLCM. Then, the input image is encoded with the logistic chaos map, and the secret key image is encoded using DNA rules. Finally, these steps are iterated on image columns once again to get the best-ciphered image. The experimental results showed that the



model has high security with low time complexity. Furthermore, it can stand against different types of attacks.

### 2.1.3 Elliptic curve based techniques

Yin et al. [196] proposed a medical image cryptosystem that utilizes an elliptic curve with homomorphic encryption. The authors in [153] discussed a new enhanced cryptographic scheme for medical image protection generated from IoHT healthcare devices using an advanced optimization technique, based on elliptical curves and Grasshopper Particle Swarm Optimization (GOPSO) in selecting the optimal key to enhancing medical Image security. The theoretical and practical results proved that the algorithm is secure and robust against various attacks compared with other optimized encryption algorithms. The experimental results show higher key sensitivity, better encryption accuracy, and high resistivity for statistical attacks.

This paper [32] addresses a new cryptographic technique for medical image protection based on combining ECC with Hill cipher (ECCHC). The authors do this combination to overcome the weakness of some encryption schemes against some attacks and the key length challenge that is not robust against brute force attacks. The efficiency of the proposed is evaluated through security tools and exhibits better security features than the state-of-the-art techniques.

Koblitz and Miller [121] designed a key-encryption algorithm based on the elliptic curve. The better complexity and small key size are the main aspects of the elliptic curve encryption technique because the elliptic curves technique is based on algebraic curves' features.

### 2.1.4 Metaheuristics-based techniques

Metaheuristics algorithms have an essential functionality in NP-Hard problems optimization. The importance of this algorithm lies in the constant parameter optimization used in encryption cryptography. EA's ability to evolve multi-appropriate outputs in single development is based on population manner [97]. However, this technique also has weak points, such as low convergence speed, etc.

In this paper [184], a secured algorithm for medical Image security. A medical image is considered a watermark and encrypted using encryption algorithms. The encryption is done using AES and RSA encryption algorithms. Different metaheuristic approaches like Genetic Algorithm (GA), Bacterial Foraging Optimization (BFOA), and Differential Evolution (DE) are proposed to preserve the integrity of the medical images.

Proposed intelligent symmetric cryptography for medical image encryption based on the quantum-based key generator and chaotic map. Janani et al. [77] introduced a new quantum-based cryptosystem with two levels of security for medical images. The algorithm applied on the cancer imaging dataset, performance evaluation of the proposed algorithm ensures the medical image integrity and reinforces confidentiality. Lin et al. [106]. The algorithm was validated using a chest x-ray database, and experimental results show robustness against the passive attacks.

### 2.1.5 Cellular automata

Vijayakumar et al. [185] presented a cryptographic scheme based on Cellular Automata (CA) and is targeted in securing medical DICOM (Digital Imaging and

Communications in Medicine) images. This architecture is implemented with a Hardware Cyclone device. The CA-based scheme consists of two diffusions and confusion. The proposed scheme is evaluated against multiple metrics, with an entropy of around 7.9975 achieved.

## 2.2 Cryptography in transform domain

Image encryption methodologies based on the transform domain are considered one of the essential image encryptions. The given media is converted from spatial to transform domain using one of the transform models for the encryption process. Examples of these techniques are gyrator transform (GT), fractional Fourier transform (FrFT), and discrete cosine transform (DCT). These algorithms are discussed below in detail.

### 2.2.1 Gyrator transform

Yatish et al. [53] demonstrate a new cryptosystem technique based on gyrator transform and phase-truncated Fourier transform using a triplet of functions to evaluate the complex function for medical image security. The complex matrix is split into two matrices, one for the real part and the other for the imaginary part. In the next step, a random distribution function is applied by one of the triplet functions. The simulation results and attack analyses showed the effectiveness and robustness of the technique against various attacks.

### 2.2.2 Fractional Fourier transform

This paper [94] introduces a new scheme of medical data security based on fractional discrete cosine transform (FrDCT) coefficients with a high degree of freedom. After that, a chaotic map is applied to FrDCT coefficients. Experiments applied to study the efficiency of the proposed method after that have been compared with state-of-the-art techniques showed that surpass is more efficient than other algorithms.

### 2.2.3 Discrete cosine transform

The authors in [7] proposed a chaotic-based encryption technique that combined discrete cosine transform (DCT) for medical images. The medical image is compressed twice, one by using DCT. And again using the arithmetic encoding technique. After that, the compressed image is encrypted using a chaotic sequence to scramble the output. The experimental results showed the efficiency of the proposed model with a PSNR value equal to 41.70 dB.

Fang et al. [51] illustrated a new encryption algorithm to secure the host medical image to protect private information; the author's algorithm is based on Bandelet Transform and Discrete Cosine Transform. The medical image is first encrypted using a Logistic chaotic map, and then the features are extracted using Bandelet Transform. The experimental results showed the robustness of the proposed algorithm and proved that it could solve the problem of information leakage.

### 3 Steganography

Digital steganography was proposed to avoid snooping on secured transmitted data. The steganography concept was the concealment of digital data. Steganography is a Greek word consisting of two words, stegano, which means “covered” and “graphy,” which indicates “write.” So the two words combined mean “covered writing” [20]. It treats various methodologies of embedding secret data like video, image, audio, text, or files into other multimedia payloads using the private key. The concealed information is called a secret message, and the container in which the secret file is embedded is called a cover file. The cover can be any multimedia file, such as video, audio, image, or text. The resulting file of the embedding operation is termed a stego file.

Irrespective of any efforts and enormous achievements achieved in steganography, the adoption ratio of steganography is still relatively weak in real-time applications in which privacy of sensitive information is crucial, such as with military documents, forensic reports, etc., and health records [81]. There is still a trade-off between integration capability and distortion. It is also essential to keep a minimum of recovery errors and resistance to data handling. In steganographic algorithms based on machine learning, sophisticated machine learning methodologies are utilized to equilibrium these trade-offs, even preserving high performance in the whole process [21].

As mentioned above in Fig. 6, steganography involves embedding an essential piece of information inside another multimedia file. Hence, steganography models need to withstand such massive information bulk, must also have a more extensive equivalent capability, called a payload, to receive the information in such a way as to maintain the image quality, called imperceptibility. A secure stego-key is used to prevent intruders and is essential to having the ability to resist any image transformations techniques that can modify or change the covered data [82]. Sathua et al. [149] mentioned that the image consists of numbers in a two-dimensional array from a computer’s point of view. These numbers represent light depth at different locations and are called pixels. The images are commonly stored in 8-bit or 24-bit format. The higher the number of bits, the higher its capacity; therefore, 24-bit images own the highest capacity for hiding sensitive data as a pixel expressed in 16,777,216 color values, as explained by Muhammad et al. [119]. Hence, image steganography uses the redundant bits in altering data without deforming the original image features. A reversible information hiding technique is proposed in [2] to preserve the visual quality of color medical images.

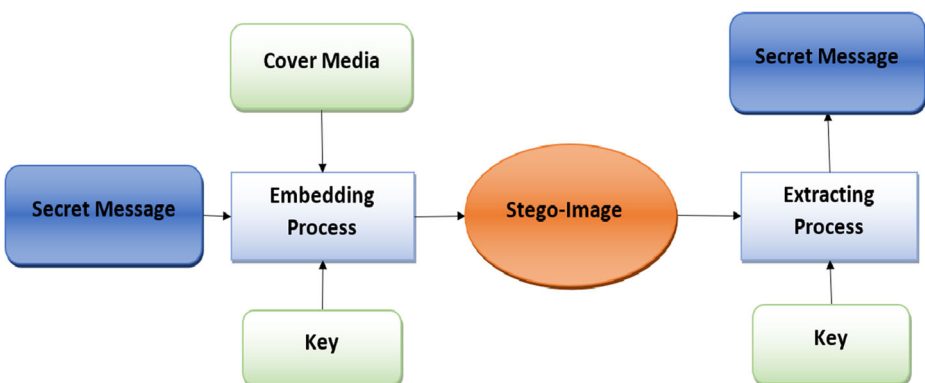


Fig. 6 Steganography Embedding and Extraction Phase

### 3.1 Steganography system properties

The authors of [22, 189] show three fundamental properties for a successful steganographic system. These properties are security, imperceptibility, and cover media payload capacity. There is also a fourth property mentioned in their research [13]. In addition to the properties mentioned above, robustness has been added, as shown in Fig. 7. These properties are considered the most influential criterion, so these parameters test most steganographic systems. Hence, any proposed algorithm should maintain most of these properties. Although the robustness property is not required in many applications, the other three properties are typically required [183].

#### 3.1.1 Imperceptibility

Steganographic methodologies' strength resides in hiding secret information in digital data, so naked eyes nor statistical analysis can detect it. But also, the steganographic algorithm should not affect the cover media. The methodology is secured when the statistical analysis for the covered image and the raw data are the same.

#### 3.1.2 Security

Security is considered the main interest to protect data access while sent through the channel by attackers. In most steganographic models, the word security refers to hiding data from unidentified outsiders with no relation between senders and receivers. So, the steganography approach is considered safe if the secret data is unnoticeable by statistical analysis methodologies.

#### 3.1.3 Payload capacity

Venkatraman showed that steganography's primary challenge is increasing the cover media capacity without affecting the security and imperceptibility. An efficient steganographic model aims to embed max payload inside minimum cover media.

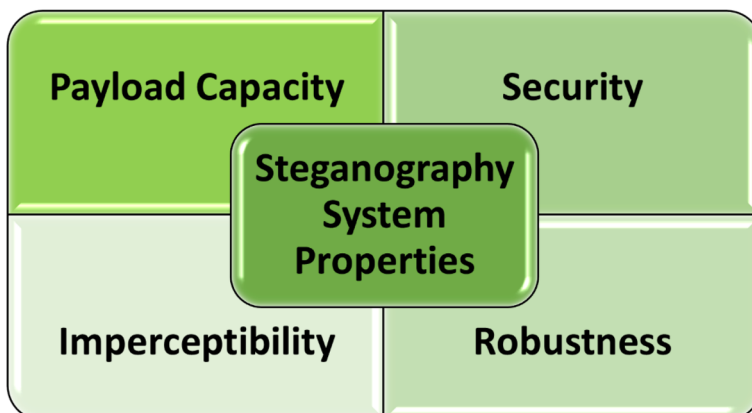


Fig. 7 Steganography System Main Properties

### 3.1.4 Robustness

In [113, 198], robustness is defined as avoiding any corruption in the stego-image and saving the embedded information's fidelity even if the carrier image is modified by an intruder using image operations like scaling, resizing, and rotation, and others.

Payload allocation performance enhancement is still a challenge in color image steganography. In standard steganography techniques, the RGB channels are assigned equally. Still, this methodology is not accurate enough as the security performance of color images is not based on embedding algorithms. Still, payload, so Liao et al. [103] proposed a channel-dependent payload partition technique to assign the embedding capacity among RGB channels adaptively. Experimental results show that the proposed scheme effectively increases the performance of the embedding.

It is still a challenge for steganographers to balance among all these different steganography requirements. The quality of the stego-image and the payload capacity of the cover image are at odds with each other, as it is challenging to maintain the imperceptibility and increase capacity simultaneously [4]. The requirements are affected by changing the cover image pixels after embedding process secrets. In recently proposed steganography techniques, slight changing of the cover image after embedding while preserving payload capacity, which indicates a high steganography algorithm, has been used to indicate higher stego-image quality and lower message detectability. The embedding efficiency indicates the ratio of changed cover images pixels by calculating the number of embedded bits per embedding change. Robustness against steganalysis increases When the embedding efficiency increases and is less detectable.

## 3.2 Steganography approaches

The primary characteristic of steganographic techniques is stego-image security while transmitting on the channel. Various techniques for steganography were utilized based on the nature of the embedding process. Hence, steganographic techniques can be categorized into spatial, transform or frequency, and adaptive domains, as presented in Fig. 8. In the following sections, this later classification will be discussed more in-depth with some recent research [96].

Abdulla et al. [6] proposed a two-step steganography mechanism to enhance undetectability of hidden data and quality of stego-image, first image size is reduced using SISR algorithm and second step embedding using bit-plane mapping algorithm based on the Fibonacci representation intensities, the experimental results proved that the new algorithm increased the robustness, increase capacity, and reduce image degradation.

### 3.2.1 Spatial domain steganography

This domain's techniques are considered the most straightforward and convenient method of information embedding in digital images by altering the carrier image's pixel rate to insert the secret information bits. These methodologies have little complexity of extraction and embedding. Some of the primary spatial domain methodologies are discussed below. Some examples from research papers are explained [82]. From these multiple-bit planes based examples, Collines et al. [42] demonstrate a method that uses pixel bit-plane values for sensitive information. Slicing the system into multi-bit planes using the ANR255 sequence is the first step in the proposed technique.

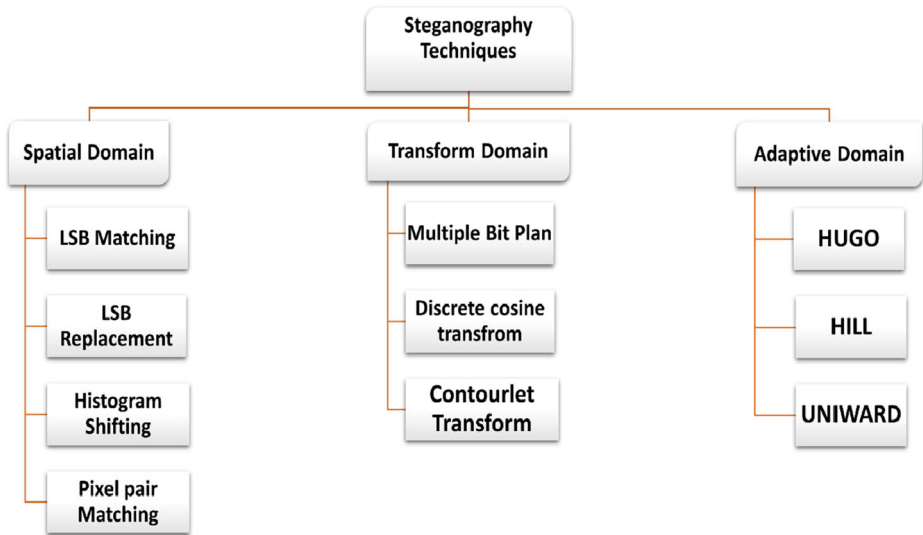


Fig. 8 Steganography Working Domains

The information has been encrypted before embedding to achieve more security. After the embedding stage, the cover media is turned into an 8-bit representation to be used as the stego-image. This technique has more than one advantage. The first is the embedding capacity. Another advantage, the randomness of embedding is very high and provides robustness for the system against the steganalysis operation. The main loophole lies in the vulnerability that the stego-image is susceptible to contra-attacks, and any slight alteration in pixel value position may deform the embedded information.

The authors in [5] proposed a hybrid technique based on two well-known schemes, LSB randomly and 2LSB, to increase the payload capacity, un-detectability, and stego quality. Experimental results proved the robustness against most statistical attacks as MLSB-WS, WS, and PoV.

To overcome the existing Least Significant Bit (LSB) steganography. The effective reversible data hiding technique and histogram shifting are used in the proposed technique [17] for hiding data in encrypted bio-medical images. Histogram expansion and histogram shifting have. The Paillier cryptosystem algorithm encrypts each pixel. The testing results showed that the embedding rate in the proposed model is higher than the existing scheme.

Santoso et al. [148] proposed a new steganography technique using Pixel Value Differencing (PVD) algorithm for hiding sensitive data in medical images. Based on the experimental results of testing, it is found that the proposed algorithm-produced images have better PSNR value than others implemented using LSB.

Stoyanov et al. [168] introduced a stego hiding scheme for medical images based on the nuclear spin generator, the efficiency of output images using the proposed algorithm measured using MSE and PSNR metrics, and the results show that the new steganographic scheme gives good performance with medical images security.

The embedding process can change the medical image structure to overcome this effect. The authors in [151] proposed a reversible data hiding technique based on shifting histograms

and RC4. The experimental results get high SSIM and PSNR, which means that the medical image can be retrieved successfully.

This paper [62] presents a new hybrid steganographic method based on Lempel Ziv Welch (LZW) and AES encryption for medical image security. Firstly the secret information is compressed using LZW and then encrypted using AES. In CEDE, after that, the encrypted image is embedded. The proposed technique provides high security with a high capacity compared with existing methods.

### 3.2.2 Transform domain steganography

The transform or frequency domain decomposes the media file into frequency coefficients before embedding essential data. This technique has many advantages for robustness against attacks. It can resist such types of attacks that can alter hidden data and imperceptibility and the capability to withstand distortion in the stego image [20]. In addition, the frequency domain also has cons, such as a lower payload than the spatial domain with high computing complexity, as Kaur and Pandey [89] mentioned in their research. In transform domain-based steganography, Fourier information has been used during the reconstruction process, which is considered a flawed tool in reconstructing the signal. Some of the used methods include integer wavelet transform (IWT), discrete cosine transforms (DCT), discrete wavelet transforms (DWT), and discrete Fourier transform (DFT).

Discrete Fourier transform is widely utilized in different image processing algorithms. DFT is a common transform technique used in signal processing. In DFT, a signal is decomposed into sines and cosines components. In image steganography, these components can be modified to be an essential tool for data hiding. Modified coefficients are returned to the original image and considered as the stego-image.

The received image is analyzed again into its transform components, and covered information is extracted from the recipient. Different steganography-based systems have been mentioned [82].

The authors in [143] proposed an LSB-based steganography technique for medical images with an encrypted DNA algorithm. The encryption algorithm applied on the patient data in the spatial domain, the proposed algorithm applied on chest x-ray images of the COVID-19 patients. From experimental results, it is evident that the algorithm shows greater robustness than others.

The authors in [131] proposed two-layer security using the LSB steganography technique with encryption for medical images. The experimental results showed that the proposed technique could preserve integrity and confidentiality compared with other hiding techniques with one level of security.

Reshma et al. [140] proposed an efficient steganography scheme for medical image security using support vector neural network (SVNN) and DWT to overcome the complex issues found in existing techniques as LSB. The SVNN classifier is utilized for selecting suitable pixels for embedding. The experimentation showed that the proposed model achieved high performance.

Thanki et al. [177] proposed a hybrid technique between steganography and cryptography for medical images in this paper. The embedding process is implemented using singular value decomposition (SVD) and discrete cosine transform (DCT) in this approach. The testing operation was done under various image processing attacks, and the experimental results show that the proposed algorithm has low computation time with higher imperceptibility of other existing approaches.

In this study, Arunkumar et al. [18]. Proposed a robust hybrid steganographic approach using the chaotic map, Singular Value Decomposition (SVD), Redundant Integer Wavelet Transform, and Discrete Wavelet Transforms (DCT). SVD and DCT achieve a higher level of imperceptibility and extra security and robustness achieved by chaotic map. By comparing the introduced method, the results applied on the UCID database show the effectiveness of this algorithm in geometric transformation resistance compared with other existing.

Jeevitha et al. [78] proposed a steganography approach for medical images based on Hidden Markov Tree Contourlet transform, canny edge detection, and Paillier cryptosystem. Firstly the cover image is mapped to the frequency domain using HMT and then applied to detect smooth image edges. The embedded information is encrypted with a pallier cryptosystem, and the Particle Swarm Optimization is utilized to select the embedding location. The experimental results show that the proposed method provides robustness compared with other techniques.

### 3.2.3 Adaptive domain image steganography

Subhedar & Mankar [169] mentioned in their research another name for the adaptive domain steganography, which is “statistics-aware embedding” and is also called “Model-Based” [146]. An adaptive method is an entire case of transforms and spatial methods. This method can select random adaptive pixels based on the cover image and select pixels with a more considerable standard deviation value for each block individually. Hajduk and Levický [60] also demonstrated that a global statistical characteristic was evaluated before interacting with the image coefficients. This statistical coefficient’s importance is for finding areas in the cover image that can be altered without image deformation. Hence, being able to neglect smooth areas that have similar coloring. This process means that images with a combination of colors are excellent for adaptive steganography techniques. Liao et al. [102] proposed two payload allocation methodologies based on distortion distribution (ES-DD) and image texture complexity (ES-ITC) to investigate payload distribution in images steganography. Experimental results proved that the proposed methodologies could perform better in multiple image steganography but not on JPEG images.

According to the mode and nature of adaptive steganography systems, they can be classified into artificial intelligence and machine learning, human visual systems, and region-based Steganography.

### 3.2.4 Human vision system steganography

In general, HVS is considered an approach for observing, comprehending, and processing optical information. HVS enhances the understanding of images, as the human vision has challenges in recognizing the finest details of image backgrounds. HVS has the primary advantage as it is indistinguishable, even if an intensive payload is embedded in edge regions and complex textures [100]. These techniques are mainly based on detecting the target region for hiding sensitive information using the transform or spatial domain techniques explained previously. Accordingly, researchers are working on this point to enhance the imperceptibility using various directions. Several examples of these directions are quad-tree segmentation used to detect smooth areas appropriate for covering data with minor distortions in the image [66]. The author here [109] defined just noticeable differences in the (JND) technique to precept changes while embedding process. It was observed that this category would adopt the



embedding payload capacity without distorting the stego image; hence, detecting whether the image is covered or not by the intruder's naked eye is very challenging. However, the embedding can be revealed using statistical analysis.

### 3.2.5 Region-based steganography

As mentioned before, the goal behind steganography techniques is to share data between the source and destination in an unnoticeable format. This way, trying to get the most uses, the most suitable regions host images for embedding secure data [25, 61]. With this technique, the embedding process focuses on edge and texture regions as the details in these regions are great [35, 39, 133]. This approach defends against image distortion due to any modifications. The main advantages of this technique include high imperceptibility and robustness, while the main disadvantage is that the embedding rate is very poor.

In this work [50], the authors proposed a hybrid security approach for medical image security. The approach comprises both Fragile Steganography and robust watermarking. The authors take care of ROI inside medical images. Firstly the features of the region of interest are computed and then embedded into the cover image. The steganalysis proved that the attacks applied on the transmitted image are not perceptible.

In [120], the high-frequency pixels used in covering secured data by the LSBM revisited algorithm has been selected according to the threshold value. In [12], the author mentioned approaches based on images' characteristics for controlling the capacitance of hiding. The researcher in [91] used the "ant colony optimization" algorithm in cover image pixels selection, then LSB was used for the embedding process.

### 3.2.6 Intelligent and machine learning techniques-based steganography

Artificial intelligence (AI) and machine learning (ML) have become widely used in various advanced applications [45, 70]. Initially, it was introduced for optimization, object retrieval, and recognition purpose [190]. Later, their usage extended for other requirements like compression, classification, segmentation, enhancement, and other image processing operations [199].

It is said to be efficient for any steganographic technique if the embedding process makes a minor distortion in the stego-image with high embedding capacity, and errors in the retrieval process are kept to a minimum. Many advanced machine learning techniques are proposed to achieve this efficiency [129]. Some of the machine learning systems used are neural networks (NN) [152], support vector machine (SVM) [179], genetic algorithm (GA) [115, 182], and decision-tree-based analysis. Some of the related research works are illustrated in the following sections.

In this study [126], Fatmanur et al. proposed a steganalysis classifier approach to detect whether a given medical image contains hidden data or not. The support vector machine is used as a classifier for stego images' pixels and cover images. As a result of the analysis, the classifier accuracy is 99.28%.

The authors in [168] illustrate a medical image steganographic approach named BOOST for medical image security, based on the nuclear spin generator. The algorithm was measured using PSNR and MSE and shows that the proposed steganographic technique can stand against different medical image attacks.

Jain et al. [73] proposed a hybrid cryptosystem and steganography approach based on a piecewise linear chaotic map and dynamic decision tree. The algorithm applied on five steps, diffusion and confusion, pseudo-random sequence using linear feedback, permutation and XORing using pseudo-random sequence, RSA encryption algorithm used for keys encryption, and dynamic decision tree for steganography algorithm. The performance analysis and histogram analysis showed that the algorithm achieved maximum embedding capacity.

With advancements in medical imaging, the need for securing this sensitive data raises. Jambhale et al. [76] proposed a neural-crypto computing steganography mechanism to achieve confidentiality and privacy of medical images. The proposed mechanism utilizes neural networks combined with RSA cryptographic algorithm. The experimental results show that the proposed algorithm improves medical image security upon existing techniques.

## 4 Watermarking

Internet and image processing techniques have made it easier to copy, modify, and distribute digital data at a low cost and without any quality degradation. Digital image watermarking provides an alternative solution for ensuring tamper detection and ownership verification [31]. Watermarking is considered a way of embedding information in the digital content without modifying its value to recognize the original author of the data.

In this survey, a review of some recent research work in medical data security is discussed. Most recently, researchers have proposed a watermarking mechanism for the security of medical data. When medical data needs verification, watermarking can be a good solution [172]. Therefore, to guarantee originality and control disintegrate, watermarking is being used to publicize medical data security. Watermarking technique overcomes steganography's limitations by inserting a watermark inside the cover image such that the embedded watermark cannot be discovered [176]. However, the embedding process should not affect the image's visual quality. Digital watermarking techniques are derived from steganography, the science of communicating information while hiding its existence. The watermark is embedded in the host media so that it can't be separated from the data. Thus, by using watermarking, the work is still available but watermarked [118].

Both watermarking and steganography belong to data hiding but have different objectives and conditions. In steganography, for example, the critical data is the internal data, and the external data is a harmless message, whereas, in watermarking, the sensitive information is the external data. The internal data are additional data for protecting the external data, which is the watermark. These methods ensure authentication, integration, tamper-resistance, and content verification of the given image [107].

A digital watermarking scheme consists of three phases as shown in Fig. 9: first, it generates the watermark, second is embedding the watermark, and last, extraction of the watermark. When the copyright of a digital image is doubtful of being tampered with, the owner can retrieve the image's watermark to ensure his copyright.

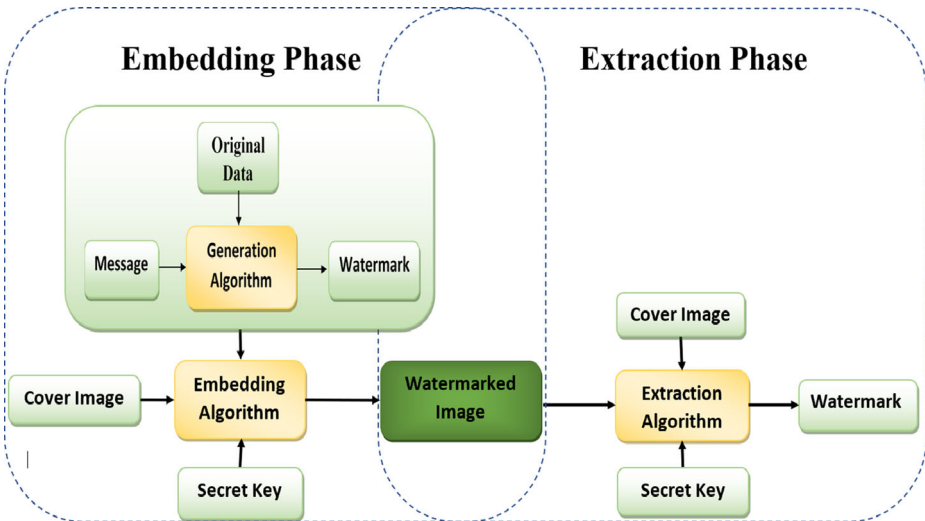


Fig. 9 Digital Watermark System

## 4.1 Main components of watermarking scheme

### 4.1.1 Phase I: Watermark embedding

The embedding algorithm embeds the generated watermark unique to the user into the cover image using different watermarking methodologies, such as LSB substitution, histogram shifting, etc. The watermarked image is sent to the receiver [27] to be verified.

### 4.1.2 Phase II: Watermark extraction

Watermark extraction is the process of extracting the embedded watermark from the watermarked image. The watermark image may be found to have been tampered with or not. The extracted watermark verifies the integrity and authenticity of the image and owner verification.

## 4.2 Primary requirements for ordinary digital image watermarking

1. **Robustness:** This is the resistance of the algorithm against various malicious and innocent attacks. Some processing operations on the image, such as resizing, compression, and cropping, are examples of accidental attacks that affect the image [28].
2. **Embedding capacity:** Generally, in data hiding techniques, this factor is considered one of the essential requirements that indicates the size of data embedded inside the cover image without image distortion.
3. **Fidelity and imperceptibility:** Used to hide the watermarked image from eavesdroppers' naked eye, so they cannot distinguish between watermarked and un-watermarked images. The fidelity factor indicates that the watermark is imperceptible and invisible and can be measured by SSIM or PSNR [19]. This factor should be a minimal value [170].

- (IV) Computational complexity (speed): This factor is considered very important for some real-time applications. It indicates the time consumed by the algorithm in the embedding and extraction process, which determines how fast the algorithm is.

### 4.3 Special requirements for medical image watermarking

In addition to the significant watermarking requirements, there are specific features for a medical watermarking system, such as:

- Reversibility:** This factor should be considered when dealing with medical images, as any distortion in this type of data could lead to an incorrect diagnosis. The algorithm is reversible; the recovered image is the same as the original without distortion after the embedding process.
- Integrity control:** This factor is used in the verification process to determine whether the eavesdropper has modified the image while being transmitted.
- Authentication:** This factor identifies the original author or the correct patient to whom the transmitted medical data belongs.

### 4.4 Watermarking approaches

Watermarking techniques could be classified as shown below in Fig. 10. The watermarking classification was categorized into four categories: domain-based, human perception-based, the reversibility of watermarking technique, and the procedure type [85]. The domain-based watermarking was also classified into transform domain and spatial domain. Watermarking is manipulated on image pixels in the spatial domain, whereas it is performed on image frequency components in the transform domain. The human perception is further classified into invisible and visible. Reversibility was categorized into reversible and non-reversible. The procedure type is divided into non-blind, semi-blind, and blind.

#### 4.4.1 Hiding domain

A review of watermarking techniques used in eHealth (Tele-Medicine, Tele-Radiology, Consultation, Microscopic surgery) application is presented in this survey. A brief introduction of each technique has been discussed in the following sections.

**Spatial domain techniques** In this domain, the pixel values are directly altered to embed the watermarked media. Techniques include least significant bit (LSB), local binary pattern (LBP), histogram modification, and spread spectrum techniques. In LSB, the watermark is embedded by substituting the rightmost bits of each pixel with the watermark bits values after converting the cover image pixels value into binary format. Finally, the pixels are transformed to their original value. LSB is considered the most straightforward technique with high embedding capacity [15].

In this paper, Huma et al. [71] proposed a watermarking technique based on joint watermarking and encryption for medical images. Patient information is encrypted using the output feedback. Advanced encryption standard algorithm. The embedding process of the

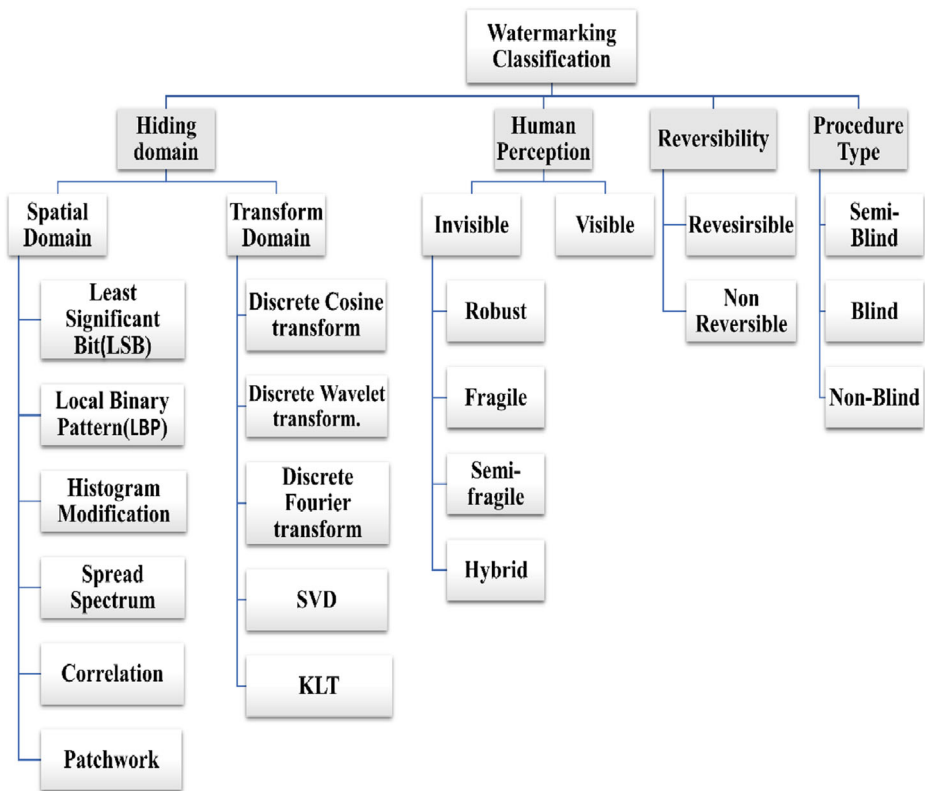


Fig. 10 Watermarking Techniques

watermark inside medical images is executed using DWT and LSB, and the testing results show that the proposed approach is secured and robust against different attacks.

Mahboubeh and Mehrabian [123] proposed a hybrid secure watermarking algorithm based on LSB, integer wavelet transform, and chaotic sequence. Using chaotic sequence in watermark encryption also achieves a high-security level, determining the embedding location and coefficient in the host image. No embedding is done inside the ROI area in the proposed algorithm, so the image is divided into ROI and RONI. Features extracted from ROI and patients’ personal and medical information are encrypted using a chaotic sequence from IC, which is embedded in the second level band of the host image. The experimental results show that the proposed algorithm has high robustness and imperceptibility compared with other state-of-the-art approaches.

Authors in this work [108] introduced a robust zero watermarking approach for medical image security to achieve robustness against geometric attacks and considered the distinguishability of similar medical images. Firstly, features are extracted from the medical image using DRZW, based on the completed local binary pattern (CLBP) to ensure robustness against geometric attacks and distinguishability. Then, the master and ownership share operator is created to ensure distinguishability and robustness, especially against geometric attacks. The proposed algorithm was applied to 200 different medical images of five types. The experimental results show that the DRZW algorithm ensures the reliability and accuracy of authentication.

This paper [55] proposed a new medical image watermarking approach based on redundant discrete wavelet transform (RDWT) and multiple histogram modification (MHM). To enhance the embedding capacity, the authors used the MHM algorithm. Then the watermark is embedded in the RDWT coefficients, which has several sub-band that provides better embedding capacity and guarantee its visual quality. The testing results proved that the proposed scheme presents better embedding capacity and robustness.

Chauhan et al. [38] present a new secure watermarking scheme for medical images based on the spread-spectrum concept. Firstly the cover image is decomposed into its frequency sub-band then a pair of pseudo-noise corresponding for each watermark pixel is embedded into each column and row sub-band. Various kinds of attacks are applied to the transmitted image in the testing phase. The experimental results showed that the technique offers more robustness than others.

In work [163], the authors illustrate multiple watermarking methods for medical images based on spread-spectrum. The telemedicine center logo and patient's personal and medical information are used as a watermark embedded in the host image. The pseudo-noise (PN) sequences are constructed according to each watermark bit then embedded into the host image selected DWT coefficients. It has been found from the experimental results that the approach.

Gives superior performance compared with other multiple watermarking methods.

Eze et al. [49] introduced an accurate digital watermarking algorithm and tamper detection for medical image security based on Spread Spectrum in this research paper. In the proposed method, the patient personal information is used as a watermark then embedded in the medical image sub-block. The experimental results show that the proposed scheme improved accuracy and tamper detection with low computational cost.

In [72], the author proposed a robust watermarking scheme based on graph coloring and vector quantization tested on an Android phone. Before the embedding process, the medical image is segmented into ROI and RONI. RONI is selected for watermark embedding using different processes like graph generation and graph coloring. Implementing the proposed technique on an Android device is considered an achievement of imperceptibility and low complexity.

**Transform domain** In the frequency domain mechanisms, the host media coefficients are rebuilt after the embedding process. The methodology includes DFT, DCT, RDWT, SVD, DWT, etc. [15]. The spatial-domain techniques are simpler in computation than the frequency domain but less robust against geometric attacks. The spatial and transform domain techniques are compared for evaluating some properties. Brief research work is discussed below in Table 2.

In DCT, the image is decomposed into low (FL), middle (FM), and high (FH). The majority of image energy is found in the low-frequency band. In DWT, the image was segmented as LL, HL, LH, and HH. "L" stands for low, and "H" stands for high.

Furthermore, the LL sub-band was also continuously segmented to achieve other levels based on the application's required number. In DFT, the image was resolved into cosine and sine forms and implemented watermark embedding using either template-based hiding or direct hiding. Therefore, it provides more protection against geometric attacks.

Kahlessenane et al. [83] proposed a new robust and blind watermarking technique for medical image security based on discrete wavelet transform. In this approach, the patient's personal information is combined with the constructed coefficients of the LL sub-bands to generate the watermark bits. With the number of experiments applied on secured images to

**Table 2** Comparison of Spatial and Transform Techniques

| Parameter          | Spatial Domain | Transform Domain |
|--------------------|----------------|------------------|
| Complexity         | Low            | High             |
| Robustness         | Low            | High             |
| Capacity           | High           | Low              |
| Imperceptibility   | Low            | High             |
| Computational Time | Low            | High             |

verify the invisibility and robustness of the proposed model, the experimental results show that the algorithm offers high robustness with excellent imperceptibility against geometric attacks.

Fares et al. [52] proposed two blind watermarking techniques for medical image exchange protection. The first one is based on Schur decomposition and Discrete Cosine Transformation to achieve high robustness and imperceptibility. The second one is based on Discrete Wavelet Transform and Schur decomposition. The experimental results prove that the proposed schemes are very robust against traditional attacks with high-quality watermarked images to protect the patient's information.

This paper [24] introduced a new watermarking method for medical image protection based on wavelet transformation and fuzzy-based Region of Interest (ROI) selection. First, the fuzzy-based algorithm is applied to the cover image to determine the sensitive points and select the ROI. Second, the wavelet transform is applied to decompose the image into sub-bands for the embedding phase. Experimental results show that the proposed algorithm is robust against various kinds of attacks.

Thanki et al. [178] proposed a blind watermarking approach for medical protection, based on Discrete Cosine Transform (DCT) and Fast Discrete Curvelet Transform (FDCuT) to get different frequency coefficients. The system is tested on various types of medical images to measure its effectiveness. Experimental results proved that the scheme is robust to different geometric attacks and others compared with the state of art schemes. Singh et al. [164] proposed a new hybrid watermarking technique in the transform domain for medical images security. To achieve high imperceptibility, robustness, and capacity. The authors combined nonsampled contourlet transform (NSCT) with singular value decomposition (SVD) and discrete cosine transform (DCT). The NDCT is used to increase hiding capacity and robustness against geometric attacks. The electronic patient record is embedded into the selected medical images sub-band. The proposed algorithm achieved high robustness against signal processing and geometrical attacks.

#### 4.4.2 Human perception

The watermark is an effect embedded in an image that may be invisible or visible to identify the ownership of the given data [59]. Digital watermarking has proved to be a promising technology for enhancing the copyright protection of images. Table 3 summarizes the techniques from a human perception point of view.

In this paper, Mata-Mendoza et al. [112] proposed a hybrid and robust watermarking technique for medical images security based on quantization index modulation algorithm and forwarding error correction to embed metadata as a robust-imperceptible watermarking.

**Table 3** Watermarking Approaches

| Technique                 | Definition   | Application  |
|---------------------------|--|--|
| Visible watermark         | It is mainly a semi-transparent text or image embedded in the cover image.   | Logo on TV channel   |
| Invisible watermark       | The watermark is embedded to be invisible to the user's naked eye, but it can easily be identified that the image is watermarked or not by the computer devices.   | Copyright protection applications  |
| Robust watermarking       | Robust watermarking techniques are resistant to multiple various attacks. The authors in [125] applied the SVD method to the medical image watermarking technique based on FDCuT-DCT. The proposed algorithm has good imperceptibility so that it can maintain the quality of medical images | used in copyright protection   |
| Fragile watermarking      | Watermark allows being demolished by straightforward alteration easily.<br>Any slight change in the watermarked image will cause the watermark to break, low imperceptibility  | integrity verification, and authentication applications.                       |
| Semi-fragile watermarking | Defend on the covered data against deliberate attacks but is frail against malignant attacks.  | Copyright protection but with Low imperceptibility                             |
| Zero watermarking         | Unlike other watermarking techniques, the watermarking process does not modify the image, as the watermark does not embed in the image itself [141].   | Copyright protection, authentication, and tamper detection for medical data    |
| Hybrid watermarking       | It is a combination of robust and fragile techniques   | Integrity verification, copyright protection, and authentication concurrently. |

The experimental results of the proposed technique show that it's efficient and robust against various traditional attacks with high imperceptibility.

In this paper [56], the authors proposed a fragile watermarking scheme for tamper detection in a medical image and region of interest protection. The medical image is divided into packets. The cyclic redundancy check code (CRC) based on standard polynomial generator CRC-32 is utilized to be applied on each packet to generate a watermark. Results of experiments prove the imperceptibility and robustness against aggressive attacks.

#### 4.4.3 Hybrid techniques

Recently, researchers have proposed a hybrid of hiding and cryptography techniques. In [174], the authors proposed a multilayer watermarking scheme based on chaotic encryption and SVD, DWT, DCT by encrypting the watermarked image. In [176], the authors proposed a robust, non-blind, and high payload using FRT and SVD hybridized with Arnold scrambling to add additional security for the proposed algorithm. Balasamy et al. [23] proposed a hybrid algorithm between watermark and encryption to increase medical image security. The experimental results of this method illustrate that the proposed scheme has better authentication than others.

Alzahrani et al. [14] proposed a robust watermarking technique to protect medical image copyright in a hybrid domain. The proposed scheme is a hybrid of three algorithms, Discrete Cosine Transform (DCT), Singular Value Decomposition (SVD), and Discrete Wavelet Transform (DWT). Firstly the medical image is divided into a region of interest (ROI) and a region of non-interest (RONI), then get high and low-frequency bands from RONI using



DWT, the appropriate block for embedding are selected using Human Visual System (HVS). The experimental results proved that the proposed technique has high imperceptibility as well as robustness.

Accurate polar complex exponential transform (APCET) based on Gaussian numerical integration (GNI) describes two similar medical images simultaneously. To overcome the limitation in most zero watermarking schemes, which only support protection for one image at a time. Chang et al. [110] proposed a new zero watermarking for protecting two similar medical images using TAPCET and chaotic mapping. The experimental results show that the proposed scheme is robust against various geometric and image processing attacks.

The current paper [3] uses a new medical image watermarking technique based on the blue monkey meta-heuristic and honey algorithms. The first is used to select the best hiding location in the host image. The second, utilized for watermark encryption before embedding. Furthermore, various image processing and geometric attacks are applied to host images for testing. The experimental results of the proposed algorithm demonstrate that it is robust and secure against most attacks.

Hosny et al. [67] introduce new geometrically invariant multiple zero-watermarking schemes to overcome the lack of security found in single watermarking algorithms for medical image security based on Gegenbauer moments of fractional orders (FrMGMs). FrMGMs are used to extract the geometrically invariant features from medical images and form the feature vector using the magnitude of these moments. The extracted features XORed with scrambled watermark image to construct ownership share. The proposed approach provided higher robustness to geometric and other attacks.

#### 4.4.4 Procedure type

The main challenge of designing a watermarking technique for medical image security should be blind or non-blind. More patient information has been embedded into the cover image to achieve robustness against various attacks. Table 4 shows techniques of procedure type classifications.

Soualmi et al. [166] presented a blind medical image watermarking technique. Based on combining the Weber descriptors (WDs), DCT transform, and Arnold chaotic map. Firstly, The DCT coefficients of each block are extracted using DCT, and then the watermark is scrambled using Arnold's chaotic map. The scrambled watermark embedded in DCT proper coefficients were selected based on WDs. The proposed technique improves the robustness against different attacks compared with other state-of-the-art algorithms.

**Table 4** Watermark Procedure Techniques

| P.O.C        | Blind  | Semi-Blind  | Non-Blind  |
|--------------|--|---|--|
| Definition   | No need for original information to extract the watermark.   | It only requires a secret key and a watermark to extract the data.  | Both secret key and watermark and cover image are required to extract the watermark. |
| Applications | <ul style="list-style-type: none"> <li>• Healthcare</li> <li>• Copyright protection</li> <li>• E-voting</li> <li>• Remote education</li> <li>• Image authentication</li> <li>• Tamper detection</li> </ul> | <ul style="list-style-type: none"> <li>• Copyright protection</li> <li>• Image authentication</li> <li>• CAD models</li> <li>• Content privacy</li> <li>• Wireless and Adhoc systems</li> </ul> | <ul style="list-style-type: none"> <li>• Copyright protection</li> </ul>             |

Soualmi et al. [167] proposed a new watermarking scheme for medical image security based on MinEigen value features, chaotic sequence, and Quantization Index Modulation (QIM). Then embed the watermark bits in  $3 \times 3$  blocks selected by using MinEigen value. The experimental results showed that the proposed approach is robust and imperceptible against compression attacks. In this work, [46], the authors proposed a hybrid image quality degree algorithm based on singular value decomposition (M-SVD) for both grey and color images. The proposed algorithm embeds a watermark in the medical image then applies several geometric and image processing attacks. Results show that the M-SVD algorithm has perfect results in medical images in both color and grey images.

#### 4.4.5 Reversibility

Abbasi et al. [1] proposed a medical image watermarking system. Firstly the image is divided into two regions region of interest (ROI) and region of noninterest (RONI). The authors embed two different watermarks, one fragile watermark in ROI and the other robust watermark in RONI. For casting the watermark, simple LSB. The system was tested using different CT medical images. The simulation results prove that the proposed system provides higher security and confidentiality of medical images.

Shehab et al. [155] proposed a new fragile watermarking technique for medical image authenticity. The proposed technique can locate and recover tampered images based on SVD and LSB. SVD help in improving the medical image authentication and detecting different attacked area of the watermarked image. Different types of attacks are applied to the testing datasets. The experimental results prove that the proposed scheme improves tamper localization and original image recovery compared with other state-of-the-art methods.

## 5 Performance metrics

The proposed algorithms can be measured from different sides as computational speed, time complexity, quality of encrypted and decrypted images, and robustness. These metrics are summarized in Fig. 11. In the following lines, some of these metrics have been discussed in Table 5.

### 5.1 Image quality measurement

One of the essential performance metrics that must be discussed. Some image encryption algorithms may result in some deformation in the ciphered images, which affects data reliability. Decrypted image accuracy is essential in some medical and military applications. Affecting the ROI leads to misdiagnosis. This metric, applied by evaluating the relationship between source and decrypted images, represents the quality of ciphered images. The widespread image aspect measurements are peak signal-to-noise ratio (PSNR), bit correct ratio (BCR), structural similarity index measure (SSIM), signal-to-noise ratio (SNR), mean absolute error (MAE), mean squared error (MSE), and standard dynamic range (SDR). Despite signal fidelity, metrics are often disputed because they have no regard for the image signal's nature. They are still widely used as image quality measures [193]. The various measures utilized are discussed next.

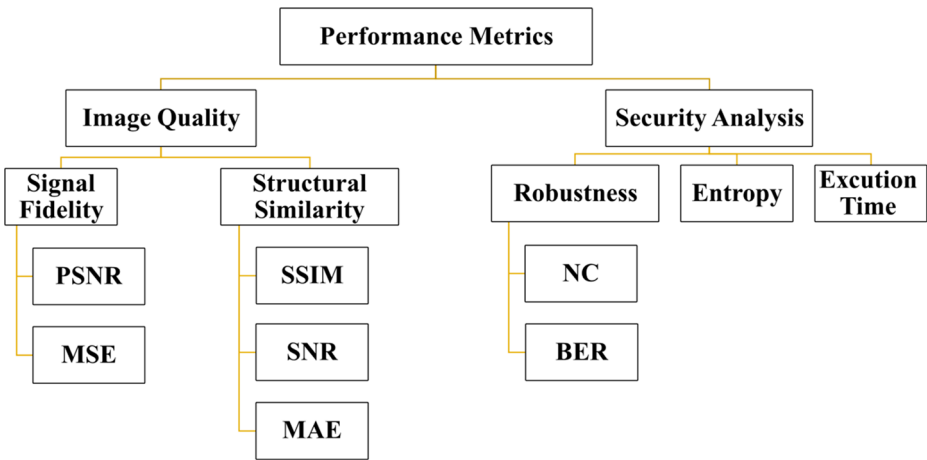


Fig. 11 Performance Metrics

In 2017, Pak and Huang [128] applied peak signal-to-noise ratio (PSNR) metrics to evaluate their proposed algorithm. As known, when the value of PSNR is large, this means that the tested algorithm results in high decrypted image quality. The experimental results of the utilized encipher technique have outstanding accomplishments in facing various attacks and noise. Li et al. [97] also applied this metric to their algorithm and got results similar to the previous test.

Table 5 Performance Metrics

| Reference | Measures | Formula   | Optimum Value  |
|-----------|----------|---|--|
| [33]      | PSNR     | PSNR criteria are used to know the proposed algorithm’s imperceptibility according to how the watermarked image and the original image are similar. A high PSNR value means a high similarity between the two images. It is represented as, | High as possible   |
|           | MSE      | $PSNR = 10 \log_{10} \frac{(255)^2}{MSE}$ Mean Square Error is:<br>$MSE = \frac{1}{X \times Y} \sum_{i=1}^X \sum_{j=1}^Y (I_{ij} - W_{ij})^2$   | Range from 0 to 1<br>Ideally =0<br>This value means the two images are identical |
|           | NC       | NC is used in calculating the similarity between the extracted and the original watermark coefficient value range between 0 and 1. It can be mathematically represented as  | Ideally, NC=1 but 0.7 is acceptable  |
|           |          | $NC = \frac{\sum_{i=1}^X \sum_{j=1}^Y (W_{orig} \times W_{recd})}{\sum_{i=1}^X \sum_{j=1}^Y (W_{org-ij}^2)}$  |  |
| [186]     | NPCR     | $NPCR : N(C^1, C^2) = \sum_{i,j} \frac{D(i,j)}{T}$  | Range from 0 to 100<br>Ideally =100  |
|           | SSIM     | SSIM is one of the most recently used criteria to find similarities between the original and the watermarked image  | Ranged from 0 to +1.<br>Ideally =1   |
| [127]     | UACI     | $UACI : U(C^1, C^2) = \sum_{i,j} \frac{ C^1(i,j) - C^2(i,j) }{F.T}$   | Range from 0 to 100<br>Ideally =100  |
| [159]     | BER      | $BER = \frac{\text{number of incorrectly decoded bits}}{\text{Total number of bits}}$   | Small as possible<br>Ideally =0  |

The MSE is used to evaluate the level of defense on encipher images. Ran et al. [136] used MSE criteria between the original image and ciphered image. Also, Wang et al. [188] used this metric in their grading. The retrieved images from their work are heavily deranged by noise but can still recognize the primary information inside the image affected by the noise. This experiment shows that the introduced methodology can withstand noise but within a certain level.

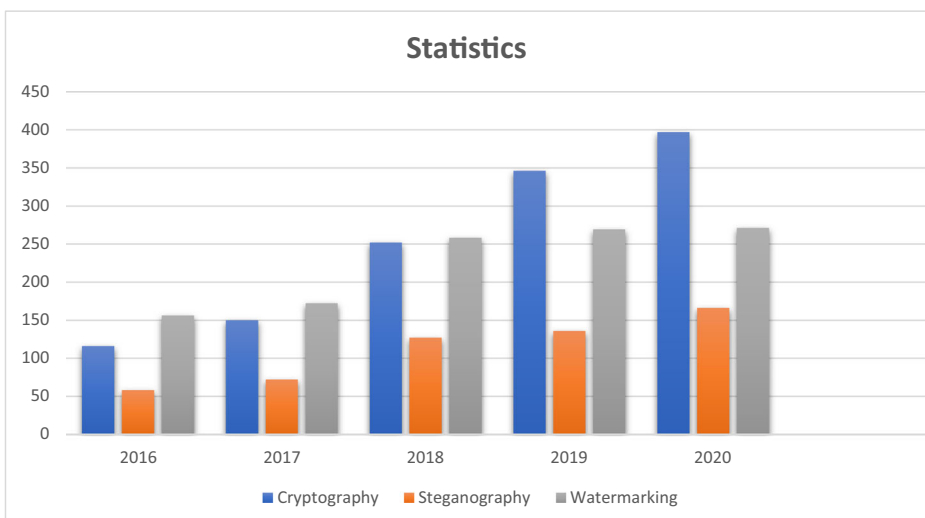
In 2018, X. Li et al. [98] preferred to use one of the structural similarity metrics, SSIM, to measure their success in reconstructing encrypted images. The results show that the introduced scheme gives high SSIM results, which give high image quality. The SSIM values calculated by the authors are nearest to one, and SSIM values range between 0 and 1, which means no distortion in the reconstructed frames when the value is close to 1.

Khan et al. [92] proposed a technique to improve the signal-to-noise ratio's strength (SNR). They prepared new statistical criteria, mean absolute error (MAE), and, as the encryption security increased with a more considerable MAE value, the authors' SNR result proved the proposed algorithm's efficiency.

## 5.2 Metrics formula and optimum value

## 6 Data sets

Digital Imaging and Communications in Medicine (DICOM) was considered as criterion formate for medical images. DICOM standard is used to guarantee a proportionate format for transmitting, processing, storing medical images. This formate facilitates sharing medical images through the internet and several servers between patients, medical centers, and vice versa [40]. Medical devices from different suppliers can transmit medical images through the network. In the following lines, many researchers' medical images datasets in their experiments have been mentioned.



**Fig. 12** The number of published studies in the last five years

**Table 6** Performance discussion for cryptography-based medical image security techniques

| Ref   | Proposed method  | Method  | Time Complexity  | Performance |         |        |       |         |        |        | Pros   |  |
|-------|--|---|--|-------------|---------|--------|-------|---------|--------|--------|--------|--|
|       |  |   |  | UACI        | NPCR    | NPCR   | SNR   | PSNR    | MSE    | SSIM   |        |  |
| [134] | Multiscale transform-based secured joint efficient medical image compression-encryption using symmetric key cryptography and ebct encoding technique | Multiscale transform using ebct encoding technique and symmetric key cryptography | Low Computational Complexity   | NA          | NA      | 76.869 | NA    | 0.0009  | 0.9999 | 0.0009 | 0.9999 | Compression time is not affected by encryption time.   |
| [130] | A novel visual medical image encryption for the secure transmission of authenticated watermarked medical images                                      | Medical image is encrypted visually with the fingerprint using IWT.               | $T=37^n$<br>Robust to brute force attack   | 0.000014    | 40.7344 | NA     | 30 dB | NA      | NA     | NA     | NA     | The proposed method presents high integrity with high imperceptibility for increasing security and authentication using fingerprint images.                    |
| [30]  | Secure visual cryptography for medical image   | This paper fuse the concept of modified cuckoo search                             | Has low computational complexity   | NA          | NA      | NA     | 49.51 | 0.0171  | NA     | NA     | NA     | The proposed scheme provides Reversibility and robustness.   |
| [63]  | A privacy-preserving cryptosystem for IoT E-healthcare   | Chaotic Map (PWLCM) and Logistic Map  | $T=0.95$ Seconds<br>For akeyframe [640x480x3]<br>With encryption speed =970 KB/-<br>Ssec | 33.465      | NA      | 99.609 | NA    | 73.5965 | 0.0028 | NA     | NA     | The proposed algorithms effectively resist various attacks besides keeping the confidentiality of the medical in-Formation.                                    |
| [34]  | Medical image encryption using edge maps   | Encryption algorithm using edge map   | Time various from 0.0129 to 1.846 s<br>for images $8 \times 8$ to $512 \times 512$       | 0.3348      | 0.9960  | NA     | NA    | NA      | NA     | NA     | NA     | The proposed algorithm has a considerable defense against the Bruce-force attack with higher pixel correlation, stronger key sensitivity, and error robustness |

Table 6 (continued)

| Ref  | Proposed method   | Method   | Time Complexity  | Performance |      |       |     |      |     |      | Pros |   |
|------|---|--|--|-------------|------|-------|-----|------|-----|------|------|---|
|      |   |  |  | UACI        | NPCR | NPCR  | SNR | PSNR | MSE | SSIM |      |   |
| [95] | Medical image encryption based on improved ElGamal encryption technique | ElGamal encryption scheme is designed to encrypt the medical image | Time various from 0.093750 s to 1.718750 s for images 256 × 256 to 1024 × 1024 | 33,41       | NA   | 99,62 | NA  | NA   | NA  | NA   | NA   | It has been proved that the proposed model presents good characteristics of a strong cipher with sound encryption and decryption speed. |

**Table 7** Performance discussion for Steganography-based medical image security techniques

| Ref                                | Performance |                   |                |        |                            |   | Cons  |
|------------------------------------|-------------|-------------------|----------------|--------|----------------------------|---|---|
|                                    | Complexity  | Imperceptibility  | Visual Quality |        | Embedding Capacity         | Steganalysis Resistivity                |   |
|                                    |             |                   | PSNR           | MSE    |                            |   |   |
| Santhi and Dheeptha [147]          | High        | Imperceptible     | 71.3896        | 0.0048 | Approx. 0.8 bpp            | Preserve the Histogram, Chi-Square      | The method needs more recourses to be applied and due to high computational cost and low payload capacity.              |
| Martini et al. [111]               | Low         | Not Imperceptible | NA             | NA     | 1 bpp                      | RS analysis                             | The proposed algorithm is not robust to image processing attacks.   |
| Al-Dmour and Al-Ami [9]            | Low         | Imperceptible     | 56.81          | 0.136  | 1 bpp                      | Histogram, STC                          | The authors did not care about the ROI region in this method, which is very important when dealing with medical images. |
| Jain et al. [74]                   | High        | Imperceptible     | 86.55          | 0.0005 | 3.6 bpp<br>Raised 43%      | RS analysis                             | The suggested method gives good results for a small amount of data.   |
| Jain and Kumar. [75]               | High        | Imperceptible     | 79.36          | 0.0021 | 1.03 bpp<br>Percentage 36% | NA                                      | The algorithm is not appropriate for real-time applications due to the high complexity                                  |
| Naidu et al. [122]                 | Low         | Imperceptible     | 73.02          | 0.0049 | Approx 1.55<br>bpp         | Pixel Difference Histogram              | The drawback of the proposed scheme was that it did not separate the image into ROI and RONI Regions.                   |
| (Nguyen et al., 2015) [124]        | High        | Imperceptible     | Approx 46      | NA     | 1.5 bpp                    | SPAM with Ensemble Out of Bag (OOB)     | NA  |
| (S. Shen et al., 2015) [156]       | Low         | Not Imperceptible | 36             | 0.045  | 1.5 bpp                    | RS analysis, Pixel Difference Histogram | Not Imperceptible   |
| (Grajeda- Marin et al., 2016) [57] | High        | Imperceptible     | 38.33          | NA     | 2.14 bpp                   | NA                                      | NA  |

Falgun et al. [173] tested the proposed algorithm on a dataset chosen from the digital imaging and communication in medicine (DICOM) as CT, X-ray of size  $1024 \times 1024$ . In this contribution [48], the authors used large numbers of large-sized X-ray images of Pneumonia infected and healthy patients from the Pneumonia Chest X-ray of the Kaggle Competition.

Singh et al. [161] experiments were done on  $565 \times 584$  pixels fundus and retinal images of the DRIVE free public dataset. Guzin et Arda [181], in their experiments, depend on the dataset that was gathered from the Internet and created by their research group, which contains several tampered (rotating, scaling, blurring) Grey-level medical images.

## 7 Discussion

### 7.1 Statistical analysis

In this section, Fig. 12 shows a statistical representation of related research papers published in archived journals (Springer, IEEE Explorer, and Science Direct) of the last five years in the field of medical data security. It is concluded that medical image security is growing and has become a big challenge because of its importance.

### 7.2 Medical data security requirements

Many recent efficient security methodologies have been proposed for medical data security. However, there is some limitation in its practicality. Based on previous studies, we focus on some potential challenges.

#### 7.2.1 Cryptography

- According to the application, encryption and decryption operations applied on medical images may lead to image distortion, so the proposed technique should be lossless.
- Computational speed is considered the main challenge in encryption and decryption.
- Compression techniques can be used to compensate for the shortage in payload capacity.

#### 7.2.2 Steganography

- Maximize embeddable regions to suit more information.
- Maintain the imperceptibility for the stego image.
- Embedding bits selection of the cover image.
- Achieve lower computational time with high robustness.
- Design steganographic systems for real-time applications with high privacy.

#### 7.2.3 Watermarking

- Put all types of image attacks into consideration while improving or developing a watermarking technique.



**Table 8** Performance discussion for watermarking-based medical image security technique

| Reference | Evaluation Metric | Geometric Attacks |             |          | Compression |         |          | Image Processing Attacks |                     |         |
|-----------|-------------------|-------------------|-------------|----------|-------------|---------|----------|--------------------------|---------------------|---------|
|           |                   | Rotation          | Translation | Cropping | Scaling     | JPEG    | JPEG2000 | Gaussian noise           | Salt & Pepper noise |         |
| [79]      | BER               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | PSNR              | NA                | NA          | 0.989    | >40         | >40     | >40      | NA                       | NA                  | >40     |
|           | NC                | NA                | NA          | 0.73814  | 0.99744     | 0.99853 | 0.99629  | NA                       | NA                  | 0.99280 |
|           | SSIM              | NA                | NA          | 41.3784  | Inf         | Inf     | inf      | NA                       | NA                  | Inf     |
| [90]      | BCR               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | BER               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | PSNR              | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | 24.3557 |
|           | NC                | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
| [160]     | SSIM              | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | BER               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | PSNR              | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | 34.88   |
|           | NC                | 0.8269            | NA          | 0.9859   | 0.9906      | 0.9882  | NA       | NA                       | NA                  | 0.9579  |
| [11]      | SSIM              | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | BER               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | WSNR              | 0.0982            | NA          | 8.1109   | NA          | NA      | NA       | 27.0916                  | NA                  | 32.1470 |
|           | PSNR              | 5.9136            | NA          | 13.7111  | NA          | NA      | NA       | 19.9203                  | NA                  | 24.6345 |
| [158]     | NC                | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | MSSIM             | 0.2728            | NA          | 0.7391   | NA          | NA      | NA       | 0.8212                   | NA                  | 0.9304  |
|           | BER               | NA                | NA          | NA       | 0.444       | 0.96    | NA       | 0.55                     | NA                  | 0.48    |
|           | BCR               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
| [175]     | PSNR              | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | NC                | NA                | NA          | NA       | 0.7375      | 0.9905  | NA       | 0.7267                   | NA                  | 0.6069  |
|           | SSIM              | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | BER               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
| [26]      | PSNR              | NA                | NA          | NA       | 0.9986      | 0.9986  | NA       | 0.9539                   | NA                  | 0.9528  |
|           | NC                | 0.9986            | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | SSIM              | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
|           | BER               | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |
| [26]      | PSNR              | 29.9297           | NA          | 35.9698  | 31.0447     | 29.2960 | NA       | NA                       | NA                  | 30.0444 |
|           | NC                | NA                | NA          | NA       | NA          | NA      | NA       | NA                       | NA                  | NA      |

Table 8 (continued)

| Reference                | Evaluation Metric                        | Geometric Attacks                    |                                  |                                  | Compression                    |                                  | Image Processing Attacks         |                                  |                                    |
|--------------------------|--|--------------------------------------|----------------------------------|----------------------------------|--------------------------------|----------------------------------|----------------------------------|----------------------------------|------------------------------------|
|                          |  | Rotation                             | Translation                      | Cropping                         | Scaling                        | JPEG                             | JPEG2000                         | Gaussian noise                   | Salt & Pepper noise                |
|                          | SSIM                                     | 0.981                                | NA                               | 0.999                            | 0.955                          | 0.978                            | NA                               | NA                               | 0.935                              |
| Image Processing Attacks |  |                                      |                                  |                                  |                                |                                  |                                  |                                  |                                    |
| Reference                | Median filter                            | Gaussian filter                      | Average Filter                   | Contrast                         | Sharpening                     | Blurring                         | Hist. Equalization               |                                  |                                    |
| [79]                     | NA<br>>40<br>0.99115<br>Inf<br>NA        | NA<br>>40<br>0.95951<br>inf<br>NA    | NA<br>NA<br>NA<br>NA<br>NA       | NA<br>NA<br>NA<br>NA<br>NA       | NA<br>NA<br>NA<br>NA<br>NA     | NA<br>NA<br>NA<br>NA<br>NA       | NA<br>NA<br>NA<br>NA<br>NA       | NA<br>NA<br>NA<br>NA<br>NA       | NA<br>NA<br>NA<br>NA<br>NA         |
| [90]                     | NA                                       | NA                                   | NA                               | NA                               | NA                             | NA                               | NA                               | NA                               | NA                                 |
| [160]                    | 0.979<br>NA<br>NA<br>NA                  | 0.8184<br>NA<br>NA<br>NA             | NA<br>NA<br>NA<br>NA             | NA<br>0.9246<br>NA<br>NA         | NA<br>NA<br>NA<br>NA           | NA<br>NA<br>NA<br>NA             | NA<br>NA<br>NA<br>NA             | NA<br>NA<br>NA<br>NA             | NA<br>NA<br>NA<br>NA               |
| [11]                     | NA<br>NA<br>NA                           | 0.2802<br>5.9212                     | NA<br>NA<br>NA                   | NA<br>NA<br>NA                   | 0.2801<br>5.9214               | NA<br>NA<br>NA                   | NA<br>NA<br>NA                   | NA<br>NA<br>NA                   | NA<br>NA<br>NA                     |
| [158]                    | NA<br>NA<br>NA<br>0.93<br>NA<br>NA<br>NA | 0.1030<br>NA<br>NA<br>NA<br>NA<br>NA | NA<br>NA<br>NA<br>NA<br>NA<br>NA | NA<br>NA<br>NA<br>NA<br>NA<br>NA | 0.1031<br>NA<br>NA<br>NA<br>NA | NA<br>NA<br>NA<br>NA<br>NA<br>NA | NA<br>NA<br>NA<br>NA<br>NA<br>NA | NA<br>NA<br>NA<br>NA<br>NA<br>NA | 0.14<br>NA<br>NA<br>NA<br>NA<br>NA |

**Table 8** (continued)

| Reference | Image Processing Attacks |                 |                |          |            |          |                    |  |
|-----------|--------------------------|-----------------|----------------|----------|------------|----------|--------------------|--|
|           | Median filter            | Gaussian filter | Average Filter | Contrast | Sharpening | Blurring | Hist. Equalization |  |
| [175]     | 0.9985                   | NA              | NA             | NA       | NA         | NA       | 0.569              |  |
|           | NA                       | NA              | NA             | NA       | NA         | NA       | NA                 |  |
|           | NA                       | NA              | NA             | NA       | NA         | NA       | NA                 |  |
|           | 0.9826                   | 0.9989          | NA             | NA       | NA         | NA       | 0.9980             |  |
|           | NA                       | NA              | NA             | NA       | NA         | NA       | NA                 |  |
| [26]      | NA                       | NA              | NA             | NA       | NA         | NA       | NA                 |  |
|           | 30.0422                  | 41.3355         | 4,908,827      | NA       | 28,6619    | 464,742  | 18,2224            |  |
|           | NA                       | NA              | NA             | NA       | NA         | NA       | NA                 |  |
|           | 0.974                    | 0.964           | 0.991          | NA       | 0.959      | 0.956    | 0.847              |  |

**Table 9** Average of evaluation metrics for various watermarking-based medical image security techniques

| Proposed Method       | Method                         | Performance                       | Drawback                               |
|-----------------------|--------------------------------|-----------------------------------|--|
| Jia and Zhou [79]     | LSB, SHA-265, MAC, AES,        | Blind, fragile                    | High computational complexity          |
| Kelkar and Mehta [90] | LBPTI and RDH                  | Reversible and Secure             | Low embedding capacity                 |
| Singh and Kumar [160] | SVD, DWT, BPNN                 | Imperceptible, robust, and secure | Computational complexity is high       |
| Al-qdah [11]          | SVD, DWT                       | Blind, secure                     | Watermark, not robust to some attacks. |
| Singh, Dave [158]     | DCT, DWT,                      | PSNR=35.84 dB,<br>NC=0.9992       | Computational complexity is high.      |
| Thakur, Singh [175]   | RDWT, NSCT, chaotic encryption | Robust and Secure                 | Embedding capacity can be enhanced.    |
| Bamal and Kasana [26] | FWT, SLT, ANN, AES,            |                                   | Low Imperceptibility                   |

- Both robustness and computational complexity of the proposed system are essential.
- ROI must be observed while embedding the watermark to not affect the features in medical images.
- The reversibility of the watermarking approach is essential in medical images.
- Hybridization between watermarking and encryption can be used to improve performance.
- Some compression techniques have been used to increase embedding capacity.

In some applications, preserving image quality is a must because it may lead to medical images diagnosis or military data transmission. Simple distortion in the image is acceptable by taking a watermarking approach, for example, selecting a watermarking technique. Fragile, blind, robust, and zero-watermarking would be used according to the application. Most sensitive image applications use zero-watermarking for security because zero-watermarking was considered one of the approaches that don't cause image distortion ratio. The watermark does not embed inside the host image, as most traditional watermarking techniques do.

The primary step for zero-watermarking is how to extract special and robust image features, robust against various image attacks, to reconstruct the watermark and verify copyright. In [80, 144], the authors discussed various global and local features. In global features, the processing is performed on whole host image pixels, as Geometric Moment Features, Space-Time Volumes (STV). In local features, the processing is performed on each pixel as GLCM, SIFT, SURF [142], and Local binary Pattern and the ability of each technique to resist attacks. Hosny et al. [69] proposed highly accurate, fast, and robust techniques for gray and color images based on computing the moments of (PCET) for the host image. The results proved that the proposed algorithm gives higher accuracy for watermarked image reconstruction with high visual imperceptibility and robustness to common attacks. Hosny et al. [68] proposed a robust watermarking algorithm based on new fractional-order exponent moments applied on color images.

### 7.3 Performance analysis and discussion

As shown above, various approaches are proposed for medical images and ordinary images with copyright protection and tamper detection as cryptography, steganography, and

**Table 10** Abbreviations

## Acronyms

|         |   |
|---------|---|
| PSNR    | Peak Signal to Noise Ratio                    |
| SSIM    | Structural Similarity Index                   |
| BER     | Bit Error Rate                                |
| NC      | Normalized Coefficient                        |
| NPCR    | Number of Pixels Changes Rate                 |
| UACI    | Unified Average Change Intensity              |
| MRI     | Magnetic Resonance Imaging                    |
| CT      | Computed Tomography                           |
| US      | Ultrasonography                               |
| ROI     | Region of Interest                            |
| RONI    | Region of Non-Interest                        |
| CFI     | Choquet Fuzzy Integral                        |
| EA      | Evolutionary Algorithms                       |
| ACM     | Arnold Cat Map                                |
| ICA     | Independent Component Analysis                |
| GA      | Genetic Algorithm                             |
| GT      | Gyrator Transform                             |
| DCT     | Discrete Cosine Transform                     |
| FrFT    | Fractional Fourier Transform                  |
| MAE     | Mean Absolute Error                           |
| SDR     | Standard Dynamic Range                        |
| SNR     | Signal to Noise Ratio                         |
| PVD     | Pixel Value Differencing                      |
| LSB     | Least Significant Bit                         |
| DWT     | Discrete Wavelet Transforms                   |
| HVS     | Human Visual System                           |
| IWT     | Integer Wavelet Transform-Based Steganography |
| AI      | Artificial Intelligence                       |
| ML      | Machine Learning                              |
| NN      | Neural Networks                               |
| SVM     | Support Vector Machine                        |
| LBP     | Local Binary Pattern                          |
| HUGO    | Highly Undetectable steGO                     |
| SSIM    | Structural Similarity Index Measure           |
| POV     | Pair of Value                                 |
| WS      | Weighted Stego Steganalyser                   |
| MLSB-WS | Multi Bitplane Weighted Stego Steganalyser    |

watermarking. Nothing proved that any of these techniques is the best for image security, so we can say that deciding to use any one of these approaches is based on application type and data sensitivity Table 6, Table 7, and Table 8 presents the most current state of art medical image security approaches.

## 8 Conclusion

A brief discussion on medical data types. Medical image security plays a significant role in various eHealth applications, including storage, retrieval, identity theft, and data management. In this paper, we have introduced the latest development of medical image security algorithms

in recent five years and analyzed the challenges of medical images security. Some famous image attacks have been listed, which are applied to data to test the proposed algorithms. Some medical image security approaches as cryptography which is presented in spatial and frequency domains, a detailed classification of steganography are presented, and several steganography approaches have been discussed, also a comprehensive survey for watermarking types, characteristics, and medical image watermarking approaches. We have discussed these approaches and their characteristics, kinds, requirements, working mechanisms for each approach, and their potential issues to support further research in this area. Also, some medical images datasets utilized by many researchers have been mentioned.

Furthermore, some performance metrics for algorithm evaluation have been demonstrated. With the help of our survey, researchers may propose new security methodologies to secure the transmission of medical data to service eHealth applications (Tables 9 and 10).

**Funding** Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

## Declarations

**Ethics declarations** No fund available for this study.  
The authors have declared that there are no competing interests exist.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

1. Abbasi F, Memon NA (2018) Reversible watermarking for the security of medical image databases. In: 21st Saudi computer society National Computer Conference (NCC). IEEE, pp 1–6
2. Abdel-Aziz MM, Hosny KM, Lashin NA (2021) Improved data hiding method for securing color images. *Multimed Tools Appl* 80(8):12641–12670
3. Abdulhammed OY (2021) Improving encryption digital watermark by using blue monkey algorithm. *Int J Comput* 20(1):129–136
4. Abdulla AA (2015) Exploiting similarities between secret and cover images for improved embedding efficiency and security in digital steganography. Ph.D. Thesis. University of Buckingham
5. Abdulla AA, Jassim SA, Sellahewa H (2013) Secure steganography technique based on Bitplane indexes. In: IEEE international symposium on multimedia. IEEE, pp 287–291
6. Abdulla A, Sellahewa H, Jassim S (2014) Stego quality enhancement by message size reduction and Fibonacci bit-plane mapping, pp 151–166
7. Afandi TMK, Fandiantoro DH, Endroyono PIKE (2021) Medical images compression and encryption using DCT, arithmetic encoding, and Chaos-based encryption. In: International seminar on intelligent technology and its applications (ISITIA), pp 1–5
8. Ahlem A, Sreetama O (2019) Cellular imaging to biometrics Alice. Springer, Singapore
9. Al-Dmour H, Al-Ani A (2016) Quality optimized medical image information hiding algorithm that employs edge detection and data coding. *Comput Methods Prog Biomed* 127:24–43

10. Ali M (2019) A survey of the Most current image encryption and decryption techniques. *Int J Adv Res Comput Sci* 10:9–14
11. Al-qdah M (2018) Secure watermarking technique for medical images with visual evaluation. *Signal Image Process Int J (SIPIJ)* 9(1):1–9
12. Al-Qershi OM, Khoo BE (2014) Controlling hiding capacity using image characteristics with a 2D-DE data hiding scheme. *AEU-Int J Electron Commun* 68:346–350
13. Altaay AAJ, Bin Sahib S, Zamani M (2012) An introduction to image steganography techniques. In: *International conference on advanced computer science applications and technologies (ACSAT)*. IEEE, pp 122–126
14. Alzahrani A, Memon NA (2021) Blind and robust watermarking scheme in hybrid domain for copyright protection of medical images. *IEEE Access* 9:113714–113734
15. Anand A, Singh AK (2020) Watermarking techniques for medical data authentication: a survey. *Multimed Tools Appl* 1-33:30165–30197
16. Aouissaoui I, Bakir T, Sakly A (2021) Robustly correlated key-medical image for DNA-chaos based encryption. *IET Image Process* 15:2770–2786
17. Arunkumar S, Subramaniaswamy V, Sivaramakrishnan N (2018) Reversible data hiding scheme using modified histogram shifting in encrypted images for biomedical images. *Int J Pure Appl Math* 119(12e): 13233–13239
18. Arunkumar S, Subramaniaswamy V, Vijayakumar V, Chilamkurti N, Logesh R (2019) SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement* 139:426–437
19. Ashour AS, Dey N (2017) Security of multimedia contents: a brief. In: *Intelligent techniques in signal processing for multimedia security*. Springer, Cham, pp 3–14
20. Atawneh S, Almomani A, Al Bazar H, Sumari P, Gupta B (2017) Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimed Tools Appl* 76:18451–18472
21. Atee HA, Ahmad R, Noor NM, Rahma AMS, Aljeroudi Y (2017) Extreme learning machine based optimal embedding location finder for image steganography. *PLoS One* 12:1–23
22. Bachrach M, Shih FY (2017) Survey of image steganography and steganalysis. *Multimedia. Security. Watermarking, Steganography, Forensics* 2:201–214
23. Balasamy K, Suganyadevi S (2020) A fuzzy-based ROI selection for encryption and watermarking in medical image using DWT and SVD. *Multimed Tools Appl*:7167–7186
24. Balasamy K, Suganyadevi S (2021) A fuzzy based ROI selection for encryption and watermarking in the medical image using DWT and SVD. *Multimed Tools Appl* 80(5):7167–7186
25. Balasubramanian C, Selvakumar S, Geetha S (2014) High payload image steganography with reduced distortion using octary pixel pairing scheme. *Multimed Tools Appl* 73:2223–2245
26. Bamal R, Kasana SS (2019) Dual hybrid medical watermarking using Walsh-slantlet transform. *Multimed Tools Appl* 78(13):17899–17927
27. Banerjee S, Chakraborty S, Dey N, Kumar Pal A, Ray R (2015) High payload watermarking using residue number system. *Int J Image Graph Signal Process* 3:1–8
28. Banerjee S, Chakraborty S, Dey N, Kumar Pal A, Ray R (2015) High payload watermarking using residue number system. *Int J Image Graph Signal Process* 7:1–8
29. Banu SA, Amirtharajan R (2020) A robust medical image encryption in dual-domain: chaos-DNA-IWT combined approach. *Med Biol Eng Comput* 58(7):1445–1458
30. Begum AAS, Nirmala S (2018) Secure visual cryptography for medical image using modified cuckoo search. *Multimed Tools Appl* 77(20):27041–27060
31. Begum M, Uddin MS (2020) Digital image watermarking techniques: a review. *Information* 11(2):110
32. Benssalah M, Rhaskali Y, Drouiche K (2021) An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimed Tools Appl* 80(2):2081–2107
33. Bhabatosh C (1977) *Digital image processing and analysis*, pp 469. PHI Learning Pvt. Ltd ISBN: 9788120343252
34. Cao W, Zhou Y, Chen CLP, Xia L (2017) Medical image encryption using edge maps. *Signal Process* 132:96–109
35. Chakraborty S, Jalal AS, Bhatnagar C (2017) LSB based nonblind predictive edge adaptive image steganography. *Multimed Tools Appl* 76:7973–7987
36. Chandel R, Gupta G (2013) Image filtering algorithms and techniques: a review. *Int J Adv Res Comput Sci Softw Eng* 3(10)
37. Chandel GS, Sharma V, Singh UP (2013) Different image encryption techniques-survey and overview. *Int J Adv Res Comput Sci Softw Eng* 3:434–437
38. Chauhan DS et al (2019) Combining Mexican hat wavelet and spread spectrum for adaptive watermarking and its statistical detection using medical images. *Multimed Tools Appl* 78(10):12647–12661

39. Chen WJ, Chang CC, Le THN (2010) High payload steganography mechanism using hybrid edge detector. *Expert Syst Appl* 37(4):3292–3301
40. Chen YP, Fan TY, Chao HC (2021) Wmnet: a lossless watermarking technique using deep learning for medical image authentication. *Electron* 10:1–12
41. Chirakkarottu S, Mathew S (2020) A novel encryption method for medical images using 2D Zaslavski map and DNA cryptography. *SN Appl Sci* 2:1
42. Collins J, Agaian S (2016) High capacity image steganography using adjunctive numerical representations with multiple bitplane decomposition methods. *Int J Cryptogr Inf Secur* 6:01–21
43. Conde JG, De S, Hall RW, Johansen E, Meglan D, Peng GC (2010) Telehealth innovations in health education and training. *Telemed E-Health* 16(1):103–106
44. Dhawan S, Gupta R (2021) Analysis of various data security techniques of steganography: a survey. *Information Security J* 30:63–87
45. Du JX, Huang DS, Zhang GJ, Wang ZF (2006) A novel full structure optimization algorithm for radial basis probabilistic neural networks. *Neurocomputing* 70:592–596
46. Elbasi E (2020) M-SVD based quality measurement in hybrid non-blind watermarked medical images. In: 43rd international conference on telecommunications and signal processing (TSP). IEEE, pp 506–510
47. El-Shafai W, Khallaf F, El-Rabaie ESM et al (2021) Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. *J Ambient Intell Humaniz Comput* 12:9007–9035
48. Eze P, Parampalli U, Evans R, Liu D (2020) A new evaluation method for medical image information hiding techniques. In: 2020 42nd annual international conference of the IEEE engineering in Medicine & Biology Society (EMBC). IEEE, pp 6119–6122
49. Eze P, Udaya P, Evans R (2018) Medical image watermark and tamper detection using constant correlation spread spectrum watermarking. *Int J Comput Electr Autom Control Inf Eng* 12(3):107–114
50. Eze P et al (2019) Integrity verification in medical image retrieval systems using spread Spectrum steganography. In: Proceedings of 2019 on international conference on multimedia retrieval, pp 53–57
51. Fang Y, Liu J, Li J, Yi D, Cui W, Xiao X, Bhatti UA (2021) A novel robust watermarking algorithm for encrypted medical image based on Bandelet-DCT. In: Innovation in medicine and healthcare. Springer, Singapore, pp 61–73
52. Fares K et al (2021) DCT & DWT based watermarking scheme for medical information security. *Biomed Signal Process Control* 66:102403
53. Fatima A, Nishchal NK (2018) Optical image encryption using a triplet of functions. *Opt Eng* 57(3): 033103
54. Fotopoulos V, Stavrinou M, Skodras A (2008) Medical image authentication and self-correction through an adaptive reversible watermarking technique. In: Proceedings of the 8th IEEE international conference on bioinformatics and BioEngineering, pp 1–5
55. Gao L, Zhang Y, Li G (2020) Reversible watermarking in medical images using sub-sample and multiple histogram modification. *J Inf Technol Res (JITR)* 13(4):75–90
56. Goléa NE-H, Melkemi KE (2019) ROI-based fragile watermarking for medical image tamper detection. *Int J High Perform Comput Netw* 13(2):199
57. Grajeda-Marín IR, Montes-Venegas HA, Marcial-Romero JR, Hernandez-Servin JA, De Ita G (2016) An optimization approach to the TWPVD method for digital image steganography. In: Mexican conference on pattern recognition. Springer, Cham, pp 125–134
58. Guesmi R, Farah MAB (2021) A new efficient medical image cipher based on hybrid chaotic map and DNA code. *Multimed Tools Appl* 80:1925–1944
59. Gupta S, Baraskar R, Agrawal S (2019) A survey on reversible watermarking techniques for image security, pp 826–836
60. Hajduk V, Levický D (2017) Accelerated cover selection steganography. In: 2017 27th international Conference RADIOELEKTRONIKA (RADIOELEKTRONIKA). IEEE, pp 1–4
61. Hamid N, Yahya A, Ahmad RB, Al-Qershi O (2012) Characteristic region based image steganography using speeded-up robust features technique. In: International conference on future communication networks. IEEE, pp 141–146
62. Hamza A et al (2021) Novel secure hybrid image steganography technique based on pattern matching. In: KSII transactions on internet and information systems (TIIS) 15.3
63. Hamza R, Yan Z, Muhammad K, Bellavista P, Titouna F (2020) A privacy-preserving cryptosystem for IoT E-healthcare. *Inf Sci* 527:493–510
64. Harshitha M et al (2021) Secure medical data using symmetric cipher based chaotic logistic mapping. In: 7th international conference on advanced computing and communication systems ICACCS, vol 1. IEEE



65. Hizukuri A, Nakayama R, Nara M, Suzuki M, Namba K (2021) Computer-aided diagnosis scheme for distinguishing between benign and malignant masses on breast DCE-MRI images using deep convolutional neural network with Bayesian optimization. *J Digit Imaging* 34:116–123
66. Hong W (2012) Human visual system based data embedding method using quadtree partitioning. *Signal Process Image Commun* 27:1123–1133
67. Hosny KM, Darwish MM (2021) New geometrically invariant multiple zero-watermarking algorithm for color medical images. *Biomed Signal Process Control* 70:103007
68. Hosny KM, Darwish MM, Fouda MM (2021) Robust color images watermarking using new fractional-order exponent moments. *IEEE Access* 9:47425–47435
69. Hosny KM, Darwish MM, Li K, Salah A (2018) Parallel multi-core CPU and GPU for fast and robust medical image watermarking. *IEEE Access* 6:77212–77225
70. Huang DS, Du JX (2008) A constructive hybrid structure optimization methodology for radial basis probabilistic neural networks. *IEEE Trans Neural Netw* 19:2099–2115
71. Huma F et al (2021) Wavelet and LSB-based encrypted watermarking approach to Hide Patient's information in medical image. In: *Proceedings of international joint conference on advances in computational intelligence*. Springer, Singapore, pp 89–104
72. Iskandar MW, Adiwijaya (2019) An implementation of text hiding in medical images based on graph coloring for android devices. *J Phys Conf Ser* 1192(1):012008
73. Jain M (2018) Medical image steganography using dynamic decision tree, piecewise linear chaotic map, and hybrid cryptosystem. *Int J Appl Eng Res* 13(15):12353–12363
74. Jain M, Choudhary RC, Kumar A (2016) Secure medical image steganography with RSA cryptography using decision tree. In: *2nd international conference on contemporary computing and informatics (IC3I)*. IEEE, pp 291–295
75. Jain M, Kumar A, Choudhary RC (2017) Improved diagonal queue medical image steganography using Chaos theory, LFSR, and Rabin cryptosystem. *Brain Inform* 4(2):95–106
76. Jambhale T, Sudha M (2021) A privacy-preserving hybrid neural-crypto computing-based image steganography for medical images. In: *Intelligent data communication technologies and internet of things: proceedings of ICICI 2020*. Springer, Singapore
77. Janani T, Brindha M (2021) A secure medical image transmission scheme aided by quantum representation. *J Inf Secur Appl* 59:102832
78. Jeevitha S, Amutha Prabha N (2020) Effective payload and improved security using HMT Contourlet transform in medical image steganography. *Heal Technol* 10(1):217–229
79. Jia S, Zhou Q, Zhou H (2017) A novel color image watermarking scheme based on DWT and QR decomposition. *J Appl Sci Eng* 20(2):193–200
80. Kabbai L, Abdellaoui M, Douik A (2016) Hybrid local and global descriptor enhanced with colour information. *IET Image Process* 11(2):109–117
81. Kadhim IJ, Premaratne P, Vial PJ (2020) High capacity adaptive image steganography with cover region selection using dualtree complex wavelet transform. *Cogn Syst Res* 60:20–32
82. Kadhim IJ et al (2019) Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. *Neurocomputing* 335:299–326
83. Kahlessenane F et al (2021) A DWT based watermarking approach for medical image protection. *J Ambient Intell Humaniz Comput* 12(2):2931–2938
84. Kamal ST, Hosny KM, Elgindy TM, Darwish MM, Fouda MM (2021) A new image encryption algorithm for Grey and color medical images. *IEEE Access* 9:37855–37865
85. Kamalraj AMS, Venkatesan GKDP, Ravi RV (2020) Digital watermarking techniques for image security: a review. *J Ambient Intell Humaniz Comput* 11(8):3221–3229
86. Karar ME, Hemdan EED, Shouman MA (2021) Cascaded deep learning classifiers for computer-aided diagnosis of COVID-19 and pneumonia diseases in X-ray scans. *Complex Intell Syst* 7(1):235–247
87. Karthik JV, Reddy BV (2014) Authentication of secret information in image stenography. *Int J Comput Sci Netw Secur* 14(6):58
88. Kaur M, Kumar V (2020) A comprehensive review on image encryption techniques. *Arch Comput Methods Eng* 27(1):15–43
89. Kaur J, Pandey S (2018) An adaptive quadtree based transform domain steganography for textual data. In: *International conference on energy, communication, data analytics and soft computing (ICECDS)*, pp 3194–3199
90. Kelkar V, Mehta JH, Tuckley K (2018) A novel robust reversible watermarking technique based on prediction error expansion for medical images. In: *Proceedings of 2nd international conference on Computer Vision & Image Processing*. Springer, Singapore, pp 131–143
91. Khan S (2018) Ant colony optimization (ACO) based data hiding in image complex region. *Int J Electr Comput Eng* (2088–8708) 8(1):379

92. Khan M, Shah T (2014) A novel statistical analysis of chaotic S-box in image encryption. *3D Res* 5(3):16
93. Konyar MZ, Öztürk S (2020) Reed Solomon coding-based medical image data hiding method against salt and pepper noise. *Symmetry* 12(6):899
94. Kumar S, Panna B, Jha RK (2019) Medical image encryption using fractional discrete cosine transform with chaotic function. *Med Biol Eng Comput* 57:2517–2533
95. Laiphrakpam DS, Khumanthem MS (2017) Medical image encryption based on improved ElGamal encryption technique. *Optik* 147:88–102
96. Laishram D, Tuihung T (2018) A survey on digital image steganography: current trends and challenges. In: *Proceedings of 3rd international conference on internet of things and connected technologies (ICIoTCT)*, pp 26–27
97. Li XW, Lee IK (2015) Modified computational integral imaging-based double image encryption using fractional Fourier transform. *Opt Lasers Eng* 66:112–121
98. Li X, Xiao D, Wang QH (2018) Error-free holographic frames encryption with CA pixel-permutation encoding algorithm. *Opt Lasers Eng* 100:200–207
99. Li J, Zhang Z, Li S, Benton R, Huang Y, Kasukurthi MV, Li D, Lin J, Borchert GM, Tan S, Li G, Ma B, Yang M, Huang J (2020) A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology. *BMC Med Inform Decis Mak* 20:297
100. Li Y, Zhu H, Yu R, Yang G, Xu J (2008) An adaptive blind watermarking algorithm based on DCT and modified watsong's visual model. In: *2008 international symposium on electronic commerce and security*. IEEE, pp 904–907
101. Liao X, Li K, Zhu X, Liu KJR (2020) Robust detection of image operator chain with two-stream convolutional neural network. *IEEE J Sel Top Signal Process* 14(5):955–968
102. Liao X, Yin J, Chen M, Qin Z (2020) Adaptive payload distribution in multiple images steganography based on image texture features. *IEEE Trans Dependable Secure Comput*:1–1. <https://doi.org/10.1109/TDSC.2020.3004708>
103. Liao X, Yu Y, Li B, Li Z, Qin Z (2020) A new payload partition strategy in color image steganography. *IEEE Trans Circuits Syst Video Technol* 30(3):685–696
104. Licks V, Jordan R (2005) Geometric attacks on image watermarking systems. *IEEE MultiMedia* 12(3):68–78
105. Lin CY, Chang SF (2001) A robust image authentication method distinguishing JPEG compression from malicious manipulation. *IEEE Trans Circuits Syst Video Technol* 11(2):153–168
106. Lin C-H et al (2021) Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images *Infosecurity*. *IEEE Access* 9:118624–118639
107. Liu J, Ma J, Li J (2020) Robust watermarking algorithm for medical volume data in internet of medical things. *IEEE Access* 8:93939–93961
108. Liu X et al (2018) Discriminative and robust zero-watermarking scheme based on completed local binary pattern for authentication and copyright identification of medical images. *Medical imaging 2018: imaging informatics for healthcare, research, and applications*. International Society for Optics and Photonics 10579
109. Luo T, Jiang G, Yu M, Xu H, Gao W (2018) Sparse recovery based reversible data hiding method using the human visual system. *Multimed Tools Appl* 77:19027–19050
110. Ma B, Chang L, Wang C, Li J, Li G, Xia Z, Wang X (2021) Double medical images zero-watermarking algorithm based on the chaotic system and ternary accurate polar complex exponential transform. *J Math Imaging Vis* 1-19:1160–1178
111. Martiri E, Baxhaku A, Barolli E (2011) Steganographic algorithm injection in image information systems used in healthcare organizations. In: *Third international conference on intelligent networking and collaborative systems*. IEEE, pp 408–411
112. Mata-Mendoza D, Cedillo-Hernandez M, Garcia-Ugalde F, Cedillo-Hernandez A, Nakano-Miyatake M, Perez-Meana H (2021) Secured telemedicine of medical imaging based on dual robust watermarking. *Vis Comput*:1–18
113. Mathkour H, Al-Sadoon B, Touir A (2008) A new image steganography technique. *2008 Int. Conf Wirel Commun Netw Mob Comput WiCOM 2008*:1–4
114. Meryem B (2018) A short survey on image zero-watermarking techniques based on visual cryptography. *9th Int. Symp Signal, Image, Video Communication*:157–162
115. Miri A, Faez K (2017) Adaptive image steganography based on transform domain via genetic algorithm. *Optik* 145:158–168
116. Mishra P, Bhaya C, Pal AK, Singh AK (2021) A medical image cryptosystem using bit-level diffusion with DNA coding. *J Ambient Intell Humaniz Comput*:1–22
117. Mohammed ZF, Abdulla AA (2021) An efficient CAD system for ALL cell identification from microscopic blood images. *Multimed Tools Appl* 80:6355–6368
118. Mondal J, Swain D (2020) A 3-layer RDH method in encrypted domain for medical information security. *Int J Electron Secur Digit Forensics* 12(1):1–15

119. Muhammad K, Ahmad J, Rehman NU, Jan Z, Sajjad M (2017) CISSKA-LSB: color image steganography using stego keydirected adaptive LSB substitution method. *Multimed Tools Appl* 76:8597–8626
120. Mungmode S, Sedamkar RR, Kulkarni N (2016) A modified high-frequency adaptive security approach using steganography for region selection based on threshold value. *Procedia Comput Sci* 79:912–921
121. Nagaraj S, Raju GSV, Koteswara Rao K (2015) Image encryption using elliptic curve cryptography and matrix. *Procedia Comput Sci* 48(C):276–281
122. Naidu CD, Koppu S, Viswanatham VM, Aarthy SL (2014) Cryptography based medical image security with LSB blowfish algorithms. *ARPN Journal of Engineering and Applied Sciences* 9(8)
123. Nazari M, Mehrabian M (2021) A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images. *Multimed Tools Appl* 80(7):10615–10655
124. Nguyen TD, Arch-Int S, Arch-Int N (2016) An adaptive multi bit-plane image steganography using block data-hiding. *Multimed Tools Appl* 75(14):8319–8345
125. Novamizanti L, Wahidah I, Wardana NPDP (2020) A robust medical images watermarking using FDCuTDCT-SVD. *Int J Intell Eng Syst* 13(6):266–278
126. Özcan FBM, Karakis R, Güler I (2020) Steganalysis on medical images with support vector machine. In: 28th signal processing and communications applications conference SIU. IEEE
127. Özkaynak F (2017) Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals. In: 2017 international conference on computer science and engineering (UBMK). IEEE, pp 621–624
128. Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. *Signal Process* 138:129–137
129. Pomponiu V, Cavagnino D, Botta M (2018) Data hiding in the wild: where computational intelligence meets digital forensics. In: *Surveillance in action*. Springer, Cham, pp 301–331
130. Priya S, Santhi B (2019) A novel visual medical image encryption for secure transmission of authenticated watermarked medical images. *Mobile networks and applications*:1–8
131. Priyadarshini A, Umamaheswari R, Jayapandian N, Priyananci S (2021) Securing medical images using encryption and LSB steganography. In: *International conference on advances in electrical, computing, communication and sustainable technologies (ICAECT)*. IEEE, pp 1–5
132. Qi G, Gong L, Song Y, Ma K, Zheng Y (2021) Stabilized medical image attacks. *arXiv preprint arXiv: 2103.05232*
133. Rabie T, Kamel I (2017) High-capacity steganography: a global-adaptive-region discrete cosine transform approach. *Multimed Tools Appl* 76:6473–6493
134. Raja SP (2019) Multiscale transform-based secured joint efficient medical image compression-encryption using symmetric key cryptography and ebcot encoding technique. *Int J Wavelets Multiresolution Inf Process* 17:1950034
135. Rajendran S, Doraipandian M (2021) Chaos based secure medical image transmission model for IoT-powered healthcare systems. *IOP conference series: materials science and engineering*. Vol. 1022. No. 1. IOP Publishing
136. Ran Q, Yuan L, Zhao T (2015) Image encryption based on nonseparable fractional Fourier transform and chaotic map. *Opt Commun* 348:43–49
137. Ravichandran D, Banu SA, Murthy B et al (2021) An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. *Med Biol Eng Comput* 59:589–605
138. Reddy PR, Prasad MV, Rao DS (2009) Robust digital watermarking of color images under noise attacks. *Int J Recent Trends Eng* 1(1):111–116
139. Renukalatha S, Suresh KV (2017) Automatic ROI extraction in Noisy medical images. *ICTACT J Image Video Process* 7(4):1505–1514
140. Reshma VK, Vinod Kumar RS (2021) Pixel prediction-based image steganography by support vector neural network. *Comput J* 64(5):731–748
141. Rocek A, Javornik M, Slavicek K, Dostál O (2021) Zero watermarking : critical analysis of its role in current medical imaging. *J Digit Imaging* 34:204–211
142. Sadek E, AbdelSabour Seada N, Ghoniemy S (2020) Computer vision techniques for autism symptoms detection and recognition: a survey. *Int J Intell Comput Inf Sci* 20(2):89–111
143. Sahoo S, Sahoo SS (2020) A new COVID-19 medical image steganography based on dual encrypted data insertion into minimum mean intensity window of LSB of X-ray scans. In: 2020 IEEE 17th India council international conference (INDICON), pp 1–6
144. Sajadi S, Fathi A (2020) Genetic algorithm based local and global spectral features extraction for ear recognition. *Expert Syst Appl* 159:113639
145. Salameh JNB (2019) A new approach for securing medical images and Patient’s information by using a hybrid system. *Int J of Computer Sci Netw Secur* 19(4):28–39

146. Sallee P (2003) Model-based steganography. In international workshop on digital watermarking. Springer, Berlin, Heidelberg, pp 154–167
147. Santhi B, Dheeptha B (2016) A novel edge-based embedding in medical images based on a unique key generated using sudoku puzzle design. SpringerPlus 5(1):1–16
148. Santoso B (2019) Color-based microscopic image steganography for telemedicine applications using pixel value differencing algorithm. J Phys Conf Ser 1175(1):012057
149. Sathua SK, Dash A, Behera A (2017) Removal of Salt and Pepper noise from Gray-Scale and Color Images: An adaptive approach arXiv preprint arXiv 5:117–126
150. Seth D, Ramanathan L, Pandey A (2010) Security enhancement: combining cryptography and steganography. Int J Comput Appl 9(11):3–6
151. Setiadi DRIM et al (2019) Secure reversible data hiding in the medical image using histogram shifting and RC4 encryption. International Seminar on Application for Technology of Information and Communication (iSemantic):1–6
152. Shahzad A, Ahmad T, Doja MN (2017) A novel edge-based chaotic steganography method using neural network. In: Proceedings of the 5th international conference on Frontiers in intelligent computing: theory and applications, pp 467–475
153. Shanthan BH, Bist AS, VijendraBabu D (2021) Medical image Detection & Privacy Management with Elliptic Curve GOPSO cryptographic optimization technique on the internet of health things
154. Sharma S, Kumar V (2018) Performance evaluation of 2D face recognition techniques under image processing attacks. Modern Physics Letters B 32(19):1850212
155. Shehab A et al (2018) Secure and robust fragile watermarking scheme for medical images. IEEE Access 6: 10269–10278
156. Shen S, Huang L, Tian Q (2015) A novel data hiding for color images based on pixel value difference and modulus function. Multimed Tools Appl 74(3):707–728
157. Shen Y, Tang C, Xu M, Lei Z (2021) Optical selective encryption based on the FRFCM algorithm and face biometric for the medical image. Opt Laser Technol 138:106911
158. Singh AK, Dave M, Mohan A (2016) Hybrid technique for robust and imperceptible multiple watermarking using medical images. Multimed Tools Appl 75(14):8381–8401
159. Singh AK, Kumar B, Dave M, Mohan A (2014) Robust and imperceptible dual watermarking for telemedicine applications. Wirel Pers Commun 80(4):1415–1433
160. Singh AK, Kumar B, Singh SK, Ghreera SP, Mohan A (2018) Multiple watermarking technique for securing online social network contents using Backpropagation neural network. Futur Gener Comput Syst 86:926–939
161. Singh A, Raghuvanshi N, Dutta MK, Burget R, Masek J (2016) An SVD based zero watermarking scheme for authentication of medical images for telemedicine applications. 2016 39th Int Conf Telecommun Signal Process TSP 2016:511–514
162. Singh L, Singh AK, Singh PK (2020) Secure data hiding techniques: a survey. Multimed Tools Appl 79: 15901–15921
163. Singh AK, Kumar B, Singh G, Mohan A (2017) Secure spread Spectrum based multiple watermarking technique for medical images. In: Medical image watermarking. Springer, Cham, pp 125–157
164. Singh S, Singh R, Singh AK, Siddiqui TJ (2018) SVD-DCT based medical image watermarking in NSCT domain. In: Quantum computing: an environment for intelligent large scale real application. Springer, Cham, pp 467–488
165. Song C, Sudirman S, Merabti M, Llewellyn-Jones D (2010) Analysis of digital image watermark attacks. In: 7th IEEE consumer communications and networking conference, pp 1–5
166. Soualmi A, Alti A, Laouamer L (2018) A new blind medical image watermarking based on weber descriptors and Arnold chaotic map. Arab J Sci Eng (Springer Sci Bus Media BV) 43(12):7893–7905
167. Soualmi A, Alti A, Laouamer L (2021) A novel blind watermarking approach for medical image authentication using MinEigen value features. Multimed Tools Appl 80(2):2279–2293
168. Stoyanov B, Stoyanov B (2020) BOOST: medical image steganography using nuclear spin generator. Entropy 22(5):501
169. Subhedar MS, Mankar VH (2014) Current status and key issues in image steganography: a survey. Comput Sci Rev 13–14:95–113
170. Surekha B, Swamy GN (2011) A spatial domain public image watermarking. Int J Secur Its Appl 5(1):1–12
171. Tan Y, Qin J, Tan L, Tang H, Xiang X (2018) A survey on the new development of medical image security algorithms. Springer International Publishing, p 11065 LNCS
172. Tan Y, Qin J, Tan L, Tang H, Xiang X (2018) A survey on the new development of medical image security algorithms. In: International conference on cloud computing and security, pp 458–467
173. Thakkar FN, Srivastava VK (2017) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl 76:3669–3697

174. Thakur S, Singh AK, Ghrera SP, Elhoseny M (2019) Multi-layer security of medical data through watermarking and chaotic encryption for telehealth applications. *Multimed Tools Appl* 78(3):3457–3470
175. Thakur S, Singh AK, Ghrera SP, Mohan A (2020) Chaotic based secure watermarking approach for medical images. *Multimed Tools Appl* 79(7):4263–4276
176. Thanki R, Kothari A (2020) Multi-level security of medical images based on encryption and watermarking for telemedicine applications. *Multimed Tools Appl* 80(3):4307–4325
177. Thanki R et al (2017) A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing (CS) theory. *Imaging Sci J* 65(8):457–467
178. Thanki R et al (2017) An efficient medical image watermarking scheme based on FDCuT–DCT. *Eng Sci Technol Int J* 20(4):1366–1379
179. Tsai HH, Sun DW (2007) Color image watermark extraction based on support vector machines. *Inf Sci (NY)* 177:550–569
180. Ud Din S, Jan Z, Sajjad M, Hussain M, Ali R, Ali A, Lee S (2020) Secure exchange of medical data using a novel real-time biometric-based protection and recognition method. *Electronics* 9(12):2013
181. Ulutas G, Ustubioglu A, Ustubioglu B, Nabiyeve VV, Ulutas M (2017) Medical image tamper detection based on passive image authentication. *J Digit Imaging* 30:695–709
182. Uma Maheswari S, Jude Hemanth D (2017) Performance enhanced image steganography systems using transforms and optimization techniques. *Multimed Tools Appl* 76:415–436
183. Venkatraman S, Abraham A, Paprzycki M (2004) Significance of steganography on data security. In: Abraham A, Paprzycki M (eds) *International conference on information technology: coding and computing, 2004. Proceedings. ITCC, vol 2*. IEEE
184. Venugopal Reddy CH, Siddaiah P (2015) Hybrid LWT-SVD watermarking optimized using metaheuristic algorithms along with encryption for medical image security. *Signal Image Process* 6:1–95
185. Vijayakumar A, Sivaraman R, Avila J (2021) Cellular automata governed confidentiality preservation of medical image on reconfigurable Hardware. In: *2nd international conference on secure cyber computing and communications (ICSCCC)*, pp 34–38
186. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. *IEEE Trans Image Process* 13(4):600–612
187. Wang XY, Gu SX, Zhang YQ (2015) Novel image encryption algorithm based on cycle shift and chaotic system. *Opt Lasers Eng* 68:126–134
188. Wang R, Shaocheng H, Zhang P, Yue M, Cheng Z, Zhang Y (2020) A novel zero-watermarking scheme based on variable parameter chaotic mapping in NSPD-DCT domain. *IEEE Access* 8:182391–182411
189. Wang H, Wang S (2004) Cyber warfare: steganography vs. steg analysis. *Commun ACM* 47(10):76–82
190. Gan DSHY, Gromiha PGMM (2010) *Advanced intelligent computing theories and applications*. Springer, Heidelberg, pp 490–498
191. Wu J-X et al (2020) Two-round symmetric cryptography for medical image Infosecurity against-hacker attacks in a picture archiving and communication system. *IEEE Access* 8:181698–181711
192. Xie Y, Ning L, Wang M, Li C (2019) Image enhancement based on histogram equalization. In *journal of physics: conference series* (Vol. 1314, no. 1, p. 012161). IOP publishing
193. Xu S, Jiang S, Min W (2017) No-reference/blind image quality assessment: a survey. *IETE Tech Rev (Inst Electron Telecommun Eng India)* 34:223–245
194. Yahya A (2019) *Steganography techniques for digital images*. Springer International Publishing
195. Yang Y, Zhang W, Liang D, Yu N (2018) An ROI-based high capacity reversible data hiding scheme with contrast enhancement for medical images. *Multimed Tools Appl* 77:18043–18065
196. Yin S, Liu J, Teng L (2020) Improved elliptic curve cryptography with homomorphic encryption for medical image encryption. *Int J Netw Security* 22(3):419–424
197. Zhang Q, Liu L, Wei X (2014) Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. *AEU Int J Electron Commun* 68:186–192
198. Zhang Y et al (2019) Multiple robustness enhancements for image adaptive steganography in lossy channels. *IEEE Trans Circuits Syst Video Technol* 30(8):2750–2764
199. Zhao WB, Huang DS, Du JY, Wang LM (2004) Genetic optimization of radial basis probabilistic neural networks. *Int J Pattern Recognit Artif Intell* 18(08):1473–1499
200. Zheng B, Yuan S, Slabaugh G, Leonardis A (2020) Image denoising with learnable bandpass filters. In: *Proc IEEE Comput Soc Conf Comput Vis pattern Recognit*, pp 3633–3642