الجمهورية الجزائرية الديمقراطية الشعبية
وزارة التعليم العالي والبحث العلمي

Kasdi Merbah University of Ouargla
جامعة قاصدي مرباح ورقلة

Academic Master Thesis

Domain: Mathematics and Computer science

Field: Computer science

Specialty: Fundamental computing

THEME

IMPACT of DWT FREQUENCY BAND on QUALITY of WATERMARK in MEDICAL IMAGES

Presented by:

- Tayeb Mekkaoui
- Abdelkader Badreddine Chelghoum

Supervised by:

Dr. Fares Kahlessenane

President: Dr. Akram Zine Eddine Boukhamla

Examiner: Dr. Mohammed Kamel Benkaddour

2023/2024

Acknowledgment

Praise be to God, and blessings and peace be upon the messenger of God.

First and foremost, we would like to praise Allah the Almighty, the Most Gracious, and the Most Merciful for His blessings during our study. We are grateful for the strength, knowledge, and ability He gave us to complete our work satisfactorily. We praise Allah for giving us faith in our abilities and the confidence to complete this thesis.

We would like to express our heartfelt gratitude and sincere thanks to our Advisor, Dr. FARES KAHLESSENANE, for his invaluable guidance and advice in accomplishing this thesis.

Furthermore, we also express our deepest gratitude to all the professors and researchers whose articles have enriched us with their knowledge and research, serving as the foundation for writing our thesis.

We extend our sincere thanks to the members of the jury for their precious time and effort devoted to reviewing our work. We are also grateful to our teachers throughout the years, without whom we could not have undertaken this journey.

Our ultimate thanks are dedicated to our beloved families—our parents, sisters, and brothers—for their endless support, love, and prayers.

Additionally, we extend huge thanks to our best friends in the Computer Science Department for every single moment of joy and sorrow we cherished together from the first day we stepped onto our campus up to this very second.

Last but not least, we want to thank ourselves for believing in us, for doing all the hard work, for never taking days off, and for never quitting.

Finally, we have great expectations that our study will be beneficial and useful for anyone interested in reading this final project.

ملخص

أدت التطورات الأخيرة في المجال الطبي إلى تحول كبير نحو الرقمنة، مع استخدام الصور الطبية على نطاق واسع في التشخيص والبحث والتعليم. وقد جلب هذا التحول فوائد عديدة، مثل تعزيز إمكانية الوصول، وتحسين التعاون بين المتخصصين في الرعاية الصحية، وزيادة كفاءة رعاية المرضى. ومع ذلك، فإنه يثير أيضًا مخاوف بالغة الأهمية بشأن مخاطر الوصول غير المصرح به إلى المعلومات الطبية الحساسة أو التلاعب بها أو سرقتها. تهدد هذه المخاطر خصوصية المريض وأمن الرعاية الصحية، حيث تحتوي الصور الطبية غالبًا على بيانات حساسة للغاية. ولمواجهة هذه التحديات، تستخدم هذه الدراسة تقنيات العلامات المائية الرقمية المتقدمة، وتحديدًا تحويل المويجات المنفصلة (DWT) وتضمين البت الأقل أهمية(LSB) ، لتضمين المعلومات النصية بشكل آمن في الصور الطبية. يسمح DWT بتضمين علامة مائية انتقائية في مجالات التردد، مما يعمل على تحسين عدم القدرة على الإدراك والمتانة، بينما يضمن تضمين LSB الحد الأدنى من التأثير الإدراكي. تهدف هذه الدراسة إلى تحقيق التوازن بين عدم القدرة على الإدراك والمتانة من خلال تقييم تأثير نطاقات التردد DWT على جودة العلامة المائية في الصور الطبية.

الكلمات المفتاحية: البت الأقل أهمية، التحويل بالمويجات المتقطعة، العلامات المائية الرقمية، الصور الطبية، المتانة، عدم القدرة على الإدراك، الأمان.

Abstract

Recent advancements in medical field have led to a significant move towards digitalization, with medical images being widely utilized for diagnostics, research, and education. This change has brought numerous benefits, such as enhanced accessibility, improved collaboration among healthcare professionals, and more efficient patient care. However, it also raises critical concerns about the risks of unauthorized access, manipulation, or theft of sensitive medical information. These risks threaten patient privacy and healthcare security, as medical images often contain highly sensitive data. To address these challenges, this thesis employs advanced digital watermarking techniques, specifically Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) embedding, to securely embed textual information into medical images. DWT allows for selective watermark embedding in frequency domains, optimizing imperceptibility and robustness, while LSB embedding ensures minimal perceptual impact. This thesis aims to balance imperceptibility and robustness by assessing the impact of DWT frequency bands on watermark quality in medical images.

Keywords: DWT, LSB, Digital watermarking, Medical images, Robustness, Security, Imperceptibility.

Résumé

Les progrès récents dans le domaine médical ont conduit à une évolution significative vers la numérisation, les images médicales étant largement utilisées à des fins de diagnostic, de recherche et d'éducation. Ce changement a apporté de nombreux avantages, tels qu'une meilleure accessibilité, une meilleure collaboration entre les professionnels de la santé et des soins plus efficaces aux patients. Cependant, cela soulève également des inquiétudes majeures quant aux risques d'accès non autorisé, de manipulation ou de vol d'informations médicales sensibles. Ces risques menacent la vie privée des patients et la sécurité des soins de santé, car les images médicales contiennent souvent des données très sensibles. Pour relever ces défis, cette étude utilise des techniques avancées de filigrane numérique, en particulier l'intégration de la transformation en ondelettes discrètes (DWT) et du bit le moins significatif (LSB), pour intégrer en toute sécurité des informations textuelles dans des images médicales. DWT permet l'intégration sélective de filigranes dans des plages de fréquences, optimisant l'imperceptibilité et la robustesse, tandis que l'intégration LSB garantit un impact perceptuel minimal. Cette étude vise à équilibrer l'imperceptibilité et la robustesse en évaluant l'impact des bandes de fréquences DWT sur la qualité du filigrane dans les images médicales.

Mot clé : l'insertion du bit de poids faible, transformation en ondelettes discrète, Tatouage numérique, Images médicales, robustesse, imperceptibilité, sécurité.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

2-D image	Two-Dimensional image
APNG	Animated Portable Network Graphics
BER	Bit Error Rate
BMP	Bitmap Format
BPP	Bits Per Pixel
CT Scans	Computed Tomography Scans
DCT	Discrete Cosine Transformation
DFT	Discrete Fourier Transformation
DICOM	Digital Imaging and Communications in Medicine
DPI	Dots Per Inch
DWT	Discrete Wavelet Transform
EBE	Edges Based Data Embedding
EHS	Electronic Health Systems
FFT	Fast Fourier Transform
GIF	Graphics Interchange Format
HH	High-High
HL	High-Low
ICT	Information and Communication Technologies
IDE	Integrated Development Environment
JPEG/JPG	Joint Photographic Experts Group
LH	Low-High
LL	Low-Low
LSB	Least Significant Bit
MNG	Multiple-image Network Graphic
MRI Scans	Magnetic Resonance Imaging Scans

MSB	Most Significant Bit
MSE	Mean Squared Error
NC	Normalized Correlation
NIST	National Institute of Standards and Technology
OCR	Optical Character Recognition
OS	Operating System
PIL	Python Imaging Library
PNG	Portable Network Graphics
PPI	Pixels Per Inch
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Differencing
RGB	Red, Green and Blue
RPE	Random Pixel Embedding
SEAC	Standards Eastern Automatic Computer
SSIM	Structural Similarity Index Measure
SVD	Singular Value Decomposition
TIFF/TIF	Tagged Image File Format
dB	Decibel

General Introduction

Recent advancements in the medical domain have witnessed a significant shift towards digitalization, with medical images being widely used for diagnostic, research, and educational purposes. This transition has brought forth numerous benefits, including enhanced accessibility, improved collaboration among healthcare professionals, and more efficient patient care. However, along with these advancements comes the pressing need to address the potential risks associated with the unauthorized access, manipulation, or theft of sensitive medical information.

The theft or unauthorized access to medical images poses serious risks to patient privacy, confidentiality, and overall healthcare security. Medical images often contain highly sensitive information, including personal identifiers, medical history, and diagnostic findings, making them lucrative targets for malicious actors seeking to exploit or manipulate such data for financial gain, identity theft, or other nefarious purposes. Furthermore, the integrity and authenticity of medical images are paramount for ensuring accurate diagnoses and treatment decisions, underscoring the critical importance of robust security measures to safeguard against unauthorized access or tampering.

In medical image watermarking, a key problem is ensuring the integrity and confidentiality of images while maintaining their quality for accurate diagnosis. Unauthorized access, tampering, and quality degradation during transmission and storage pose significant challenges that need to be addressed to protect sensitive medical information.

In this thesis, we have used DWT and LSB methods to solve the problem of ensuring image integrity and authenticity in medical image watermarking. DWT decomposes images to embed watermarks in sub-bands components. LSB embedding minimizes visual distortion, preserving image imperceptibility and quality for accurate diagnosis, effectively balancing security and fidelity.

This thesis is structured as follows:

Chapter 1 provides some general definitions about the main domains we addressed in order to position the problems we focused on. We will thus come back on digital image fundamentals, exploring their characteristics, formats, and the technological principles that

underpin their creation and manipulation, This foundational knowledge is crucial for understanding the subsequent topics discussed in this thesis.

Chapter 2 is devoted to digital watermarking, where we delve into the techniques used to embed imperceptible markers into digital media. These markers are essential for verifying authenticity, tracking ownership, and enforcing copyright protection. This chapter will cover the evolution of digital watermarking, various methodologies, and the challenges faced in implementing these techniques effectively in the digital age.

In Chapter 3, we explain our approach to integrating the principles of digital watermarking into practical applications. This includes outlining the methodology we propose, as well as analyzing the imperceptibility and effectiveness of our approach.

Chapter I
Digital Images

I.1 Introduction

The images in our lives, such as photographs, drawings, and logos, enrich our experiences and communication by adding visual context and aesthetic value. We encounter these images daily, from the pictures on our social media feeds to the graphs in business reports. However, at the computer level, these images are interpreted in a fundamentally different way.

A digital image is a representation of visual information in a format that can be processed by a computer. Unlike traditional images, which are typically created using physical mediums like paper and film, digital images are composed of binary data—sequences of ones and zeros. This binary data encodes the color and brightness of each pixel, the smallest unit of a digital image. Computers interpret this binary data to render images on screens or other display devices, allowing for efficient and accurate processing, storage, and display of visual information.

Digital images can represent a wide variety of visual content, including photographs, drawings, graphs, logos, and individual frames from videos. They can also include specialized images like medical scans, such as X-rays, MRIs, and CT scans, which are crucial for diagnosing and treating medical conditions. Digital images can be created through various means, such as digital cameras, scanners, or software, and can be stored electronically on any storage device, making them integral to modern computing and digital communication.

Understanding how digital images work requires us to delve into the concepts of pixel representation, color models, and image formats. In this chapter, we will explore the world of digital images. We will uncover how images are created, stored, and displayed by computers, and we will examine the various formats and compression techniques used to manage image data. Additionally, we will look at the role of digital images in medical imaging, highlighting their importance in modern healthcare.

I.2 History of Photography

The history of photography provides valuable insights into the evolution of computer vision, illustrating how technological advancements have transformed our ability to capture, process, and understand images. This progression from early photographic techniques to sophisticated computer vision systems underscores the interplay between photographic innovation and computational development.

I.2.1 Analog Photography and Digital Photography

The word “photography,” translated literally, means “writing with light.” Photography occurs when the light from what is in front of the camera refracts through the lens and projects an image on the back of the camera. [1]

I.2.1.1 Analogue photography:

also known as film photography, is the process of capturing images using an analogue camera and chemical-based film. A roll of film is loaded into the camera and the magic begins once you start clicking: light interacts with the chemicals in the film and an image is recorded. Images are captured on film through continuous variations in light intensity. The film undergoes chemical processing to reveal the image, which can then be printed on photographic paper.

I.2.1.2 Digital Photography:

instead of a piece of film, images are captured using electronic sensors that convert light into digital signals, which are then processed and stored as binary data (ones and zeros). Unlike the piece of film, which is purchased, processed and printed separately from the camera, the sensor and the rest of the camera can be used over and over to transform the image projected onto it into a picture that can be instantly and infinitely reproduced.

I.2.2 First Digital Image

In 1957 NIST (the National Institute of Standards and Technology) computer pioneer Russell Kirsch asked, "What would happen if computers could look at pictures?" and helped start a revolution in information technology.

Kirsch and his colleagues at NIST, who had developed the nation's first programmable computer, the Standards Eastern Automatic Computer (SEAC), created a rotating drum scanner and programming that allowed images to be fed into it. The first image scanned was a head-and-shoulders shot of Kirsch's three-month-old son Walden.

Figure I-1 The first digital image made on a computer in 1957 showed researcher Russell Kirsch's baby son.

The ghostlike black-and-white photo only measured 176 pixels on a side—a far cry from today's megapixel digital snapshots—but it would become the Adam and Eve for all computer imaging to follow. In 2003, the editors of Life magazine honored Kirsch's image by naming it one of "the 100 photographs that changed the world." The ghostlike black-and-white photo only measured 176 pixels on a side—a far cry from today's megapixel digital snapshots—but it would become the Adam and Eve for all computer imaging to follow. In 2003, the editors of Life magazine honored Kirsch's image by naming it one of "the 100 photographs that changed the world." [2]

Peter Noble built a sensor that could convert light into digital information in 1968. This was called an Active Pixel Sensor, a photodetector that registered how light fell across it and converted this into digital information. Noble's sensor could create a digital image from life, without the need for any analogue intermediary images.

By 1973 Steve Sasson, a researcher in the Kodak laboratories, had built upon this idea to create a fully digital camera that could capture and store electronic photographs. [3]

I.3 Digital Image Characteristics

Digital images possess several key characteristics that determine their quality, usability, and suitability for various applications. Understanding these characteristics is essential for effectively capturing, processing, and displaying digital images.

I.3.1 Pixel

As a broad generalization, pixel is the elementary constituent of raster graphics images, imaging sensors, and displays. It is the smallest unit of a digital image that can be displayed and represented on a digital display. They serve as the building blocks of digital images, used to display everything from text to intricate graphics and photos.

The pixel definition takes its meaning from a combination of two words: "picture" and "element." It describes the smallest controllable element of a digital image on a display device. Over time, "picture element" was shortened to "pixel" (pix = picture, el = element) for convenience and has become the standard term in digital imaging and computer graphics. [4]

Let's say we have an image with a size of 200 x 200 (width x height). The total number of pixels in the picture is 400000.

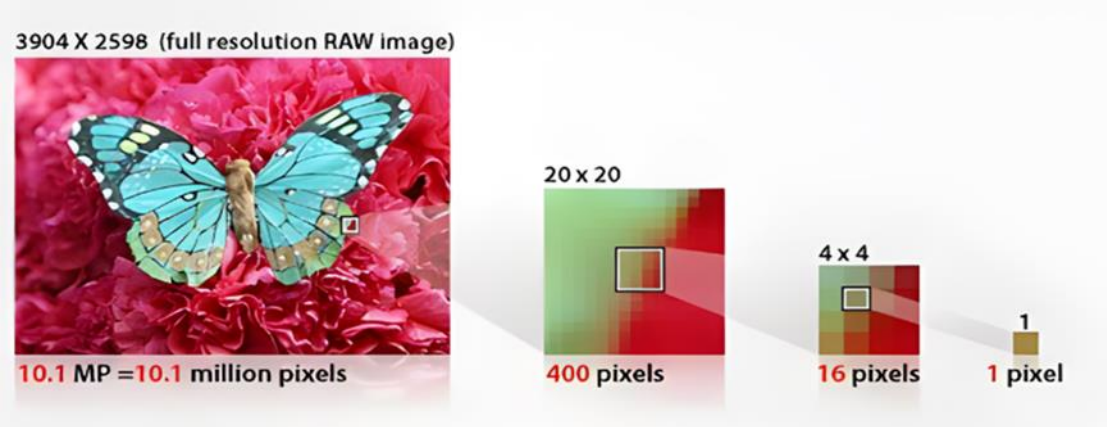

Figure I-2 Representation of the pixel

Each image we see on a screen is made up of tiny pixels, each of which can display a specific color. These pixels are arranged in a grid, and the combination of their colors forms the complete image. The color and brightness of each pixel are determined by binary data, which computers can manipulate to perform tasks such as image compression, enhancement, and recognition.

I.3.2 Resolution

Image resolution refers to the ability to distinguish fine detail in an image. It is quantified by the number of pixels in the image, with higher resolutions indicating a greater density of pixels and finer detail. High-resolution images exhibit greater pixel density and intricate texture details, which are crucial for applications such as medical imaging, remote sensing, and video analysis.it is typically measured in dots per inch (dpi) or pixels per inch (ppi). [5]

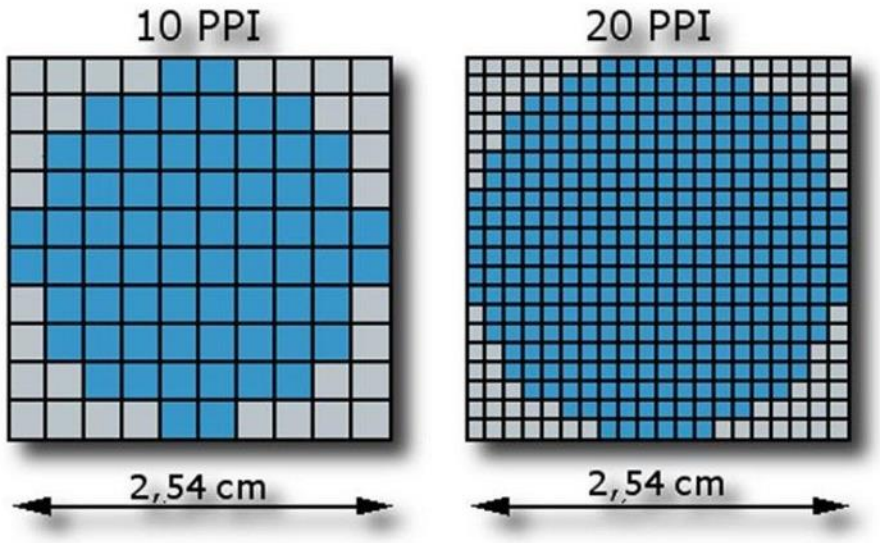

Figure I-3 Example of deferent resolution

I.3.3 Bit Depth

Bit depth, also known as pixel depth, refers to the number of bits used to represent the color of a single pixel in an image. Specifically, it determines the precision with which colors can be expressed. Common bit depths include:

- 8-bit grayscale: Allows for 256 shades of gray.
- 24-bit true color: Uses 8 bits for each of the red, green, and blue channels, resulting in over 16 million colors.
- 30-bit, 36-bit, or 48-bit deep color: Used for professional applications and high-quality displays.

Higher bit depths allow for more accurate color representation and smoother gradients.

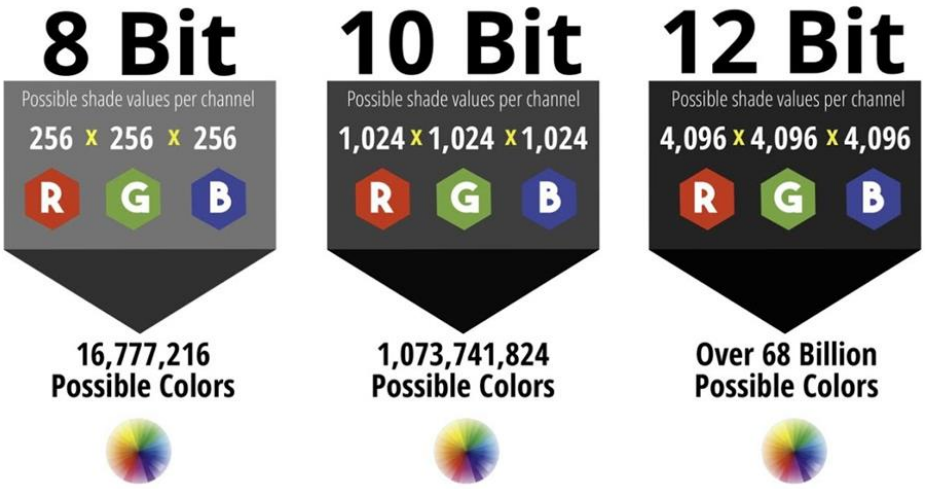

Figure I-4 Bit Depth

I.4 Types of Digital Image

Digital images come in various types, each suited to different applications and uses, we will consider 5 types of digital images.

I.4.1 Binary images

Binary images are the simplest type of images and can take two values, typically black and white, 0 represents black entirely and 1 represents white.

A binary image is referred to as a 1-bit image because it takes only 1 binary digit to represent each pixel. These types of images are frequently used in applications where the only information required is general shape or outline, for example optical character recognition (OCR). [6]

Binary images are often created from the gray-scale images via a threshold operation, where every pixel above the threshold value is turned white ('1'), and those below it are turned black ('0'). [6]

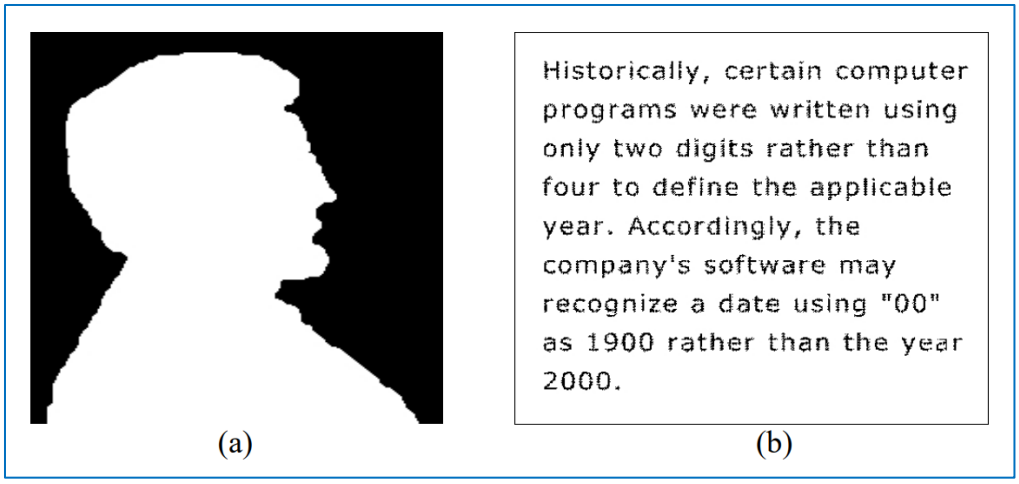

Figure I-5 Binary images. (a) Object outline. (b) Page of text used in OCR application

I.4.2 Gray-scale images

Gray-scale images are referred to as monochrome (one-color) images, they contain gray-level information, no color information.

Grayscale images contain shades of grey, providing more detail than binary images. Each pixel in a grayscale image typically carries a value representing the intensity of light at that point, with varying levels of brightness from black to white. Grayscale images are widely used in applications like medical imaging, where detail and contrast are important but color information isn't necessary. [7]

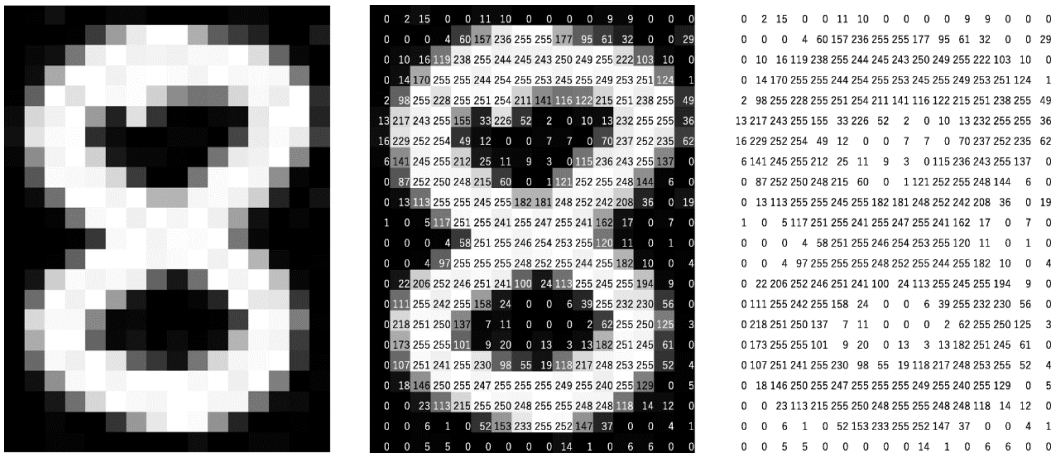

Figure I-6 Gray-scale image

In an 8-bit grayscale image, the pixel is an integer value between 0–255. Zero is entirely black, and 255 is white. Gray falls around 127 leading to the white color.

These images are also known as 8-bit color format images. This format was used initially by early models of the operating systems UNIX and the early color Macintoshes.

I.4.3 Color images

Color images can be modeled as three-band monochrome image data, where each band of data corresponds to a different color. The actual information stored in the digital image data is the gray-level information in each spectral band.

Typical color images are represented as red, green, and blue (RGB images). Using the 8-bit monochrome standard as a model, the corresponding color image would have 24-bits/pixel (8-bits for each of the three color-bands red, green, and blue). [6]

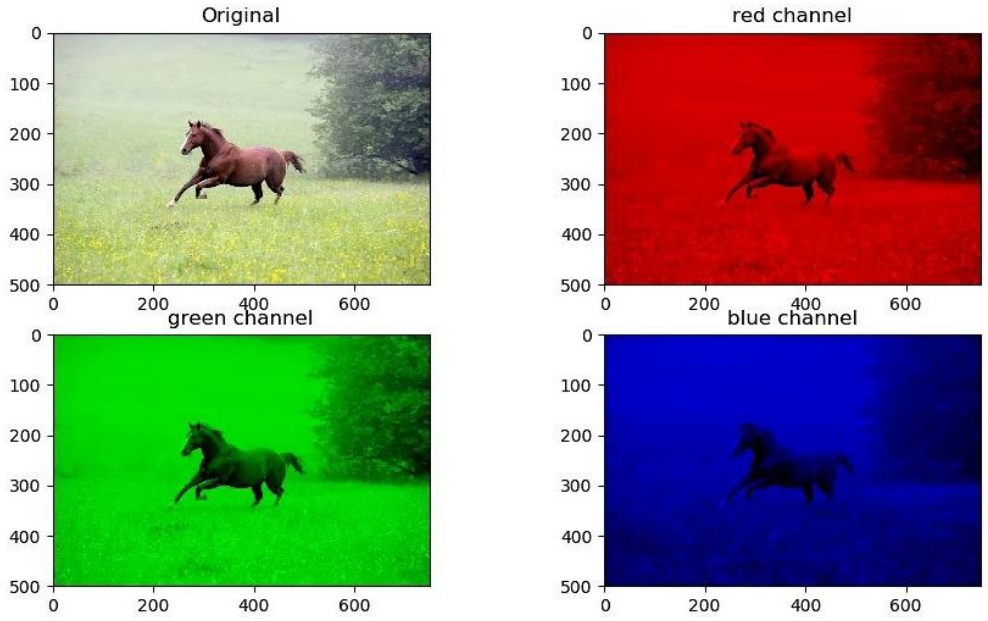

Figure I-7 Representation of a typical RGB color image

These images are represented in a 3-D matrix or a 3-dimensional array.

$$\text{RGB Image } f(x,y) = \begin{bmatrix} r(x,y) \\ g(x,y) \\ b(x,y) \end{bmatrix}$$

These images are the most complex and contain colored pixels. Each pixel in a color image has three values, allowing for a wide range of colors. Color images are crucial in fields where visual appearance and color information are vital, like in digital photography and video processing. [7]

I.4.4 Indexed Images

In indexed images, each pixel value points to a color in a separate color palette or lookup table. This type of image is efficient for storing graphical images like icons and maps, where a limited color palette suffices. [7]

An indexed image consists of an array, called X in this documentation, and a colormap matrix, called map. The pixel values in the array are direct indices into a colormap.

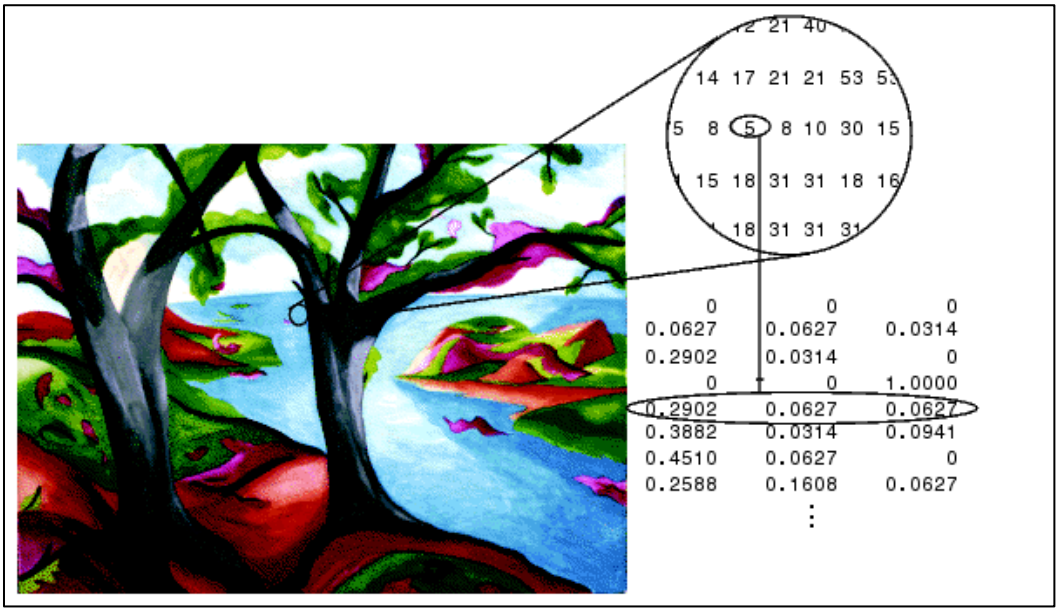

Figure I-8 Relationship of Pixel Values to Colormap in Indexed Images

I.4.5 Multispectral images

Multispectral images typically contain information outside the normal human perceptual range. This may include infrared, ultraviolet, X-ray, acoustic, or radar data. These are not images in the usual sense because the information represented is not directly visible by the human system. However, the information is often represented in visual form by mapping the different spectral bands to RGB components. [8]

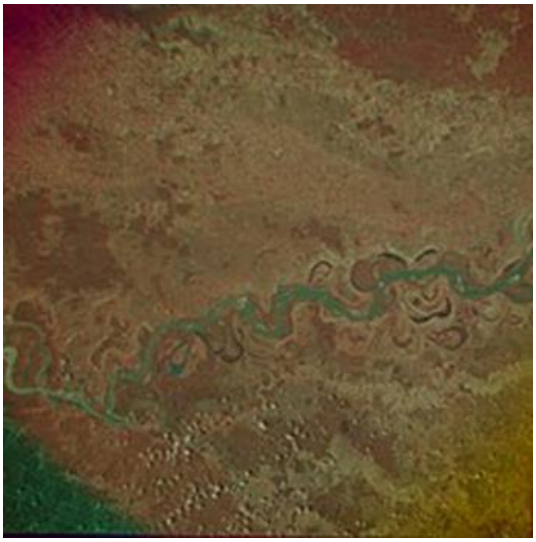

Figure I-9 Multispectral image of part of the Mississippi River

I.5 Image Formats and Compression

Image formats are digital file types used to store visual information. They vary in compression methods, quality, and use cases.

I.5.1 Lossless Compression

Lossless compressors are generally two-step algorithms. The first step transforms the actual image to some other format in which the inter-pixel redundancy is minimized. The second step uses an entropy encoder to eliminate the coding redundancy. The lossless decompressor is an ideal inverse process of the lossless compressor. [9]

And this is some of the lossless image representation formats:

I.5.1.1 Portable Network Graphics (PNG)

The PNG (Portable Network Graphics) image format stands out in the world of raster digital images due to its unique features. Unlike other formats, PNG offers integrity checking and the ability to detect transmission errors. It emerged as a free and open-source alternative to GIF, overcoming its limitations. PNG supports a wide range of color depths, from 8-bit to 48-bit, while GIF is limited to 256 colors and a single transparent color.

Compared to JPEG, PNG excels, especially with large images, as it retains data integrity during compression. Its animation formats, MNG and APNG, provide options for animated content. PNG finds common use in graphs, diagrams, and any application where flat colors and lines are prominent, without requiring scaling up. Overall, PNG's versatility, reliability, and lossless compression make it a preferred choice for various digital image needs. [10]

I.5.1.2 Bitmap (BMP)

BMP files are image files that show the way windows stores bit mapped images. Bitmap files are usually large and uncompressed, but the images are rich in color, of high quality, simple and compatible in all windows OS and programs. These files are made of millions and millions of dots called „pixels", with different colors and arrangements to come up with an image or pattern. It might an 8-bit, 16-bit or 24-bit image. [11]

I.5.1.3 Tagged Image File Format (TIFF/ TIF)

TIFF format is very flexible and dynamic especially in terms of image storage. Multiple images can be stored in a single file unlike other image formats. It comes in both lossy or lossless forms and it is supported by several imaging programs.

It is capable of recording halftone image data with different pixel intensities, thus is the perfect format for graphic storage, processing and printing. [11]

I.5.2 Lossy Compression methods

Usually nearly all lossy compressors are three-step algorithms, each of which is in accordance with three types of redundancy (Psycho-visual, Inter-pixel and Coding Redundancy).

The first phase is a transform to get rid of the inter-pixel redundancy to group information competently. Then a quantizer is applied to take out psychovisual redundancy to symbolize the packed information with as few bits as achievable. The quantized bits are then resourcefully encoded to get extra compression from the coding redundancy. [9]

And this is some of the lossy image representation formats:

I.5.2.1 Joint Photographic Experts Group (JPEG or JPG)

JPEG, developed in the early 1990s, is a compression algorithm created for photographic images. Unlike GIF, it offers 24-bit color encoding, allowing for 16.7 million colors. JPEG's strength lies in its significant compression capabilities, reducing file sizes up to 1/20th of the original. It features progressive display and is not patented. However, JPEG is a lossy compression technique, leading to data loss and potential image degradation with each compression, along with the possibility of introducing distortions, such as Gibbs' phenomenon, in certain images.

I.6 Medical Imaging

Since the discovery of the X-ray radiation by Wilhelm Conrad Roentgen in 1895, the field of medical imaging has developed into a huge scientific discipline. [12] Medical imaging refers to several different technologies that are used to view the human body in order to diagnose, monitor, or treat medical conditions. Each type of technology gives different information about the area of the body being studied or treated, related to possible disease, injury, or the effectiveness of medical treatment. [13]

I.6.1 Medical Imaging Techniques

A variety of machines and techniques can create pictures of the structures and activities inside your body. The type of imaging your doctor uses depends on your symptoms and the part of your body being examined. [14]

Technique	Description
X-Rays (Radiography)	X-rays are a type of radiation called electromagnetic waves. X-ray imaging creates pictures of the inside of your body. The images show the parts of your body in different shades of black and white.
CT Scans	Computed tomography (CT) is a type of imaging. It uses special x-ray equipment to make cross-sectional pictures of your body.
Nuclear Scans	Nuclear scans use radioactive substances to see structures and functions inside your body. They use a special camera that detects radioactivity.
MRI Scans	Magnetic resonance imaging (MRI) uses a large magnet and radio waves to look at organs and structures inside your body.
Ultrasound	An ultrasound is an imaging test that uses sound waves to make pictures of organs, tissues, and other structures inside your body.

Table I-1 Medical Imaging Techniques

I.6.2 DICOM Image Format

Digital Imaging and Communications in Medicine (DICOM) is the international standard for transmitting, storing, retrieving, printing, processing, and displaying medical imaging information. DICOM image files are sourced from different modalities, either standalone or integrated. DICOM format files (or simply DICOM files) are stored with the file extension ".dcm" DICOM can accept other popular file formats such as JPEG, TIFF, GIF, and PNG. As communication technology has rapidly changed, this standard's adaptive capabilities and wide availability have led to a global reliance on it within the radiological equipment industry.

A DICOM file contains a header and image data sets combined into one file. The header consists of tags such as patient demographics, including the patient's name, date of birth, age, gender, and more. The header can contain study parameters such as image dimensions, acquisition parameters, pixel intensity, and matrix size.

There are instances where sensitive patient information can be removed from the DICOM header. Unintentional instances result from exporting the image into other formats such as JPEG. Intentional instances include "anonymization" or removing patient data when sharing or exporting for research purposes. [15]

I.6.3 The Importance of Medical Images

Medical imaging has forever changed healthcare for the better, and With medical imaging going digital it provides invaluable insights that increase the chances of successful treatment. As medical tools, medical images help doctors see more clearly what's going on inside our bodies, They make diagnosing and treating patients in all kinds of medical areas easier, and they also bring several benefits. [16]

- **Convenient storage and accessibility:** These digital images can be securely stored and easily accessed, which speeds up doctor's appointments and leads to better diagnoses.
- **Improved image quality:** These high-quality images assist doctors in making more precise diagnoses.
- **Easier to Share:** Doctors in different places can look at and discuss these images easily, which is great for patient care.

Medical images are important to making the right diagnosis and starting the best treatment. Patients receive better care when medical records, including imaging, are easier to access for doctors.

I.7 Conclusion

Digital images are a fundamental aspect of modern technology, permeating various facets of daily life, from personal photography to medical imaging, entertainment, and beyond. Their versatility and ease of manipulation enable a broad range of applications, including social media, scientific research, and digital art. The development of advanced imaging techniques and powerful software has made it possible to capture, edit, and share high-quality images with unprecedented precision and creativity. As technology continues to evolve, digital images are likely to play an increasingly significant role in communication, analysis, and expression, highlighting the importance of ongoing innovation and ethical considerations in their use.

Chapter II
Digital Watermarking

II.1 Introduction

Digital watermarking is a potent tool for protecting intellectual property and copyrighted material. It involves embedding a marker within digital content, such as images, videos, audio files, and documents, to identify the source and ownership of the copyrighted material. This embedded information, known as a watermark, can be either visible or invisible and serves various purposes, including copyright protection, authentication, and tracking.

The concept of watermarking has historical roots in traditional paper watermarks, which were used to prevent counterfeiting and identify the paper manufacturer. With the advent of digital media, these principles were adapted to digital formats, giving rise to digital watermarking in the 1990s. This period marked the beginning of widespread digital content distribution and the need for effective methods to protect and manage digital assets.

This chapter aims to provide a comprehensive overview of digital watermarking, laying the foundation for a deeper understanding of its importance, types, techniques, and applications, with a specific focus on image watermarking. Understanding the principles and practices of digital watermarking allows for an appreciation of its role in our increasingly digital world.

II.2 Information Hiding

Information-hiding techniques have recently become important in several application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly. the communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver, or its very existence. [17]

II.2.1 History of Information Hiding

Understanding the history of information hiding helps us appreciate the evolution and importance of techniques like watermarking. The idea of communicating secretly is as old as

communication itself. we will briefly discuss the history of information hiding techniques such as steganography/ watermarking. Early messages were sent on foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger.

The famous Greek tyrant Histiaeus, while in prison, used unusual method to send message to his son-in-law. He shaved the head of a slave to tattoo a message on his scalp. then waited until the hair grew back before sending him. Ancient Romans used Invisible inks to write between lines based on readily available substances such as fruit juices, urine and milk. When heated, the invisible inks would darken, and become legible. Invisible inks were used as recently as World War II. Modern invisible inks fluoresce under ultraviolet light and are used as anti-counterfeit devices. [18]

Watermarking technique has evolved from steganography. The use of watermarks is almost as old as paper manufacturing. Their earliest use seems to have been to record the manufacturer's trademark on the product so that the authenticity could be clearly established without degrading the aesthetics and utility of the stock.

The digitization of our world has expanded our concept of watermarking to include immaterial digital impressions for use in authenticating ownership claims and protecting proprietary interests. However, in principle, digital watermarks are like their paper ancestors. They signify something about the token of a document or file in which they inherit. [19]

II.2.2 Information Security

Information security is the practice of protecting data and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

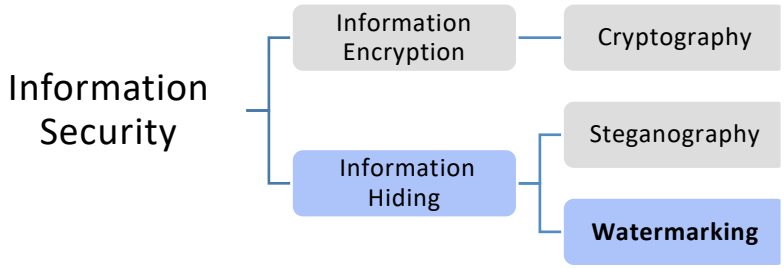

Figure II-1 Classification of the security system [44]

It encompasses various techniques to ensure the confidentiality, integrity, and availability of information. information security is divided into two main components Information Hiding & Information

II.2.2.1 Cryptography

Cryptography is the science of securing data by transforming it into an unreadable format to prevent unauthorized access. It involves techniques such as encryption, where plain text is converted into ciphertext, and decryption, where ciphertext is reverted to plain text using cryptographic keys. Cryptography ensures data confidentiality, integrity, and authenticity, and is essential for protecting sensitive information during transmission and storage in various applications, including banking, e-commerce, and communications.

II.2.2.2 Steganography

Steganography can be defined as the science and art of secret communications which involves the hiding of information inside another information. Compared to cryptography, steganographic messages are not self-revealing because data is concealed in a manner that makes its detection to the human eye difficult. Steganography as a word was derived from two Greek words "Stegos" and “Grafia”, meaning "cover" and "writing", respectively. This gives the literary meaning of steganography as "covered writing".

II.3 Classification of Digital Watermarking

Digital watermarking can be categorized based on various characteristics that include robustness, type of digital data, perceptivity, detection process, and domain. The classification of watermarking techniques is represented in Figure II-2. [20]

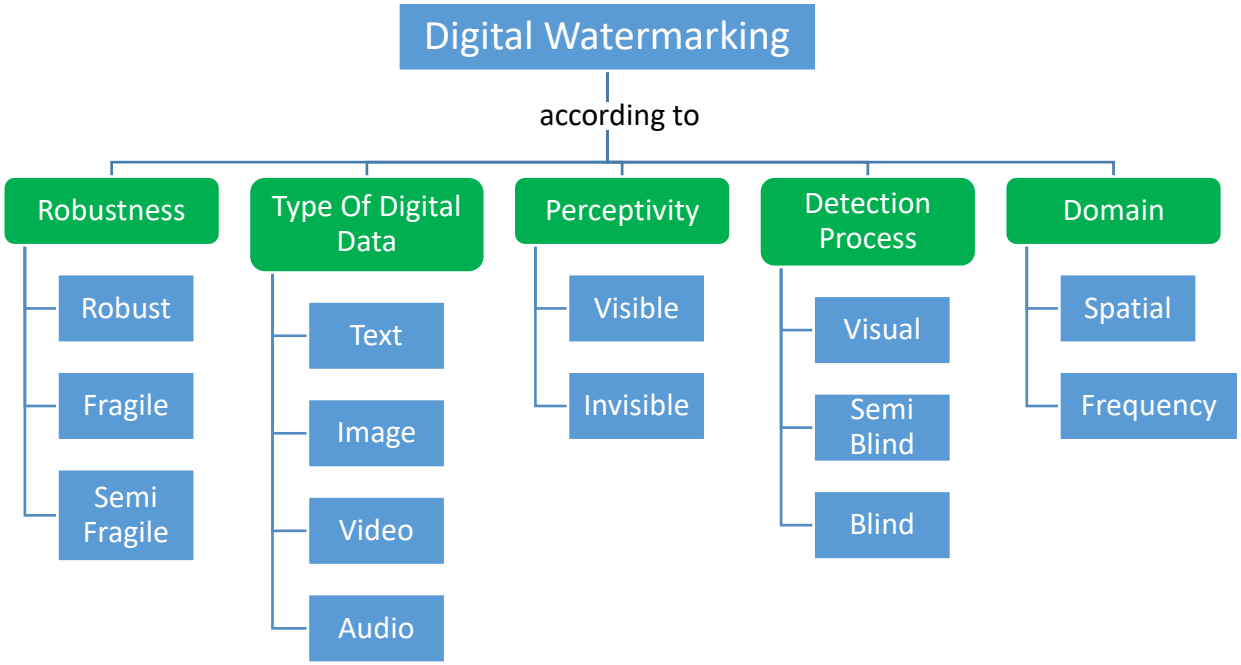

Figure II-2 Classification of Digital Watermarking

II.3.1 According to Robustness

Robustness is the ability of a watermark to withstand various types of manipulations and attacks. It is divided into three categories, The robust Watermarks are designed to survive various forms of attacks and processing, on the other hand, the Fragile Watermarks are easily altered or destroyed by any modification to the host media. These are useful for detecting tampering. Semi-fragile watermarks can withstand benign processing (like compression) but will break if the media is tampered with. This balance allows for detecting malicious alterations while tolerating some level of media processing.

II.3.2 According to Type of Digital Data

Watermarking techniques vary depending on the type of digital media

- **Text**: Watermarking techniques for text documents. These can include altering the text format, adding hidden text, or modifying the arrangement of text.

- **Image**: Techniques specifically designed for images, such as altering pixel values or using frequency domain transformations.
- **Video**: Methods for embedding watermarks into video files, which may involve altering frames or encoding information within the video stream.
- **Audio**: Techniques for embedding watermarks in audio files, such as modifying audio samples or using frequency modulation.

II.3.3 According to Perceptivity

Perceptivity refers to the visibility or audibility of the watermark to human senses, Visible Watermarks are intentionally made visible in the media. For example, a visible logo on an image or video. These are often used for branding or to indicate ownership.in the other hand, Invisible Watermarks are embedded in a way that they are not perceptible to human senses but can be detected by appropriate software. These are commonly used for copyright protection and verification.

II.3.4 According to Detection Process

The detection process defines how the watermark can be extracted or detected

1- **Visual**: This kind of technique needs an original media. This method can extract information using possible distorted image and the original media.
2- **Semi-Blind**: In this technique requires some information about the original media, but not the original media itself. For example, certain parameters or a key used during the embedding process.
3- **Blind**: Watermarks that can be detected without any reference to the original unwatermarked media. This kind of techniques are also referred as public watermarking techniques.

II.4 Watermarking Techniques

Based on their embedding domain, watermarking schemes can be classified either as Spatial Domain or Transformed Domain.

II.4.1 Spatial Domain Techniques

In spatial domain watermarking, the process involves directly changing the pixel intensities of the image to embed the watermark. This means that the watermark bits are directly incorporated into the pixels of the original image. These techniques are clear and cost-effective in terms of computational resources, as they do not necessitate a preliminary transformation stage. They are particularly suitable for real-time watermarking applications needed in environments with low computing power.

There are many Spatial Domain techniques, all directly change some bits in the image pixel values in hiding data. This some of Spatial domain techniques: [21] [22]

1- Least significant bit (LSB)
2- Pixel value differencing (PVD)
3- Edges based data embedding method (EBE)
4- Random pixel embedding method (RPE)
5- Mapping pixel to hidden data method
6- Labeling or connectivity method

II.4.1.1 Least Significant Bit (LSB)

LSB insertion, a prevalent technique in the spatial-domain category, stands out as one of the most popular methods for embedding secret messages within host images. This approach is straightforward, involving the utilization of the least significant bits (LSBs) of each pixel in one image to conceal the most significant bits (MSBs) of another. By modifying the LSB of a pixel, slight alterations in pixel intensity occur, yet these changes remain imperceptible to the human eye. During the retrieval phase, the embedded data is extracted, and unveiled the concealed message. [23]

The Least Significant Bit (LSB) technique embeds a secret message in an image by converting both to binary. Replace each pixel's LSB with message bits, then reconstruct the image. Extract the message by converting pixel values back to binary and retrieving the LSBs.

LSB Embedding Technique Steps

- upload the original image (in our case grayscale image)
- converted binary matrix (8-bit)
- The secret message to be embedded should be represented as a binary sequence, for example, 't' >>> 01110100
- The LSB of each pixel value is replaced with the corresponding bit from the secret message, for example, 150 (10010110) >>> Modified to 151 (10010111) to embed bit 1
- convert the matrix to an image after embedding all the secret message

Note that the changes in the LSB are minimal and do not significantly alter the image's visual appearance.

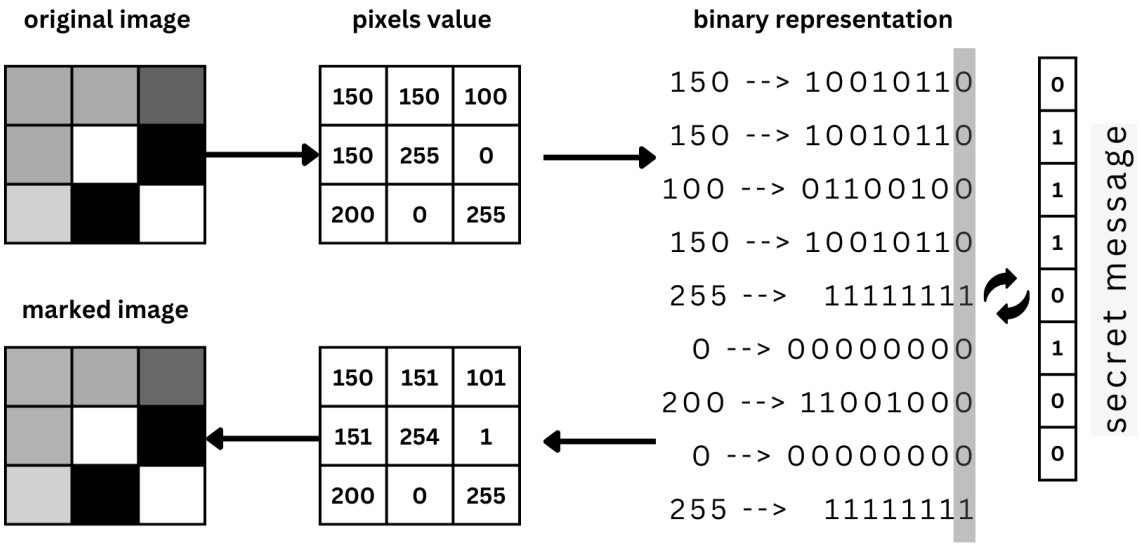

Figure II-3 LSB Embedding Technique

LSB Extraction Technique Steps

- upload the marked image, which contains the embedded secret message

- Convert the pixel values of the marked image to their 8-bit binary forms
- Extract the least significant bit (LSB) from each binary representation of the pixel Continue this process for all the pixels in the image taking into account the length of the original message
- Group the bits as per the original message encoding and Convert to Human-Readable Form (e.g., text)

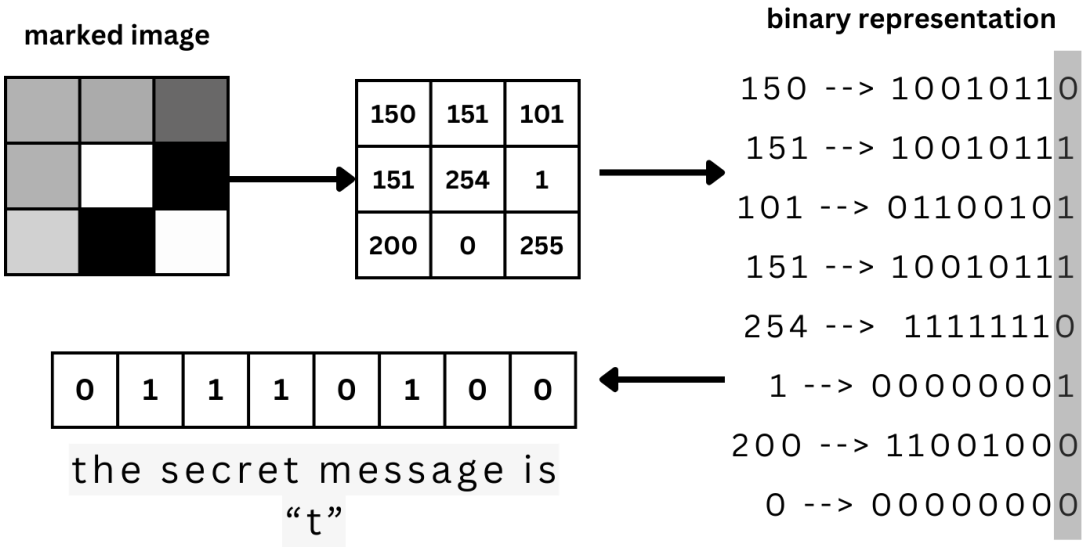

Figure II-4 LSB Extract Technique

II.4.1.2 Pixel Value Differencing (PVD)

Pixel Value Differencing (PVD) represents a more secure and integrity-preserving alternative to the widely used Least Significant Bit (LSB) substitution technique. Researchers Wu and Tsai observed that pixels situated along the edges of an image possess greater capacity to conceal data compared to other regions. Building on this insight, they introduced the PVD method. In PVD, an image is divided into blocks, and the differences between adjacent pixels within each block are leveraged to hide data by adjusting their values. This alteration is executed in a manner that preserves the overall grayscale proportions of the image. PVD proves particularly effective in enhancing pixel quality within the edged regions of an image. Moreover, the selection of the pixel value range in the PVD scheme factors in the response of the human visual system to the grey value range of 0-255.

In summary, PVD provides a superior and more straightforward approach for producing impactful output compared to conventional LSB replacement methods. [24]

II.4.2 Transform (or Frequency) Domain Techniques

This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it. Frequency domain watermarking involves embedding watermarks into the spectral coefficients of an image. Unlike spatial domain methods that directly modify pixel values, frequency domain techniques operate on transformed representations. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. As a result, most of the strong watermarking systems today operate within the transform domain, and those techniques involve applying invertible transforms to the host image before embedding the watermark. This process includes modifying the coefficients in the transform domain to embed the watermark and then applying the inverse transform to retrieve the marked image. Commonly used transforms for watermarking purposes include:

1- Discrete Fourier transformation technique (DFT)
2- Discrete cosine transformation technique (DCT)
3- Discrete Wavelet transformation technique (DWT)
4- Singular Value Decomposition (SVD)
5- Embedding in coefficient bits

II.4.2.1 Discrete Cosine Transform (DCT)

It is used to transform the image from the spatial domain to the frequency domain. This transformation is done in various steps which includes division of the image into blocks of 8*8 followed by the reduction of dynamic range by subtracting value 127 from each pixel value so that new range lies between [−128, 127] instead of [0,255]. These new values are then transformed into the frequency domain using a discrete cosine transform. This transformation divides the whole image into different frequency bands (low, medium and high). The watermark is embedded in the middle frequency because the visibility of the image remains unaffected.

Low sub-band contains the visual part of the image; high-frequency sub-band is removed by the quantization process. Final step is quantization process, which is applied on the block due to given fact "human eye is fairly good at observing the small difference over a large area but not so good in case of high-frequency brightness operation". For this process JPEG compression table is used, which is predefined and makes all high-frequency values rounded to zero and rest component values small in number. [25]

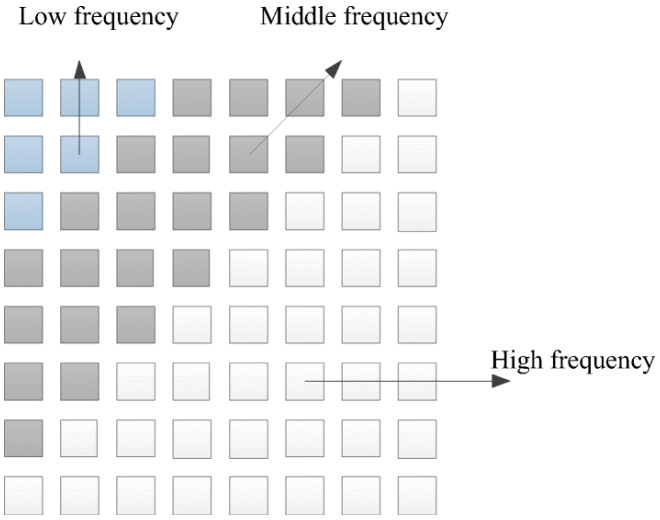

Figure II-5 Frequency Regions of DCT Coefficients

The DCT of an N × N block size (f) for (i, j) = 1, 2… N is calculated as follows:

$$F_{u,v} = \frac{1}{\sqrt{2N}} C_u . C_v \sum_{x=1}^{N} \sum_{y=1}^{N} f_{x,y} . cos\left[\frac{(2x+1)u\pi}{2N}\right] cos\left[\frac{(2y+1)v\pi}{2N}\right]$$

$$C_u = \begin{cases} \frac{1}{\sqrt{2N}} & if \quad u = 0 \\ 1 & if \quad u > 0 \end{cases}$$

II.4.2.2 Discrete Fourier Transform (DFT)

The Fourier transform breaks down a signal or image into simpler components that are both easy to analyze and implement. These components, which are periodic and complex, enable thorough examination of a system's amplitude and phase.

For an image f (m, n) with dimensions M × N, the discrete Fourier transform is defined as: [26]

$$F(u,v) = \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} f(m,n) e^{-j2\pi(\frac{u.m}{M}+\frac{v.n}{N})}$$

Where u and v denote the spatial frequencies for a position m and n. From the Fourier transform

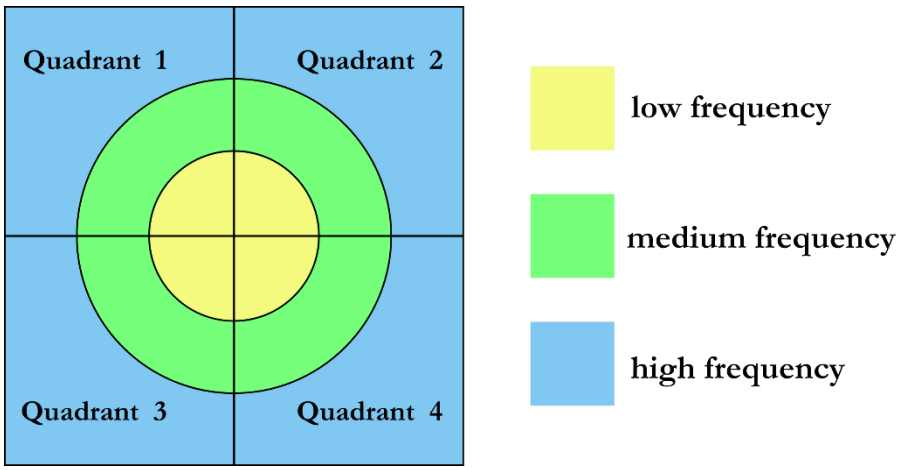

Figure II-6 Frequency distribution in the Fourier transform module

Figure II-6 shows the frequency distribution in the module of the Fourier transform. Due to the hermitian symmetry properties of the FFT, the modules in the first and second quadrants are equal to the coefficients in the fourth and third quadrants respectively.

II.4.2.3 Discrete Wavelet Transform (DWT)

Wavelets serve as special functions akin to sines and cosines in Fourier analysis, employed as fundamental functions for signal representation. In the context of 2-D images, applying the Discrete Wavelet Transform (DWT) involves convolving the image with 2-D filters along each dimension. These filters partition the input image into four distinct multi-resolution sub-bands: LL1, LH1, HL1, and HH1. Among these, LL1 represents the coarse-scale DWT coefficients, while LH1, HL1, and HH1 represent the fine-scale DWT coefficients.

To derive the next level of wavelet coefficients at a coarser scale, further processing of the LL1 sub-band is conducted until reaching a final scale denoted as N. At this point, there will be 3N+1 sub-bands, comprising multi-resolution sub-bands LLN and LHx, HLx, and HHx, where x spans from 1 to N.

The Discrete Wavelet Transform (DWT) offers exceptional spatial-frequency localization properties, making it highly suitable for identifying areas within the host image where a watermark can be effectively embedded. This property allows leveraging the masking effect of the human visual system, ensuring that modifications to DWT coefficients only affect the corresponding regions. Typically, a significant portion of the image energy is concentrated in the lower frequency sub-bands LLx. While embedding watermarks in these sub-bands might degrade the image quality, it could considerably enhance robustness. Conversely, the high frequency sub-bands HHx, containing edges and textures, are less perceptible to changes by the human eye, facilitating watermark embedding without noticeable visual impact. Many DWT-based watermarking algorithms strike a balance by embedding the watermark in the middle frequency sub-bands LHx and HLx, achieving a satisfactory trade-off between imperceptibility and robustness. [27]

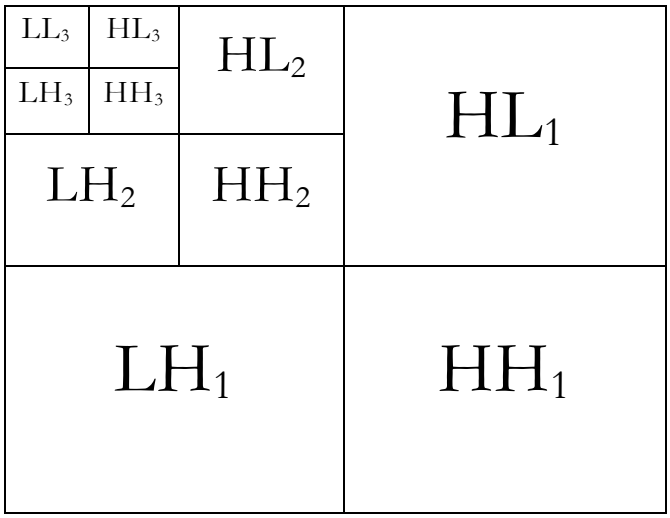

Figure II-7 Three Phase Decomposition Using DWT

There are various types of wavelets among which Haar wavelet is the simplest technique.

The Haar transform is a mathematical operation applied using Haar wavelets. Renowned for its simplicity, the Haar transform serves as a fundamental reference for other wavelet transforms. Its principle lies in decomposing a discrete signal into two sub-signals, each half the length of the original. One sub-signal represents the average trend, while the other depicts the difference or fluctuation. The Haar transform is lauded for its simplicity, cost-effectiveness, and ease of application. However, its drawback lies in its inability to efficiently compress and remove noise in audio signal processing applications. As an alternative to the Haar wavelet, the Daubechies wavelet emerges but is encumbered by its complexity and cost. Symlets, another type of wavelet, present a modified version of the Daubechies wavelets, aiming to enhance symmetry. [28]

we can calculate with the Haar filter as follows:

$$LL(x,y) = \frac{\mathrm{p(x,y)} + \mathrm{p(x,y+1)} + \mathrm{p(x+1,y)} + \mathrm{p(x+1,y+1)}}{2}$$

$$LH(x,y) = \frac{\mathrm{p(x,y)} + \mathrm{p(x,y+1)} - \mathrm{p(x+1,y)} - \mathrm{p(x+1,y+1)}}{2}$$

$$HL(x,y) = \frac{\mathrm{p(x,y)} - \mathrm{p(x,y+1)} + \mathrm{p(x+1,y)} - \mathrm{p(x+1,y+1)}}{2}$$

$$HH(x,y) = \frac{\mathrm{p(x,y)} - \mathrm{p(x,y+1)} - \mathrm{p(x+1,y)} + \mathrm{p(x+1,y+1)}}{2}$$

This process can be repeated to perform multi-level decompositions. [29]

We can express the above mathematical equations with this diagram:

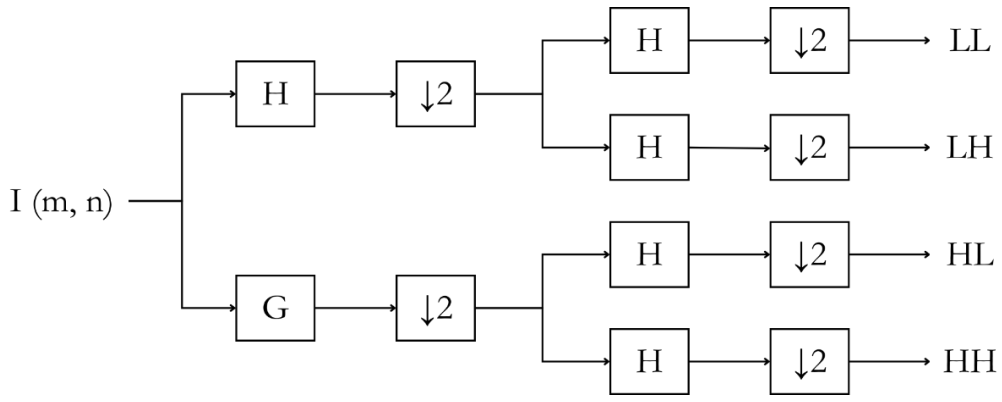

Figure II-8 DWT process

To reconstruct the image from DWT process, used Inverse DWT (IDWT) method and it will produce the original cover image. The formula to perform IDWT method as follows:

$$p(x,y) = \frac{\mathrm{LL(x,y)} + \mathrm{LH(x,y)} + \mathrm{HL(x,y)} + \mathrm{HH(x,y)}}{2}$$

$$p(x,y+1) = \frac{\mathrm{LL(x,y)} + \mathrm{LH(x,y)} - \mathrm{HL(x,y)} - \mathrm{HH(x,y)}}{2}$$

$$p(x+1,y) = \frac{\mathrm{LL(x,y)} - \mathrm{LH(x,y)} + \mathrm{HL(x,y)} - \mathrm{HH(x,y)}}{2}$$

$$p(x+1,y+1) = \frac{\mathrm{LL(x,y)} - \mathrm{LH(x,y)} - \mathrm{HL(x,y)} + \mathrm{HH(x,y)}}{2}$$

II.5 Requirements of Digital watermarking

In a digital watermark, there are four basic properties which are intimately linked. These properties are robustness, imperceptibility, capacity, and security. A compromise must be found between these parameters to achieve an effective and balanced watermarking system. [30]

Figure II-9 Digital Watermarking Requirements

II.5.1 Robustness

The robustness is the ability to detect the watermark after some signal processing modification such as spatial filtering, scanning and printing, lossy compression, translation, scaling, and rotation, and other operations like digital to analog (D/A), analog to digital (A/D) conversions, cutting and image enhancement. In addition, not all watermarking algorithms have the same level of robustness, some techniques are robust against some manipulation operations, however, they fail against other stronger attacks. Moreover, it's not always desirable for the watermark to be robust, in some cases; it's desired for the watermark to be fragile. [31]

II.5.2 Capacity

Capacity (also known as Data Payload) describes how many information bits can be embedded. It addresses also the possibility of embedding multiple watermarks in one document in parallel. The capacity of an image could be different according to the application that watermark is designed for. Moreover, studying the capacity of the image can show us the limit of watermark information that would be embedded and at the same time satisfying the imperceptibility and robustness. [31]

II.5.3 Imperceptibility (Invisibility, Fidelity)

The watermark should not be noticeable to the viewer nor should the watermark degrade the quality of the content. The term imperceptible is widely used in this case. It should be invisible in images and videos, and inaudible in audio files, ensuring that the user experience is not affected. Imperceptibility is crucial for maintaining the aesthetic and functional integrity of the media, ensuring that the watermark does not interfere with its intended use and enjoyment.

II.5.4 Security

Security is the ability to resist against intentional attacks. These attacks intended to change the purpose of embedding the watermark. Attacks types can be divided into three main categories: unauthorized removal, unauthorized embedding, and unauthorized detection.

According to the specific usage of watermarking, the specific feature should be available in the watermark to resist the attacks. [31] An unauthorized user cannot distinguish, retrieve or modify the inserted watermark. Nowadays the researcher is giving prime importance to the security of watermark.

II.5.5 Computational Cost

One of the features that a user of a watermarking technology may be interested in is the computational cost for embedding and extracting a watermark into a host media should be minimal. This cost includes two main issues —the total time required for embedding and extracting the watermark, and the total number of embedders and detectors involved in the watermarking technique. A good trade-off between robustness and computational complexity must be maintained. [32]

II.6 Image Watermark Quality Measures

Any processing applied to an image, including watermarking, may cause a significant loss of information or quality. Image quality refers to how accurately the imaged scene is reproduced and can be affected by degradation factors such as sharpness, dynamic range, color blending, contrast, blocking effect, or blur. Evaluating image quality is essential in watermarking applications to ensure that the embedded watermark does not significantly degrade the original image.

Image quality evaluation methods can be divided into objective and subjective methods. Subjective methods are based on human observations or perceptions and operate informally without explicit criteria. they cannot be taken as standards because human observation is based on some critical factors such as environment, motivation and mood. Objective methods, on the other hand, are based on explicit numerical criteria and comparisons. These methods can use various references, such as ground truth or prior knowledge expressed through statistical parameters and tests. [33]

The measures provide a quantitative assessment of image quality, facilitating the evaluation and optimization of watermarking techniques to minimize their impact on the original image while ensuring the watermark remains effective and detectable.

II.6.1 Imperceptibility Analysis Measures

Imperceptibility in watermarking refers to the degree to which the watermark is invisible or unnoticeable to the human eye. High imperceptibility means that the watermark does not affect the visual quality of the original image. Here are some key metrics for analyzing imperceptibility:

II.6.1.1 Mean Squared Error (MSE)

defined as the average squared difference between a reference image and a distorted image. is used to verify mutilations between cover image & watermarked image. This helps to recognize any alteration within the watermarked image.

MSE is the most common estimator of image quality measurement metrics. It is a full reference metric and the values closer to 0 indicate acceptable degradation. It is calculated by the formula given below:

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j) - f^{1}(i,j)]^{2}$$

Where f and f ^{1} are the host and watermarked image Pixel values. MxN the size of the images.

II.6.1.2 Peak Signal to Noise Ratio (PSNR)

is used to determine the Efficiency of Watermarking with respect to the noise. The noise will degrade the quality of image. The visual quality of watermarked and attacked images is measured using the PSNR and is computed in decibel form, any image with more than 30 dB is accepted in general. [34] It is calculated by the formula given below:

$$PSNR = 10\log_{10}\left(\frac{MAX^{2}}{MSE}\right)(db)$$

Where MAX is the maximum possible value that a pixel in the host or watermarked can take.

II.6.1.3 Structural Similarity Index Measure (SSIM)

is a perception based model. In this method, image degradation is considered as the change of perception in structural information. SSIM Compares the similarity between the original and watermarked images based on luminance, contrast, and structure. Values range from -1 to 1, with higher values indicating better imperceptibility. It is calculated by the formula given below:

$$\text{SSIM}\,(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\delta_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\delta_x^2 + \delta_y^2 + C_2)}$$

where μ_x and μ_y are the mean intensities, σ_x^2 and σ_y^2 are the variances, σ_{xy} is the covariance of images x and y

II.6.2 Robustness Analysis Measures

Robustness in watermarking refers to the ability of the watermark to withstand various attacks or modifications to the watermarked image. Robust watermarks remain detectable and retrievable even after such transformations. Some Key metrics for robustness analysis include:

II.6.2.1 Normalized Correlation (NC)

Normalized correlation measures the similarity between the extracted watermark and the original watermark. The following equation is utilized to calculate normalized correction for two images. the values closer to 1 indicate higher similarity and thus higher robustness.

$$NC = \frac{\sum_{i=1}^{n} Wi \times W'i}{\sqrt{\sum_{i=1}^{n}(Wi)^2 \times \sum_{i=1}^{n}(W'i)^2}}$$

Where n is the size of watermark, and W is the original watermark and W' is the extracted watermark.

II.6.2.2 Bit Error Rate (BER)

BER is defined as ratio between number of incorrectly decoded bits and total number of bits of embedded watermark. It is suitable for random binary sequence watermark. Ideally it should be zero

$$BER = \frac{Number\ of\ incorrectly\ decoded\ bits}{Total\ number\ of\ bits}$$

II.6.3 Capacity Analysis Measures

Capacity analysis in image watermarking refers to the evaluation of how much information can be embedded within an image without compromising its quality or integrity. Here are some key metrics for analyzing imperceptibility:

II.6.3.1 Bits Per Pixel (BPP)

Bits Per Pixel allow to measure payload capacity, it accurately represents the possible number of bits integrated objectively compared to the image's pixel count.

$$BPP = \frac{Number\ of\ secret\ bits\ embedded}{Total\ pixels\ in\ the\ cover\ image}$$

II.7 Digital Watermark Applications

Digital Watermark can be used in a wide variety of applications. In general, if it is useful to associate some additional information with a media file, this metadata can be embedded as a watermark. Of course, there are other ways to associate information. Still, because Watermarking is distinguished from other techniques, this makes digital watermarking a suitable method for associating additional information for certain applications.

II.7.1 Classification Of Watermark Applications

There are numerous watermarking application scenarios. in this table, we classify the watermark applications based on the nature of the information contained in the watermark.

Application Class	Purpose of the embedded watermark	Application Scenarios
Protection of Intellectual Property Rights	Convey information about the content ownership and intellectual property right	– Copyright Protection – Copy Protection – Fingerprinting – Signature
Content Verification	Ensures that the original digital document has not been altered, and/or helps determine the type of alteration	– Authentification – Integrity Checking
Information Hiding	Represents side channel used to carry additional information	– Broadcast Monitoring System – Enhancement

Table II-1 Classification Based on The Nature of The Information Contained in The Watermark [35]

II.7.2 Electronic Health Systems (EHS)

Electronic Health Systems (EHS) are advanced technological platforms that enable healthcare providers to capture, store, and manage patient data, medical histories, and treatment plans in a centralized digital format. These systems are integral to modern healthcare, allowing for the seamless sharing of patient information and medical records across various specialties and care settings. By leveraging Information and Communication Technologies (ICT), EHS facilitate better coordination of care, improve patient outcomes, and enable remote healthcare services such as teleconsultation, telemonitoring, and teleassistance.

II.7.3 Medical Application of Digital Watermarking

As EHS become more widespread, ensuring the protection of patient privacy and confidentiality is paramount. Watermarking plays a crucial role in addressing these concerns by embedding unique identifiers or biometric data into medical records and images. This process helps ensure the authenticity, integrity, and confidentiality of patient information.

Application Area	Description
Secure Data Transmission	Watermarking, coupled with encryption techniques, ensures that patient data remains secure during transmission between different healthcare providers and systems.
Authentication and Integrity	Watermarking ensures that medical records and images have not been altered or tampered with. By embedding biometric data such as fingerprints or iris patterns, watermarking can confirm the identity of the person accessing the data.
Privacy and Confidentiality	Watermarking enhances patient privacy by embedding biometric data directly into medical records.
Enhanced Data Management	embedding additional information into medical records helps track the source and access history of medical records, making it easier to audit and monitor data usage.
Protection of Intellectual Property Rights	protect the intellectual property rights of medical imaging technologies and techniques. By preventing unauthorized copying or distribution of proprietary imaging data.

Table II-2 Role of Watermarking in Electronic Health Systems

II.8 Digital Watermark Attacks

A digital Watermarking scheme is always assessed by the fact of how robust it is over attacks. An attack is any processing that may impair the detection of the watermark or communication of the information conveyed by the watermark. The processed, watermarked data is then called attacked data. The usefulness of an attacked data can be measured by its perceptual quality and the amount of watermark impairment can be measured by criteria such as miss probability, probability of bit error, or channel capacity. An attack succeeds in defeating a watermarking scheme if it impairs the watermark beyond acceptable limits while maintaining the perceptual quality of the attacked data.

The wide class of existing attacks can be divided into four main groups: removal attacks, geometrical attacks, cryptographic attacks and protocol attacks. [36] Nex Figure summarizes the different types of attacks

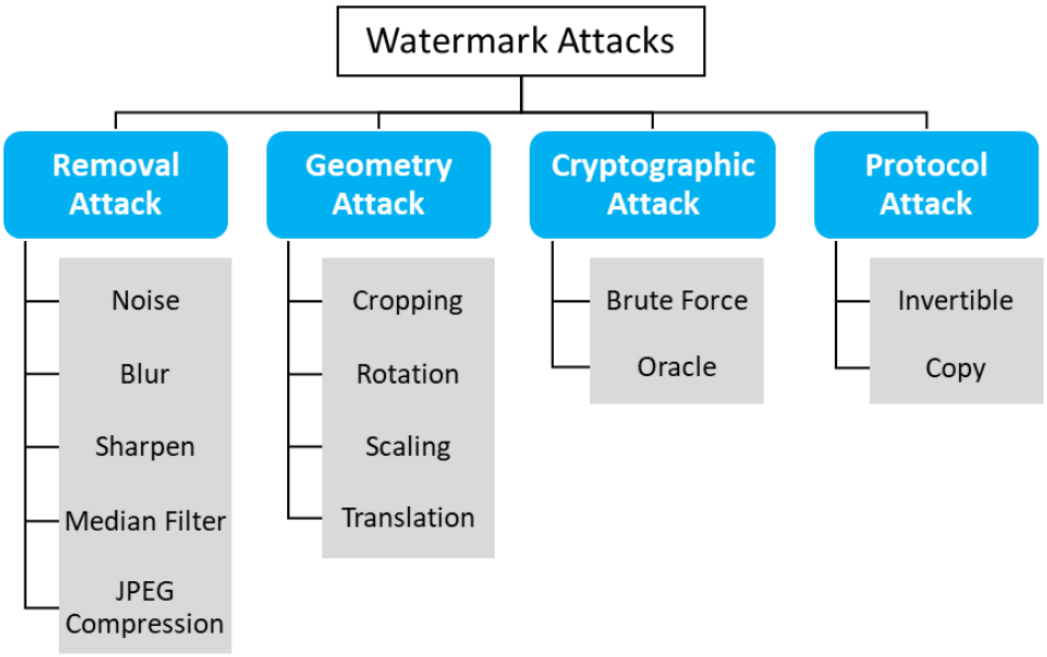

Figure II-10 Classification of watermark attacks [45]

II.8.1 Removal Attacks

Removal attacks aim at the complete removal of the watermark information from the water-marked data without cracking the security of the watermarking algorithm (e.g., without the key used for watermark embedding). That is, no processing, even prohibitively complex, can recover the watermark information from the attacked data. This category includes denoising, quantization (e.g., compression), remodulation, and collusion attacks. Not all of these methods always come close to their goal of complete watermark removal, but they may nevertheless damage the watermark information significantly. [36]

II.8.2 Geometric Attacks

Geometric distortions are specific to videos and images including operations such as rotation, scaling, translation, cropping .... etc. In contrast to removal attacks, geometric attacks do not actually remove the embedded watermark, but intend to distort the watermark detector synchronization with the embedded information. The detector could recover the embedded watermark information when perfect synchronization is regained. However, the complexity of the required synchronization process might be too great to be practical. [37]

II.8.3 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 water-marks. One such technique is brute-force search for the embedded secret information. Another attack in this category is the so-called Oracle attack, which can be used to create a non-water-marked signal when a watermark detector device is available. Practically, application of these attacks is restricted due to their high computational complexity. [36]

II.8.4 Protocol Attacks

Protocol attacks aim at attacking the entire concept of the watermarking application. One type of protocol attack is based on the concept of invertible watermarks.

The idea behind inversion is that the attacker subtracts his own watermark from the watermarked data and claims to be the owner of the watermarked data. This can create ambiguity with respect to the true ownership of the data.

Another protocol attack is the copy attack. In this case, the goal is not to destroy the watermark or impair its detection, but to estimate a watermark from watermarked data and copy it to some other data, called target data. The estimated watermark is adapted to the local features of the target data to satisfy its imperceptibility. signal-dependent watermarks might be resistant to the copy attack. [36]

II.9 Conclusion

Digital watermarking offers a robust solution for copyright protection and content authentication in digital media. By embedding imperceptible information into multimedia content, it enables ownership verification and tracking. Various watermarking techniques exist, each with unique strengths and weaknesses, requiring consideration of application-specific requirements. Robustness against attacks, perceptual transparency, and capacity for payload insertion are critical factors in designing effective watermarking systems.

Chapter III

Proposed Approach and Implementation

III.1 Introduction

Watermarking encompasses a wide range of techniques aimed at embedding information into digital media to ensure authenticity, copyright protection, and data integrity. These techniques vary significantly in terms of complexity, robustness, and application areas.

In this chapter, we present the details of our proposed approach for watermarking, along with the implementation and evaluation of its performance. The primary focus of this chapter is to provide a comprehensive understanding of the methodology used to embed and extract the watermark, as well as to analyze the Imperceptibility and effectiveness of the proposed algorithm.

In the proposed approach, the discrete wavelet transform (DWT) will be used with the modified LSB technique we call Parity LSB. We will begin by describing the algorithmic steps of this technique. The implementation details are then elaborated, showcasing the results obtained from testing our algorithm. Various performance metrics are used to quantify the effectiveness of the watermarking approach. Additionally, we provide an analysis of the algorithm's performance

In this chapter, we aim to provide a comprehensive overview of the development, execution, and evaluation of the DWT watermarking algorithm, highlighting its strengths and identifying areas for potential improvement.

III.2 Software and Tools Used

In our project, we used the Python programming language due to its numerous advantages such as ease of use, clarity, and extensive library support, making it an ideal choice for implementing complex algorithms. Additionally, we employed the PyCharm Integrated Development Environment (IDE) for development, as it provides powerful tools for efficient coding, debugging, and project management.

III.2.1 Python

Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development. Python's simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. Python supports modules and packages, which encourages program modularity and code reuse. [38]

Figure III-1 Python Logo

We used an advanced Python version which is Python 3.11 to ensure compatibility with the latest libraries and tools.

III.2.2 PyCharm

PyCharm is a dedicated Python Integrated Development Environment (IDE) developed by JetBrains, providing a wide range of essential tools for Python developers, tightly integrated to create a convenient environment for productive Python, such as intelligent code completion, syntax highlighting, refactoring tools, and built-in support for version control systems such as Git. PyCharm also includes powerful debugging and profiling tools, as well as integration with popular frameworks and libraries. [39]

Figure III-2 PyCharm Logo

III.2.3 Libraries

The table III-1 shows the primary Libraries we used

Library	Description	Usage	Version
NumPy	NumPy is the fundamental package for scientific computing in Python. It is a Python library that provides support for large, multi-dimensional arrays and matrices, along with a collection of mathematical functions to operate on these arrays efficiently. [40]	Efficient array manipulation and mathematical operations required during the implementation	1.26.3
Math	provides access to the mathematical functions defined by the C standard. [41]	Performing mathematical operations essential for the implementation of the watermarking algorithm.	Built-in Python module
Pillow (PIL)	The Python Imaging Library adds image processing capabilities to your Python interpreter. It provides a solid foundation for a general image processing tool. [42]	Basic image processing tasks such as reading, writing, and manipulating images.	10.2.0

Table III-1 Used Libraries

III.2.3.1 PyWavelets

PyWavelets is a Python library for wavelet transforms and wavelet-based signal processing. It provides functions for performing discrete wavelet transforms (DWT) and inverse discrete wavelet transforms (IDWT) on one-dimensional and multi-dimensional data.

Notice: Through our experiences and several tests, we observed that the PyWavelets Library was not convincing in its results, so we had to write the DWT & IDWT functions we needed with the appropriate mathematical formula for our project. Still, it is the famous Open Source library for processing signals in Python.

III.3 Method

Our algorithm relies on two main methods Discrete Wavelet Transform (DWT) and Parity Least Significant Bit (LSB). In this section, we will describe each of these methods in detail, explaining how they are utilized in the watermarking process.

III.3.1 Discrete Wavelet Transform (DWT)

As we explained in Chapter II, the Discrete Wavelet Transform (DWT) is a fundamental technique in image processing that allows for the decomposition of an image into different frequency sub bands. In the DWT method, the image is decomposed into four sub bands: LL (low-low), LH (low-high), HL (high-low), and HH (high-high). The LL sub band contains the approximation coefficients, which represent the low-frequency components of the image, while the LH, HL, and HH sub bands contain the detail coefficients, representing the high-frequency components. This decomposition is crucial for our watermarking algorithm as it enables us to embed the watermark in the less perceptually significant parts of the image, thus maintaining the visual quality. The figure III-3 illustrates the effect of the DWT application on an image and the resulting sub bands.

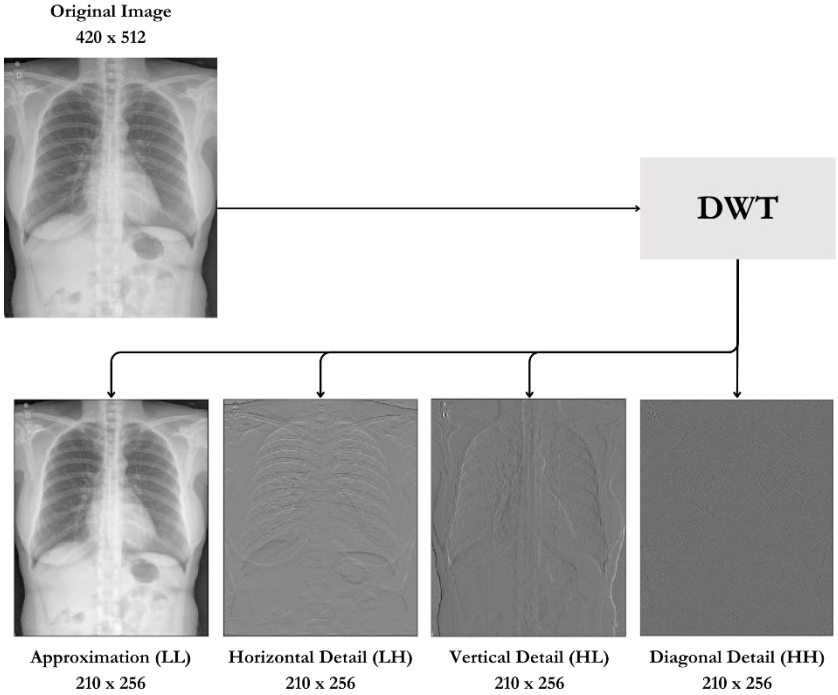

Figure III-3 DWT sub-band of an image

By embedding the watermark in the sub bands, we achieve a balance between imperceptibility and robustness. The inverse DWT is then applied to reconstruct the watermarked image from the modified sub bands. This process provides us a better way to embed a watermark and ensures that the watermark remains imperceptible to the naked eye.

The detailed implementation of the DWT and its integration with the Parity LSB method will be discussed in the Implementation section.

III.3.2 Parity LSB

We provide this embedded technique as a novel embedding technique that embeds secret information into digital images. It builds upon the foundational concepts of the LSB method but enhances the process by incorporating parity. Parity refers to the odd or even nature of the total number of '1' bits in a binary sequence. In the context of this method which we will call Parity LSB, instead of directly replacing the LSB of each pixel, the method adjusts the pixel values to ensure that the parity of the pixel's binary representation matches the corresponding bit of the watermark.

the embedding method should preferably be unique and uncommon, this helps to improve the security of the watermark system and make it more resistant to the watermark extraction and removal systems, with this proposed embedding technique we can make the system provide these advantages

III.3.2.1 Algorithm of Embedding

We suggest the following steps of the embedding phase method and the related diagram is shown in figure III-4.

Step 1: Preparation of host image and watermark (text or image)

1- Read the Image
2- Convert cover image to Grayscale If the image is not a grayscale image
3- Convert the host image to matrix form
4- convert watermark to binary sequence

Step 2: Parity calculation

1- Convert the pixel value of host image to its 8-bit binary representation
2- Calculate the sum of the 1bits in the binary representation, ex: (10011011)>>5 the parity of the pixel (10011011) is odd cause 5 is odd

Step 3: Comparison

1- For each bit of the binary sequence watermark, the bit value is compared with the parity of corresponding pixel
2- If the watermark bit is '1' the parity must be odd
3- If the watermark bit is '0' the parity must be even

Step 4: LSB changing

1- Changing of the least significant bit depending to the watermark bit value
2- If watermark bit is '1' and the parity is even we change the LSB to make parity odd
3- If watermark bit is '0' and the parity is odd we change the LSB to make parity even
4- If watermark bit is '1' and the parity is odd or watermark bit is '0' and the parity is even we don't change the LSB

Step 5: After embedding all the watermark bits Save the marked image.

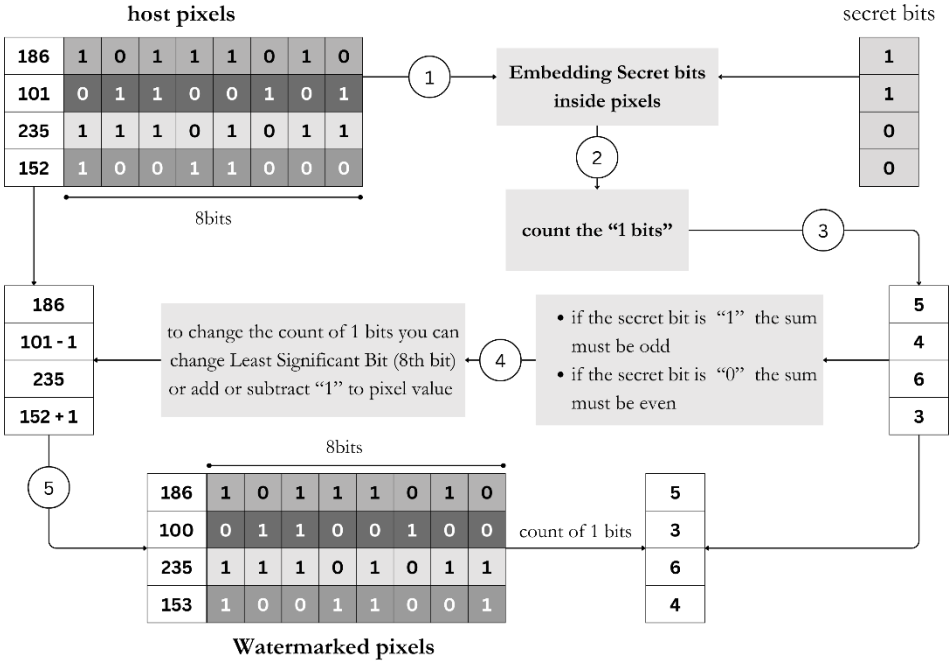

Figure III-4 Parity LSB Embedding Method

III.3.2.2 Algorithm of Extracting

We suggest the following steps of the extraction phase method and the related diagram is shown in figure III-5.

Step 1: Preparation of marked image

1- Read the Image
2- Convert the marked image to matrix form

Step 2: Parity calculation

1- Convert the pixel value of host image to its 8-bit binary representation
2- Calculate the sum of the 1bits in the binary representation

Step 3: Extracting the watermark

1- For each pixel in marked image, the parity of the pixel refers to the watermark bit value
2- If the parity is odd mean the watermark bit value is '1'
3- If the parity is even mean the watermark bit value is '0'
4- Extract the parity from the pixel while the size of watermark is not achieved

Step 4: Reform the results

1- Reform the list of watermark bits to original form (text or image)
2- Save the watermark

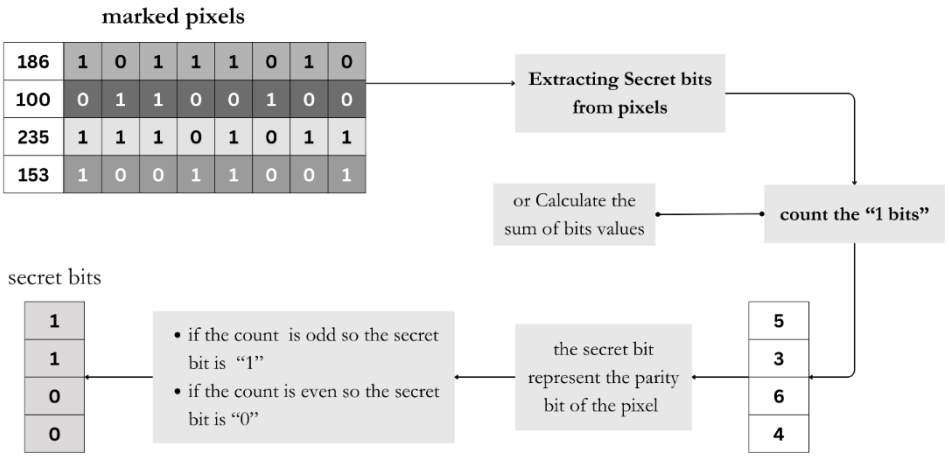

Figure III-5 Parity LSB Extracting Method

III.4 Implementation

In this section, we present the comprehensive implementation of our watermarking algorithm, which integrates the Discrete Wavelet Transform (DWT) with the Parity Least Significant Bit (LSB) method. The implementation process is meticulously detailed and divided into two primary steps: watermark embedding and watermark extraction. Each step is thoroughly described and illustrated to provide a clear understanding of the process.

III.4.1 Watermark Embedding Procedure

The watermark embedding procedure is depicted in Figure III-6 and described in detail in the following steps.

Step 1: Preparation of host image and watermark (text or image)

1- Read the Image
2- Convert the host image to matrix form
3- Reformulate the watermark into a string of zeros and ones binary representation

Step 2: Perform DWT

1- Apply DWT to the host image in order to decompose it into four sub-bands LL, LH, HL, HH
2- Choose one of 4 sub-band to embedding the watermark in it

Step 3: Embedding the Watermark with Parity LSB

1- Embed the watermark binary sequence in the selected DWT sub-band using Parity LSB

Step 5: Perform IDWT

1- Apply the inverse DWT (IDWT) on the DWT transformed image, including the modified sub-band, to produce the marked image

Step 6: Save the image

The format in which you save the marked image is very important, in the context of our implementation we noticed that the TIFF and PNG and BMP formats have produced better results, in this thesis we use PNG format to save images.

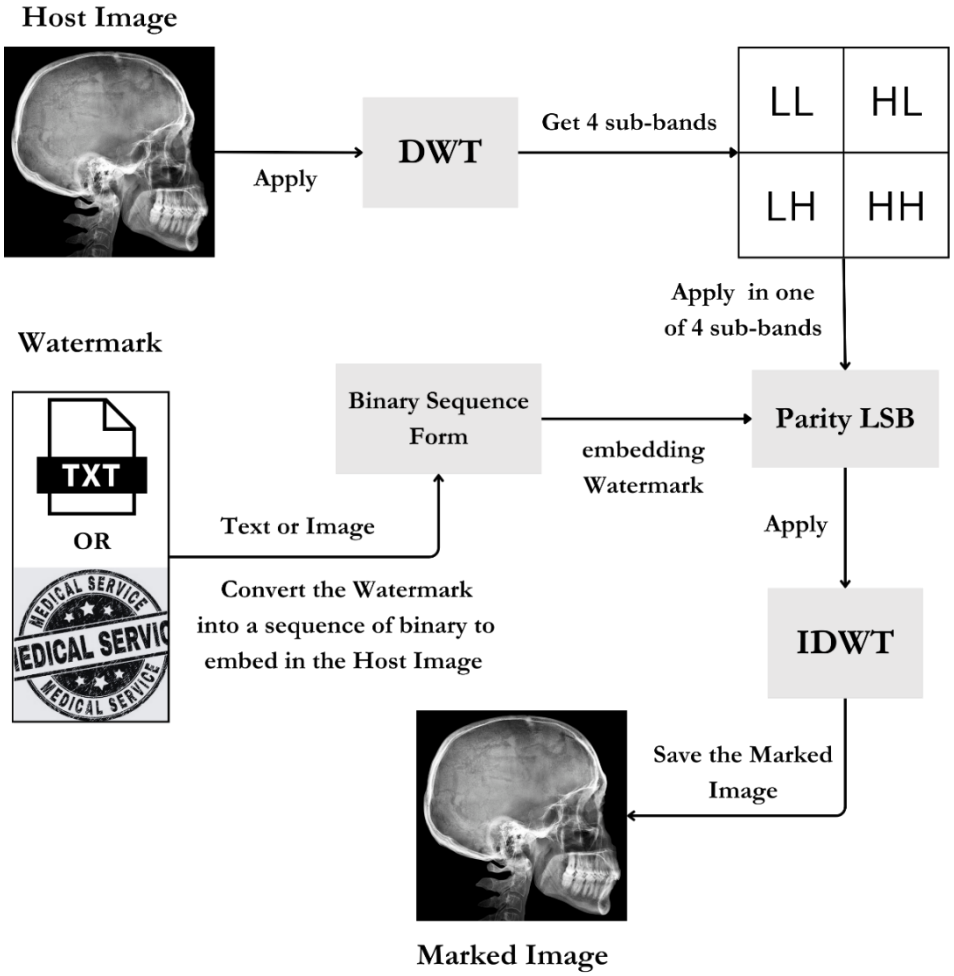

Figure III-6 Watermark Embedding Method

III.4.2 Watermark Extraction Procedure

The watermark extraction procedure is depicted in Figure III-7 and described in detail in the following steps. Since our watermarking algorithm is a semi-blind watermarking algorithm, the original host image is not required in the watermark extraction procedure but some information is required including the watermark size and the watermark original format (text or RGB image or …), Also the Sub-band where the watermark was embedded (LL or LH or HL or HH).

Step 1: Preparation of marked image

1- Read the Image
2- Convert the marked image to matrix form

Step 2: Perform DWT

1- Apply DWT to decompose the watermarked image into four sub-band LL, LH, HL, HH
2- Choose the Sub-band where the watermark was embedded

Step 3: Extracting the Watermark with Parity LSB

1- Extract the bits of watermark using extracting Parity LSB

Step 4: Save the watermark

1- Reconstruct the watermark using the extracted watermark bits
2- Reform the watermark to original form (text or image) and save it

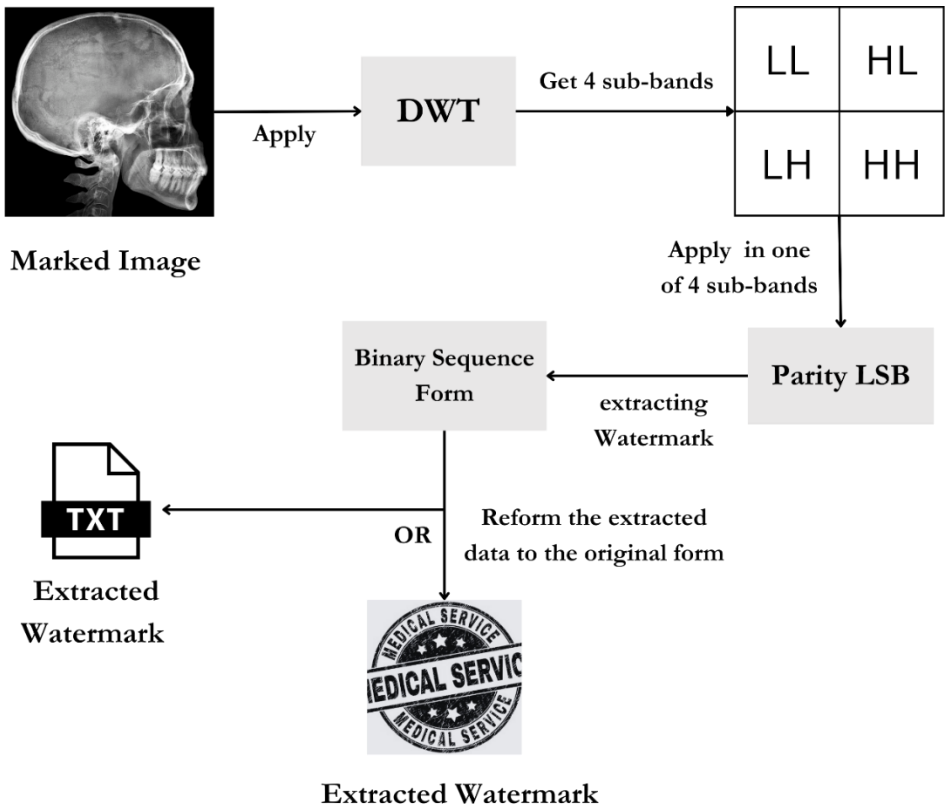

Figure III-7 Watermark Extracting Method

III.4.3 Watermark Implementation Example

We implemented our algorithm on a medical image by embedding a watermark. The host image is a grayscale medical image with dimensions 2000 x 2000 pixels, with a watermark image RGB logo with dimensions 180 x 180 pixels. The watermark was embedded into four different sub-bands of the DWT: LL, LH, HL, and HH, the following graph illustrates the implementation.

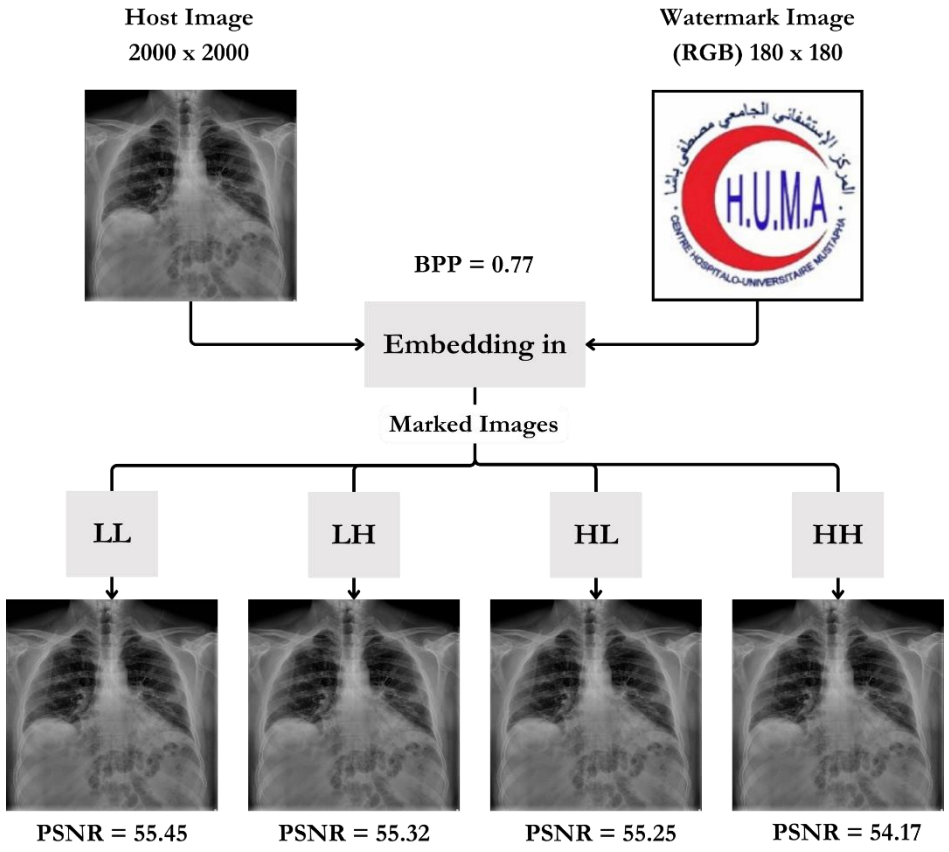

Figure III-8 Implementation Example

III.5 Experiments and Results

This section presents a detailed analysis of the experiments conducted to evaluate the performance of the DWT + Parity LSB algorithm in term of imperceptibility.

The results of these experiments will be discussed, highlighting the algorithm's strengths and potential areas for improvement. By examining the performance metrics, we aim to provide a comprehensive evaluation of our method's capability to preserve the visual quality of the cover images with perfect watermark retrieval.

III.5.1 About Dataset

The proposed watermarking techniques are tested on a large database of medical images. we used Body Parts X-Ray Images in PNG (Classify Body Parts from X-Ray images - Unifesp competition) available at Kaggle platform [43]. This dataset was uploaded in 2022 by ICARO BOMBONATO, we chose this dataset because it contains a large number of various medical images of different dimensions and sizes. The images were extracted from source DICOM Images and are in PNG format in this dataset.

Figure III-9 Some Images from Dataset

III.5.2 Results

The results of our watermarking algorithm were evaluated on a dataset of 681 images from ICARO BOMBONATO dataset. The algorithm was applied with three different bits per pixel (BPP) values to assess its performance under varying conditions. The evaluation focused manually on Peak Signal-to-Noise Ratio (PSNR), which measure the quality of the visual quality of marked images. The detailed outcomes of these evaluations are presented in the following tables, where we analyze the impact of our algorithm in different BPP values on the effectiveness and robustness of the watermarking process.

- Table III-2 shows the results with bits per pixel (BPP) ≈ 20

Sub-band	PSNR (db)	SSIM	MSE
LL	61.50485353	0.999511149	0.046909488
LH	61.20681711	0.999443688	0.049424514
HL	61.20377134	0.999444325	0.049454522
HH	61.24620608	0.999446058	0.048971866

Table III-2 Results with bpp = 20

- Table III-3 shows the results with bits per pixel (BPP) ≈ 50

Sub-band	PSNR (db)	SSIM	MSE
LL	57.39656984	0.998773424	0.11935537
LH	57.20947753	0.998637454	0.123925422
HL	57.20297594	0.998635996	0.124110446
HH	57.247927	0.998641762	0.122836046

Table III-3 Results with bpp = 50

- Table III-4 shows the results with bits per pixel (BPP) ≈ 100

Sub-band	PSNR (db)	SSIM	MSE
LL	54.36306292	0.997402973	0.239728881
LH	54.2099366	0.997148032	0.247414192
HL	54.20208552	0.997142934	0.247873884
HH	54.25084101	0.997157519	0.245086868

Table III-4 Results with bpp = 100

III.5.3 Analysis Results

The results of the watermarking algorithm applied are summarized in three tables, each corresponding to different bits per pixel (BPP) values 20, 50, and 100, The primary metrics used for evaluation were Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Mean Squared Error (MSE).

For a BPP value of 20, the results indicate minimal distortion and excellent visual quality, as evidenced by the high PSNR and SSIM values across all sub-bands (LL, LH, HL, HH). The low MSE values further support the negligible loss in image quality due to watermarking.

As the BPP value increases to 50, The PSNR and SSIM values exhibit a slight decline compared to the BPP 20 scenario, indicating a moderate increase in image distortion. The MSE values have increased, suggesting that the image quality is somewhat affected, although it remains within acceptable limits.

At the max value of BPP (100), the PSNR and SSIM values show a more pronounced decrease, indicating increased image distortion. The MSE values are higher, reflecting a greater degree of quality degradation. This trend suggests that while the algorithm remains effective, the watermark's visibility and the overall image quality are more noticeably impacted at this higher BPP level.

The LL sub-band consistently shows the best performance in terms of maintaining image quality, but the differences between the sub-bands are minimal, indicating a relatively uniform impact of the watermarking process across all sub-bands.

Overall, the evaluation suggests that while the watermarking algorithm maintains effectiveness across varying BPP values, higher BPP values lead to increased image distortion. Therefore, the choice of BPP value should be carefully considered based on the specific requirements for watermark imperceptibility and image quality.

III.6 Conclusion

In this thesis, we applied a digital watermarking technique to medical images. Our technique combined the Discrete Wavelet Transform (DWT) and parity Least Significant Bit (LSB) for embedding the watermark. Our results demonstrated high imperceptibility of the watermark. This was evidenced by the high Peak Signal Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) values obtained in our experiments. These metrics indicate that the watermarking process did not cause noticeable alterations to the medical images, thereby preserving their diagnostic value.

General Conclusion

The increasing digitization of medical systems has brought significant advancements in the storage, retrieval, and transmission of medical images. However, this digital transformation also presents challenges related to the security and authenticity of these images. Ensuring the integrity and confidentiality of medical images is crucial for maintaining trust in medical diagnoses and treatments. Digital watermarking has emerged as a vital technique for embedding additional information into medical images, thereby providing a means to verify their authenticity and detect tampering without compromising their diagnostic quality.

In this thesis, we applied a digital watermarking technique to medical images by using DWT and LSB methods. Our approach aimed to embed watermarks in such a way that the visual quality of the medical images remained high, ensuring their usability for diagnostic purposes.

Our experimental results demonstrated that the watermarking process achieved high imperceptibility, as indicated by the high Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM) values. These metrics confirmed that the embedded watermarks did not cause noticeable alterations to the medical images. and the differences between the sub-bands (LL, LH, HL, HH) were minimal, indicating a relatively uniform impact of the watermarking process.

We have high expectations that our thesis will significantly contribute to the healthcare system by offering enhanced security, integrity verification, and the preservation of diagnostic quality.

Future objectives of our work could include enhancing the effectiveness and applicability of the watermarking technique in the medical domain by focusing on the following areas:

- **Robustness Against Attacks:** Investigate the robustness of the watermarking algorithm against various types of attacks, including geometric and cryptographic attacks, to ensure the watermark's integrity and security under adverse conditions.

- **Optimization of BPP Values:** Explore optimization techniques to determine the ideal BPP value that balances watermark imperceptibility and robustness without significantly compromising image quality.
- **Multi-media Applications:** Extend the current technique to other types of multimedia content, such as videos and audio files, to evaluate its versatility and effectiveness across different digital media.
- **Machine Learning Integration:** Incorporate machine learning algorithms to enhance the detection and extraction processes of watermarks, potentially improving the accuracy and speed of these operations.

By addressing these areas, future work can contribute to the development of more advanced and reliable digital watermarking techniques, further enhancing the security and authenticity of digital media in the medical field and beyond

Bibliography

[1] A. Online, "Digital photography vs. film photography," 14 December 2021. [Online]. Available: https://asuonline.asu.edu/newsroom/online-learning-tips/digital-vs-film-photography/. [Accessed June 2024].

[2] NIST, "Fiftieth Anniversary of First Digital Image Marked," NIST (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY NIST), 24 May 2007. [Online]. Available: https://www.nist.gov/news-events/news/2007/05/fiftieth-anniversary-first-digital-image-marked. [Accessed June 2024].

[3] S. a. M. Museum, "THE FIRST DIGITAL PHOTOS, FROM VICTORIAN TECHNOLOGY TO THE INTERNET," Science Museum Group, 24 April 2020. [Online]. Available: https://www.scienceandmediamuseum.org.uk/objects-and-stories/first-digital-photos. [Accessed June 2024].

[4] V. Beal, "Pixel," Techopedia, 13 May 2024. [Online]. Available: https://www.techopedia.com/definition/24012/pixel. [Accessed June 2024].

[5] X. Wang, L. Sun, A. Chehri and Y. Song, "A Review of GAN-Based Super-Resolution Reconstruction for Optical Remote Sensing Images," *Remote Sensing,* vol. 15, no. 20, 2023.

[6] W. N. Ibrahem, "Image Processing," in *Ibrahem, Wasseem Nahy*, university of technology iraq, pp. 1-3.

[7] S. Sinha, "Fundamental Steps In Digital Image Processing," Scaler topics, 25 Jan 2024. [Online]. Available: https://www.scaler.com/topics/fundamental-steps-in-digital-image-processing/. [Accessed june 2024].

[8] J. A. Richards and X. Jia, Remote sensing digital image analysis, Berlin: Springer Verlag, 2006.

[9] R. Kaur and P. Choudhary, "A Review of Image Compression Techniques," *International Journal of Computer Applications,* vol. 142, no. 1, 2016.

[10] a. abdulgader, "A Comparative Study on Steganography Digital Images: A Case Study of Scalable Vector Graphics (SVG) and Portable Network Graphics (PNG) Images Formats," *International Journal of Advanced Computer,* vol. 9, no. 1, 2018.

[11] R. O. Oyeleke, F. O. Alamu and A. Akinwole, "On the Performance of Lossless Wavelet Compression Scheme on Digital Medical Images in JPEG, PNG, BMP and TIFF Formats," *International Journal of Computer Applications,* vol. 81, no. 15, pp. 33-37, 2013.

[12] F. Ritter, T. Boskamp, A. Homeyer, H. Laue, M. Schwier, F. Link and H.-O. Peitgen, "Medical Image Analysis," *IEEE Pulse,* vol. 2, no. 6, pp. 60-70, 2011.

[13] U. F. &. D. ADMINISTRATION, "Medical Imaging," U.S. FOOD & DRUG ADMINISTRATION (FDA), 28 8 2018. [Online]. Available: https://www.fda.gov/radiation-emitting-products/radiation-emitting-products-and-procedures/medical-imaging. [Accessed June 2024].

[14] MedlinePlus, "Diagnostic Imaging," National Library of Medicine, 3 March 2016. [Online]. Available: https://medlineplus.gov/diagnosticimaging.html. [Accessed June 2024].

[15] Intelerad, "What is DICOM Image Format & Why is It Important in Radiology?," Intelerad, 23 February 2023. [Online]. Available: https://www.intelerad.com/en/2023/02/23/handling-dicom-medical-imaging-data/. [Accessed June 2024].

[16] ChartRequest, "What is Digital Medical Imaging?," ChartRequest, 21 November 2023. [Online]. Available: https://chartrequest.com/what-is-digital-medical-imaging/. [Accessed June 2024].

[17] F. A. P. PETITCOLAS, R. J. ANDERSON and M. G. KUHN, "Information Hiding—A Survey," *Proceedings of the IEEE,* vol. 87, no. 7, pp. 1062-1078, July 1999.

[18] S. M. Thampi, "Information Hiding Techniques: A Tutorial Review," *ArXiv,* 2008.

[19] S. P. Mohanty, "Digital Watermarking: A Tutorial Review," *CiteSeer,* May 2003.

[20] S. Priya, R. Varatharajan, G. Manogaran, R. Sundarasekar and P. M. Kumar, "Paillier homomorphic cryptosystem with poker shuffling transformation based water marking method for the secured transmission of digital medical images," *Personal and Ubiquitous Computing,* April 2018.

[21] M. Hussain and M. Huss, "A Survey of Image Steganography Technique," *International Journal of Advanced Science and Technology,* vol. 54, May 2013.

[22] Arpit, "Everything that you need to know about Image Steganography," Medium, 17 Jan 2020. [Online]. Available: https://medium.com/@arpitbhayani/internals-of-image-steganography-b0d1d60425bf. [Accessed June 2024].

[23] S. A. Nie, G. Sulong, R. Ali and A. Abel, "The use of Least Significant Bit (LSB) and Knight Tour Algorithm for image steganography of cover image," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 9, no. 6, pp. 5218-5226, 2019.

[24] C. Patil, D. Thakur and V. Patil, "PIXEL VALUE DIFFERENCING: ADVANCEMENTS IN STEGANOGRAPHY FOR SECURE DATA EMBEDDING WITHIN IMAGES," *International Research Journal of Modernization in Engineering Technology and Science,* vol. 05, no. 05, pp. 8083-8087, May 2023.

[25] A. Chopra, S. Gupta and S. Dhall, "Analysis of frequency domain watermarking techniques in presence of geometric and simple attacks," *Multimedia Tools and Applications,* 2019.

[26] K. Fares, K. Amine and E. Salah, "A robust blind color image watermarking based on Fourier transform domain," *Optik,* vol. 208, 2020.

[27] A. Al-Haj, "Combined DWT-DCT Digital Image Watermarking," *Journal of Computer Science,* vol. 3, no. 9, pp. 740-746, 2007.

[28] S. Thakral and P. Manhas, "Image Processing by Using Different Types of Discrete Wavelet Transform," *Advanced Informatics for Computing Research,* p. 499–507, 2018.

[29] F. Kahlessenane, A. Khaldi, K. M. Redouane and E. Salah, "DCT & DWT based watermarking scheme for medical information security," *Biomedical Signal Processing and Control,* vol. 66, 2021.

[30] A. F. Eldaoushy, M. I. Desouky, S. A. El-Dolil, A. S. El-Fishawy and F. E. A. El-Samie, "Efficient hybrid digital image watermarking," *Optics,* vol. 09, June 2023.

[31] M. Abdullatif, A. M. Zeki, J. Chebil and T. S. Gunawan, "Properties of Digital Image Watermarking," in *2013 IEEE 9th International Colloquium on Signal Processing and its Applications*, Kuala Lumpur, Malaysia, 2013.

[32] M. Begum and M. S. Uddin, "Digital Image Watermarking Techniques: A Review," *Information,* vol. 11, p. 110, 2020.

[33] A. Horé and D. Ziou, "Is there a relationship between peak-signal-to-noise ratio and structural similarity index measure?," *IET Image Processing,* vol. 7, no. 1, p. 12–24, 2013.

[34] U. Sara, M. Akter and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *Journal of Computer and Communications,* vol. 7, no. 3, pp. 8-18, 2019.

[35] J. Sen, A. Sen and K. Hemachandra, "AN ALGORITHM FOR DIGITAL WATERMARKING OF STILL IMAGES FOR COPYRIGHT PROTECTION," *Indian Journal of Computer Science and Engineering (IJCSE),* vol. 03, February 2012.

[36] 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, p. 118–126, 2001.

[37] T. GÖKOZAN, "TEMPLATE BASED IMAGE WATERMARKING IN THE FRACTIONAL FOURIER DOMAIN," *MSc thesis, MIDDLE EAST TECHNICAL UNIVERSITY (METU),* 2005.

[38] P. TM, "What is Python? Executive Summary," Python TM, [Online]. Available: https://www.python.org/doc/essays/blurb/. [Accessed June 2024].

[39] JetBrains, "Quick start guide," JetBrains, 26 May 2024. [Online]. Available: https://www.jetbrains.com/help/pycharm/quick-start-guide.html. [Accessed June 2024].

[40] N. Developers, "NumPy documentation," NumPy, [Online]. Available: https://numpy.org/doc/stable/index.html. [Accessed June 2024].

[41] P. TM, "math — Mathematical functions," Python TM, [Online]. Available: https://docs.python.org/3.11/library/math.html#module-math. [Accessed June 2024].

[42] Pillow, "Pillow (PIL Fork) documentation," Pillow, [Online]. Available: https://pillow.readthedocs.io/en/stable/. [Accessed June 2024].

[43] I. Bombonato, "Body Parts X-Ray Images in PNG," Kaggle, 2022. [Online]. Available: https://www.kaggle.com/datasets/ibombonato/xray-body-images-in-png-unifesp-competion. [Accessed June 2024].

[44] A. Cheddad, J. Condell, K. Curran and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing,* vol. 90, no. 3, p. 727–752, 2010.

[45] S. Wadhera, D. Kamra, A. Rajpal, A. Jain and V. Jain, "A Comprehensive Review on Digital Image Watermarking," in *EASTON 100 - 5th International Conference on Computing Sciences (ICCS 2021)*, 2021.

[46] MathWorks, MATLAB - Image Processing Toolbox™ User's Guide, MathWorks, Inc, 2013.