Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 1, 2026

SECURING MEDICAL IMAGES WITH ENCRYPTION-BASED WATERMARKING TECHNIQUES

[1]Huzaifah Bin Khawar, [2]Talha Nadeem, [3]Muhammad Zarar, [4] Hood Khizer

[1] AI Researcher, Research and Development Department, Trouve Labs, AHOY DMCC and The Superior University Lahore, Pakistan huzaifahkhawar.ieee@gmail.com

[2] Systems Architect AI/ML, Research and Development Department, Trouve Labs, AHOY DMCC and The Superior University Lahore, Pakistan talhanadeem.ieee@gmail.com

[3] AI Researcher, Research and Development Department, Trouve Labs, AHOY DMCC and The Superior University Lahore, Pakistan muhammadzarar.ieee@gmail.com

[4] CEO Trouve Labs, CTO AHOY DMCC, Research and Development Department, Trouve Labs,

DOI:https://doi.org/10.5281/zenodo.24134711

Keywords
Watermarking, medical image, discrete wavelet transform, singular value decomposition, quantization, chaos cryptosystem.

Article History
Received: 10 Jan, 2026
Accepted: 18 Jan, 2026
Published: 31 Jan, 2026

Copyright @Author

Corresponding Author: *
Talha Nadeem*

Abstract

This paper presents an encryption-based image-watermarking algorithm for wavelet-based medical images using customized quantization of wavelet coefficients and a chaotic Singular Value Decomposition (SVD) cipher. To strengthen resilience and provide an additional security layer, an SVD-CHAOS embedding and extraction process scrambles the watermark logo during preprocessing. An r-level discrete wavelet transform is applied to the host image during embedding, while adaptive low-bit quantization selects high-frequency coefficients to carry the scrambled watermark. The method is designed to withstand common attacks and recover the hidden watermark without significant degradation of diagnostic image quality. Performance is evaluated using peak signal-to-noise ratio (PSNR), normalized correlation (NC), mean squared error (MSE), and structural similarity (SSIM), and the reported results are compared with related techniques.

1. INTRODUCTION

Digital watermarking is a data hiding technique that involves embedding information, such as a number, text or image, into the digital media, such as audio, video or an image, to protect the copyright and investor and legal rights of the owner. One of the requirements of sharing is medical image where the confidential data of the patient is not to be accessed by third parties and so sharing them via internet has become extremely common nowadays in telediagnosis, telesurgery and teleconsultation [1]. A significant portion of

data storage and transfer is encompassed by most hospitals and healthcare systems including medical images, patient data and administrative records.

This data includes patient information, medical images, among others, which should be protected from any malicious intent. Three requirements are needed to ensure that the information of a patient is not attacked, i.e., integrity, medical images privacy, and authenticity of medical images are needed [2]. Currently, medical images do take up a large percentage of all medical information in the hospitals and digital information management systems are emerging to play an increasing role in the modern medical system. But, since the popularization and application of the Internet, there are more and more information security problems. If we send the diagnosis medical pictures via the Internet, the patients' personal information is written on the medical pictures, and you can counterfeit, tamper or rearrange it.

Medical image digital watermarking [3]-[4], or, in other words, inserting the personal information into the medical images in the form of a digital watermark, is a good solution to this issue. Currently, the research in the field of medical image watermarking mainly revolves around two aspects: the spatial domain and the transform domain. Common transform domains include Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). All add watermarks by changing the gray level of some of the pixels, or change some of the coefficient of the transform domain. Small in computation and compatible with international data compression standards (JPEG, MPEG) the DCT is now the hotspot in the research area of frequency domain digital watermarking algorithms [4]-[5].

In general, literature tends to use the approach to embed the watermark information in a Region Of Non-Interest (RONI) in the image considering special demands of preserving the medical image focal zones. Medical images Region of Interest (ROI) can be considered as the focus of interest of the pathological region of interest or the medical clinic data, and affix the watermark at ROI may cause the misdiagnosis. Nevertheless, ROI identification can be time and energy consuming, and an error during the process can adversely harm the diagnosis of a doctor [6]. Geometric attack is, as yet, one of the major issues to be resolved in the research area on digital watermarking of medical images.

Not yet the research on how to fight effectively the conventional attacks and geometric attacks. In fact the medical digital watermark image would in most cases be compromised by both attacks. In addition, the study of medical images needs to tackle the problem of disclosing and changing patients' information or privacy in the process of watermark extraction. Given the above problem, some kind of pretreatment can be carried out, which can be called encryption as some secondary protection to achieve the improvement of the protection of the watermark information [7]-[8]. Medical images should have their copyright safeguarded using image watermark. Patient's information can be protected from illegal access by watermarking techniques.

These applications comprise medical imaging, telehealth and telemedicine among others. Medical imaging involves the visualization of tissues, organs or any other section of the body, using information and communications technologies. Alongside the fundamental needs of

a standard watermarking system as discussed above there are other unique features required of the medical watermarking system. These are explained in greater detail below [9]. Image imperceptibility is referred to and can be measured with statistical criteria such as SSIM (Structural Similarity Index) [18] that quantifies the difference between two similar images as a quality reference unit between the original and modified image:

• Imperceptibility: The amount of invisibility of a watermarked image in comparison to non-watermarked PSNR (peak signal-to-noise ratio).

• Reversibility: The ability to confirm that the image has not been altered without permissions, due to the image quality, the applied method for medical watermarking should be reversible, that is, one should be able to exactly recover the original image after extracting the watermark.

• Authentication: Determining who the source of the image is, and confirming that the image is that of the relevant patient. This paper introduces a powerful crypto-watermarking algorithm of medical images on the ground of a DWT (discrete wavelet transform) and a Chaos cryptosystem-SVD (Singular value decomposition). The rest of this paper will be structured in the following way: Section 2 will provide an overview of digital Image watermarking. The research material of Section 3 is the counterpart of this section and provides a brief overview of the latest approaches.

In Section 4 introduces basic concepts of (DWT, SVD and LBM quantization) and PROPOSED CHAOS-SVD CRYPTOSYSTEM. Section 4 contains the suggestions of watermark embedding and extraction steps. The experimental results and performance comparisons are given in Section 6. Finally, the conclusion is given in Section 6.

2. AN OVERVIEW OF DIGITAL WATERMARKING

The watermarking embedder Implantation of a message in digital media Referred to as the watermarking embedder, the watermarking embedder begins the process of creating the watermarked image by adding both cover and watermark image data. The aim is to present a natural and/or copyrighted digital media. A digital watermarking has structures that consist of two main parts: the embedding of watermark which comes first and is the watermark identification and recovery comes second. To watermark a digital document, say, images, you will require an image (I), a watermark(W) having the confidential information, a security key (K) and an embedding algorithm to obtain a watermarked image (IW).

The signature and the cover image(I) are passed through the embedding algorithm which produces the watermarked image (IW) with additional parameters such as a scaling factor (strong coefficient) to be used to extend the watermarking embedded. The embedding and the extraction operation is shown in figure (1). The watermark is considered to be robust if it is embedded in such a way that the watermark can survive even if the watermarked image (IW*) go through severe distortions. The watermark should be highly challenging to delete, or cause damage by the attacks to the media. Watermark extractor or detector is a two-step process, the first being Watermark retrieval, a sequence otherwise known as retrieved watermarks is extracted using some scrambling algorithms.

In step 2, the watermarks embedded in the suspected signal that may include watermarks are detected and retrieved from the suspected signal. The second step would approximately involve an

analysis and comparison between the unreliable watermark and the original watermark and the outcome may be various forms of confidence assessment characterizing the reflection between the extracted watermark and the original watermark. The Watermark (W) is extracted after the extraction loads the watermarked, normal or corrupted image (LW*).

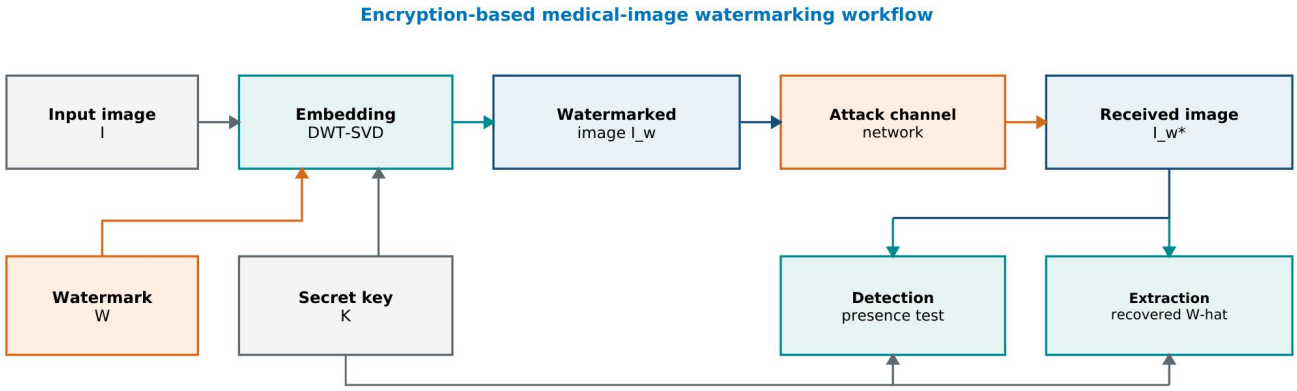


Figure 1. Encryption-based medical-image watermarking workflow

2.1. Digital Watermarking Requirements

Since the applications of the digital watermarking are diverse, each of the applications has different requirements. In global, Digital watermarking system has the following set of requirements:

Transparency: his is a demand for any watermarking technique, to be transparent to the receiving user. Copyright material has to be well visible in the gadget of the legitimate owner. Only the watermark detector has the ability to see the watermark.

Ease of embedding and retrieval: Ease of embedding and retrieval: ease of integration and retrieval: ideally, the watermark of the digital media should be programmable so that it can be done automatically. The number of calculations required from the algorithm adopted should be reduced.

Robustness: It is the ability to withstand the embedded mark, even though the watermarked image is subjected to a set of attacks or intruder(s). Intended or unintended actions with the potential to modify the data counts as an attack. In this direction, studies failed to consider the maliciousness of the attack, and the intentions and intent of the attacker to desire to destroy the mark or to substitute. With this aim, the notion of security has arisen.

Security: Only authorized parties have access to the information in the watermark. Only they should be able to read the watermark information. The content of the watermark can be changed by the legitimate parties. Encryption is an appropriate way of deterring unauthorized access to watermarked data.

Effect on bandwidth: Watermarking should be done in such a way that it does not increase the amount of bandwidth required for transmission. Watermarking will only be denied on the unnecessary bandwidth.

Interoperability: Digitally watermarked digital content must be interoperable to ensure that it can be easily accessed via the different networks and played on a wide variety of playback devices, both watermark aware and unaware.

2.2. Importance of Digital Watermarking

Today, the rate of Internet dissemination is so rapid that copyrights are no longer significant since many copyrighted material in pictures, music and videos are now accessible via the

Internet. But we find a high piracy risk as well to the content owners. Large capacity digital recording equipment makes this threat of piracy more likely. The delivery of the digital media is ideal on the Internet; without having to stock and even remove from the warehouses, it is relatively inexpensive and the delivery time is very short. Any other individual or group of individuals capable of generating exact copies of digital data without corrupting the original information and share the copies over the network.

Piracy is also at a high risk to content owners. This risk of piracy is heightened by the number of high-quality digital recording equipment. Pirated copies were generally of lower quality than the original when the only medium available to the average customer to do this was on a made-up tape and usually the quality of a second-generation pirated copy (a copy of a copy) was way worse. However, with digital recording devices, songs and movies can be recorded with little, if any, degradation in quality. With these kinds of recording devices and the Internet as a medium for disseminating, potential pirates can easily record and disseminate copyrighted information without the proper compensation being paid to the original copyright holder.

This has resulted in a great need for distributing secure and reliable data over networks. One such method that aims at resolving this issue is the digital watermarking. The concept of digital watermark is a digital process where a watermark is introduced in the digital content of copyrighted information to safeguard the value of the content and thus cannot be used by unauthorized users. The first owner of technological content turn towards is the cryptography. The most widespread source of the protection of digital content is likely to be encryption. One of the best-developed sciences, it is definitely. Content is coded and only delivered to those who buy the content in a legitimate way and they are supplied with a decryption key.

The encrypted file can then be made public on the Internet, but would be useless to a pirate without an appropriate key. Unfortunately, the seller is unable to monitor the user's activities with respect to the content after the decryption process.

2.3. Classification of Digital Watermark

Besides watermark robustness, watermarks can be classified into some types. From the visibility point of view watermarks can be clustered into visible and invisible types, visible watermarks are perceptible to a viewer like logos which are inserted into or overlaid on images. However, invisible watermarks are undetectable and won't alter the look of the pictures. For our work, it is about invisible watermarks taking care of the privacy of patient information, this time we have to embed the personal information into medical images as a digital watermark.

2.3.1. Visible Watermarks

The idea of logos is extended with the creation of the Visible watermarks. This kind of watermarks can only be added to pictures. The picture is marked with these logos, but in a transparent manner. The watermarks can't be removed by cutting out the center part of the picture. Moreover, such watermarks are not vulnerable to statistical analysis. The disadvantages of visible watermarks are that the quality of the image is ruined, and they can only be noticed by visual inspection. So, they are difficult to find. through special programs or equipment. Graphics, maps and software user interface are some uses of such watermarks.

2.3.2. Invisible Watermark

Invisible watermark is hidden in the content and designed to be beyond normal human's observation. The vision of normal human is not able to identify the differentiation of the original and the shrouded information. Content and /or author authentication as well as detecting unauthorized copier are done with various types of watermarks. It is designed to be so obscure that the wrongful agents can't locate it, but the rightful licensor can easily find it and it will help the licensor to sue a fake infringing party.

2.4. Applications of Digital Watermarking

Digital Watermarks could be used for many applications and include:

2.4.1. Digital Watermarking Technology for Rights Management

A traditional use of watermark is for copyright protection. The primary reason for using watermarks is to identify the owner of the content by an invisible hidden "mark" that is imprinted into the image. The watermark in most instances is applied to the content encryption where the method of securing distribution is through digital watermarking: the content owners to the receivers and the watermark version offers the content owners a chance to track the contents and where the duplications and unlawful utilization are found. If the content is not in the safes of the digital realm anymore and the watermark is gone, the content owner will no longer have a control after the content is given to the consumer.

To maintain the protection and offer the content owners the possibilities to protect the rights and properties of the electronic distributed contents, digital watermark is employed. The owner signature, content ID and content restriction can be etched into the contents, and accompany the contents wherever they go. This mechanism prolongs the opportunity of guarding the contents following the launching of the contents in the open ambiance. The most important technical specifications of this application are as follows:

- The watermark imposes no visible (or audible artifacts) on the normal users.
- The watermark cannot be dependent on the data format.
- The watermark information is resistant to contents manipulations, compression, etc.
- The watermark can be detected and is provided at the cost of the content that is not watermarked.
- The watermark can be identified by some kind of "keys" that are used to identify large number of individual contents uniquely.

2.4.2. Digital Watermarking Technology for Authentication and Tamper Proofing

Contents authentication and tamper proofing are another usage of digital watermark. The aim is not to stop the duplication and theft of the contents, but to offer a way through which the image can be authenticated to guarantee the integrity of the image. Ever since the entry of low-end digital camera into the consumer market it was quickly sprawling into a few more industrial applications also, since the use of a digital image is much more cost effective and also they can save time and cost to the Developing/ Printing/Exposing (DPE) in comparison to a chemical photo. But there are also some essential points to consider regarding some specific uses, when the photos are considered as evidence or the material to some sort of a business judgment.

As an example, insurers of automobiles even sometimes rely on photographs of the damaged vehicle that the repair shop has provided to estimate the cost of repairing their cars. It will be a huge time and cost saver to be able to digitize photos such as these. Nevertheless, the digital photographs could be manipulated to look extra-

damaged, or even created out of nothing, as the editing of the digital photograph is increasingly becoming simpler as some powerful photo-retouching software exists. This can result in massive amounts of extra insurance payout, or possibly even the insurance company's credibility being lost. A type of digital watermark, called tamper-detect watermark, might resolve this problem, and provide a secure environment for the evidence photos.

This feature may be accomplished by applying an authentication signature to a digital image, by embedding a layer of the authentication signature in a subject digital image, using a digital watermark. This extra layer of watermark is then employed as a "sensor" to detect the change. Our recent implementation allows us to determine even the location of the change in the modified picture from the modified picture. We have developed a joint study with a major insurance company in Japan, and confirmed the technical feasibility of the technology to the above-mentioned industrial applications. This application has the following technical requirements:

- Are not seen by the regular users.
- It can be used with compressed image format (which is used by most digital cameras is compatible with JPEG).
- Sensitive to content manipulations, compression, and so on.

2.4.3. Visible Reversible Watermarking for Electronic Distribution

The visible reversible watermark, in comparison to other digital watermarking systems mentioned above, is visible. It is available as a commercial product. IBM's innovative watermarking technology lets the watermark be a visible shape or logo mark (company's logo), which is overlaid on top of the image. Only with the usage of a proper key of decryption, watermark remover software, the mark can be removed (the watermark is reversed). This is done by altering the Discrete Cosine Transformation (DCT) coefficients of the JPEG compressed image based on a pre-defined rule and a visual effect analysis result, to make the image 50% transparent (no complete damage is done).

The key will be used along with the mark removal program to remove the mark from the image. The disappearance of a visible mark might be associated with the purpose of inserting a second invisible mark to be followed. The visible red line on the picture makes self defense content visible, and the content owners can share the entire picture as a sample to other open media, or to the Internet. If a user would like to use a clean version of the image, he/she only has to ask you for an "decryption" key and you'll have to pay for it. This will minimize the security risk and the volume of data to be transmitted for every buy/sell transaction [5].

2.4.4. Watermarking as Communication System

Watermarking system may be considered to be a certain communication. The message P is a payload message that is encoded as a watermark W and modulated and sent over a communication channel to the watermark detector. The cover work in this model constitutes a medium of communication and as such it may be considered a single source of noise. A normal signal processing distortion and attacks are the other source of noise. It will be important to model watermarking as communication, as it is now possible to use known techniques of communication systems here such as coding, spread spectrum communication, modulation,

error correction, matched filtering and communication with side information.

Those techniques could be used to help design key building blocks of a watermarking system which deal with the following:

• How to embedding and detect one bit. Select the area of the image to be processed/embedded.

• Finding the way to be imperceptible with the help of side information.

• Embedding Multiple bits: Use of multiplexing and modulation techniques to embed multiple bits.

• How can I enhance the strength and security of my system, the definition of robustness could be termed as a watermark resistance of my system to normal signal processing and security could be termed as a watermark resistance of my system to intentional attacks [6].

2.5. Distortions and Attacks

First, we need to distinguish two reasons for attack to watermark image: Hostile attack or malicious attack which is an attempt to weaken, eliminate or change the watermark image, and Coincidental attack can be occurred in common image process without the intention to tamper the watermark image. The commonest of its attacks on which a watermarking scheme has to resist is known as loss image compression. The harsh term "attack" can be easily justified: an efficient image compression has to suppress or discard perceptually irrelevant information the invisible watermark. A wide variety of attacks have been described in the literature. There are four general attack methods can be used to attack a watermarking system:

• Removal attacks
• Geometrical attacks
• Cryptographic attacks
• Protocol attacks

2.5.1. Removal Attacks

Removal (simple) attacks are those that attempt to split up and remove the watermark. When an individual attempts to destroy the watermark in the data, it is termed as a removal attack. Filter models borrowed out of statistical signal theory are the most commonly used means. It is believed that the de-noising techniques of merging image with median or high-pass filter, nonlinear truncation or predicting spatial watermarks will be very successful. The aim is to introduce distortion of the host image, which makes the watermark invisible or invisible [4]. If after the attack the watermark is no longer detectable in the image, but the image remains intelligible, then the attack is successful and the image can be used for a specific target that has been determined.

A large number of attack procedures have been suggested:

• Image compression that is lossy (JPEG, JPEG 2000)
• Gaussian noises added.
• Denoising
• Filtering
• Consecutive median and blurring.
• Signal enhancement (sharpening, contrast enhancement)

2.5.2. Compression

The compression is primarily an accidental assault, and this is clearly emerged in the use of multimedia very often. All images (which are now being sent via the Internet) are compressed. The watermark should be able to resist different levels of compression; usually the watermark embedding is suggested to be in the domain where the compression is applied. To make this point clear, consider how the image watermarking, in the Discrete Cosine Transform domain can withstand JPEG compression, compared to the spatial-

domain watermarking. Also the Watermarking in the Discrete Wavelet transforms Domain is also robust to JPEG 2000 compression.

2.5.3. Additive Noise

A random signal (e.g. Gaussian, uniform, Poisson, Bernoulli) is accidentally made on the image. In some applications, the additive noise can be due to Analog to Digital converter (ADC), or due to transmission errors. An attacker can introduce perceptually shaped noise (image-dependent mask) with the largest power that can go unnoticed. This will typically increase its operation level of the correlation detector. Denoising considers the idea that a watermark is a sort of additive noise (that may be modeled statistically) to the original picture. These attacks consist of the following: trimmed mean filtering, local median, midpoint, Wiener filtering and hard and soft thresholding.

2.5.4. Filtering Attacks are Linear Filtering

The image processing operations that are considered as filtering attacks include High-pass, low pass, Gaussian and sharpening filtering etc. In watermarked image, low-pass filtering, does not cause significant damage, but can radically affect the performance since spread-spectrum-like watermarks have non negligible high-frequency spectral contents. To design Robust Filtering Schemes against filtering attacks that might be applied to the watermarked image, the watermark message should be inserted in such a way to have most of its energy in the frequencies which filters change the least.

2.5.5. Statistical Averaging

Averaging and collusion attacks are in this category. If several images of the same embedded watermark exist, it is possible to estimate the watermark by statistically averaging all the images, this is problematic if the watermark does not significantly rely on the data. This is one of the reasons to use perceptual masks to make a watermark. Attack of collusion is a malicious watermark attack removal, where hacker can access multiple copies of identical content with a key or different watermark and attempts to erase the watermark by averaging. The resulting signal can be a good approximation of the watermark that can be utilized in removing it on the watermarked data.

2.5.6. Geometrical Attacks

Unlike to removal attacks, these attacks are not aimed at removing the embedded watermark, but try to distort the watermark detector synchronization with the embedded information. Their aim is to break the correlation detection between the extracted watermark sequence and the original watermark sequence. When the ideal synchronization is restored, the detector would be capable of recovering the watermark that was embedded in it. This can be accomplished by “shuffling” the pixels. The couple matched in the attacked and in the original image has the same values of the pixels. However, the location of these has been altered. These attacks can be divided into attacks with general affine transformation, and projective transformation attacks.

Cropping is a highly ubiquitous form of attack because in most instances the attacker is interested in a small section of the watermarked object, e.g.: portions of a particular picture or frames of a video sequence. With this in mind, in order to survive, the watermark needs to be spread over the dimensions where this attack takes place. In most cases, geometric attack resistance in general has been assumed to rely on one of the following 2 directions: (1) a transform-invariant domain (Fourier-Melline) or (2) an auxiliary template or specially designed periodic

watermarks whose auto-covariance property can be utilized for estimating the geometric attack.

2.5.7. Mosaic Attack

Again, this is very generally applicable, and has the first of two shocking characteristics that it is possible to unmark a picture and it can then be displayed pixel-to-pixel exactly as the marked picture was displayed by a very standard browser [24]. The purpose of an attack was a deployed copyright piracy detection system (fielded watermarking scheme) and a web crawler to download net pictures and check whether there is a copyright watermark. It involves breaking down an image into a series of smaller images, and inserting them into an appropriate sequence into a web page. All popular web browsers display juxtaposed sub-images which are glued together.

This type of attack appears to be extremely general; any marking scheme should make sure there is at least some "minimal size" of the marked-out image, that is, one cannot hide a large mark in a single pixel. So, the mark detector will be deceived by splitting an image into a small number of segments. The best that one can hope for is that the minimal size could be quite small and the method might therefore not be very practical.

2.5.8. Cryptographic Attacks

Cryptographic attacks aim at cracking the security methods in watermarking schemes and thus finding a way to remove the embedded watermark information or to embed misleading watermarks [24]. One method is to use brute force to search for the secret information embedded in it. These attacks, in practice, are not actually feasible to compute, as they are quite complex in the diseases they are used. They involve, among others, direct attacks to find out the secret key or attacks known as collusion attack. Cryptographic attacks are very similar to the attacks used in cryptography. These are the brute force attacks where the secret information being sought is obtained via an exhaustive search.

Because a lot of Watermarking schemes utilize a secret key, secure length of keys is of great importance. One more attack belonging to this regime is known as a so-called Oracle attack that can be utilized to produce an image that does not have a watermark in case the user possesses a watermark detector device.

3. RELATED WORK

The research of medical images needs to tackle the problem of disclosing and changing of patient's information or privacy in the process of watermark extracting. The scrambling technology proposed algorithm is mainly used to provide secondary encryption to secure medical watermark information and enhance the privacy of the watermark of a medical image. It also uses the phase characteristics of the image to determine a balance between the invisibility and strength of the watermark. According to a survey report done by Navas et al. [9] the goals of medical image watermarking (MIW) can be subdivided into integrity and authentication and concealing electronic patient record (EPR) information.

There is a need to embed watermark in the medical images. The digital watermarking scheme can be used to get the correct information and to treat patients appropriately for the needs of privacy, integrity and authenticity. According to the applicability, the medical image watermarking techniques are categorized into three types in the paper [13] such as authentication, data concealing and authentication and data hiding. El-Sheimy N. et al. [10] proposed a new way of securing information relating to patients whereby the medical image is subjected to a discrete wavelet packet transform (DWPT) where the information

is then stored as a watermark. The benefit of having a better frequency resolution representation is known to be achieved using wavelet packets.

Another benefit of wavelet packet is that it is also equipped with the security as the basis is chosen with the help of the secret key. To insert binary watermark in medical images, Rupinder K. in [11] Proposed in a semi-fragile watermarking method that uses the Discrete Cosine Transform (DCT) domain. The binary watermark attains a low degree of corruption of host image hence quality is high. Ray et al. [14] developed a watermarking method which was built on the Rivest Shamir Adleman (RSA) algorithm. First level DWT is used to retrieve various frequency subbands of the host image, whereas, SVs of a watermark are achieved which are further encrypted by using RSA algorithm.

The watermark image is transformed and these encrypted SVs of watermark image are embedded in the transformed host image.These encrypted SVs of watermark image are embedded in transformed host image. It seems that the designed approach creates minimum imperceptibility, but considering that it makes use of the RSA algorithm, the scheme security is enhanced. A novel technique of image watermarking involving Arnold Transform and dual tree complex wavelet transform (DTCWT) was suggested by Kaur et al. [15]. DTCWT divides a host image into several sub-bands, and often is used in a similar way to an encrypted watermark image with Arnold Transform used to encrypt the watermark. More embedding is embedded on all the sub bands especially in the case of inverse DTCWT to create watermarked image.

The developed method, however, is a non-blind method as a prerequisite of the method of extraction, it is necessary to have the original host image. Where the authors have outlined the pertinent attributes of various types of watermarking, this actually assists the researchers in giving roadmap as to the creation of some more watermarking methods. Researchers have proposed a novel dual image watermarking technique in [16] where R Level DWT, the nonsubsampled contourlet transform (NSCT), Arnold Transform and Singular Value Decomposition (SVD) transforms are effectively used. This approach uses dual image watermarks as opposed to set partitioning in hierarchical tree (SPIHT) algorithm that is effectively used to compress the image with the watermark.

Naheed et al. [5] proposed a new watermarking technique of medical image which was based on the interpolation and genetic algorithm (GA). Here, the interpolation and a GA were used to calculate watermark embedding locations. After getting the best location, watermark image was inserted in the position of the original medical image to get the watermarked image. The scrambling transform is the technique used to make the information more difficult to discover or impossible to access, and may be frequently applied in the watermark's pre-processing stage, in image encryption technology. After scrambling transformation, a meaningful watermark image will be meaningless. Without knowing the algorithm for scrambling or the key, the watermark can't be restored by the attacker even after successful extraction of water mark.

In this way the digital image is further encrypted. Furthermore, the correlation of image position after the scrambling, corresponding to the position of the pixel of the image, will be uniformly scattered in the space of the carrier image. This way, the strength of the algorithm can

be enhanced. It is possible to utilize image scrambling algorithm (Arnold transform two-level). It is possible to recover the original image, by using the inverse Arnold transform on the scrambled image, after some iterations. This is a step cycle called Arnold transform. In other words, it is able to retrieve the original image at the definite of iteration. This amount of rearrangement and number of scrambling turns malicious decryption into a more complex task.

So, without the initial image's cycle and iterations, there's no way here we'll be able to recycle the initial image. The key by scrambling transformation. and the number of iterations can be turned into the private key. Meanwhile, the number of iterations for a scrambling transformation is related with the effect of the scrambling and the effect of the recovery that is called for by various images [17]–[18]. The reason why the resistibility of most medical image watermarking algorithms is low, today, is the following: During the embedding step of embedding a digital watermark in pixels or transform coefficients, the small geometric transformation of the medical image can result in a significant change in the pixel values or transform coefficient values.

Hence, the watermark that is inserted would be susceptible to attacks. When we are able to compute the visual feature vectors of the image that capture the geometric aspect of the image, the visual feature value of the image will not be very strongly influenced by a small geometric transformation of the image. The experiment with Hayes indicated that the phase is more important than amplitude in terms of the image feature. Such kind of watermark signal boasts cryptography security. Meanwhile, the embedded watermark is zero watermark in real sense and will not the quality of medical image, thus effectively solving the problems in embedding and extracting of medical image watermark.

The latter approach does not need to select ROI artificially, nor does it need the limit capacity nor are original medical images included in the process of extracting the watermarks. It is able to deal effectively with compression attacks as well as the traditional attacks in the medical image application thereby further safeguarding privacy of patient information. To sum up, it's just a more easy-to-use and useful approach! Our examination of lots of the complete graphic DWT information revealed that once we provide typical compression transformation to a medical image, the worth of low-frequency coefficient can shift to some amount but the sign of the coefficient is fundamentally the same.

In [19], a zero-watermarking algorithm of medical Images developed by using dual-tree complex wavelet transform (DTCWT) is presented. In contrast to the conventional scheme of watermarking, the key concepts of the zero-watermarking embedding in medical imaging is that no watermark would be put into the image itself, the watermarking step would not do any changing operation to the image itself, the Hidden features would be extracted of the original image and it combined with the watermark, and then an encryption is made with the help of it and a key is obtained, the extraction of the internal representative feature information in the image data is the important step in the zero-watermarking process.

This novel algorithm proposes to implement DTCWT on medical images. Next, a medical image's visual feature image is retrieved from the low-frequency coefficients of DTCWT with a lower frequency under the geometric attack. Last

but not least, in conjunction with the idea of zero-watermarking, the watermark is coded by the logistic map. With this as a premise, regular watermarking technology is used in combination with chaotic encryption. The secret key will then be stored to be used in the extraction of watermarks.

4. PRELIMINARIES

4.1. Discrete Wavelet Transform (DWT)

DWT has excellent spatial localization and multi-resolution characteristics, which are similar to the theoretical models of the human visual system [15]. DWT decomposes the original image into four sub-band images: three high frequency images (HL, LH, HH) that are called the detail sub-images and one image of low frequency (LL), that is called the approximate sub-image. The detail sub-bands contain the fringe information and the convergence of strength of the original image is the approximation sub-bands. Because the detail sub-images contain much less of the image's energy than the approximate sub-image, is much more stable. Needless to say, pictures are two dimensional data files. Two dimensional wavelets can be used in transforming images or use the one-dimensional transform in each row and column of the image in turn as separable two-dimensional transform.

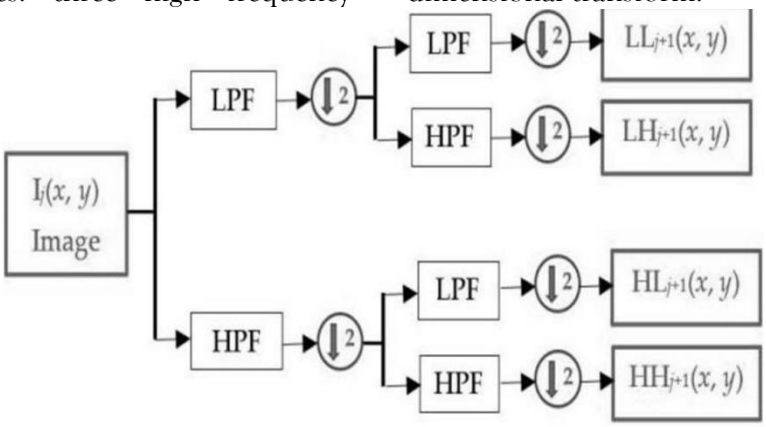


Figure 2. Two-dimensional DWT decomposition of I from level j to j + 1 into LL, LH, HL, and HH sub-bands

4.2. Quantization

Quantization is a process of decreasing large number of values to a smaller number of values. The size of the data can be reduced by means of quantization, which will not compromise the visual quality. There would be some quantization techniques such as scalar quantizer and vector quantizer. A quantization that has a scalar input and output is called scalar quantization and one that has a vector input and output is called a vector quantization. [16]. Based on whether the quantization step is uniform or not, quantization techniques can be divided into uniform and non-uniform quantization. The cells in the uniform scalar quantizer are not of different lengths but in the non-uniform scalar quantizer they are different lengths.

4.3. Singular Value Decomposition

SVD is a powerful numerical analysis that is applied to matrices [17]. In SVD transformation, a matrix can be broken down into three matrices of the same size that of the original matrix. In the eyes of linear algebra, an image is a sequence of positively-valued scalar samples that can be thought of as a matrix. In addition, the singular value decomposition is computed for all matrices (scalar, rectangular and square). Let I be an image, with a size of M×N. The formalism of the SVD of the identity matrix is presented in equation (1). In this case, $(\cdot)^T$ represents transpose and the

diagonal entries of Σ are non-negative and represent the singular values of I.

The diagonal entries $\Sigma = \text{diag}(\sigma_1, \sigma_2, \ldots, \sigma s)$ satisfy $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma s$. The singular values of Σ provide image-energy information, small changes in these values do not usually affect the quality of the diagnostic image seen; the values of the singular values are relatively stable for common attacks. The SVD technique can be used for digital image cipher and watermarking. The image can be split into three segments then secure them in a variety of ways so that only at the time all the three image segments come together and are multiplied with the right order the information could be retrieved [17].

4.4. Scrambling Transform Technology

Digital image encryption has two approaches, whereby the value of the pixel is altered, and in the other approach, the position of the pixel is altered (scrambling). The latter ones are trying to alter the pixel value to make the original image unreadable without being familiar with the encryption method used such as Lorenz, Rossler, Chue and Nien [4]-[6] (without knowing the encryption method used). The other, similar to the Arnold modification to Cat Map, is a pixel position change in order to achieve the aim encryption. [7]-[8]. Nevertheless, it was possible to decrypt the value or the location of the pixel. The most crucial factor that can control the key space of the chaos system is the initial condition where it give theoretically infinite key space resulting in more immunity towards brute-force attack [9].

There are a great variety of chaotic systems that can be used to produce encryption sequences. We make use of a logistic map in this work. One of the most widely used chaotic systems is the 1D Logistic Map. The logistic recurrence is formalized in Equation (3), where x_n lies in (0, 1), x_0 is the starting point of the sequence, μ a parameter defined by the user and used to create a chaotic sequence; and n is the iteration index. The curves are chaotic periodic when $\mu > 3.57$. When $3.5699456 \leq \mu \leq 4$, logistic mapping will be in chaos condition. The sensitivity (depending on one system parameter μ and an initial condition x0) are the main weakness of a 1D logistic map.

The more the control parameters, the less the statistical complexity. Another drawback is periodic sequences in the chaotic region that is more vulnerable to all differential attacks, most notably chosen plain text attack. Same conditions can undergo a lot of secret being revealed. In order to prevent this issue, we apply logistic map that incorporates the chaotic element in order to encrypt a binary watermark picture and the element will guarantee privacy of the presented scheme.

5. SIMULATION RESULTS

Peak signal to noise ratio (PSNR), normalized correlation (NC) [18], are the parameters which are employed for evaluating performance of the proposed technique. An experiment of the proposed system was conducted in MATLAB for assessing its effectiveness. Three standard benchmark images in grayscale from the kaggle database were tested: Various types of medical images (MRI, radiography, ultrasound) were used, coded within 256 levels of gray in BMP format, with images dimension of size 256 × 256 and the watermark logo of size 64 × 64 was considered.

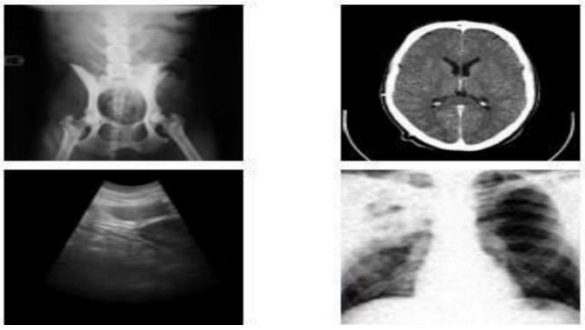


Figure 3. Types of medical images used in the evaluation



Figure 4. Binary watermark images used in the embedding experiments

The embedding process and the extraction process was performed for the test images as represented in figure 5. The watermarked medical images do not show apparent degradation for the aforementioned value of the mentioned parameters (α = 0.1, Y(1), a = 1, b = 0.5).

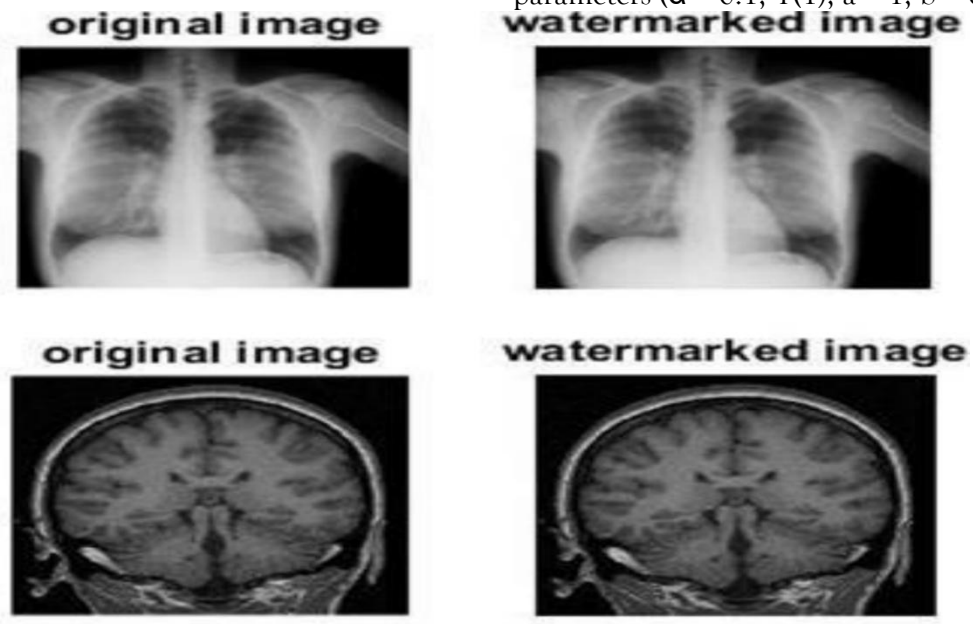


Figure 5. Original and watermarked medical images

As the results are shown in Figure 6, the histogram of the encrypted image has a regular intensities' distribution. In fact, on comparing the histogram of the watermarked encrypted image with the histogram of the host image, therefore, the experimental results recommend that the encryption process can generate reliable results and is highly secure for medical imagery with a uniform distribution and maximum dissimilarity of pixel values without leaving any clue for statistical analysis and attacks. In the absence of any type of attack, the PSNR equal to 45.73, it is

important to get an NCC = 1 (without attacks) and a good value of PSNR.

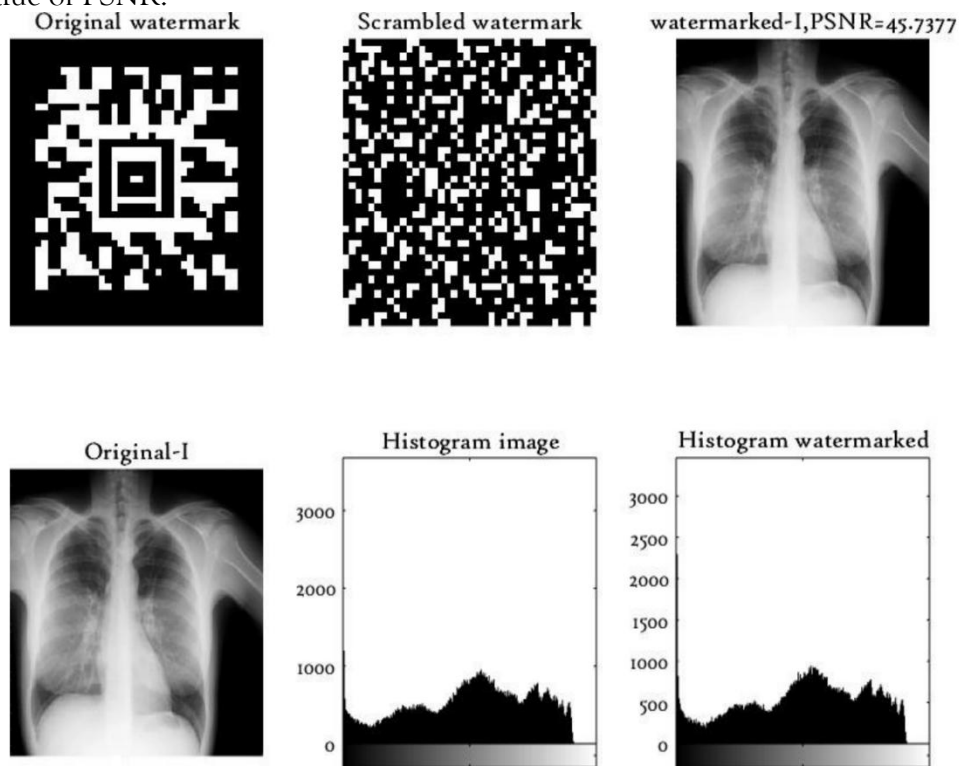


Figure 6. Histogram comparison of the original and watermarked medical images

5.1. ROBUSTNESS ANALYSIS

The proposed algorithm was tested against normalized correlation (NC) following common image-processing attacks such as 25% top left cropping, Gaussian noise (variance 0.01), salt-and-pepper noise (density 0.05), sharpening and 2 × 2 averaging/median filtering operations, JPEG compression (quality 80) and 1-degree rotation. The mean values of the reported NCs of the test images are summarized in Fig. 7.

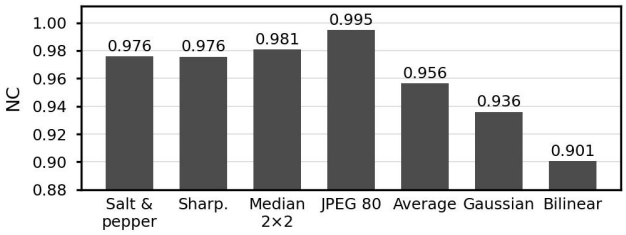


Figure 7. Robustness NC values under image-processing attacks

Table 1. Comparison of average NC values with prior methods [19]-[23]

Attack	[23]	[22]	[19]	[21]	[20]	Proposed
Crop 25%	0.8445	0.9997	–	–	0.9966	–
Noise (0.01)	0.9114	0.9589	–	–	–	–
Salt-and-pepper	0.9099	0.9589	–	–	0.9758	0.97572
Sharpening	0.9852	–	0.9018	0.9977	0.8898	0.97570

Gaussian filter	0.9488	–	0.9322	–	–	–
Median 2×2	0.9494	–	–	–	0.6973	0.98093
JPEG 80	–	–	–	–	–	0.99468
Average filter	0.9407	–	–	0.9354	–	0.95643
Gaussian noise	0.9114	–	–	–	0.9144	0.93589
Rotation 1°	0.9881	–	–	0.9728	0.9460	–
Bilinear crop	–	–	–	–	–	0.90069

When there are no measurements available for a specific study, this will be indicated by a dash. The proposed method keeps the values of NC within the range of (0.90069 – 0.99468) when the reported attacks are under consideration. It gives the best results compared with the comparator in median filtering, JPEG 80, average filtering, Gaussian noise and bilinear cropping and [21] have a high value of sharpening.

5.2. SECURITY ANALYSIS

There's two phases of security. The watermark is scrambled by a logistic map with a key and protected in the CHAOS-SVD preprocessing phase. Secondly, coefficient modification during watermark insertion is received under the influence of the embedding-strength factor. The recovery of the embedded watermark is also difficult unless the initial state of noise is chaotic, the control parameter is proper, the permutation is correct, the DWT depth is correct, the quantization step is proper and the embedding strength is correct.

5.3. MATHEMATICAL AND ALGORITHMIC SPECIFICATION

This subsection is the formalization of the process of the DWT-SVD watermarking based on encryption. The algorithm is not broken-up into pieces across pages, and the notation is the same.

5.3.1. Notation

Table 2. Mathematical notation used in the proposed framework

Symbol	Definition	Range or unit
I	Original medical image	M × N pixels
W	Binary watermark	P × Q bits
K	Secret key (x_0 , μ, r, α, Δ)	Tuple
I_w	Watermarked image	M × N pixels
I_a	Attacked image	M × N pixels
$\hat{W}$	Recovered watermark	P × Q bits
r	DWT decomposition level	Positive integer
x_n	Chaotic state	0 < x_n < 1
μ	Logistic-map parameter	3.57 < μ ≤ 4
α	Embedding strength	α > 0
Δ	Quantization step	Δ > 0
c_k, c′ _k	Selected coefficients	Real-valued
L_max	Maximum intensity	255 for 8-bit images
MSE	Mean squared error	Non-negative
PSNR	Peak signal-to-noise ratio	dB
NC	Normalized correlation	0 to 1
SSIM	Structural similarity index	−1 to 1

5.3.2. Core Equations

$$I = U\Sigma V^{\mathrm{T}} \tag{1}$$

$$\left[\mathrm{LL}_r, \mathrm{LH}_r, \mathrm{HL}_r, \mathrm{HH}_r\right] = \mathrm{DWT}_r(I) \tag{2}$$

$$x_{n+1} = \mu x_n(1 - x_n), \qquad 0 < x_n < 1 \tag{3}$$

$$W_s = \Pi_K(W) \tag{4}$$

$$c'_k = Q_\Delta(c_k, w_k) = \Delta \mathrm{round}\left(\frac{c_k}{\Delta}\right) + \Delta\left(\frac{1}{4} + \frac{w_k}{2}\right) \tag{5}$$

$$I_w = \mathrm{IDWT}_r\left(\mathrm{LL}_r, \mathrm{LH'}_r, \mathrm{HL'}_r, \mathrm{HH'}_r\right) \tag{6}$$

$$\mathrm{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - I_w(i,j)]^2 \tag{7}$$

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{L_{\max}^2}{\mathrm{MSE}}\right) \tag{8}$$

$$\mathrm{NC}(W,\widehat{W}) = \frac{\sum_i \sum_j W(i,j)\widehat{W}(i,j)}{\sqrt{\left(\sum_i \sum_j W(i,j)^2\right)\left(\sum_i \sum_j \widehat{W}(i,j)^2\right)}} \tag{9}$$

$$\mathrm{SSIM}(I,I_w) = \frac{(2\mu_I\mu_{I_w} + C_1)(2\sigma_{I,I_w} + C_2)}{(\mu_I^2 + \mu_{I_w}^2 + C_1)(\sigma_I^2 + \sigma_{I_w}^2 + C_2)} \tag{10}$$

Algorithm 1. Encryption-Based DWT-SVD Watermark Embedding and Extraction

Require: medical image I; watermark W; key K = (x_0, μ, r, α, Δ); received image I_a

Ensure: watermarked image I_w; recovered watermark Ŵ; MSE, PSNR, NC, and SSIM

1. Validate the dimensions of I and W; normalize image intensities.
2. Generate {x_n} using the logistic map and derive permutation Π_K.
3. Compute W_s = Π_K(W) and apply SVD to the encrypted representation.
4. Compute [LL_r, LH_r, HL_r, HH_r] = DWT_r(I).
5. Select PQ stable high-frequency coefficients in the region of non-interest using K.
6. For k = 1, ..., PQ, perform Step 7.
7. Embed w_k by computing c′_k = Q_Δ(c_k, w_k) with strength α.
8. End the coefficient-embedding loop.
9. Reconstruct I_w using IDWT_r; compute MSE, PSNR, and SSIM.
10. Decompose I_a and decode each bit from its quantization interval.
11. Apply inverse SVD and inverse permutation to recover Ŵ.
12. Compute NC(W, Ŵ).
13. Return (I_w, Ŵ, MSE, PSNR, NC, SSIM).

Computational complexity: For an M × N image and an s × s SVD watermark representation, DWT and inverse DWT require O(MN), chaotic permutation requires O(PQ), and SVD requires $O(s^3)$. Overall time complexity is $O(MN + PQ + s^3)$, with O(MN + PQ) working memory.

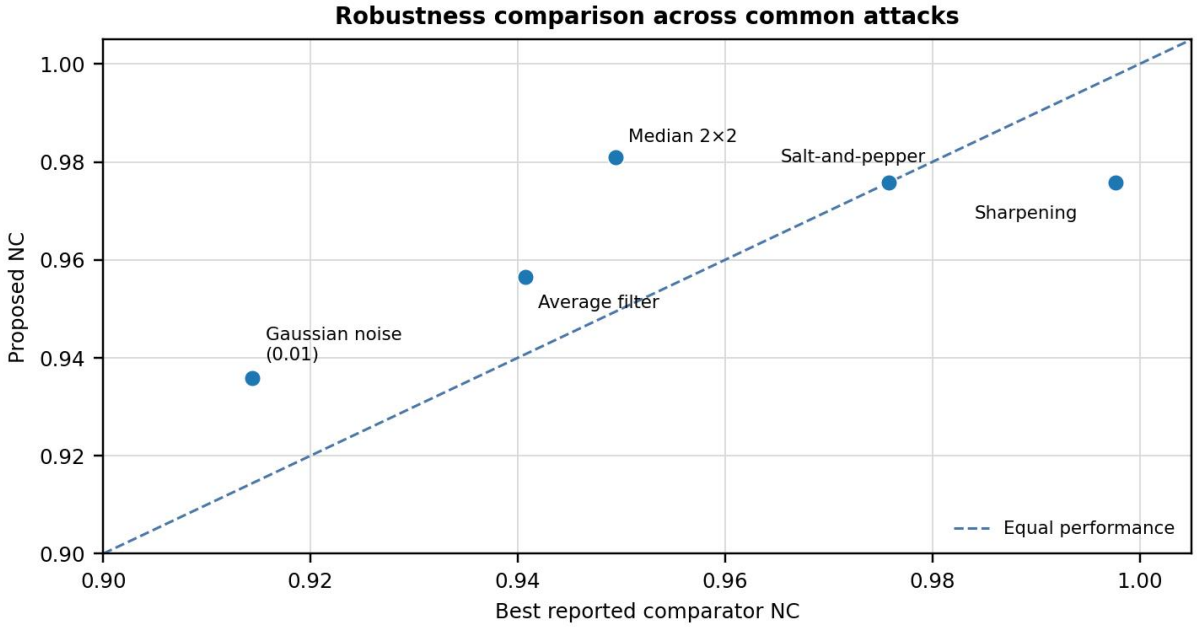


Figure 8. Proposed NC versus the best reported comparator for common attacks

Points above the diagonal indicate improvement over the best reported comparator. Missing values are excluded rather than treated as zero.

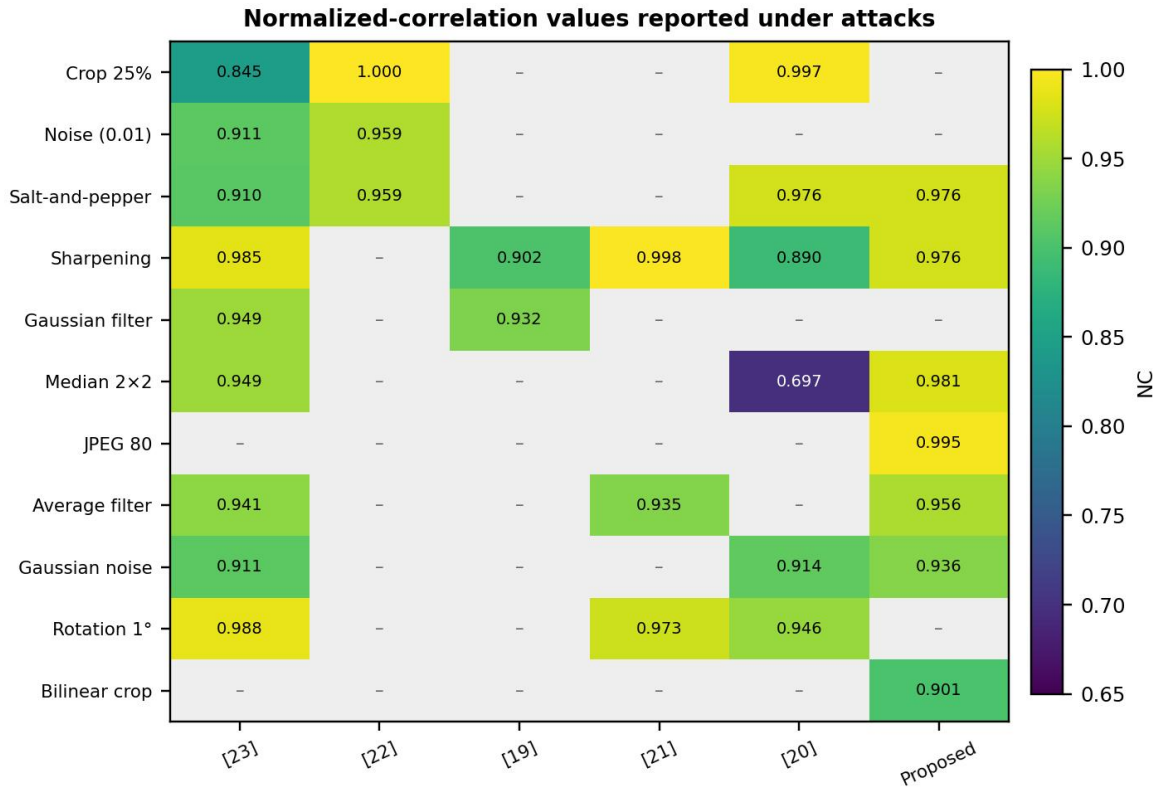


Figure 9. Heatmap of normalized-correlation values reported for the proposed and comparison methods

6. CONCLUSION

The scheme proposed watermarks the selected DWT blocks that fails to spoil the diagnostic quality of image while still being robust. The preprocessing of CHAOS-SVD secures the watermark against the attacks of information leakage and spoofing, cloaks the watermark in false information, and applies the watermark encryption. The recovered watermarks are still clearly recognizable and are very similar to the original watermarks. The reported average NC is still greater than 0.90 and the average PSNR is 53.45 dB. Further efforts are needed to strengthen against geometric and filtering attacks, as well as a selective joint encryption-compression scheme for safe medical-image transmission.

REFERENCES

1. A. K. Ray, S. Padhihary, P. K. Patra, and M. N. Mohanty, "Development of a new algorithm based on SVD for image watermarking," in Computational Vision and Robotics, Springer, New Delhi, pp. 79-87, 2015.
. A. Serdean and J. Tomazic, "Attacks on digital wavelet image watermarks," Journal of Electrical Engineering, vol. 59, no. 3, pp. 131-138, 2008.
. C. Kumar, A. K. Singh, P. Kumar, R. Singh, and S. Singh, "SPIHT-based multiple image watermarking in NSCT domain," Concurrency and Computation: Practice and Experience, 2018, e4912.
. D. S. Chauhan, A. K. Singh, B. Kumar, and J. P. Saini, "Quantization based multiple medical information watermarking for secure e-health," Multimedia Tools and Applications, vol. 78, pp. 3911-3923, 2019, doi: 10.1007/s11042-017-4886-4.
. J. C. Dagadu and J. Li, "Context-based watermarking cum chaotic encryption for medical images in telemedicine applications," Multimedia

Tools and Applications, vol. 77, pp. 24289-24312, 2018.
6. N. El-Sheimy, A. K. Salwa, A. S. Tolba, F. M. Abdelkader, and M. E. Hisham, "Wavelet packets-based blind watermarking for medical image management," The Open Biomedical Engineering Journal, vol. 4, pp. 93-98, 2010.
7. F. Yu, Z. Lu, H. Luo, and P. Wang, Three-Dimensional Model Analysis and Processing. Berlin, Germany: Springer-Verlag, 2001.
8. F. Y. Shih and S. Y. Y. Wu, "Combinational image watermarking in the spatial and frequency domain," Pattern Recognition, vol. 36, no. 4, pp. 969-975, 2003.
9. J. Huang, Y. Q. Shi, and Y. Shi, "Embedding image watermarks in DC components," IEEE Transactions on Circuits and Systems for Video Technology, vol. 10, no. 6, pp. 974-979, 2000.
10. Joint NEMA/COCIR/JIRA Security and Privacy Committee, "Defending medical information systems against malicious software," National Electrical Manufacturers Association, USA, 2003.
11. M. Kutter and F. A. Petitcolas, "Fair evaluation methods for image watermarking systems," Journal of Electronic Imaging, vol. 9, pp. 445-456, 2000.
12. K. Mandeep and K. Rupinder, "Reversible watermarking of medical images: Authentication and recovery-a survey," Journal of Information and Operations Management, vol. 3, no. 1, pp. 241-244, 2012.
13. M. Tayachi et al., "Tamper and clone-resistant authentication scheme for medical image systems," 2020.
14. O. Bruyndonckx, J.-J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital images," in Proc. IEEE Workshop on Nonlinear Signal and Image Processing, Neos Marmaras, Greece, pp. 456-459, 1995.
5. P. Moulin and M. K. Mihcak, "The data-hiding capacity of image sources," IEEE Transactions on Image Processing, 2002.
6. R. Shah, A. Agarwal, and S. Ganesan, "Frequency domain real-time digital image watermarking," Oakland University, MI, USA, 1998.
7. R. Bausys and A. Kriukovas, "Reversible watermarking scheme for image authentication in frequency domain," in Proc. International Symposium ELMAR 2006, Zadar, Croatia, pp. 47-50, 2006.
8. K. Rupinder, "A medical image watermarking technique for embedding EPR and its quality assessment using no-reference metrics," International Journal of Information Technology and Computer Science, vol. 2, pp. 73-79, 2013.
9. S. M. Haque, "Singular value decomposition and discrete cosine transform based image watermarking," M.S. thesis, Blekinge Institute of Technology, Sweden, 2008.
0. S. A. Parah, J. A. Sheikh, F. Ahad, N. A. Loan, and G. M. Bhat, "Information hiding in medical images: A robust medical image watermarking system for e-healthcare," Multimedia Tools and Applications, vol. 76, pp. 10599-10633, 2017.
1. S. Kaur and R. Talwar, "Arnold transform based security enhancement using digital image watermarking with complex wavelet transform," International Journal of Electronics Engineering Research, vol. 9, pp. 677-693, 2017.
2. S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," Multimedia Tools and Applications, vol. 78, pp. 3457-3470, 2019.
3. A. Umamageswari, U. Ferni, and G. R. Suresh, "A survey on security in medical image communication," International Journal of Computer Applications, vol. 30, no. 3, 2011.

24. X. G. Xia, C. G. Boncelet, and G. R. Arce, "A multi-resolution watermark for digital images," in Proc. IEEE International Conference on Image Processing, vol. 1, pp. 548-551, 1997.

5. J. M. Zain and M. Clarke, "Reversible region of non-interest (RONI) watermarking for authentication of DICOM images," International Journal of Computer Science and Network Security, vol. 7, no. 9, pp. 19-28, 2007.