T.C.

ALTINBAS UNIVERSITY

Institute of Graduate Studies

Department

BIOMEDICAL SIGNAL PROCESSING AND CONTROL

LOBABH SATTAT MOHAMMED MOHAMMED

Master of Science

Supervisor

Assoc. Prof. SEFER KURNAZ

Istanbul, 2021

AN INTELLIGENT IMAGE WATERMARKING SCHEME BASED ON HUMAN VISUAL SYSTEM CHARACTERISTICS WITH GUI INTERFACE

by

LOBABH SATTAR MOHAMMED MOHAMMED

Electrical and Computer Engineering

Submitted to the Institute of Graduate Studies

in partial fulfillment of the requirements for the degree of

Master of Science

ALTINBAŞ UNIVERSITY

2021

The thesis titled “An Intelligent Image Watermarking Scheme Based on Human Visual System Characteristics with GUI Interface” prepared and presented by “LOBABH SATTAR MOHAMMED MOHAMMED” was accepted as a Master of Science Thesis in Department.

Asst. Prof. SEFER KURNAZ

Supervisor

Thesis Defense Jury Members:

Assoc. Prof. SEFER KURNAZ	School of Engineering and Natural Sciences, Altinbas University	_____
Prof. Osman Nuri Uçan	School of Engineering and Natural Sciences, Altinbas University	_____
Asst. Prof. Zeynep Altan	School of Engineering and Computer Engineering, Beykent university	_____

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

Approval Date of Institute of Graduate Studies:

24/02/2021

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

LOBABH SATTAR
MOHAMMED MOHAMMED

Signature

ACKNOWLEDGEMENTS

I have been extremely fortunate to have had the support of my family, Friends, and colleagues near and far, without this support this thesis would not have been possible.

I am grateful to my family for their constant love and support, thank you Mom and Dad, and my sisters Omama and Luma , and my Brothers Nawfal and Hassan, Thanks for your understanding, your never-ending encouragement, and for always being there for me, Your support has meant more, to me than you could possibly realize, Without you, I could never have reached this current level of success.

Finally, my heartfelt gratitude to my loving friends for the moral support and encouragement throughout the studying days.

ABSTRACT

TITLE OF THE THESIS/DISSERTATION

MOHAMMED, LOBABH SATTAR MOHAMMED,

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor:Asst. Prof. SEFER KURNAZ

Co-Supervisor:

Date: 01/2021

Pages: 66

the fast growing of digital medical photos and the need to be forced to exchange them with experts and hospitals for better and even more accurate detection need the preservation of the privacy of patients. As a part of this, a medical image watermarking provision applies. Medical image watermarking, moreover, needs to be done with extra caution for two reasons. Firstly, the process of watermarking should not affect the image standard. Second, sensitive patient information embedded in the image should be cleanly recoverable without the possibility of mistake as image pressure is applied. Throughout this thesis, we appear to suggest a powerful Technique of non-blind image watermarking and its comparative output analysis, the watermark image will embedded by integrating Redundant discrete wavelet transform (RDWT), fast Walsh Hadamard transform (FWHT) and singular value decomposition (SVD) within the region of non-interest (RONI) of medical image, By using human visual system (HVS) model, RONI of the cover medical image is recognized, we can use particle swarm optimization (PSO) to increase the strength-of-the-watermark (scaling factor) . In order to do the complete watermarking process (embedding-attacks-detection) on a Windows panel rather than typing application line

options, we also prefer to plan a software package that provides a graphical user interface to use the watermarking system.

Keywords: Image Processing, Digital Watermarking, Medical Application, Human Visual System (HVS), Particle Swarm Optimization (PSO).

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

LIST OF CHARTS

Pages

LIST OF ABBREVIATIONS

IOT	:	INTERNET OF THINGS
IOMT	:	INTERNET OF MEDICAL THINGS
IOHT	:	INTERNET OF HEALTHCARE THINGS
RONI	:	REGION OF NONINTEREST
RDWT	:	REDUNDANT. DISCRETE WAVELETS TRANSFORM
FWHT	:	FAST WALSH HADAMARD TRANSFORM
SVD	:	SINGULAR VALUE DECOMPOSITION
HVS	:	HUMAN VISUAL SYSTEM
PSO	:	PARTICLE SWARM OPTIMIZATION
DCT	:	DISCRETE COSINES TRANSFORM
DWT	:	DISCRETE WAVELETS TRANSFORM
EPR	:	ELECTRONIC PATIENT RECORD
GUI	:	GRAPHICAL USER INTERFACE.
LSB	:	LEAST SIGNIFICANT BIT
ROI	:	REGION. OF INTEREST SELECTION

PSNR : PEAK SIGNAL-TO-NOISE RATIO

MSE : MEAN SQUARE. ERROR

SSIM : PERCEPTUAL SIMILARITY. IMAGE QUALITY

NC : NORMALIZED CROSS-CORRELATION.

1. INTRODUCTION

Within recent times, the Internet of Things IoT, merging of medical devices at intervals has led to the increase the Internet of Medical. Things IoMT, or. Internet of Health. Things IOHT. [1]

Modern Diagnostic types and methods of treatment such as telemedicine, internet-health, Hierarchy diagnosis, and smart therapy, are rapidly emerging, More and more advanced terminals for diagnosis and recovery, diagnostic sensors , Augmented Reality medical equipment, Virtual Operation etc., Allow doctors to use not only CT scan and MRI, ultrasound and other medical aids for disease detection and diagnosis; Clouds of medical images and distant centers , Archiving and communication facilities for cloud image reading, remote consultation and evaluation are also available. [2]-[5]. Yet, medical photographs are distinct from Common pictures. to guarantee the authenticity for the diagnostics, the doctors are usually adding patient name, his gender, his age and some other personal data in the medical photos, these pictures provide important A guide to doctors to gather and identify information regarding patient's real illness [2]. In the industry of medicine, the consistency of medical records that used in diagnosis is very stringent and no modifications are tolerated to the initial data.

The key challenge is many of IoMT systems were susceptible and defenseless to cyber-attack precisely Since medical instruments are either poorly shielded or not safe from future opponents at all, Some cyber-attack would has dramatic effects, risking the lives of patients, and would delay the broader implementation of IoMT, They are also closely related to critical patient records, including their identities, addresses, medical photos, and health problems, rendering them vulnerable to sophisticated threats (for example ransomware attacks) affecting its key aspects of security , honesty, and privacy. The reputation, acceptance, and large rollout of IoMT systems will be seriously affected by this.

1.1 IOMT Healthcare Systems Criteria

IoMT healthcare networks have more strict protection and privacy standards than traditional IoT-based infrastructures. Since an especially significant kind of privacy is medical privacy. Not only does illness make us prone to worry, suffering, body degradation and likely even death, it also

makes us susceptible to social harms such as stigma, bigotry, guilt, and exploitation. Therefore, there are several additional security standards for IoMT healthcare networks.

For any form of security regulation, the three core cyber security requirements are defined as the Secrecy, Honesty, and Availability (CIA) principles.

i. **Confidentiality** indicates that only the authorized users, under identified conditions, have access to the data.

ii. **Reliability** is based on two aspects: integrity and authentication. Integrity ensures that the information has not been manipulated in an unauthorized manner. Authentication confirms that the information refers to the right patient and was released from the correct source.

iii. **Availability** points out the ability of an information system to be accessed, as required by authorized users, in regular situations.

1.2 Attacks On IOMT Healthcare Systems

1.2.1 Data Confidentiality Attacks

The most important thing is to gather information to influence security for data of IoMT. Patients turn out to be more vulnerable to detected by secrecy (snuffling) attack caused by the transparent plus accessible IoMT nature which is wireless communications. Therefore, the risk of either leakage, hijacking, manipulating or even stealing personal and private information is seriously high. However, it is possible to carry out multiple passive attacks to do this. This entails eavesdropping, monitoring of traffic, and assaults by brute force. Table presents the main confidentiality attacks. [6]

Table 1.1: Different types of data confidentiality attacks with their corresponding solutions.

Data confidentiality	attack Solutions	Possible reason(s)
Eavesdropping	Encryption	• Broadcast nature of messages via wireless channels.
		• Unencrypted communication channel.
Data interception	Encryption	• Non-Secure Channels.

Data confidentiality	attack Solutions	Possible reason(s)
		• Open Wireless Communications.
Packet capturing	Encryption	• Open Wireless Communications.
		• Non-Secure Channels.
		• Lack of Encryption.
Wiretapping	• Secure Communications	• Open Wireless Communication.
	• Closed Communications	• Non-Secure Channels.
Dumpster diving	• Enhanced Employee Training	• Lack of Employee Training.
	• Paperless Process	• Lack of Awareness.

1.2.2 Privacy Attack

Ensuring patients' privacy is one of the most important challenges in IoMT. Preserving patients' privacy is mainly related to preventing the disclosure of their real identities, in addition to their location and information[7], [8].This requires patients to keep their private information protected such as their identity, their behavior, their past and present location, the main privacy attacks are listed and described in Table 1.2.

Table 1.2: Different types of privacy attacks with their corresponding solutions.

Privacy attack	Solutions	Possible reason(s)
Traffic analysis	• VPNs & Proxies	• Source and destination information are not encrypted.
	• Non-Link ability	• Lack of secure channels.
	• Pseudonyms	• Weak encryption algorithm.
Identity/Location tracking	• Anonymity	• Lack of secure channels.
	• Non-link ability	• Location and identification parameters are not encrypted.
	• Pseudonyms	

1.2.3 Attacks Against Integrity of Data and Message Authentication

Integrity attacks are based on the ability to alter the messages that are being transmitted to target the integrity of a system or data. Different attacks can be carried out to achieve this goal, such as injection attacks and data interception. Therefore, it is essential to secure and maintain the integrity of data as much as possible.

1.3 Security Schemes for IOMT Healthcare Systems:

Currently, Cryptography and watermarking are used to provide authenticity and confidentiality of medical record [9]–[12].

1.3.1 Cryptography

There are generally two common types of cryptographic algorithms: symmetrical and asymmetrical (public-key). Compared to symmetric encryption, asymmetric cryptosystems provide better security protection but require significantly more computational capability. Due to the limited computational capacities of IoMT devices in the sensor level, any data encryption and decryption solutions proposed for securing IoMT devices should be light-weight and the overhead of the communication channels should be minimized. Whereas data transmission between personal server level and medical server level should be protected with much stronger security schemes, as the data is often transmitted via public channels such as the internet.[13]

1.3.2 Watermarking

Digital watermarking is the process of embedding information or mark into a multimedia object, such that the mark can be extracted or detected at the receiving end. [14] the information insertion process has been performed mainly in two domains. One rolls up in spatial domain, where selected pixels are directly modified [15]. The other one is the frequency domain where the secret data is embedded into the best frequency portions of the protected image. Multiple transforms [16] may also be utilized to improve system performance. Frequency domain offers a better robustness, but spatial domain schemes are simple to implement, less time consuming, and offering a better imperceptibility with respect to the frequency domain methods.

1.4 Steganography Vs. Watermarking

The watermarking concept is closely related to two other fields: cryptography and steganography. These areas fall under the domain called data security system.

Cryptography is a method for sending a message in a secure format that only the authorized person can decode and read. This is known as a “secret writing.” Even though the encrypted message can be protected during the transmission, once the message is decrypted, it is not

protected anymore, and this is the main shortcoming of cryptography techniques when compared with watermarking [17]. Furthermore, most of the cryptographic methods are complex and provide weak copyright protection property.

Steganography is derived from the Greek word “steganos” and “graphei” which mean “covered” and “writing,” respectively. Despite some similarities between steganography and watermarking, there are some differences between them as explained below:

i. The objective of steganography is to embed an unrelated secret message into a cover work, while in watermarking, the embedded information and cover work are related to each other.

ii. In steganography, the message should be invisible, but in watermarking, the embedded information can be either visible or invisible.

iii. The main goal of steganography is to hide the message into the cover data in a way so that an invader cannot detect it, while the main purpose of watermarking is to embed the data into the cover data in a way that it cannot be removed or replaced by an intruder [17].

Based on these Advantages and disadvantages That could be inferred that the perfect option to maintain security foe digital image is watermarking. In addition, the data can be encrypted as a second layer of security before the watermark is embedded. A summary of a security framework, as viewed in the Figure 1.1.

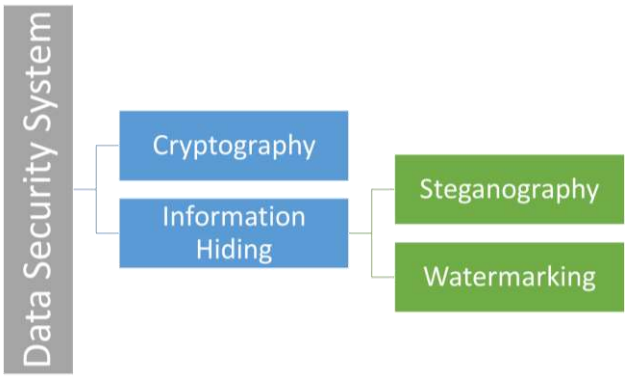


Figure 1.1: overview of a security system.

2. DIGITAL IMAGE WATERMARKING SYSTEM

Watermarking will ensure copyright ownership and identify copyright theft by integrating unique details into Digital features such as still photos, voice, film, etc. The special data could be the serial number of the author, business mark, meaningful text, and so on. The embedded data in the watermark is strong enough to withstand attacks, in comparison to the camouflage. However, if it is a public watermarking algorithm, and attackers know a secret key, it is always hard to remove the hidden watermark (in the idyllic situation it is impossible).

The famous Kerkhof's principle [18] Means going like this in cryptography: The encryption mechanism still secure, however if the attacker has information of the theory and algorithm but does not have info about the correct key. Robustness needs that an algorithm for watermarking embedding less details than camouflage in public data. Instead of opposing steganography and watermarking are opposite.

2.1 Digital Watermarking Basic Model

The hiding of information inside a digital item is digital watermarking. To validate the authenticity of the object, the embedded data may then be detected/extracted. For the development of security properties [19]-[21], it can be used along with certain current security tools, such as cryptography, cryptographic hash function, digital signature, perceptual hashing, etc. The automated watermarking system's basic model consists of three components: creation of watermarks, embedding of watermarks, and extraction of watermarks [22].

2.1.1 Watermark Generation

In this phase, a suitable watermark is created according to the purpose of the watermarking approach. In simple applications, such as ownership verification, the watermark data can be a text or an image. In developed applications, the watermark may have special characteristics based on the required purpose. For example, in medical applications, the watermark may need information about patients or features of medical images to verify the authenticity and integrity of the images.

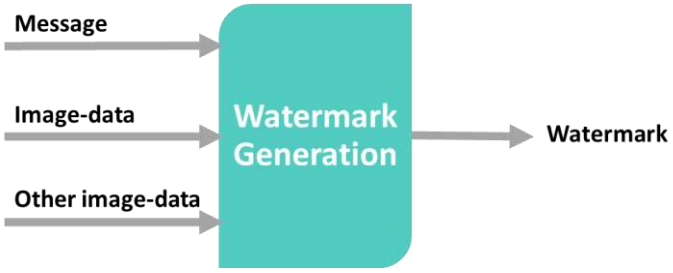


Figure 2.1: watermark generation.

2.1.2 Watermark Embedding

The watermarked data is generated by encoding the watermark into the original object using a certain algorithm and a secret key. Various techniques can be utilized to encode the watermark into digital data. Selecting a suitable watermarking technique depends on the purpose of the application.

Figure 2.2: watermark embedding.

2.1.3 Watermark Extraction

In this stage, the encoded data is detected/extracted from the watermarked object by reversing the hiding algorithm that was used to encode the watermark. The secret key and/or the original object are required for retrieving the embedded data successfully.

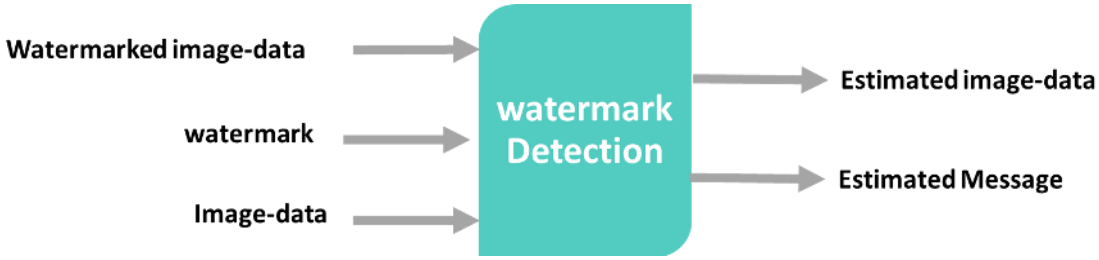


Figure 2.3: watermark detection.

2.2 WATERMARKING CLASSIFICATION

Digital watermarking schemes can be classified into many groups in various ways (Figure 2.4), including object type, embedding domain, perceptibility, and reversibility [23].

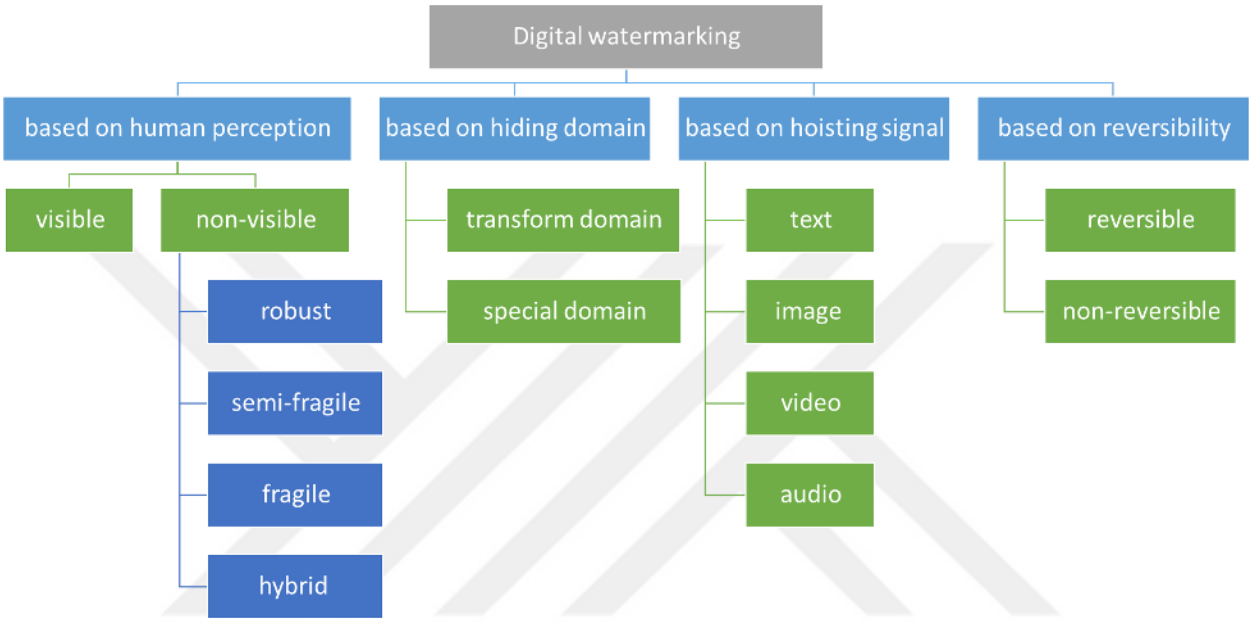


Figure 2.4: Classification of digital watermarking based on four various criteria.

2.2.1 Based on Human Perception

From the viewpoint as to whether the embedded watermark can be seen by bare human eyes or not, all watermarking techniques can be classified as visible techniques and invisible techniques. For example, Figure 2.5(c) shows a picture which contains a visible logo of Altinbaş university in its top-left corner and Figure 2.5(d) shows a picture which contains an invisible watermark.

(a)

(b)

(c)

(d)

Figure 2.5: An example of applying the visible watermarking technique and invisible. watermarking technique to a given picture. (a) The original picture. (b) The watermark. (c) The watermarked picture containing a visible logo in its top-left corner. (d) The watermarked picture containing an invisible watermark therein.

Obviously, at least two disadvantages exist in visible watermarking techniques:

i. The visible watermark is not difficult to be removed as shown in Figure 2.6 .

ii. The visible watermark degrades the visual quality of the host picture.

In the invisible type of watermarking techniques, the embedded watermark is invisible. It is difficult to distinguish between the original image and the watermarked image. Thus, it is not easy to remove or destroy the embedded watermark without degrading the visual quality of the watermarked image significantly[24].

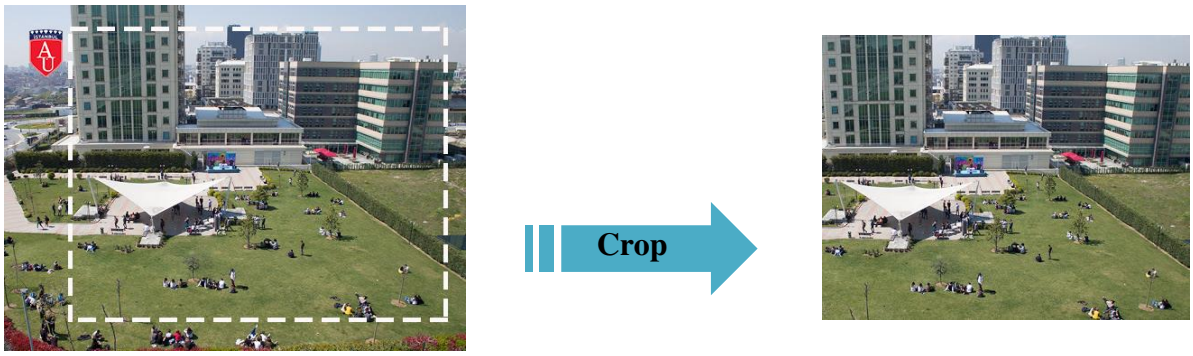


Figure 2.6: An example of removing visible watermark.

Invisible watermarking methods can be divided into four groups: fragile, semi-fragile, robust, and hybrid methods [25], [26]. The fragile method allows the watermark to easily be destroyed by the smallest of modifications. Applications for this kind of watermarking are limited to authentication and integrity verification. The semi-fragile method protects the hidden data against intentional attacks but is fragile against malicious attacks. The robust watermarking method, which is usually used for copyright protection purpose, should be resistant against multiple different attacks. The robustness of these methods can be measured by applying different attacks on the watermarked images and comparing the embedded and extracted watermark by different benchmarks. The lists of various attacks and benchmarks are introduced in the following sections. Finally, the hybrid watermarking is a mixture of robust and fragile techniques to provide authentication, integrity verification, and copyright protection simultaneously[25], [27].

2.2.2 Based On Hiding Domain

We can divide watermarking based on hiding domain to spatial-domain-based techniques, transform-domain-based techniques, In the spatial domain, the watermark information is embedded directly in the pixel value of the host or cover image, and to preserve the image quality, the watermark is usually embedded into the least significant bits of the host image. These methods are fast and simple and provide high capacity for embedding watermarks. The other advantage of these techniques is that a small watermark can be embedded several times, so the possibility of removing all watermarks by any kind of attack is very low. Hence, even a single surviving watermarking may fulfill the needs[28]–[31].

However, spatial domain approaches cannot survive against noise or lossy compression attacks [32]. Furthermore, once the method is uncovered, embedded watermark can be easily modified by a third party.

For transform-domain-based techniques, the raw data of the host image are first transformed into frequencies using the discrete cosine transform (DCT), the discrete wavelet transform (DWT), or other types of transforms. These frequencies are then modified according to the watermark bits so that the goal of data hiding can be achieved. Then, the inverse transform is executed, and a watermarked image is formed.

The transform-based techniques usually have better robustness and good visual quality in watermarked result. However, they consume more time in the transform and inverse-transform procedures[24].

2.2.3 According To Host Signal

The host or cover signal could be[33]:

i. **Text Watermarking:** it inserts a watermark in the font shape and the space between characters and line spaces.

ii. **Image Watermarking:** this embeds special information to an image and detects or extracts it later for ownership confirmation.

iii. **Video Watermarking:** it is an extension of image watermarking. This method requires real time extraction and robustness for compression.

iv. **Audio Watermarking:** this application area becomes a hot issue because of the internet music, MP3.

2.2.4 Reversibility

A watermarking algorithm is said reversible if the watermarked signal can be converted to a non-watermarked signal after the embedded watermark is extracted. By contrast, watermarking algorithms that cannot convert the watermarked signal to a non-watermarked signal are named non-reversible watermarking algorithms. Currently, most of the existing watermarking

algorithms are non-reversible algorithms since the selected signals of the cover media have been changed permanently for carrying the watermark bits [24].

2.3 Characteristics Of Digital Watermarks

Digital image watermarking techniques add a watermark into multimedia data to ensure authenticity and to protecting a copyright holder from the unauthorized manipulation of their data [34]. Figure 2.7 illustrates key characteristics of digital watermarks[35], [36] which are:

a) **Robustness:** A digital watermark is called robust if it resists a designated class of transformations and thus can be used for copyright protection. The robustness criterion focuses on two issues i.e. (1) whether the watermark is present after distortion in the data and, (2) whether it can be detected by the watermark detector.

b) **Imperceptibility:** The imperceptibility can be considered as a measure of perceptual transparency of watermark, and it refers to the similarity of original and watermarked images.

c) **Capacity:** It is the amount of information that can be embedded in a cover. This amount of information highly depends on the applications such as copyright protection, fingerprinting, authentication and confidentiality of medical data, as the information to be embedded may be a logo image, a number etc.

d) **Security:** The security of watermark implies that the watermark should be difficult to remove or alter without damaging the cover image. The level of watermark security requirement can vary depending upon the application.

e) **Data-payload:** The data payload of a watermark can be defined as the amount of information that it contains e.g., if a watermark contains ‘n’ bits, then there are 2n possible watermarks with actually 2^{n+1} possibilities as one possibility can be that no watermark is present. A good watermark should contain all the required data within any arbitrary and small portion of the cover.

f) **Fragility:** The fragile watermark basically aims at the content authentication. This is reverse of the robustness criterion. The watermarks may be designed to withstand various degrees of

acceptable modifications in the watermarks on account of distortions in the media content. Here, watermark differs from a digital signature which requires 100% match.

g) **Computational cost:** The computational cost basically refers to the cost of embedding the watermark into a cover and extracting it from the digital cover. In some applications, it is important that the embedding process be as fast and simple as possible while the extraction can be more time consuming. In other applications, the speed of extraction is crucial.

h) **Tamper resistance:** Tamper-detection of watermarks is used to check the authenticity of digital photographs. Watermarks of this type are sensitive to any change of the watermark data; thus, by checking the integrity of the watermark, the system can determine whether or not the watermark has ever been modified or replaced.

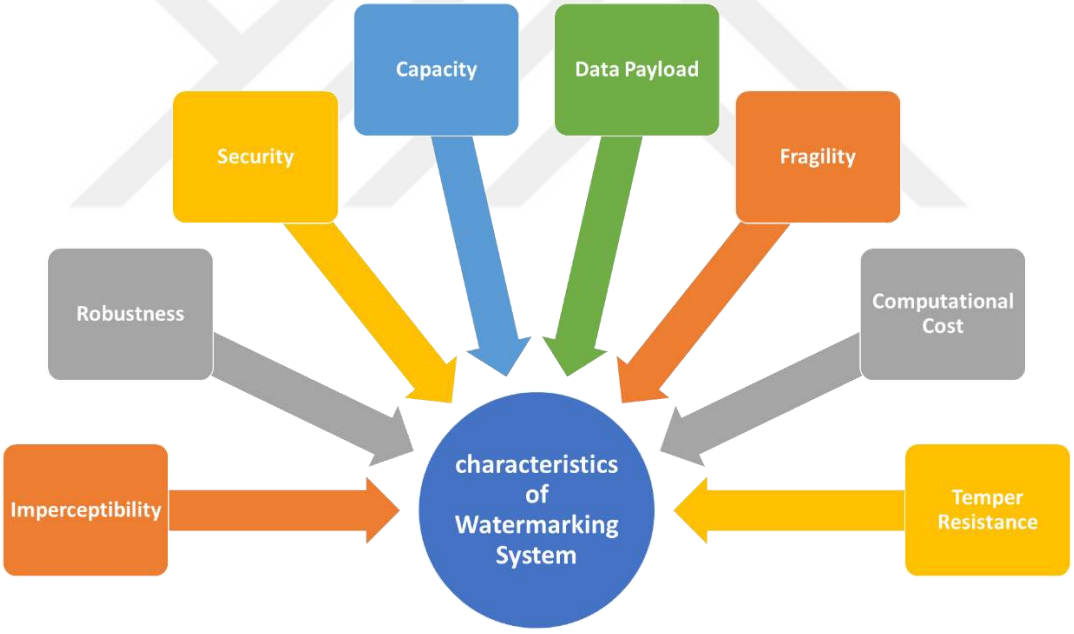


Figure 2.7: characteristics of digital watermarking techniques

2.4 Important Medical Image Watermarking Requirements

In recent time, tele-medicine, tele-ophthalmology, tele-diagnosis and tele consultancy services, medical images play a prominent role for instant diagnosis, understanding of crucial diseases as well as to avoid the misdiagnosis. Further, medical identity theft has been a serious security

concern in telemedicine [37], [38]. Robert Siciliano, CEO of safr.me, an identity theft expert, says, that would be a big fat yes. It's almost like the perfect crime as far as medical identity theft is concerned. The long-distance nature of this type of treatment fuels the anonymity of it all. Medical images contain sensitive information, and when they are transmitted over the unsecured network, they become vulnerable to corruption by noisy transmission channels and attacks by hackers or individuals with malicious intents. These attacks may include obtaining confidential information about the patient, changing patient information in the image header, and tampering with the image pixel content. In addition to that medical identity theft is a growing and dangerous crime and identity theft resource center produced a survey shown that the medical-related identity theft accounted for nearly half of all identity thefts as reported in the United States in 2013, USA Today reports said[39]. These demand development of secure medical data/image watermarking schemes. Figure 2.8 shows some potential advantages of medical image watermarking. The major advantages of the medical image watermarking [40]–[42] are:

a) Smaller storage space is required for storing the medical image and the patient record together as the patient record is embedded inside the image.

b) Reduced bandwidth requirement during transmission as the additional requirement of bandwidth for the transmission of the metadata can be avoided if the data is hidden in the image itself.

c) Ownership identification and confidentiality of the patient data is maintained as this data is hidden in the cover image.

d) Protection against tampering as the after-effects of a tampered medical data may cost a life due to wrong diagnosis.

e) The hidden watermarks can play the role of keywords, based on which efficient archiving and data retrieval from querying mechanisms take place. Further, it provides a valuable solution for potential issues such as medical data management and distribution [43].

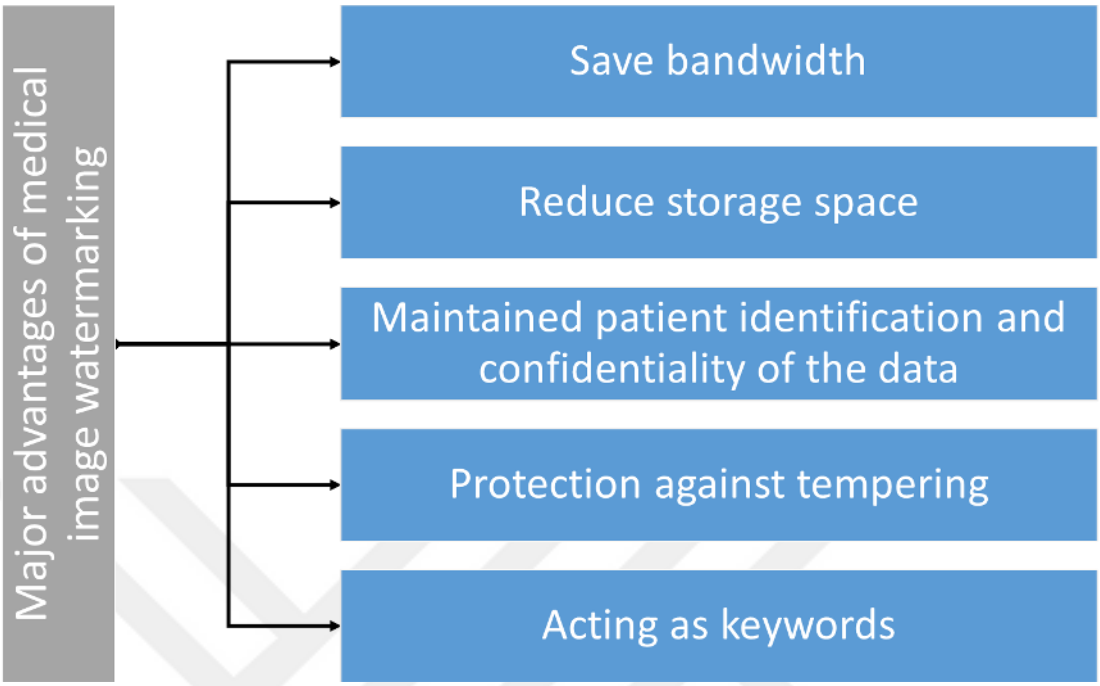


Figure 2.8: Main advantages of medical image watermarking

However, the medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. The electronic patient record (EPR) data exchange through unsecured channels required high degree of security. As depicted in , it includes three mandatory security requirements [44]:

a) Confidentiality means only the authorized users must access the information.

b) Reliability has two important outcomes: (a) Integrity—the information has not been modified by unauthorized people, and (b) Authentication—a proof that the information belongs indeed to the correct source. Further, the traceability is important components of the reliability and use to trace the information along its distribution.

c) The availability is an ability of information system to be used by entitled users in the normal scheduled conditions of access and exercise. The authentication, integration and confidentiality are the most important issues concerned with EPR data exchange through unsecured channels[45], [46]. All these requirements can be fulfilled using suitable watermarks.

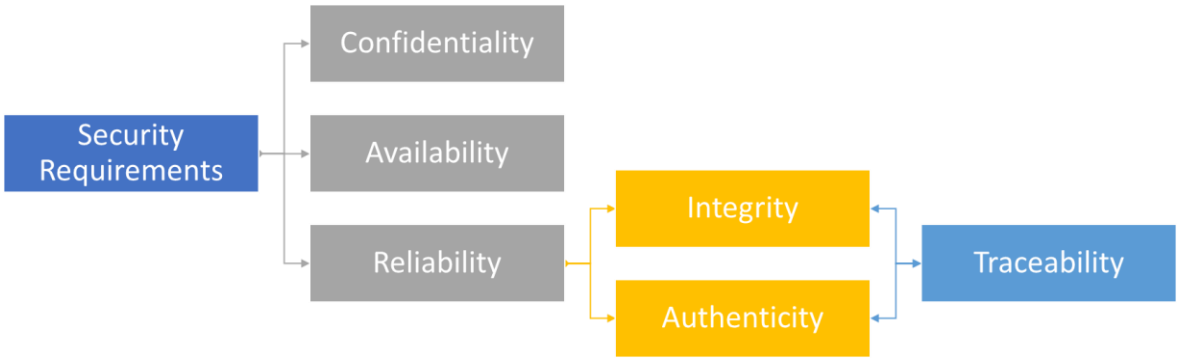


Figure 2.9: Major security requirements for EPR data[44]

3. APPLICATIONS AND CHALLENGES OF WATERMARKING SYSTEM

3.1 Applications For Digital Image Watermarking

A main application of the digital watermark is depicted in Figure 3.1. The important and latest

Figure 3.1: Applications of Watermarking

potential applications are [47]as follows.

a) **Fingerprinting:** It is the mechanism in which the watermarked content contains the intended recipient's identification information to trace back the source of illegal distribution.

b) **Broadcast monitoring:** The broadcast monitoring is an application which enables content owners to automatically verify where, when and how long their content was broadcast via terrestrial, cable or satellite television. Also, the e-commerce has become a huge business and a driving factor in the development of the Internet. Online shopping services and online delivery of digital media is very popular today and will become an increasingly important part of e-commerce and mobile e-commerce. The digital watermarking techniques play an important role to protect an intellectual property in e-governance, e-commerce applications, copy control, media identification and tracking.

c) **Copyright protection:** Providing copyright protection to digital data by hiding secret information is main goal of digital watermarking. Many content owners to embed digital watermarks in images to communicate and protect image copyrights. This ensures that image users or licensees are acting in compliance with guidelines and allows legal departments to effectively communicate and enforce image copyrights.

d) **Digital signatures:** A mechanism employed in public-key cryptosystems that enables the originator of an information object to generate a signature, by encipherment (using a private key) of a compressed string derived from the object. The digital signature can provide a recipient with proof of the authenticity of the object's originator.

e) **Medical applications:** In this application the watermarking provides both authentication and confidentiality in a reversible manner without affecting the medical image in any way. Recently, telemedicine, tele-ophthalmology, tele-diagnosis, tele-consultancy, tele-cardiology, tele-radiology applications play an important role in the development of the medical field. However, protect the transmission, storage and sharing of EPR data between two hospitals or via open/unsecured channel are the most important issues in this field. Telemedicine can be divided into number of medical related technologies using computers for health care like tele-radiology, tele-pathy, tele-care, telesurgery, tele-neurology etc. Medical image watermarking requires extreme care when embedding additional data within the medical images because the additional information must not affect the image quality. Confidentiality, authentication, integrity and availability are important security requirements with EPR data exchange through open channels. All these security requirements can be fulfilled using suitable watermarks.

f) **Indexing:** Video mail can be indexed, where comments can be embedded in the video content; movies and news items can also be, where markers and comments can be inserted that can be used by search engine.

g) **Source tracking:** A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known.

h) **Secured e-voting systems:** With rapid growth of computer network, Internet has reached to common villagers of country and worldwide as well. Due to widespread use of the Internet with information and communication technologies in order to get their inevitable benefits like accuracy, speed, cost saving etc. more secure transactions such as shopping, banking, submitting tax returns are done online. Obviously, electronic voting is a possible alternative for conducting elections by maintaining security in election process. For the election commission of India and other countries to conduct free and fair polls is always challenging task. Current research focuses on designing and building 'voting protocols' that can support the voting process, while implementing the security mechanisms required for preventing fraud and protecting voters' privacy. So, we need a highly secured e-voting system is required. Further, digital watermarks are also used to protect state driver licenses by providing covert and machine-readable layer of security to fight against various issues such as digital counterfeiting, fraud, identity theft etc.

i) **Remote education and insurance companies:** Due to the shortage of teachers and other problems in rural areas in, distance education is gaining popularity of developing any diverse countries. So, there is a strong need for intelligent technologies to create a deployable remote education solution. However, dissemination of valuable content and teacher-student interaction are some of the major challenges in the distance education solution. The secured transmission of data is part of distant learning. Digital watermarking may provide one of the important solutions for the remote education. Also, different insurance companies such as health and vehicle nowadays use image processing application. Health insurance companies are storing the scanned copies of the medical data of their clients. The database may require processing and transmitting to central administrative offices. The car companies' image databases are referred for insurance-

related decision making in case of damage to vehicles during accidents. The digital image watermarking protection is provided to such image database.

3.2 Digital Image Watermarking Challenges

To be stable enough against attacks is an essential aspect of the system of watermarking. Each process which could result in damaging recognition of the watermark or degradation of the watermark contact is identified as an assault. The data of the processed watermark is then marked as attacked data [48]. Those threats (that may be intentional or not intentional) distort the representation of the watermark (Figure 3.2), and include active attacks, passive attacks, geometric attacks, removal attacks, protocol attacks, cryptographic attacks, blind attacks, informed attacks, tampering attacks, simple attacks, attacks based on key estimation, destruction attacks, and synchronization attacks, among others [49].

3.2.1 Active Attacks

Active attack occurs when the vulnerability of a watermark recognition feature is found by an intruder, deleting or destroying the watermark, this really is, An opponent will easily distort a watermarked image by merely modifying the buffer function. Removal, colluding, Falsifying, copying, incomprehension, masking, and scramble attacks are the most common active attacks for image watermarking. The watermark image will never be identified in removal attacks, but the attacker aims to create the same production photo Where the clone attack creates the copy without a watermark. In another side, the targeted watermarked image also retains an Imperceptible Watermark by current sensors with a masking attack. In distortion attacks, such compression methods can be used universally, either over the entire watermark picture or part of it. In an attack of forgery, the detector can authenticate a wrong watermark image to perform a not authorized embed by an opponent. although, an unsure threat also happens if the adversary produces a finding as a falsification right though the watermark picture is validated. By labeling a legitimate watermarked image as a false image, a scrambling attack can be triggered by [50]. For e.g., protections should be protected against active attacks that are used for fingerprinting, copyright, and copy protection.

3.2.2 Passive Attacks

When an attacker wants to figure out whether or not, a watermark is present without reference to the elimination of the watermark (destruction and deletion), a passive attack occurs. The intruder does not seek to change the tools for watermarking, but rather to access the information correlated with it. Different levels of passive attacks may be considered at this time to accomplish different purposes that are essential in secret contact.

3.2.3 Removal Attacks

Unless the key in the watermark integration is used, removal attack aims to delete a watermark from the host image. Such attacks are significant, and the category involves, among others, the removal of blind watermarks, conspiracy attack, remodulation, intrusion attack, noise attack, denoise, Compression of amounts and destruction. Those attacks do not entirely erase the watermark but aim to seriously destroy the information about the watermark.

As it diminishes, the ruggedness of the watermark signal, the original owner finds it more difficult, due to removal attacks, to locate the watermark. A reshaping attack Adjusts the representation of the watermark using the modulation process. This attack demodulates the same picture of the watermark with the aid of opposite modulation processes. Collusion attacks, on the other hand, occur when hackers delete watermarks from the original data and create a new copy from separate versions of the same original data without a watermark. Different watermarking techniques are required for each original copy. In noise attack the data sender is distracted by all forms of noise, such like gaussian tone, Additive input and noise from salt and poppers. A noise signal is applied to the watermarked picture. An interference attack can emerge as a result of additional noise on the watermarked image [51]. Those threats are planned To Harm the Watermark Embedded [52], [53], without degrading file material.

3.2.4 Geometric Attacks

The existing conventional watermarking algorithms are said to be efficient if they are robust against (intentional or unintentional) geometric attacks. These do not try to remove the watermark image itself but, rather, attempt to distort the watermark detector synchronization by using the inserted information. This is opposite in manner to removal attacks, and results in great

difficulty in the required synchronization process in recovering the embedded watermark information by the detector. Therefore, synchronization errors between the original watermark and the extracted watermark occur during the watermark extraction process. However, the watermark still exists in the watermarked image, due to changed positions. Hence, image transformation, image degradation, image enhancement, image compression, cropping, and image adjustment are all sorts of geometric attacks, as such manipulation affects the image geometry, which must be rejected to ensure the robustness of the system. Image transformation can prevent the blind detection of a public watermark by only performing rotation, scaling, and translation (RST) operations on an image to reduce the robustness level of that image. Hence, a robust watermarking system for images must be designed which is invariant to RST operations. The algorithm proposed by Lin [53], where an RST-invariant signal is created by taking the Fourier transform of the image and then resampling and integrating along the radial dimension. Additionally, removing some parts of the host image degrades the image quality, resulting in image degradation attacks. Degradation attacks need to be designed for some restoration methods for reducing or eliminating the degradation. Another attack processes a given image by increasing the dynamic range of the chosen features to obtain more suitable results for a specific application. These attacks can be easily detected, and this property is known as image enhancement. Image compression attack reduces the amount of data of the watermark image and cuts the bandwidth required to represent a digital image. Finally, the alteration of brightness, contrast, gamma value, and saturation result in image adjustment attacks, which change the watermark image.

3.2.5 Protocol Attacks

Attacks that are directly aimed at the watermarking application are known as a protocol attack. A protocol attack can be either an invertible attack, an ambiguity attack, or a copy attack. Non-invertible watermarks may be needed for copyright protection applications, where a watermark can never be extracted from a non-watermarked document. Invertible watermark attacks happen when the watermark is subtracted from the watermarked data by the attacker, who claims they are the owner of the watermarked data, which creates ambiguity about the original owner of the data [54]. This scheme results in ambiguity attacks, inversion attacks, deadlock attacks, fake-original attacks, or fake watermark attacks. A copy attack copies the watermark to some other

data, called target data, after estimating it from the watermarked data without destroying the watermark or impairing the watermark detection [54].

3.2.6 Cryptographic Attacks

Cryptographic attacks may be either a security attack or an oracle attack, aimed at cracking the security in watermarking schemes by removing the embedded watermark information. A brute-force search embeds secret information which misleads the watermark. Another attack, which creates a non-watermarked signal with an available public watermark detector device, is known as an oracle attack [54]. Applications must restrict these types of attacks used in cryptography due to their high computational complexity.

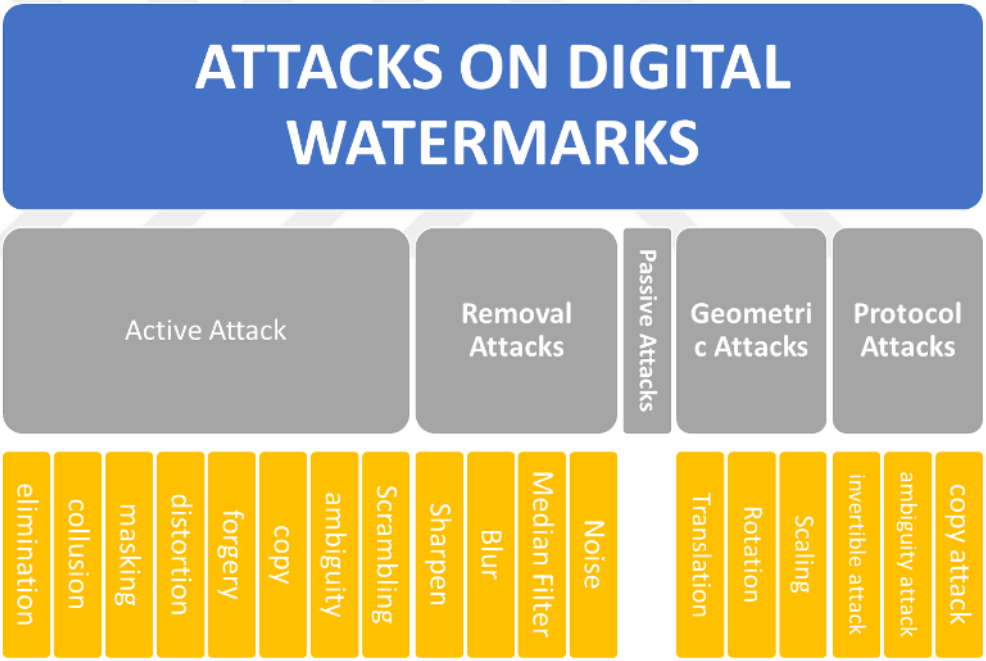


Figure 3.2: Classification of Digital Image Watermarking Attacks

4. IMPLEMENTATION OF WATERMARKING SCHEME

With the latest infrastructural growth of computer networks, the flow of multimedia data is growing in many ways. The evidence of ownership dilemma for multimedia data has now come to the surface as an imminent obstacle. The watermarking technique could be used as an invaluable method to deal with this problem. Since multimedia information also suffers from multiple forms of communication channel attacks, certain diseases should be resistant to the technique. The method of watermarking is then used to cover digital information during transmission. Usually, the watermark is used to prove the possession of those host signals. To build stable and imperceptible watermarks, many algorithms have been suggested in the thesis. We have created a program that offers a graphical user interface GUI to use a watermarking framework, so that instead of typing command line options, you can do the whole watermarking mechanism (embedding-attacks-detection) on a Windows screen.

4.1 Literature Review

Since multimedia information also suffers from multiple forms of communication channel attacks, certain diseases should be resistant to the technique. The method of watermarking is then used to cover digital information during transmission. Usually, the watermark is used to prove the patient's ownership and make him assured that his knowledge is protected, and that unauthorized people cannot access it. Many algorithms have been proposed in order to produce stable and imperceptible watermarks.

A method of watermarking based on the DWTSVD technique was suggested in[55]. Using Haar wavelet, the DWT decomposes the host image and the watermark images. Two level of decomposition was applied on the host image and single level decomposition on the watermark images, by altering the specific values of the host image, On the HL ban d, and LH bands of the host file, the watermark images are added. their approach was resilient to different types of attacks.

While [56] present an implementation of SVD, LSB, DCT, DWT, and a Hybrid DWT-SVD techniques to the embedding process and extraction phase of medical picture that is invisible watermarking, the findings indicate that DWT provides greater imperceptibility, yet is robust for

only a few attacks, SVD provides consistent robustness for attacks, although it is few imperceptible than DWT .

A block-based medical image watermarking approach suggested by Wakatani, A. [57] is a digital watermarking system that prevents ROI image data from being corrupted by embed signature info in areas other than. the ROI. The signature information is used as a signature image that is compressed using algorithm for progressive coding . In a closest field to the ROI, the most relevant signature data information is embedded. Their experiment results show that the signature image could be detect with moderate quality from any clipped images containing ROI area, and the signature is produced using the clipped image involving just a portion of the ROI by splitting the ROI contour into several sections.

In [58], the reversible visible image watermarking method founded on the human being visual structure (HVS) and technique of interest collection (ROI selecting) is suggested. initially Dividing the cover image into blocks that do not overlap. After that, to adaptively change the pixel values, a visual effect factor VEF on the basis of HVS is introduced, the visible watermark and the cover picture would have a greater fusion effect. The VEF value is calculated by using the watermarked and non-watermarked blocks measured within each block's neighborhood. Finally, using the conventional difference-expansion method, the visible watermark is included ın separated blocks, and a ROI-selection technique is developed to identify the most appropriate regions for embedding watermarks. The feasibility and superiority of the suggested scheme relative to any current works is demonstrated by experimental findings.

A watermarking system for a digital image on the basis of DWT-DCT-SVD using particle swarm optimization (PSO) suggested in[59] s evaluated Using different picture processing and compression attacks and success has been achieved, in checking similarities between the original. Therefore, their solution is stable as well as accurate watermarking methodology.

In[60], the invisible and robust not blind Digital watermarking algorithm has been proposed ,with the aid of the Singular Value. Decomposition SVD, as well as Particle Swarm. Optimization PSO. The implementation for such a scheme offers an avenue for maximizing the watermark power (scaling factor) to reach high resistance against attacks by watermarking while maintaining the visual appearance of the cover object.

Two new methods of blind watermarking picture founded on DWT-SVD and RDWT-SVD were introduced in[61]. Any of the schemes displayed resistance to assaults. Although the DWT-SVD system is more vulnerable to few attacks, like JPEG compression, filtering, and scaling, RDWT - SVD system Well performed against the rest of the above attacks. The RDWT - SVD and DWT - SVD are Probabilistic in efficiency. but, Due to RDWT-SVD device ability to resist geometry attacks and the ability to produce RDWT without lack of imperceptibility (other than scaling attacks). SVD-RDWT has been found to be more stable than DWT -SVD.

The RDWT-SVD based watermarking approach for embedding a watermark image that could be as much as wide, the cover of image suggested in[62] provides high robustness against typical attacks by changing specific cover image values in the RDWT domain. Because of RDWT implementation, high imperceptibility, and continuity between the initial and extracted image of the watermark is another advantageous point of the algorithm. The findings revealed that, relative to DWT-based approaches, the proposed approach is more stable for different attacks. RDWT is shift invariant, and a full frame extension is introduced by its redundancy Frame expansion is known to improve robustness with respect to additive noise. Thus, signal processing based on RDWT appears to be more stable than techniques based on DWT. The probability of embedding a large watermark in the co v er picture is another value of this process.

A multiple hybrid watermark technology is proposed [63], to secure medical picture that combines discrete. wavelet transformation (DWT), fast Walsh. Hadmard transformation (FWHT) and decomposition of singular. value (SVD). In their proposed approach, two watermark images are placed in a single medical cover. The findings conclude that the contribution gives invisibility-capacity-robustness a better balance compared to other techniques mentioned.

For non-blind watermarking of still gray level images using discrete wavelet transformation, an entropy-based approach is proposed in [64]. In the embedding step of the watermarking algorithm, Discrete Wavelet Transform (DWT), and Human Visual. System (HVS) characteristics were used. The suggested approach also demonstrates improved results in competition with well-known DWT-based approaches and against the attacks on life.

A (DWT) an d (S V D) based digital image watermarking technique is suggested in[65]. The size factor that Particle Swarm Optimization obtains (PSO). Study and experimental findings suggest

that the methodology proposed is more effective against traditional attacks on image manipulation.

In [66] and its Discrete Wavelet Transform (DWT) and DWTF at Walse Hadamard Transform Comparative Output Study Singular Value Decomposition (DWT-FWHT-SVD) domains. the non-blind optical image watermarking technique. For different noise adds and filtering attacks, the suggested DWT-FWHT-SVD based approach is highly resilient. With Fibonacci-Lucas transform along Using affine transformation, the encryption is applied.

4.2 PROPOSED SCHEME

We suggest a nonblind imae watemarking techique and its coparative perfomance analyss, the image of the watermark will be inserted by integrating Redundant Discrete Wavelet Transform (RDWT), fast Walh Hadamar Trnsform (FWHT), and sinular valu decmposition (SVD) with in the regin of nninterst (RONI) of medical image, the RONI of the coer medcal image is found using Human Visual Systm (HVS). In addition, uing Paricle Swrm Optimization (PSO) for increase a strength o f a watermark. We often prefer to prepare a software pack containing a graphical user interface GUI to use a watermarking framework so that the complete Process of watermarking (embedding, attacks, detection) can be done on a Windows screen instead of typing program lines, as seen in Figure 4.1.

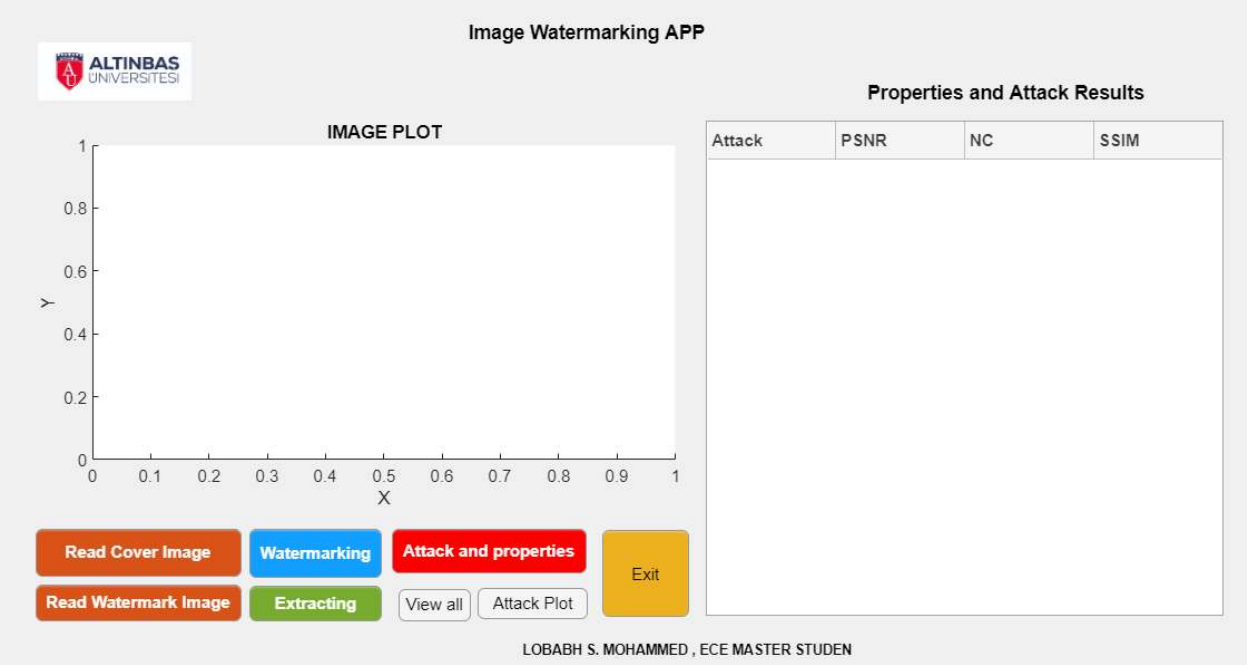


Figure 4.1: GUI interface to use watermarking scheme.

4.2.1 Theoretical Background(methods)

4.2.1.1 Region of Interest (ROI) and Region of Non-Interest (RONI)

Every image can be represented by various region based on information it has. For any medical image, two regions are used for the representation of the image. These regions are called as Region of Interest (ROI) and Region of Non interest (RONI). The ROI contains most and more important information about patient diagnosis while RONI contains mainly black background with some text information. So that if RONI of the medical image is corrupted or degraded by any manipulation than this degradation doesn't effect on diagnosis and treatment of the patient. So visible watermarking is done in RONI of the medical image instead of any position of the image [67]. The ROI and RONI of the medical image are shown in Figure 4.2.

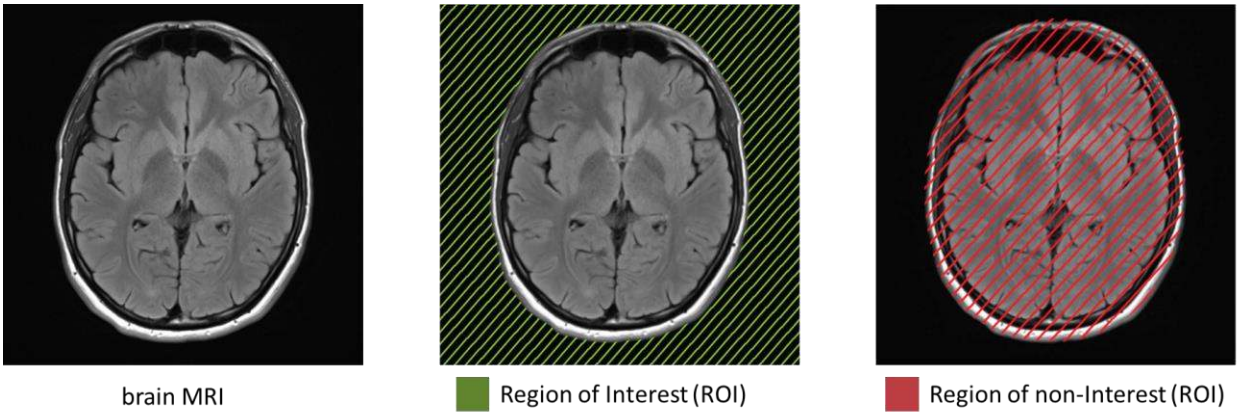


Figure 4.2: Region of Interest (ROI) and Region of Non-Interest (RONI)

4.2.1.2 Human Visual System (HVS)

The Human Visual System (HVS) has been studied for hiding secure information[58], [64]. Since each pixel has a different tolerance to noise and a different effect on its neighboring pixels, in the proposed scheme, HVS characteristics are exploited to achieve higher imperceptibility and more robustness through selecting embedding block regions regarding visual entropy and edge entropy. Visual entropy is used to determine the quantity of tissue content of an image. That means, it is a popular benchmark to describe the texture of an image. Regarding the shannon's definition, the entropy of an image is computed as shown in Eq.(4-1).

$$H_1 = -\sum_{i=0}^{L=1} p_i \log p_i \qquad \textbf{(4-1)}$$

Eq.(4-1): the entropy of an image.

Where pi means the probability of a "i" level occurring with $0 \leq P_i \leq 1$ and $L-1$ $i=0$ $p_i = 1$. [29] proposed edge entropy regarding the benefits of image edge information. In fact, the effect of the neighboring pixel values is estimated by edge entropy. Edge entropy is calculated based on Eq. (4-2):

$$H_2 = \sum_{i=0}^{L=1} b_i \exp^{1-b_i} \quad \textbf{(4-2)}$$

Eq.(4-2): Edge entropy.

where $1-b_i$ means the ignorance or uncertainty of the pixel value.

4.2.1.3 Redundant Discrete Wavelet Transform (RDWT)

DWT is a popular transform in image watermarking due to its performance with respect to DCT. However, DWT generates shift variances due to down-sampling of its bands. This results in a significant alteration of the wavelet coefficients even for a small shift in the input image. Shift variances with DWT produce inaccuracy during image extraction process . Therefore, to overcome this issue, RDWT can be used which is able to eliminate the shift variance by discarding down-sampling and up-sampling of coefficients. Figure 4.3 shows one-dimensional RDWT and its inverse transform. RDWT eliminates the down-sampling and up sampling of coefficients. RDWT analysis and synthesis are provided as follows:

- RDWT analysis:

$$c_j[k] = (c_{j+1}[k] * h_j[-k]), \quad (6)$$
$$d_j[k] = (c_{j+1}[k] * g_j[-k]) \quad (7)$$

(4-3)

- RDWT synthesis:

$$c_{j+1}[k] = \frac{1}{2}(c_j[k] * h_j[k] + d_j[k] * g_j[k]) \quad (8)$$

Eq.(4-3): RDWT

where f [n] denotes the corresponding input signal; h[−k] and g[−k] imply the low- and high-pass analysis filters; h[k] and g[k] represent low- and high-pass synthesis filters; c j and dj indicate the low- and high-band of the coefficient at level j. LL sub-bands obtained from block-based RDWT are transformed by SVD which is described in the next subsection. [68]

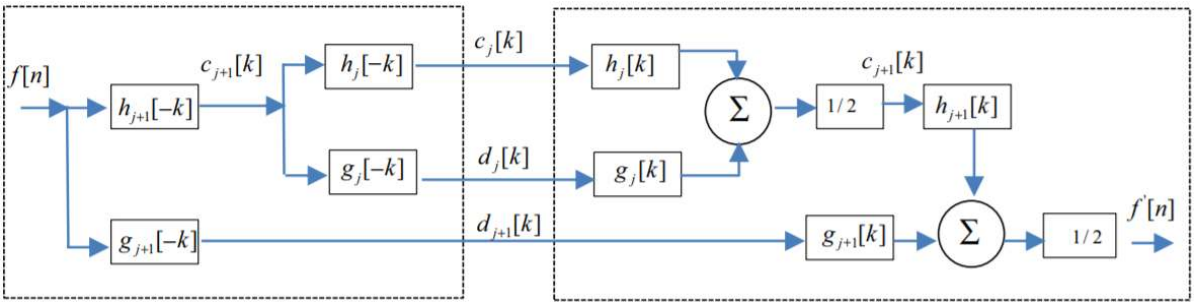


Figure 4.3: Illustration of 1-D RDWT analysis and synthesis filter banks

The advantages of RDWT are given as follows:

i. RDWT provides better quality for image watermarking than the DWT [69]. RDWT produces less distortion in the watermarked images than the conventional DWT. It is proved by an existing research in [70].

ii. RDWT also performs better than DCT, since it does not suffer from blocking artifact at block boundaries. The quality of watermarked images with RDWT has stronger imperceptibility than that with DCT transform.

iii. RDWT eliminates down-sampling and up-sampling of the coefficients that appear in DWT at each filter-bank iteration. By removing down-sampling in RDWT analysis, redundancy of the input sequence can be excluded.

iv. Signal processing with RDWT is more robust than that with DWT. RDWT can increase robustness in case of additive noise [62] and geometrical attacks [61].

4.2.1.4 Singular Value Decomposition (SVD)

Singular value decomposition (SVD) is one of the linear algebraic techniques which diagonalizes a matrix into three matrices. From the perspective of image processing, an image can be viewed as nonnegative scalar entries. The SVD of an image A of size M x N is defined as:

$$\mathrm{A} = \mathrm{U}\mathrm{S}V^{T} \qquad \textbf{(4-4)}$$

Eq.(4-4): SVD equation of an image

Where U and V are orthogonal matrices, U^T U=I, V^T V=I, and S=diag ($\lambda_1, \lambda_2, \lambda_3, \ldots\ldots \lambda_r$). The diagonal values of S are called the singular values of A and each value represents the luminance of an A where r is the rank of A. The columns of U and V are called the left and right singular vectors of A and it preserves the geometrical properties of the image. US are called the principal components of A. UV together called as the SVD Subspace of A. The following are the some of the properties of SVD [55], [63], [65].

a) The singular values of an image have very stability, i.e., when a small perturbation is added to an image, large variation of its singular value does not occur.

b) For an image A, row flipped of A, Arf and column flipped of A, Acf have the same non-zero singular values.

c) Singular values represent intrinsic properties.

4.2.1.5 fast Walsh Hadamard transform (FWHT)

The Walsh-Hadamard transform decomposes a signal into a set of basic functions that are rectangular or square waves with values of + 1 or -1. These basis functions are non-sinusoidal, orthogonal transformation technique. The FWHT can represent signals with sharp discontinuities more accurately using fewer coefficients than the FFT. For 2-D images FWHT coefficients are calculated by first row wise then column n wise. The FWHT and inverse of FWHT for a signal x (t) of length N are defined as [63], [66] :

$$y_n = \frac{1}{N}\sum_{i=0}^{N-1} x_i \;\; WAL(n,i) \qquad \textbf{(4-5)}$$

Eq.(4-5): FWHT equation**.**

$$x_i = \sum_{i=0}^{N-1} y_n \;\; WAL(n,i) \qquad \textbf{(4-6)}$$

Eq.(4-6): inverse of FWHT equation**.**

Where i = 0, 1, ... N-l and WAL (n,i) are Walsh functions. Some examples of 1x1, 2x2 Hadamard matrices are defined by (Eq.(4-7)) and (Eq.(4-8)) respectively:

$$H_{0=1} \tag{4-7}$$

Eq.(4-9): 1*1 Dimension Walsh array**.**

$$H_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{4-8}$$

Eq.(4-10): 2*2 Walsh array.

The first eight Walsh functions have these values:

Table 4.1: values of the first eight Walsh function

Index	Walsh Function Values							
0	1	1	1	1	1	1	1	1
1	1	1	1	1	-1	-1	-1	-1
2	1	1	-1	-1	-1	-1	1	1
3	1	1	-1	-1	1	1	-1	-1
4	1	-1	-1	1	1	-1	-1	1
5	1	-1	-1	1	-1	1	1	-1
6	1	-1	1	-1	-1	1	-1	1
7	1	-1	1	-1	1	-1	1	-1

FWHT offers advantages such as its simplicity of implementation and its fastness of calculation of the coefficients of Hadamard (less computational complexity) [66].

4.2.1.6 Particle Swarm Optimization (PSO) for Scaling Factor Evaluation

The scaling factor is a key point in the SVD-based image watermarking which has a significant effect on both robustness and the fidelity of the watermarked image. The scaling factor is an image dependent parameter, so we are providing scaling factor in the matrix form instead of a scaling value. For finding the suitable scaling factors, we have used particle swarm optimization.

Particle Swarm optimization (PSO) is an evolutionary computation technique and population driven algorithm, developed by Kennedy and Eberhart, 1995 [71]inspired by social behavior and movement dynamics of insects, birds, and fish. It is one of the metaheuristic algorithms like

genetic algorithm, ant colony etc. Some of the attractive features of the PSO include ease of implementation and the fact that no gradient information is required. In PSO, the potential solutions, called particles and the group of particles are called swarm; fly through the problem space by following the current optimum particles. Each particle keeps track of its coordinates in the problem space which are associated with the best solution (fitness) it has achieved so far. This value is called p_{best} (p_b). Another "best" value that is tracked by the particle swarm optimizer is the best value, obtained so far by any particle in the neighbors of the particle. This location is called l_{best}. When a particle takes all the population as its topological neighbors, the best value is a global best and is called g_{best} (g_b). The fitness values are evaluated from the fitness function (objective function). It is totally problem dependent. Let s denote the swarm size. Each individual particle i ($1 \leq i \leq s$) has the following properties: a current position x_i in search space, a current velocity vi, and a personal best position pi in the search space, and the global best position P_{gb} among all the p_i During each iteration, each particle in the swarm is updated using the following equation [59].

$$v_i(t+1)=k\,[w_i\,v_i\,(t)+c_1\,r_1\,(pb-x_i(t))+c_2r_2\,(gb-x_i(t))] \quad (1)$$

$$x_i\,(t+1)=x_i(t)+v_i(t+1) \quad (2) \qquad \textbf{(4-9)}$$

Eq.(4-11): pso function.

where vi[t] is the particle velocity, xi[t] is the particle position at i the iteration, p_b and g_b are defined as stated before. r_1 and r_2 are random numbers between (0,1). c_1, c_2 are acceleration factors, k is the constriction factor and w_i is inertia weight which are responsible for convergence of the scheme.

4.2.1.7 Arnold

Although the transform is simple in Arnold Transform Map, but it not only scrambles the pixel position by encoding the number of iterations, but it also reduces the key storage and transfer spaces Assume that on the one hand, the original watermark image pixels are (x, y), if these pixels are scrambled N times, it results in the scrambled pixels (x', y'). On the other hand, Arnold transforming is reversible and to obtain the original state of the watermark image, a fixed time of the transforming should be applied on the scrambled watermark image. Thus, the

watermark image scrambling time can be regarded as a watermark key. Suppose the watermark image is with size of M×M; in addition, x and y are the coordinates of the watermark image's pixel; moreover, x' and y' are the coordinates after transforming. Accordingly, 2-dimensional Arnold transformation is computed based on the following Equation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (\text{mod } M) \qquad \textbf{(4-10)}$$

Eq.(4-12): Arnold transformation**.**

where x,y ∈ {0, 1, .., M − 1} and all pixels in the watermark image are transformed based on the above Equation to obtain the scrambled watermark image.[72]

4.2.2 Embedding

The embedding process will be in the following steps, also it's shown in figure 4.4:

a) Read the cover Medical image and check it , if it is RGB image then converts it to grayscale by eliminating the hue and saturation information while retaining the luminance.

b) Apply Region of Non-Interest (RONI) search algorithms on the cover medical image to get RONI of the medical image where watermark is inserted.

HVS —Apply→ Host image=[ROI,RONI]

c) Using RDWT transform to decompose RONI of the medical image into four bands [host_LL, host_LH, host_HL, host_HH].

RDWT —Apply→ RONI=[host_LL, host_LH, host_HL, host_HH]

d) Apply Fast Discrete Walsh-Hadamard Transform on host_HL sub band of the medical image to find host_temp.

e) Apply SVD transform, as following:

SVD —Apply→ Host_temp= U^i, S^i, V^i

f) Read the watermark image (ERP) and encrypt it using Arnold transform,

watermark —Arnold encryption→ Host_temp= U^i, S^i, V^i

The watermark image will contain the following:

I. Doctor identity

II. Indexing for database of the patient,

III. Information about medical test and patient situation.

g) Modify the Singular Values S by embedding the encrypted watermark directly, and then again apply SVD to it, respectively, as follows:

$$S_{new} = S + alpha * epr; \quad \textbf{(4-11)}$$

Eq.(4-13):modifying S values.

Where alpha is scaling factor and will be founded automatically by training PSO algorithm.

h) Rebuild image to find the watermarked image by using the following steps.

I. Inverse SVD transform as the following:

SVD —Inverse→ U * S_{new} * V

II. Apply inverse of FWHT transform to find the modified host_HL sub band

III. Apply inverse of RDWT transform to find RONI of medical watermarked image.

IV. At the last step we will combine ROI and modified RONI to find the watermark medical image.

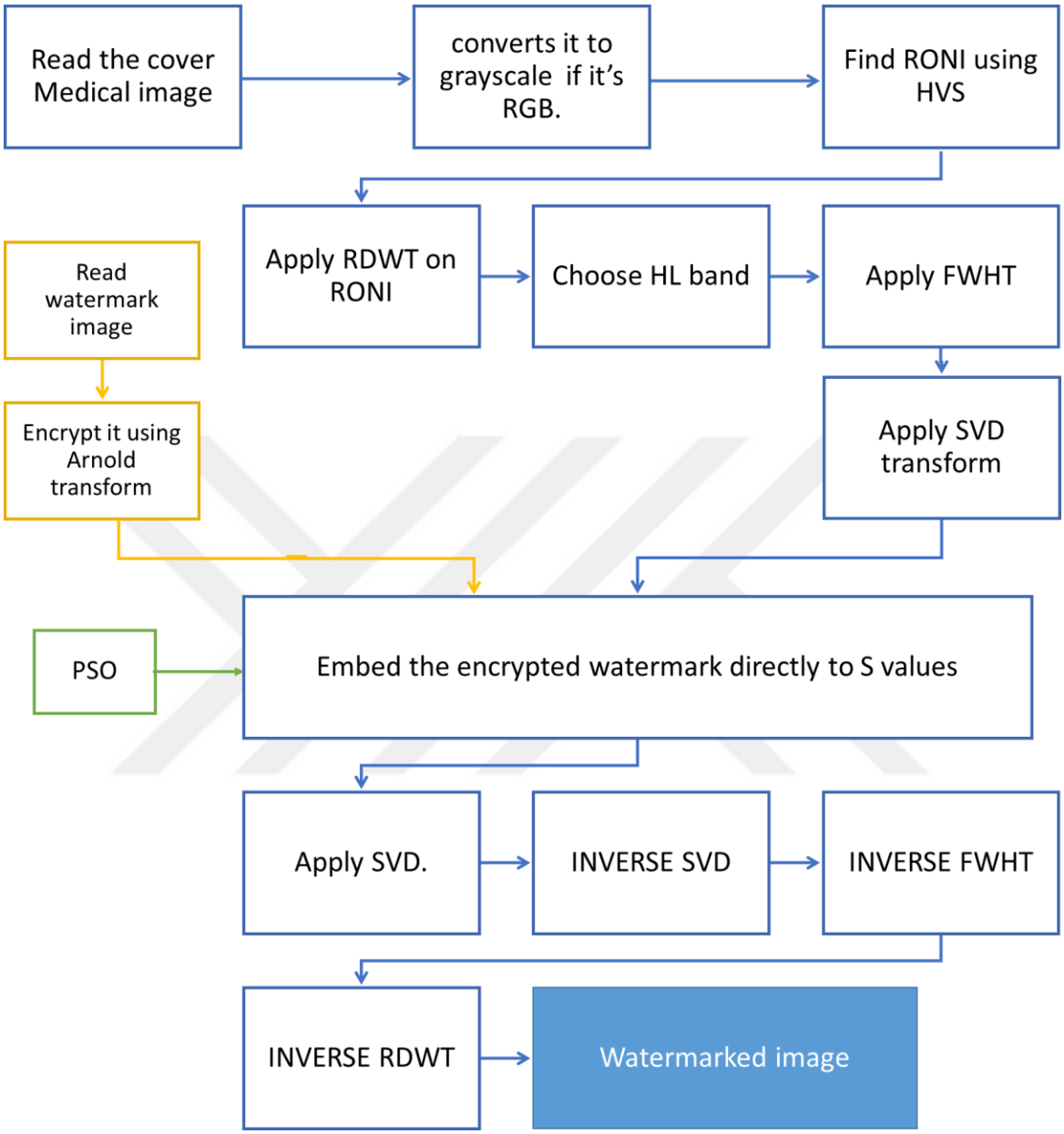


Figure 4.4: watermarking process

4.2.3 Extracting

The steps of watermark extraction process are given below.

a) Read the watermarked medical image,

b) Find the region on noninterest of the image.

c) Apply RDWT transform on RONI of the watermarked medical image to get four sub bands, [retrieved_LL,retrieved_LH,retrieved_HL,retrieved_HH].

d) After that apply FWHT on the HL sub band.

e) Apply SVD transform on the modified band ,as following: $I_{new}=S^{i}*V^{i*}D^{i}$.

f) Extract the encryption watermark image, and it can be done using the following equation:w

$$E_n = (S_{new} - S)/\ alpha \quad \textbf{(4-12)}$$

Eq.(4-14):extract image.

Where E_n is the encrypted watermark and S is the singular values of the original image.

g) Decrypt image by applying inverse of Arnold transform.

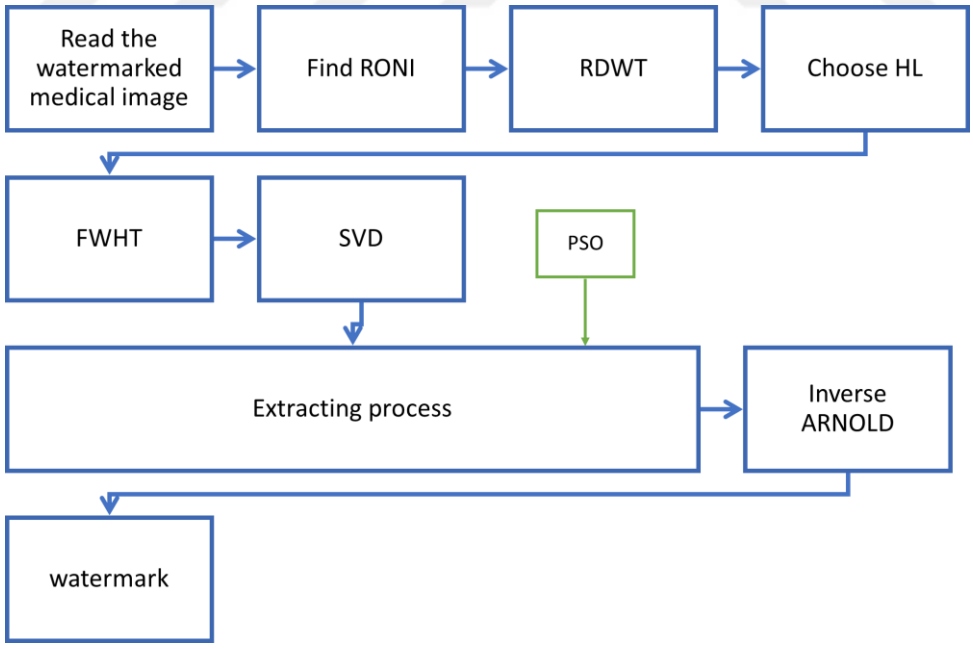


Figure 4.5:extracting.

4.3 Results And Performance Analysis

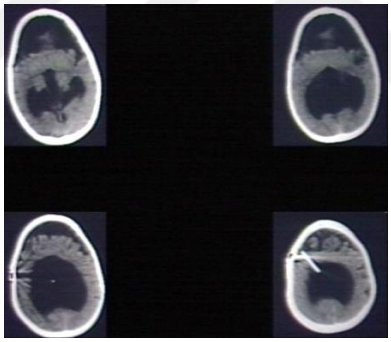
The proposed scheme and GUI app was implemented in Matlab R2020b. Various experiments are performed on seven cover medical images hand x-ray, lung x-ray, femur and hip MRI, hip MRI, brain CT scan, chest CT scan, kidney MRI of size “512x512” shown in Figure 4.6. Two size of watermark images used “512x512” and “256x256”.

(a) lung x-ray.

(b) hand x-ray.

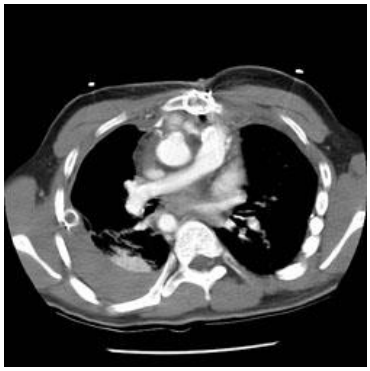
(c) femur and hip MRI.

(d) hip MRI.



(e) brain CT scan.

(f) kidney MRI.



(g) chest CT scan.

Figure 4.6: Cover medical images.

Each digital image watermarking scheme must achieve the necessary requirements which are imperceptibility, robustness, capacity, and security. The imperceptibility requirement to indicate the similarity between the host image and the watermark image. If the watermark image is looking same as the host image, which means the scheme achieved the imperceptibility.

The PSNR (Peak Signal-to-Noise Ratio) is used to estimate the similarity between the cover medical image and the watermarked image. High PSNR means good imperceptibility. It is calculated as follows:

$$PSNR = 10\log_{10}[\frac{max(x(i,j))^2}{MSE}] \quad \textbf{(4-13)}$$

Eq.(4-15): Peak Signal-to-Noise Ratio.

Where the Mean Square Error (MSE) between the host image x and the watermarked image y is defined as:

$$MSE = \frac{1}{m*n}\sum_{i=1}^{m}\sum_{j=1}^{n}[x(i,j) - y(i,j)]^2 \quad \textbf{(4-14)}$$

Eq.(4-16): Mean Square Error.

Also, perceptual similarity image quality (SSIM) gives a similarity measure between host image and the watermarked image. SSIM can take a value in the range of −1 to 1, when a value of 1 means that the two images are completely like each other.

To evaluate the robustness of the proposed schemes, the watermarked images are exposed to various attacks. The Normalized Cross-Correlation (NC) measures the similarity between the original watermark and the extracted watermark from the attacked image. The NC is defined as:

$$NC(w,\overline{w}) = \frac{\sum_{i=1}^{N} w_i\overline{w_i}}{\sqrt{\sum_{i=1}^{N} {w_i}^2}\sqrt{\sum_{i=1}^{N} \overline{w_i}^2}} \quad \textbf{(4-15)}$$

Eq.(4-17): Normalized Cross-Correlation.

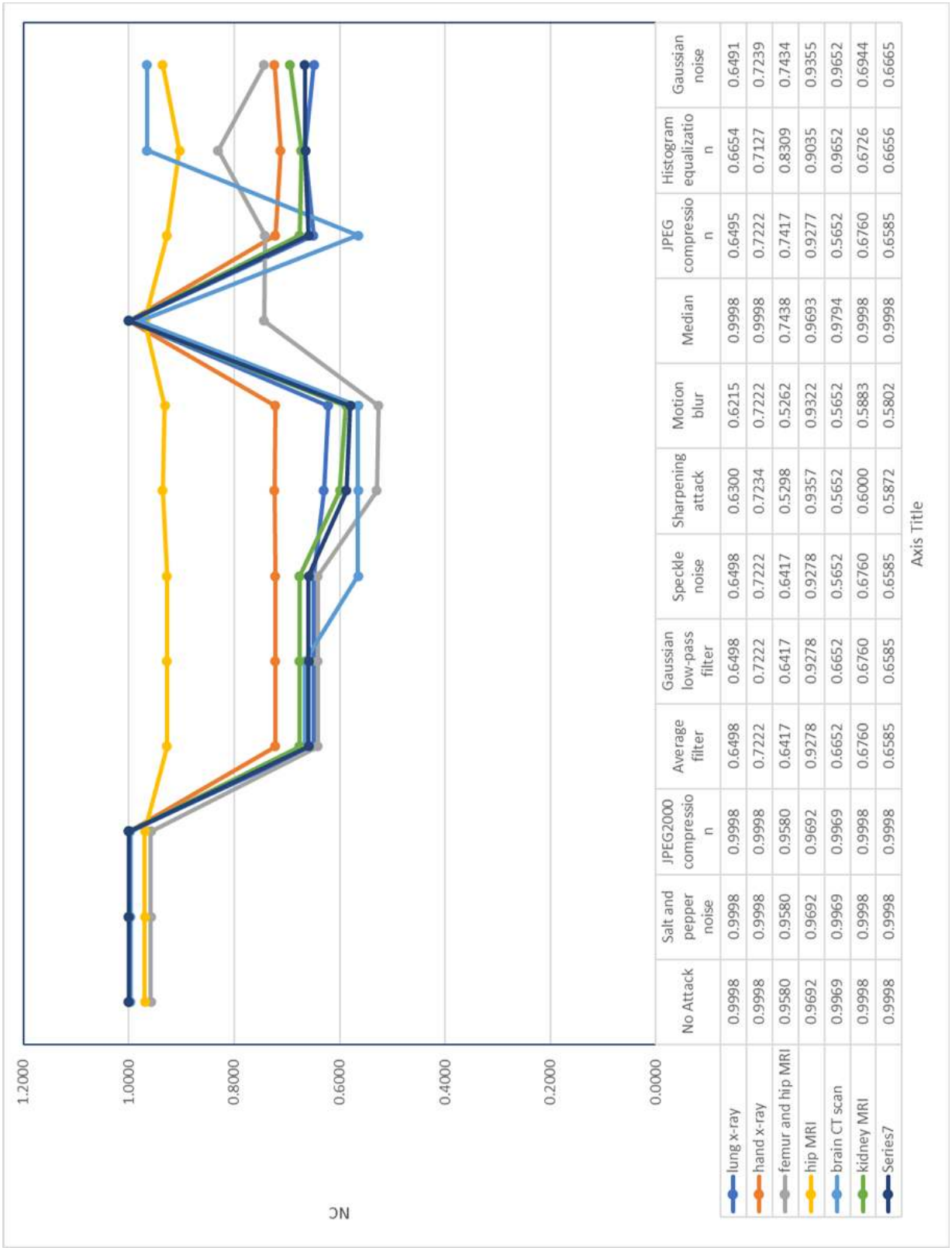
After implementing our scheme, it shows high imperceptibility and robustness as shown in table below:

Table 4.2: PSNR, NC, SSIM on different images with zero attack**.**

image	PSNR	NC	SSIM
lung x-ray	Inf	1.00	1.00
hand x-ray	Inf	1.00	1.00
femur and hip MRI	Inf	0.97	1.00
hip MRI	48.57	0.97	0.98
brain CT scan	48.57	0.97	0.98
kidney MRI	Inf	1.00	1.00
chest CT scan	Inf	1.00	1.00

Our scheme has been tested under different extreme attacks. NC values of extracted watermark image under severe image processing, compression and geometrical attacks are presented in chart (4.1) , some image processing attacks such as low-pass filter, Gaussian noise, sharpening, median filter, pepper and salt noise, speckle noise, histogram equalization, JPEG, JPEG2000 and JPEG XR are simulated to evaluate the performance of the proposed scheme.

Chart 4.1: NC varies multiple attack.



	No Attack	Salt and pepper noise	JPEG2000 compression	Average filter	Gaussian low-pass filter	Speckle noise	Sharpening attack	Motion blur	Median	JPEG compression	Histogram equalization	Gaussian noise
lung x-ray	0.9998	0.9998	0.9998	0.6498	0.6498	0.6498	0.6300	0.6215	0.9998	0.6495	0.6654	0.6491
hand x-ray	0.9998	0.9998	0.9998	0.7222	0.7222	0.7222	0.7234	0.7222	0.9998	0.7222	0.7127	0.7239
femur and hip MRI	0.9580	0.9580	0.9580	0.6417	0.6417	0.6417	0.5298	0.5262	0.7438	0.7417	0.8309	0.7434
hip MRI	0.9692	0.9692	0.9692	0.9278	0.9278	0.9278	0.9357	0.9322	0.9693	0.9277	0.9035	0.9355
brain CT scan	0.9969	0.9969	0.9969	0.6652	0.6652	0.5652	0.5652	0.5652	0.9794	0.5652	0.9652	0.9652
kidney MRI	0.9998	0.9998	0.9998	0.6760	0.6760	0.6760	0.6000	0.5883	0.9998	0.6760	0.6726	0.6944
Series7	0.9998	0.9998	0.9998	0.6585	0.6585	0.6585	0.5872	0.5802	0.9998	0.6585	0.6656	0.6665

The following figures shows watermarked image and extracted image that we applied for all images and PSNR value and Nc value for each one of them:

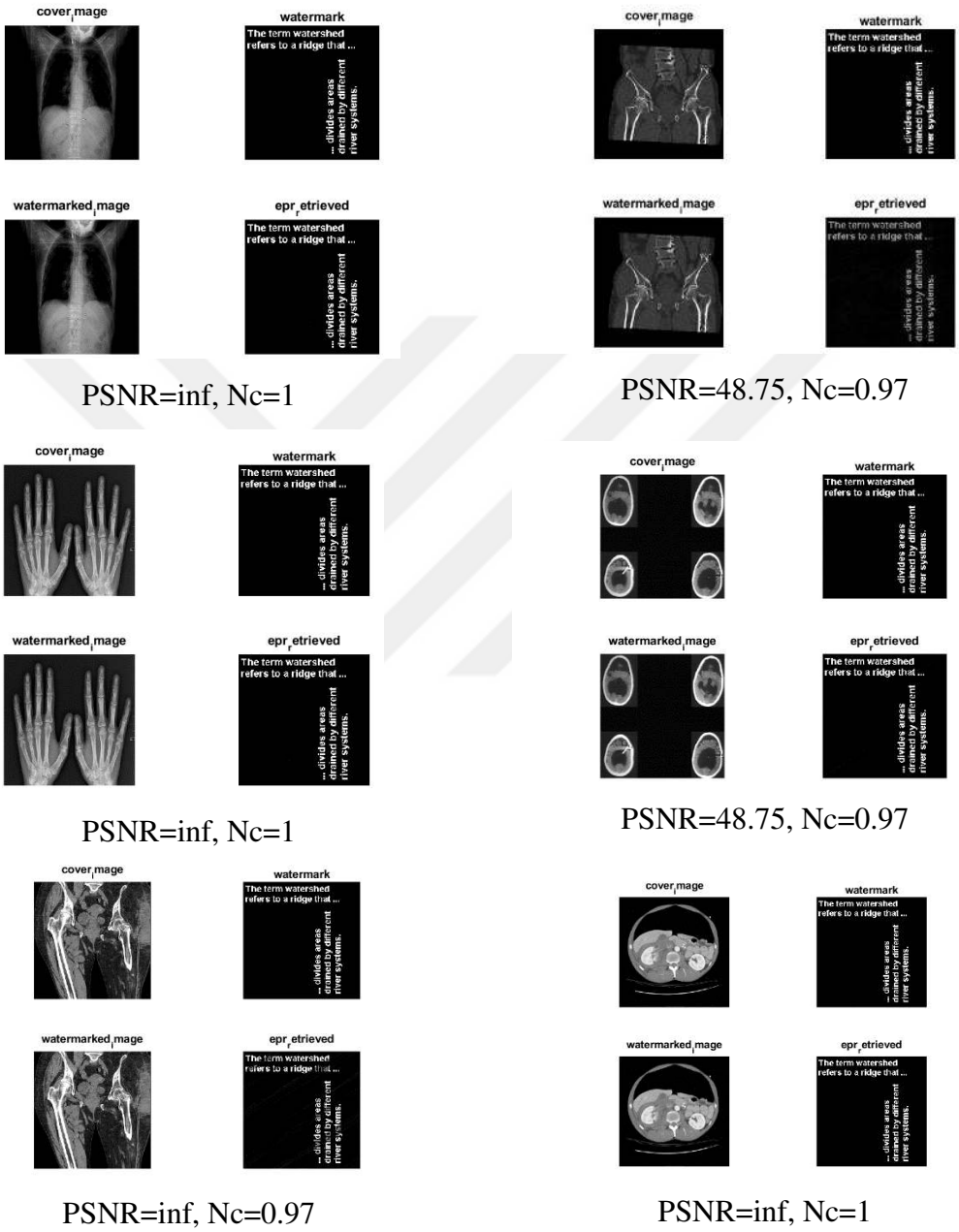


Figure 4.7:embedding and extracting of medical images and values of PSNR and NC without attack.

4.4 GUIDE FOR THE APP

Apps provide point-and-click control of the software applications, eliminating the need for others to learn a language or type commands to run the application. we can share apps both for use within MATLAB and as standalone desktop or web apps.

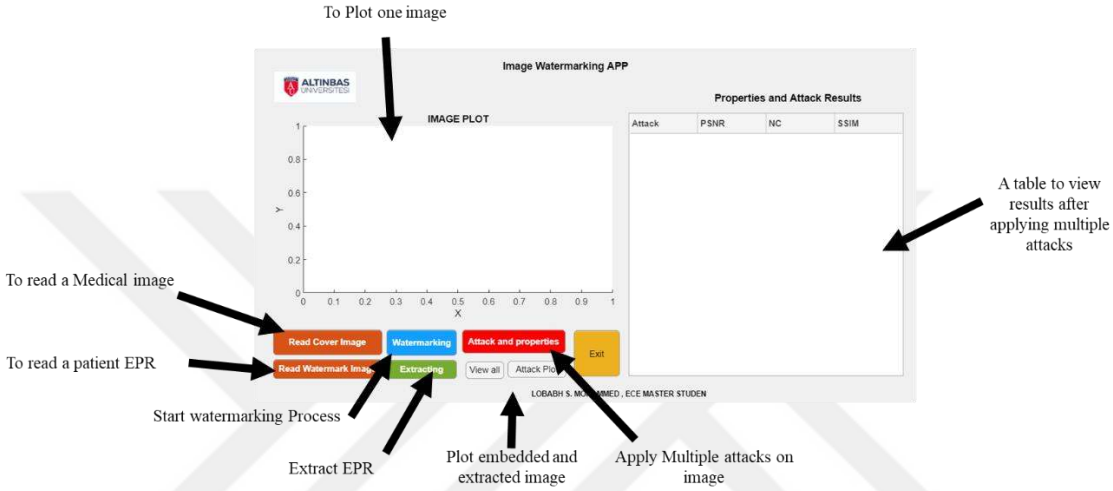


Figure 4.8: explanation for each buttons function.

After we click on watermarking button a message will popup contain information about watermarking process and tell the user when it will finish as shown in figure below:

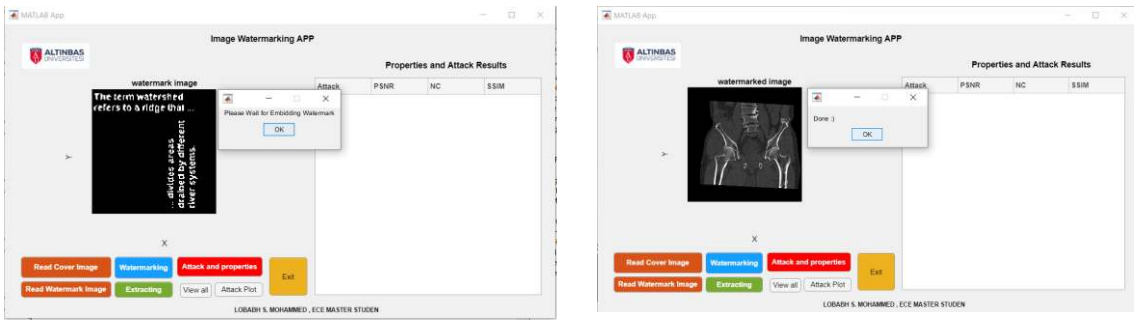


Figure 4.9: watermarking notification.

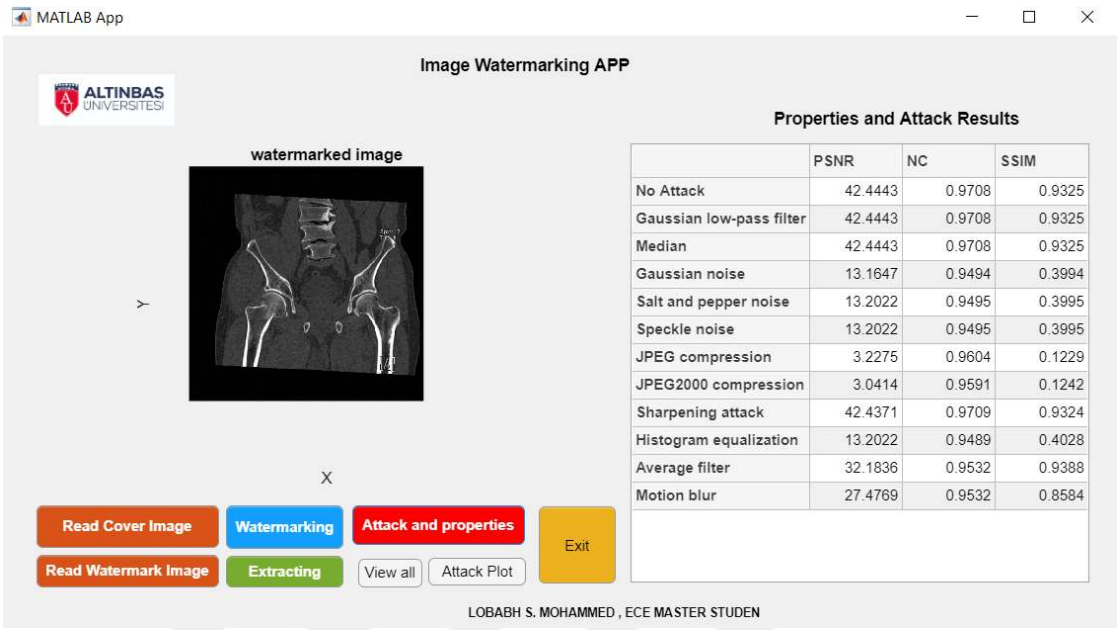


Figure 4.10: properties and attack results properties in app interface.

4.5 CONCLUSION

We presented a hybrid non-blind watermarking method of grayscale images based on RDWT-FWHT-SVD-PSO in aim of protecting privacy of patients where watermark image in will embedded in RONI of medical cover image based on HVS So that, if the RONI of a medical image is corrupted or Being degraded Through some manipulation than this degradation doesn't effect on diagnosis and treatment of the patient.

The results have shown that the approach proposed is more stable for diverse attacks. Also using a specialized PSO gives more imperceptibility and compatibility between the original and extracted watermark. And one more advntage of this metod is the possiility to emed a large watermark in the cove image.

Finally, a GUI interface make easy to use by any user and we can share it via multiple workspaces.

4.6 FUTURE WORK

As a future work, we can extend this methodology to RGB pictures, even by making a minor adjustment the method may be changed to be dual image watermarking or insert Roi of medical image as a backup copy of the original image.

REFERENCES

[1] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2960617.

[2] A. Bakshi and A. K. Patel, "Secure telemedicine using RONI halftoned visual cryptography without pixel expansion," *Journal of Information Security and Applications*, vol. 46, Jun. 2019, doi: 10.1016/j.jisa.2019.03.004.

[3] J. C. Dagadu and J. Li, "Context-based watermarking cum chaotic encryption for medical images in telemedicine applications," *Multimedia Tools and Applications*, vol. 77, no. 18, Sep. 2018, doi: 10.1007/s11042-018-5725-y.

[4] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimedia Tools and Applications*, vol. 76, no. 3, Feb. 2017, doi: 10.1007/s11042-016-3928-7.

[5] J. Cheng, J. Zhou, Q. Liu, X. Tang, and Y. Guo, "A DDoS Detection Method for Socially Aware Networking Based on Forecasting Fusion Feature Sequence," *The Computer Journal*, vol. 61, no. 7, Jul. 2018, doi: 10.1093/comjnl/bxy025.

[6] J.-P. A. Yaacoub *et al.*, "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, Apr. 2020, doi: 10.1016/j.future.2019.12.028.

[7] N. P. Terry, "Protecting Patient Privacy in the Age of Big Data," *SSRN Electronic Journal*, 2012, doi: 10.2139/ssrn.2153269.

[8] L. Ohno-Machado, P. S. P. Silveira, and S. Vinterbo, "Protecting patient privacy by quantifiable control of disclosures in disseminated databases," *International Journal of Medical Informatics*, vol. 73, no. 7–8, Aug. 2004, doi: 10.1016/j.ijmedinf.2004.05.002.

[9] P. Aparna and P. V. V. Kishore, "Biometric-based efficient medical image watermarking in E-healthcare application," *IET Image Processing*, vol. 13, no. 3, Feb. 2019, doi: 10.1049/iet-ipr.2018.5288.

[10] Q. Dai, J. Li, U. A. Bhatti, Y.-W. Chen, and J. Liu, "SWT-DCT-Based Robust Watermarking for Medical Image," 2019.

[11] T. K. Araghi and A. A. Manaf, "An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD," *Future Generation Computer Systems*, vol. 101, Dec. 2019, doi: 10.1016/j.future.2019.07.064.

[12] J. Liu, J. Li, J. Ma, N. Sadiq, and Y. Ai, "FDCT and Perceptual Hash-Based Watermarking Algorithm for Medical Images," 2019.

[13] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks*, vol. 2018, 2018, doi: 10.1155/2018/5978636.

[14] S. Sinha Roy, A. Basu, and A. Chattopadhyay, "On the implementation of a copyright protection scheme using digital image watermarking," *Multimedia Tools and Applications*, vol. 79, no. 19–20, May 2020, doi: 10.1007/s11042-020-08652-9.

[15] R. P. G. S. B. C. Deepshikha Chopra, "Quality Evaluation for LSB Replacement Watermarking of Grayscale Images," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 3, no. 5, May 2014.

[16] A. Zear, A. K. Singh, and P. Kumar, "A proposed secure multiple watermarking technique based on DWT, DCT and SVD for application in medicine," *Multimedia Tools and Applications*, vol. 77, no. 4, Feb. 2018, doi: 10.1007/s11042-016-3862-8.

[17] S. P. Mohanty, K. R. Ramakrishnan, and M. Kankanhalli, "A dual watermarking technique for images," 1999, doi: 10.1145/319878.319891.

[18] F. A. P. Petitcolas, "Kerckhoffs' Principle," in *Encyclopedia of Cryptography and Security*, Boston, MA: Springer US, 2011.

[19] A. S. Brar and M. Kaur, “High Capacity, Reversible Data Hiding Using CDCSAlong with Medical Image Authentication,” *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 8, no. 1, Jan. 2015, doi: 10.14257/ijsip.2015.8.1.05.

[20] Y. Liu, S. Tang, R. Liu, L. Zhang, and Z. Ma, “Secure and robust digital image watermarking scheme using logistic and RSA encryption,” *Expert Systems with Applications*, vol. 97, May 2018, doi: 10.1016/j.eswa.2017.12.003.

[21] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat, “Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption,” *IEEE Access*, vol. 6, 2018, doi: 10.1109/ACCESS.2018.2808172.

[22] H. Nyeem, W. Boles, and C. Boyd, “A Review of Medical Image Watermarking Requirements for Teleradiology,” *Journal of Digital Imaging*, vol. 26, no. 2, Apr. 2013, doi: 10.1007/s10278-012-9527-x.

[23] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, “Watermarking Techniques used in Medical Images: a Survey,” *Journal of Digital Imaging*, vol. 27, no. 6, Dec. 2014, doi: 10.1007/s10278-014-9700-5.

[24] F.-H. Wang, J.-S. Pan, and L. C. Jain, *Innovations in Digital Watermarking Techniques*, vol. 232. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009.

[25] N. A. Memon, A. Chaudhry, M. Ahmad, and Z. A. Keerio, “Hybrid watermarking of medical images for ROI authentication and recovery,” *International Journal of Computer Mathematics*, vol. 88, no. 10, Jul. 2011, doi: 10.1080/00207160.2010.543677.

[26] Vaishali S. Jabade and Dr. Sachin R. Gengaje, “ Literature Review of Wavelet Based Digital Image Watermarking Techniques.,” *International Journal of Computer Applications*, vol. 31, no. 7, pp. 28–35, Oct. 2011.

[27] N. A. Memon, S. A. M. Gilani, and A. Ali, “Watermarking of chest CT scan medical images for content authentication,” Aug. 2009, doi: 10.1109/ICICT.2009.5268167.

[28] M.-S. Hwang and W. Nan-I, “Data Hiding: Current Status and Key Issues,” *nternational Journal of Network Security*, vol. 07, pp. 1–9, Jan. 2007.

[29] Z. Wenyin and F. Y. Shih, “Semi-fragile spatial watermarking based on local binary pattern operators,” *Optics Communications*, vol. 284, no. 16–17, Aug. 2011, doi: 10.1016/j.optcom.2011.04.004.

[30] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark,” doi: 10.1109/ICIP.1994.413536.

[31] E. F. Badran, M. A. Sharkas, and O. A. Attallah, “Multiple watermark embedding scheme in wavelet-spatial domains based on ROI of medical images,” in *2009 National Radio Science Conference*, 2009, pp. 1–8.

[32] J. Mohamad Zain and M. Clarke, “Reversible Region of Non-Interest (RONI) Watermarking for Authentication of DICOM Images,” *Computing Research Repository - CORR*, vol. 7, Jan. 2011.

[33] Ensaf Hussein and Mohamed A. Belal, “Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media: A Survey,” *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)*, vol. 1, no. 7, Sep. 2012.

[34] C.-M. Pun, “High Capacity and Robust Digital Image Watermarking,” 2009, doi: 10.1109/NCM.2009.85.

[35] A. K. Singh, B. Kumar, M. Dave, S. P. Ghrera, and A. Mohan, “Digital Image Watermarking,” in *Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security*, IGI Global , 2016.

[36] H.-C. Huang and W.-C. Fang, “Techniques and applications of intelligent multimedia data hiding,” *Telecommunication Systems*, vol. 44, no. 3–4, Aug. 2010, doi: 10.1007/s11235-009-9262-x.

[37] T. Mark, “Medical Identity Theft and Telemedicine Security,” *Telemedicine and e-Health*, vol. 15, no. 10, Dec. 2009, doi: 10.1089/tmj.2009.9932.

[38] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, “Multiple Watermarking on Medical Images Using Selective Discrete Wavelet Transform Coefficients,” *Journal of Medical Imaging and Health Informatics*, vol. 5, no. 3, Jun. 2015, doi: 10.1166/jmihi.2015.1432.

[39] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, "Digital Image Watermarking: Concepts and Applications," in *Medical Image Watermarking*, Cham: Springer International Publishing, 2017.

[40] A. K. Singh, B. Kumar, G. Singh, and A. Mohan, "Robust and Secure Multiple Watermarking for Medical Images," in *Medical Image Watermarking*, Cham: Springer International Publishing, 2017.

[41] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Robust and Imperceptible Dual Watermarking for Telemedicine Applications," *Wireless Personal Communications*, vol. 80, no. 4, Feb. 2015, doi: 10.1007/s11277-014-2091-6.

[42] A. Sharma, A. K. Singh, and S. P. Ghrera, "Robust and Secure Multiple Watermarking for Medical Images," *Wireless Personal Communications*, vol. 92, no. 4, Feb. 2017, doi: 10.1007/s11277-016-3625-x.

[43] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management," *IEEE Transactions on Information Technology in Biomedicine*, vol. 10, no. 4, Oct. 2006, doi: 10.1109/TITB.2006.875655.

[44] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, and R. Collorec, "Relevance of watermarking in medical imaging," doi: 10.1109/ITAB.2000.892396.

[45] C.-H. Huang and J.-L. Wu, "Attacking Visible Watermarking Schemes," *IEEE Transactions on Multimedia*, vol. 6, no. 1, Feb. 2004, doi: 10.1109/TMM.2003.819579.

[46] Liu Yongliang and Wen Gao, "Secure watermark verification scheme," doi: 10.1109/ICME.2004.1394352.

[47] N. Agarwal, A. K. Singh, and P. K. Singh, "Survey of robust and imperceptible watermarking," *Multimedia Tools and Applications*, vol. 78, no. 7, Apr. 2019, doi: 10.1007/s11042-018-7128-5.

[48] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: its formal model, fundamental properties and possible attacks," *EURASIP Journal on Advances in Signal Processing*, vol. 2014, no. 1, Dec. 2014, doi: 10.1186/1687-6180-2014-135.

[49] K. Chitra and V. P. Venkatesan, “Spatial Domain Watermarking Technique,” Aug. 2016, doi: 10.1145/2980258.2980363.

[50] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, “Attacks on digital watermarks: classification, estimation based attacks, and benchmarks,” *IEEE Communications Magazine*, vol. 39, no. 8, Aug. 2001, doi: 10.1109/35.940053.

[51] C.-Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, M. L. Miller, and Y. M. Lui, “Rotation, scale, and translation resilient watermarking for images,” *IEEE Transactions on Image Processing*, vol. 10, no. 5, May 2001, doi: 10.1109/83.918569.

[52] J. Dittmann, P. Wohlmacher, and K. Nahrstedt, “Using cryptographic and. watermarking algorithms,” *IEEE Multimedia*, vol. 8, no. 4, 2001, doi: 10.1109/93.959103.

[53] M. Kutter, S. v. Voloshynovskiy, and A. Herrigel, “Watermark copy attack,” May 2000, doi: 10.1117/12.384991.

[54] K P Soman, K I Ramachandran, and N G Resmi, *Insight into wavelets : from theory to practice*, 3rd ed. New Delhi [India]: PHI Learning, 2010.

[55] A. Joseph and K. Anusudha, “Robust watermarking based on DWT SVD,” 2013.

[56] Usha Verma and Neelam Sharma, “Hybrid Mode of Medical Image Watermarking To Enhance Robustness and Imperceptibility,” *International Journal of Innovative Technology and Exploring Engineering*, vol. 9, no. 1, Nov. 2019, doi: 10.35940/ijitee.A4126.119119.

[57] A. Wakatani, “Digital watermarking for ROI medical images by using compressed signature image,” doi: 10.1109/HICSS.2002.994129.

[58] W. Qi, G. Yang, T. Zhang, and Z. Guo, “Improved reversible visible image watermarking based on HVS and ROI-selection,” *Multimedia Tools and Applications*, vol. 78, no. 7, Apr. 2019, doi: 10.1007/s11042-018-6812-9.

[59] V. S. Rao, R. S. Shekhawat, and V. K. Srivastava, “A DWT-DCT-SVD based digital image watermarking scheme using particle swarm optimization,” Mar. 2012, doi: 10.1109/SCEECS.2012.6184795.

[60] M. Roychowdhury, S. Sarkar, S. Laha, and S. Sarkar, “Efficient Digital Watermarking Based on SVD and PSO with Multiple Scaling Factor,” 2015.

[61] T. H. Rassem, N. M. Makbol, and B. E. Khoo, “Performance evaluation of RDWT-SVD and DWT-SVD watermarking schemes,” 2016, doi: 10.1063/1.4965108.

[62] S. L. -, M. S. -, and M. F. -, “A New Robust Watermarking Scheme Based on RDWT-SVD,” *International Journal of Intelligent Information Processing*, vol. 2, no. 1, Mar. 2011, doi: 10.4156/ijiip.vol2.issue1.3.

[63] I. Assini, A. Badri, K. Safi, A. Sahel, and A. Baghdad, “Hybrid multiple watermarking technique for securing medical image using DWT-FWHT-SVD,” May 2017, doi: 10.1109/ATSIP.2017.8075569.

[64] A. Tabibiazar, R. Safabakhsh, and S. Zaboli, “Entropy-Based image watermarking using DWT and HVS SETIT 2005 ENTROPY-BASED IMAGE WATERMARKING USING DWT AND HVS.” [Online]. Available: https://www.researchgate.net/publication/228386448.

[65] V. Verma, V. K. Srivastava, and F. Thakkar, “DWT-SVD based digital image watermarking using swarm intelligence,” Mar. 2016, doi: 10.1109/ICEEOT.2016.7755292.

[66] B. L. Gunjal and S. N. Mali, “Comparative performance analysis of digital image watermarking scheme in DWT and DWT-FWHT-SVD domains,” Dec. 2014, doi: 10.1109/INDICON.2014.7030391.

[67] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, “A RONI Based Visible Watermarking Approach for Medical Image Authentication,” *Journal of Medical Systems*, vol. 41, no. 9, Sep. 2017, doi: 10.1007/s10916-017-0795-3.

[68] F. Ernawan and M. N. Kabir, “A block-based RDWT-SVD image watermarking method using human visual system characteristics,” *The Visual Computer*, vol. 36, no. 1, Jan. 2020, doi: 10.1007/s00371-018-1567-x.

[69] L. Gao, T. Gao, J. Zhao, and Y. Liu, “Reversible Watermarking in Digital Image Using PVO and RDWT,” *International Journal of Digital Crime and Forensics*, vol. 10, no. 2, Apr. 2018, doi: 10.4018/IJDCF.2018040103.

[70] T. D. Hien, Z. Nakao, and Y.-W. Chen, “RDWT Domain Watermarking based on Independent Component Analysis Extraction,” in *Applied Soft Computing Technologies: The Challenge of Complexity*, Berlin/Heidelberg: Springer-Verlag.

[71] Xiaohui Hu, “Particle Swarm Optimization,” *http://www.swarmintelligence.org/*, 2006. .

[72] S. B. B. Ahmadi, G. Zhang, M. Rabbani, L. Boukela, and H. Jelodar, “An intelligent and blind dual color image watermarking for authentication and copyright protection,” *Applied Intelligence*, Oct. 2020, doi: 10.1007/s10489-020-01903-0.