Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

Kasdi Merbah University – Ouargla

Faculty of New Technologies of Information and Communication
Department of Computer Science and Information Technology

THESIS OF ACADEMIC MASTER

Realized by:

BERRACHED MAROUA

Titled:

A blind and irreversible approach to watermarking medical images in the spatial domain

Committee Members:

Supervisor:	KHALDI AMINE	UKM OUARGLA
President:	MEZZATI MESSAOUD	UKM OUARGLA
Examiner:	ZERDOUMI OUSSAMA	UKM OUARGLA

Academic year: 2021/2022

ACKNOWLEDGEMENT

We thank God the Almighty for having given us the health and the will to start and finish this thesis.

First of all, this work would not be as rich and could not have been born without the help and guidance of Mr. KHALDI Amine,

We thank him for the quality of his exceptional supervision, for his patience, his rigor and his availability during the preparation of this thesis.

We thank the members of the jury for having taken the trouble to read and judge this work.

We do not forget before closing my thank you page to address a special thanks to ABDELMOUNAIM SAGGAI. for his patience and unconditional support without which we could never have finished our work.

Our thanks also go to all our professors in the specialty for their help.

Abstract

As information and communication technology continues to evolve, the major problem remains how to exchange data over the Internet while preserving their integrity and confidentiality against various attacks. In this context, several IT solutions based on access control techniques exist but they remain insufficient, hence the emergence of digital watermarking as a complementary solution in order to contribute to the security of images shared on the network. The objective of our work is the development of a digital image watermarking algorithm. The information to be inserted is data related to the image, the insertion of the mark is performed in the spatial domain. The inserted mark must however respect two fundamental constraints: imperceptibility and indelibility. The contribution of digital watermarking is the security of the images; it is necessary to ensure that the mark does not degrade the visual quality. In this sense, we wish to provide a optimal coding approach that aims to guarantee the performance trade-off between embedding capacity, imperceptibility and robustness of the watermarking images. In order for a digital watermarking to be effective it must be robust, imperceptible and statistically invisible.

Key words: Digital watermarking, medical image, telemedicine, spatial domain

RESUME

Alors que les technologies de l'information et de la communication ne cessent d'évoluer, le problème majeur reste de savoir comment échanger des données sur Internet tout en préservant leur intégrité et leur confidentialité contre diverses attaques. Dans ce contexte, plusieurs solutions informatiques basées sur des techniques de contrôle d'accès existent mais elles restent insuffisantes, d'où l'émergence du tatouage numérique comme solution complémentaire afin de contribuer à la sécurité des images partagées sur le réseau. L'objectif de notre travail est le développement d'un algorithme de tatouage numérique d'images. L'information à insérer est une donnée liée à l'image, l'insertion de la marque est réalisée dans le domaine spatial. La marque insérée doit cependant respecter deux contraintes fondamentales : l'imperceptibilité et l'indélébilité. L'apport du tatouage numérique étant la sécurisation des images, il est nécessaire de s'assurer que la marque ne dégrade pas la qualité visuelle. Dans ce sens, nous souhaitons fournir une approche de codage optimal qui vise à garantir le compromis de performance entre la capacité d'intégration, l'imperceptibilité et la robustesse des images de filigrane. Pour qu'un filigrane numérique soit efficace, il doit être robuste, imperceptible et statistiquement invisible.

Mots Clés : Tatouage numérique, image médicale, télémédecine, domaine spatial

ملخص

مع استمرار تطور تقنيات المعلومات والاتصالات ، تظل المشكلة الرئيسية هي كيفية تبادل البيانات الطبية على الإنترنت مع الحفاظ على سلامتها وسريتها ضد الهجمات المختلفة. في هذا السياق ، توجد العديد من حلول تكنولوجيا المعلومات القائمة على تقنيات التحكم في الوصول ولكنها تظل غير كافية ، ومن ثم ظهور العلامة المائية الرقمية كحل تكميلي للمساهمة في أمن الصور المشتركة على الشبكة. الهدف من عملنا هو تطوير خوارزمية العلامة المائية للصور الرقمية. المعلومات المراد إدراجها هي بيانات مرتبطة بالصورة ، ويتم إدخال العلامة في المجال المكاني. ومع ذلك ، يجب أن تحترم العلامة المُدخلة قيدين أساسيين: عدم الإدراك وعدم القدرة على المحو. مساهمة العلامة المائية الرقمية في تأمين الصور ، فمن الضروري التأكد من أن العلامة لا تقلل من الجودة المرئية. بهذا المعنى ، نرغب في تقديم نهج ترميز أمثل يهدف إلى ضمان مفاضلة الأداء بين قدرة التضمين وعدم الإدراك وقوة صور العلامة المائية. لكي تكون العلامة المائية الرقمية فعالة ، يجب أن تكون قوية وغير محسوسة وغير مرئية من الناحية الإحصائية.

الكلمات المفتاحية: الوشم الرقمي ، الصورة الطبية ، التطبيب عن بعد ، المجال المكاني

CONTENTS

LISTE OF FIGURES

LISTE OF TABLES

GENERAL INTRODUCTION

Information and communication technologies are increasingly revolutionizing various economic and industrial sectors, including medical imaging for telemedicine. The latter continues to occupy an important place in various medical applications, but the main problem remains the exchange of data over the Internet, while maintaining its integrity and confidentiality against various attacks. In this context, Information technology solutions based on the use of access control technologies are numerous, but they are not yet sufficient, hence the emergence of digital watermarking as a complementary solution to contribute to the security of medical images shared on the network. [1] The objective of our work is to develop native digital image watermarking algorithms based on the Last Significant Bit (LSB) method to ensure authentication and integrity. A digital watermark consists of inserting an invisible mark, also called a signature or watermark, into an image or other digital document, for various purposes such as anti-fraud, computer intrusion and copyright protection.

LSB techniques are based on modifying the least significant bit layer of images. This technique based on the fact that the changes in least significant bits in an image would not have any effect on an image. [2]

The information to be captured is patient data, the signature of the health institution or the doctor in images of all kinds.

In the first chapter, our study focuses specifically on digital images. We introduced the concept of "digital image" and became familiar with its characteristics and types.

In the second chapter, we first provided the definition of digital watermarking, then we mentioned the elements of a digital watermarking system after that we discussed the limitations and types of watermarking systems as well as the application areas.

Then, in the third chapter, we discussed watermarking for images in the spatial and frequency domains, with a mention of some techniques in each domain.

The fourth chapter is devoted exclusively to the introduction of our watermarking method, and we first present the tools and methods used, and then the application of watermarking and the obtained results.

CHAPTER 1

DIGITAL IMAGES

Introduction

In this chapter, we discover the basic notions of digital images, it different types and characteristics.

1.1. Definition

a digital image is a matrix representation of a two-dimensional image using a unite number of points cell elements, usually referred to as pixels that can be stored and handled by a digital computer. [3]

- **Raster image:** A raster image is composed of a set of points called pixels. This type of image is suitable for display on screen but not very suitable for printing because in case of enlargement a loss of quality can occur. [4]
- **Vector image:** A vector image is represented using mathematical formulas. This then makes it possible to resize it without any loss of quality. [4]

1.2. property of a digital image

1.2.1. Pixel

The pixel is the smallest point in the image. Each pixel of the image conveys information, the quantity of this information gives nuances between images at the level of gray (monochrome) and images of color. [5]

1.2.2. Dimension

The dimension of an image is the number of pixels in it, given by the product of the number of rows and the number of columns of the matrix associated with the image. [6]

1.2.3. The resolution

The resolution of an image is the number of pixels per inch (1 inch = 2.54 centimeters). The more pixels per inch, the more information there will be in the image. [6]

Figure1.1: the different resolution into an image.

1.3. Type of a digital image

1.3.1. The different color spaces

Color is an interesting data for an image. It modifies the perception that we have of the image, there are several modes to represent colors, the most used is space colorimetric red, green and blue RGB (RGB). In this mode, the different colors are obtained by mixing the three primary colors. This process is called additive synthesis. However, there are also other modes of representation, such as the CMYK (CMYB) mode which uses subtractive synthesis. The colors are obtained by mixing the three "primary" colors: Cyan (C), Magenta (M) and Yellow (Y), but this time with subtraction of the primary colors to get the other colors. Subtracting all the primary colors together gives the color black. [7]

There are possibly other modes of color representation:

- Hue, saturation, luminance (TSL or HSL), where the color is coded following the circle colors,
- YUV optimal color base, Y representing the luminance, U and V two orthogonal chrominance.

It should be noted that these different modes of color representation are created by the need to reproduce colors on different media, such as screens, paper, etc.

with efficiency and fidelity to the original or real image. For example, the RGB mode is only used in PC monitors to display images. It is not at all suitable for offset or digital printing.

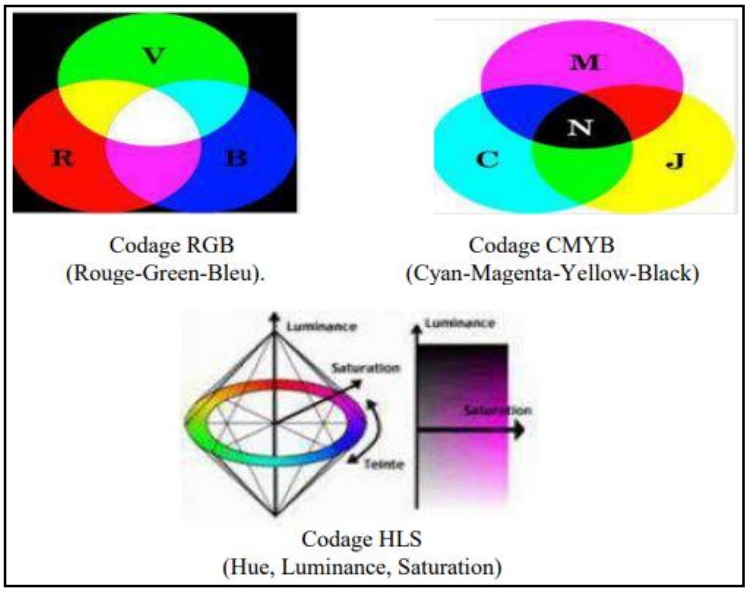


Figure1.2 :Components of RGB and CMYB and HLS color models.

1.3.2. grayscale

A grayscale image is represented on a single so-called monochrome channel; each pixel is coded on a byte of 256 possible values.

1.3.3. Color image

A color image corresponds to the additive synthesis of 3 images, red, green and blue (R, G, B). Each pixel is therefore coded on 3 × N bits.

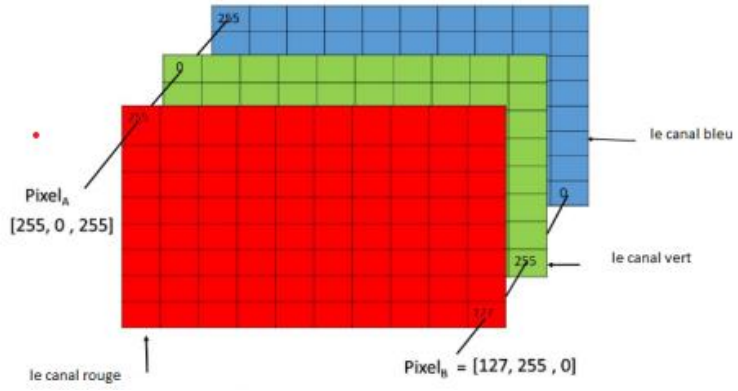


Figure1.3 :presentation of pixel color.

1.4 Rester format

A raster image can be represented in different ways. Among the main raster formats: Windows bitmap (BMP), Portable Network Graphics (PNG) and Joint Photographic Experts Group (JPEG).

1.4.1. BMP (bitmap)

The BMP file format, also known as bitmap image file, device independent bitmap (DIB) file format and bitmap are a raster graphics image file format used to store bitmap digital images two-dimensional both monochrome and color, in various color depths, and optionally with data compression, alpha channels, and color profiles. The Windows Metafile (WMF) specification covers the BMP file format.

1.4.2. PNG (Portable Network Graphic)

The PNG format is standardized by the W3C (World Wide Web Consortium). This proprietary format is also widely used on the web. It allows maximum optimization of the visual weight, because it uses an indexed color system. In addition, it is possible to use only specific color values. In addition, it allows 13 recording from 1 to 48 bits and also the management of transparency. [8]

1.4.3. JPEG (Joint Photographic Expert Group)

It designates a digital recording and compression format, imagined and developed by a group of experts in still image compression. It is in the field of digital photography that we are therefore most likely to encounter this format. It then takes the form of a .JPEG extension, also available in .jpeg, .JPG or .jpg.

JPEG is based on an algorithm that allows it to significantly reduce the volume of digital data and it is based on a compression and decompression process comprising six stages ranging from color transformation to decoding, via cutting / un buildable pixel blocks. [8]

1.4.4. GIF (Graphics Interchange Format)

Developed by CompuServe Inc. the .GIF format is based on the bitmap images used on the Web. This format is to be used for 8-bit images, with or without transparency, highly compressed to reduce file transfer time. It supports images with 256 colors or less.GIF format allows you to store multiple bitmap images in a single file. When several images are displayed in rapid succession, it is an animated GIF file: GIF 89 [9] [10].

1.4.5. TIFF (Tagged Image File Format)

It is an uncompressed image format that can be compressed. It is designed to be a standard; it is completely customizable. There are several variations of this format. It allows the black and white, grayscale and color. TIFF images can be 1, 4, 8 or 24 bits

per pixel. TIFF files can store color mode information RGB, CMYK and Lab, True Colors [10].

1.5. Conclusion

In this chapter we have introduced the different concepts concerning digital images and have become familiar with its characteristics and types.

To protect these types of images, we use digital watermarking techniques that we'll talk about more about in the next chapter

CHAPTER 2

DIGITAL WATERMARKING

Introduction

This chapter presents a state of the art on digital watermarking methods. We start by introducing the digital watermarking technique or (watermarking), these constraints, the different concepts and techniques used, as well as the different fields of application.

2.1. Definition

The basic idea of a digital watermark is to hide information in a document by adding additional information to a digital document called a media or medium that includes programming, images, audio and video, and the message (called mark or signature) embedded in this medium, this signature can be a series of bits, Letter, binary logo Digital watermarks are undetectable by the naked eye but act as beacons when copyrighted material is downloaded or reproduced. [11]

There are generally two classes of watermarks: visible and invisible

2.2. Watermarking process

A watermarking system is composed of two main phases: the insertion (Embedding) phase, and the extraction phase.

Any watermarking system takes the form given in the following figure:

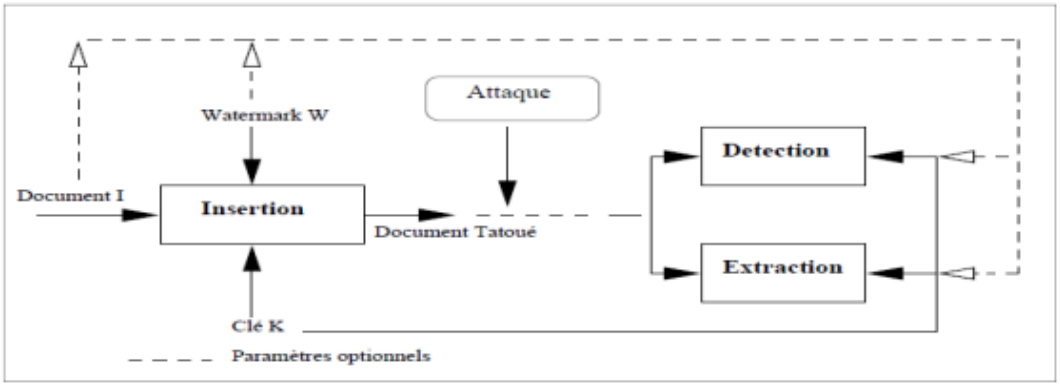


Figure 2.1:watermarking process.

2.2.1. Insertion phase

The inputs of the watermark insertion are the mark, the original data.

The mark can be a string of numbers, a series of binary bits, or image.

The key is used to improve the security of the watermark system.

The output of the insertion process is watermarked data, and there are two ways to insert the mark: substitutive and additive methods.

- **Substitutive methods**

It is a watermark insertion mechanism consists of modifying bits of the original medium in order to make them correspond to the watermark to be inserted [5]

- **Additive methods**

mainly consist in adding the mark to the support. It is the most used mechanism that can be done on the image in the spatial domain or frequency [5]

$$It = I0 + w \quad (1.1)$$

Where ***Io*** represents the original document and **w** marks it to insert it into the watermarked document, ***It*** represents the watermarked document.

2.1.2. Extraction phase

This is the phase which makes it possible to verify that the extracted mark is indeed the original one, there are three diagrams:

- **Blind extraction**

This is the mark extraction technique that just requires the object to be analyzed and the key.

- **Non-Blind Extraction**

It is the extraction technique that requires the original object to extract the mark. It is more robust than blind extraction but it is less used because it requires the original object.

- **Semi-Blind Extraction**

it does not require an original object for extraction but we need input some information of data (for example: length of message).

2.3. Requirements of digital watermarking systems

To design a high-performance watermarking algorithm, must respect a few essential factors.

these factors are: imperceptibility, robustness, and capacity. These factors are represented schematically in the following figure:

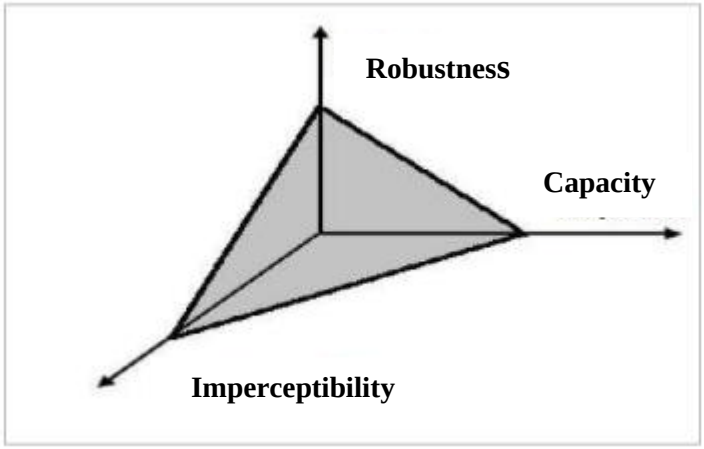


Figure 2.2:Trade-off among the imperceptibility, robustness and capacity

2.3.1. Capacity

Means the amount of information or mark that can be inserted into the image, the larger the size of the mark, the greater the degradation.

2.3.2. Imperceptibility

Imperceptibility or fidelity is perceptual similarity between the original and the watermarked versions of the cover work. The digital watermark should not affect the quality of the original image after it is watermarked. [2]

2.3.3. Robustness

It is the ability of a watermarking algorithm to resist external attacks, voluntary or not, for example compression, filtering, noise, cuts... ect. using widely available software. These modifications then entail a risk of deterioration of the watermark. [5]

2.4. Watermarking Classification:

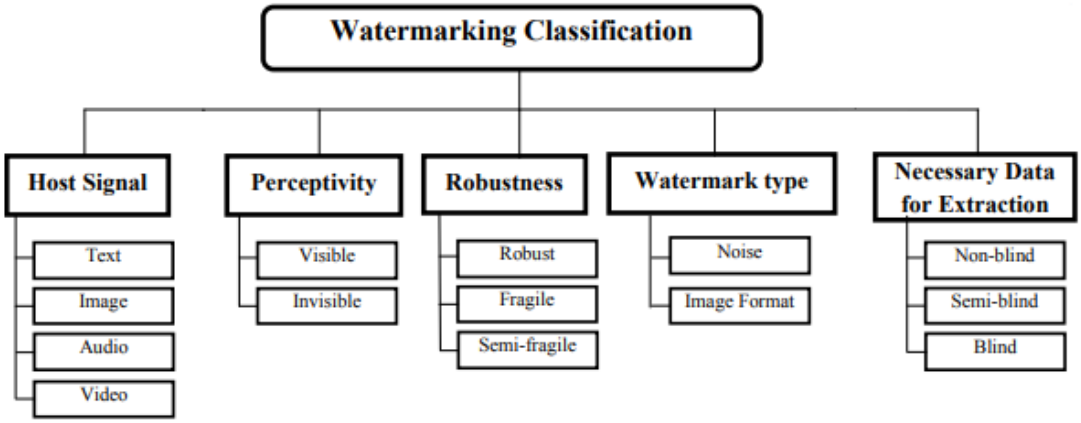


Figure 2.3:Classification of watermarking.

2.4.1. According to perceptivity

Digital watermarking is divided into two main categories: visible and invisible.

- **Visible watermark:** Or the mark will be clearly visible, for example adding a picture to mark another.
- **Invisible watermarking:** It is used to identify copyright data, like author, distributor, and so forth but it's more complex.

2.4.2. According to robustness

- **Robust:** resist various attacks, geometrical or non-geometrical without affecting embedded watermark. [2]
- **Fragile:** fragile watermark is designed to be easily destroyed if a watermarked image is manipulated in the slightest manner. This watermarking method be used for the protection and the verification of original contents**.** [2]
- **Semi-Fragile:** is capable of tolerating some degree of the change to a watermarked image, such as the addition of quantization noise from lossy compression. [2]

2.5. Application of watermarking

Digital Watermarks useful in many applications, including:

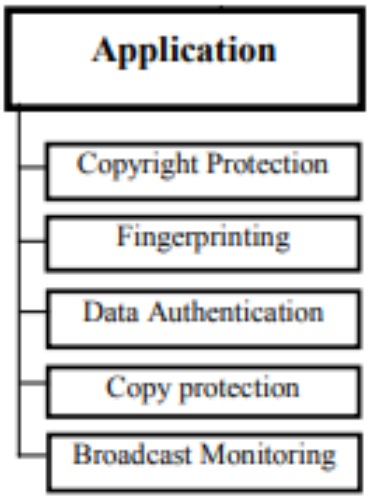


Figure2.4:Application of watermarking.

2.5.1. Copyright Protection

Copyright protection was one of the first applications of watermarking. In the event of a legal dispute, the owner of an image is able to prove that he is the owner even if it has suffered damage (attacks). Such an application must ensure great robustness against attacks. The robustness of the mark is in this case required in order to protect the mark against any attempt to erase it (destructive attack), to make its detection fail (geometric attack) or to create an ambiguity in the decision (protocol attack). [12]

2.5.2. Data authentication

The basic idea of this application is to insert a fragile mark in an image which serves to alert the user to possible modification of the image by an unauthorized person and to precisely locate the manipulated regions. This application is generally used in the legal and medical field.

2.5.3. Audience Monitoring

This is a new application where the hidden information is the name of the channel in the soundtrack of TV channels. The panelists have a device placed on the TV which picks up the ambient sound in the room, decodes the watermark and sends the name of the channel watched by the family via the Internet. They can measure audience and live market share [5]

2.5.4. Broadcast control

You can insert a mark in an advertisement, in order to ensure that certain advertisements have actually been broadcast. [5]

2.5.5. Image fingerprint

Associating unique information about each distributed copy of digital content is called fingerprinting, and watermarking is an appropriate solution for that application because it is invisible and inseparable from the content. This type of application is useful for monitoring or tracing illegally produced copies of digital work. [13]

2.5.6. Copy Protection:

Digital data can be duplicated without suffering any deterioration in quality. In this context, if a person holds a digital document and if he is malicious, he can illegally produce an unlimited number of copies of this document with a quality equal to the original document. Watermarking can cope with this situation. Information relating to the number of authorized copies is encrypted in the mark. This principle has been used in videos where the mark indicates whether the video can be copied or not. [12]

2.6. Conclusion

In this chapter, we have presented the elementary notions related to the digital watermarking domain. We have explained the insertion and extraction phases as well as the constraints of digital watermarking systems, we have also detailed the application domains of watermarking.

CHAPTER 3

DIGITAL IMAGE WATERMARKING

Introduction

In order to provide more watermarks and reduce the distortion of the watermarked image, a new technique is introduced using spatial and frequency domains. In this chapter, we explain the concept of spatial and frequency domain by mentioning some techniques for both.

3.1. Insertion Domain:

The common watermarking techniques described can be grouped according to their domains of insertion into two classes, techniques working in the spatial and the frequency domain.

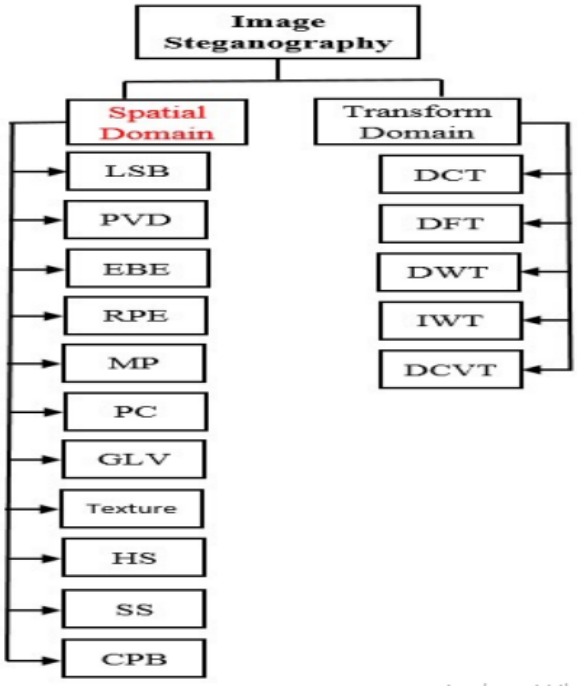


Figure 2.5:Classification of image steganography techniques.

3.2. Spatial domain technique

Consists of directly modifying the pixel values of the image as no initial processing is required.

Spatial domain watermarking schemes are simple and inexpensive in computation time. They also offer a regulation between robustness, capacity and imperceptibility.

Their downside is that they are not robust against image processing attacks, so the watermark can be destroyed easily. [14]

3.1.1. Least Significant Bit (LSB):

Least Significant Bit is one of most common and easiest technique used in steganography. In this technique, secret bits are hiding within the least significant bits of cover image pixels. Hiding in least significant bit ensures less change in the image pixels value. This technique is generally called LSB substitution [15]

3.1.2. Pixel value differencing (PVD):

In this technique, two sequential pixels are chosen in order to hiding secret data. Payload capacity of hiding data is determined by checking the difference among two sequential pixels, this is used to distinguish whether the two pixels belongs to an edge area or smooth area [16]

3.1.3. Random pixel embedding method (RPE):

In this method, the secret data is embedded randomly to increase the security inside image pixels. Random pixel is generated by using Fibonacci algorithm. [17]

3.3. Frequency Domain technique

Frequency domain transfers an image to its frequency representation and the image is segmented into multiple frequency bands. The embedded watermark in the frequency domain of a signal can provide more robustness than spatial domain. It is strong against attacks like compression, cropping where spatial domain is not. Several reversible transforms like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) can be used. Each of these transforms has its own characteristics and represents the image in different ways. [18]

3.3.1. Discrete Fourier Transform (DFT)

It's alteration invariant and revolution strong, which interprets to powerful robustness to geometric assaults. DFT uses difficult numbers, whilst DCT uses just real numbers. In DFT, low frequency coefficients amendment can reason seen artifacts within the spatial domain, so low frequency coefficients should be evaded. The best way to avoid the both lower and higher frequencies weakness is to embed the watermark in the midlevel frequency. [19]

The DFT (discrete Fourier transform), of image I (x, y) size M * N with f (x, y) means spatial image and f (u, v) image in the frequency domain is given as follows:

$$F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) e^{-j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (3.1)$$

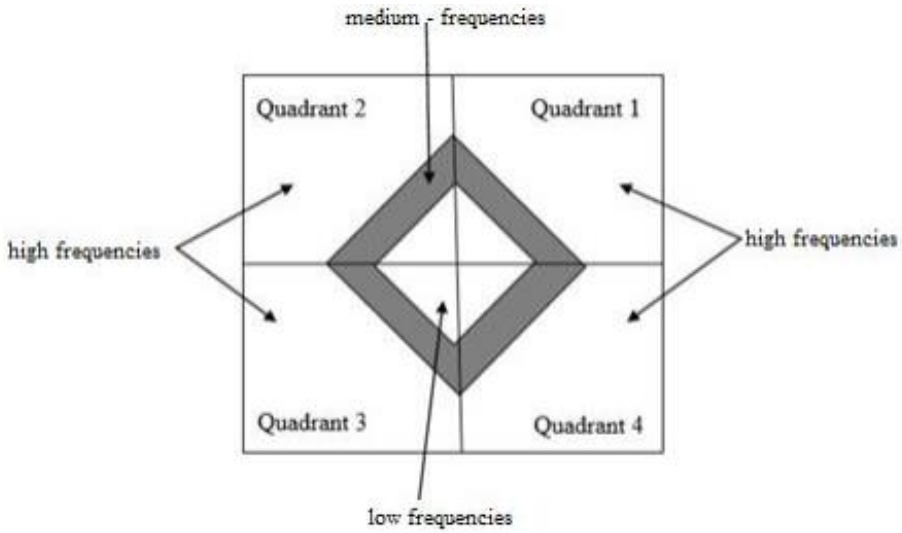


Figure 3.1:Frequency distribution of the modulus coefficients of a DFT.

The inverse transformation is given by:

$$f(x,y) = \frac{1}{M \times N} \sum_{u=0}^{M-1} \sum_{v=0}^{N-1} F(u,v) e^{j2\pi(\frac{ux}{M}+\frac{vy}{N})} \quad (3.2)$$

3.3.2. Discrete Cosine Transform (DCT)

The DCT is an invertible linear function or equivalently an invertible N*N square matrix. The DCT, and in particular the DCT-2, is widely used in signal and image processing, and especially in compression. DCT has an excellent energy aggregation property: the information is essentially carried by the low frequency coefficients. [20]

The low frequencies are located at the top left of the matrix, and the high frequencies at the bottom right. This transformation is often calculated on blocks of the image of size 8x8, i.e. 64 coefficients. These coefficients are distributed over three zones: low, medium and high frequencies

[21].

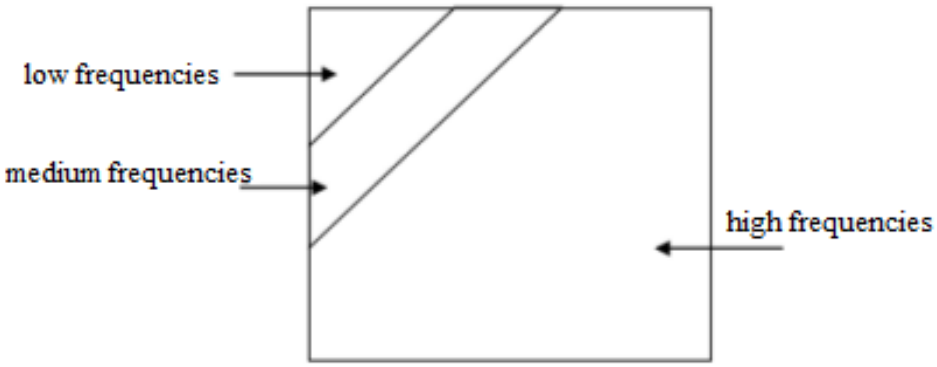


Figure 3.2: distribution of frequencies in a DCT block.

The DCT transform is calculated as follows:

$$C(u,v) = c(u)c(v)\frac{2}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j)\cos\left(\frac{\pi}{N}u\left(i+\frac{1}{2}\right)\right)\cos\left(\frac{\pi}{N}v\left(j+\frac{1}{2}\right)\right) \quad (3.3)$$

$$C(x) = \begin{cases} 2^{\frac{-1}{2}} & \text{si } x = 0 \\ 1 & \text{si } x > 1 \end{cases} \quad (3.4)$$

The inverse DCT transform is calculated as follows:

$$I(i,j) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} c(u)c(v)C(u,v)\cos\left(\frac{\pi}{N}u\left(i+\frac{1}{2}\right)\right)\cos\left(\frac{\pi}{N}v\left(j+\frac{1}{2}\right)\right) \quad (3.5)$$

DCT based watermarking techniques are more robust compared to simple spatial domain watermarking techniques

3.3.3. Discrete Wavelet Transform (DWT)

A discrete wavelet transform (DWT) is any wavelet transform where the wavelets are sampled discretely.

The wavelet transform uses filters to transform the image, a key advantage that it has over the DWT. The wavelet transform uses filters to transform the image, a key advantage it has over Fourier transforms is temporal resolution: it captures both the frequency and time information. This formulation is based on the use of a time-divisional model of the image. This formulation is based on the use of recurrence relations to generate This formulation is based on the use of recurrence relations to

generate increasingly fine discrete samples of an implicit wavelet function in this case, each resolution is twice the previous scale. [5]

The discrete wavelet transform has a wide range of applications in science, engineering, mathematics and computer science. In particular, it is used for the coding of in particular, it is used for signal coding, to represent a discrete signal in a more redundant form, often as a precondition for the In particular, it is used in signal coding, to represent a discrete signal in a more redundant form, often as a prerequisite for data compression. [5]

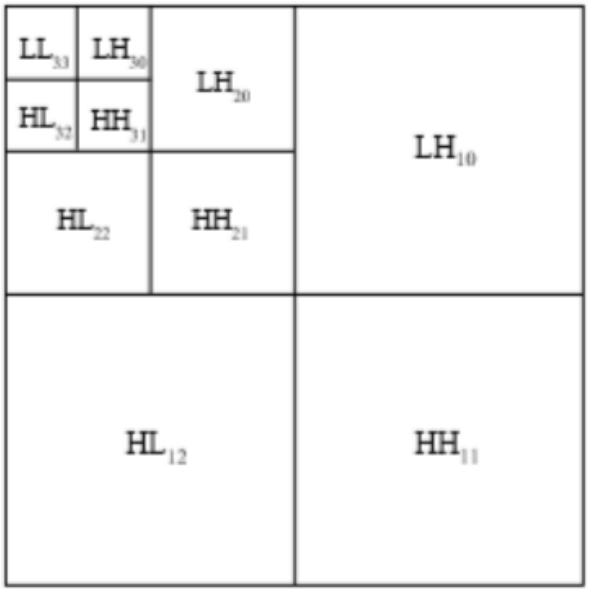


Figure 3.4:wavelet image composition.

The approximation image (LL) is a reduced and smoothed version of the initial image while the horizontal (LH), vertical (HL) and diagonal (HH) detail images contain only local texture and contour information of the image regions, at a given resolution and along a given direction.

3.4. Attacks and Robustness

A watermark method can be fragile or robust, robustness is the ability of a method to resist against attacks of alteration or destruction of the watermark. We can classify attacks into two categories, unintentional and intentional.

Unintentional attacks can happen due to innocent action such as downsizing of an image. Intentional attacks are meant to destroy the tattoo for falsification or theft of property rights, in this section we will explain some attacks.

3.4.1. Filtering

Filtering is an image processing technique that consists of scanning the image through a finite analysis window. It is used mainly to improve its appearance. For example, to make an image softer by a smoothing operation or to remove a noise (the mark) present in the image. [22]

3.4.2. Compression

The large size of a digital image poses major problems for transmission or storage.

Compression is a technique that removes redundant information from images in order to reduce the size of the image file. As the watermark is invisible, it can therefore be considered as insignificant and therefore also be removed.

3.4.3. Rotation

Rotation is one of the geometrical attacks that can prevent watermarking detection. If the mark is inserted in the spatial domain, it will undergo the same transformations as the image. Small rotation angles can make the watermark undetectable. In particular, when blind extraction is imposed. Extraction in blind mode.

3.4.4. Noise

The objective of this attack is to get as close as possible to the waveform of the watermark to be able to remove it. The watermark can be estimated using specific filters. The general idea is to estimate the brand from the tattooed image is the filtered image. [23]

3.5. Evaluation metrics for watermarking algorithms

3.5.1. Mean Squared Error (MSE)

The degraded image I' is always compared to the original I to determine its similarity ratio [25]. This criterion is the most widely used. It is based on the measurement of it is based on the measurement of the mean square error (MSE) calculated between the original and processed pixels:

$$MSE = \frac{1}{M \times N} \sum_{m=1}^{M} \sum_{n=1}^{N} (I(m,n) - I'(m,n))^2 \quad (3.6)$$

Where (M Ö N) is the size of the image, and I*p* and I'*p* are respectively the amplitudes of the pixels in the original and degraded images. It is likely that the eye It is likely that the eye takes much more account of errors with large amplitudes, which favors the quadratic measurement. [24]

3.5.2. Peak Signal to Noise Ratio (PSNR)

PSNR (Peak Signal to Noise Ratio) 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 Peak Signal to Noise Ratio. [25]

$$PSNR = 10\log_{10}\left(\frac{{I_{max}}^2}{MSE}\right) \quad (3.7)$$

Where p= maximum value in host image. Imperceptibility of image is determined by this factor. More the PSNR shows that Watermarked image is perceptible or watermark is not recognized by naked eyes.

3.5.3. Structural Similarity Index Measure (SSIM)

Is a measure of similarity between two digital images, it was developed to measure the visual quality of a deformed image, compared to the original image [26], The measure between two windows x and y is given by the following formula:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\varphi_{xy} + c_2)}{({\mu_x}^2 + {\mu_y}^2 + c_1)({\varphi_x}^2 + {\varphi_y}^2 + c_2)} \quad (3.8)$$

μ and ϕ are respectively the mean and the variance of the window, c1, c2 two variables destined to stabilize the division when the enumerator is very small.

3.5.4. Number of Pixel Change Rate (NPCR)

NPCR means the change rate of the number of pixels of the cipher image when only one pixel of the plain image is modified. NPCR ∈ [0,1] [27].

NPCR = 0 means no change.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (3.9)$$

W and H the dimensions of the image with:

$$D(i,j) = \begin{cases} 0 & If \quad (C_1(i,j) = C_2(i,j)) \\ 1 & If \quad (C_1(i,j) \neq C_2(i,j) \end{cases} \tag{3.10}$$

C1 and C2 are the original image and the ciphered image.

3.5.5. Unified Average Changing Intensity (UACI)

The unified average changing intensity (UACI) measures the average intensity of differences between the plain image and ciphered image [27].

$$UACI = \frac{1}{W \times H}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100 \tag{3.11}$$

C1 and C2 are the original image and the ciphered image.

3.5. Conclusion

In this chapter, we have introduced the initial concepts related to digital watermarking domains, using spatial and frequency domains and mentioned some techniques for both. and metrics that allow us to evaluate watermarking algorithms.

CHAPTER 4

CONCEPTION ANDIMPLEMENTATION

Introduction

In this chapter we present the design and implementation of our digital watermarking application. We present in detail the techniques and tools used in our work. In addition to the functions performed by this application, an experimental study is then carried out to evaluate the performance of our watermarking algorithm.

4.1. Tools used

In order to realize our digital watermarking application, we used the python programming language and the QT designer application for the graphical interface.

4.1.1. Python

Python is a widely used general-purpose, high-level programming language. It was initially designed by Guido van Rossum in 1991 and developed by Python Software Foundation. It was mainly developed for emphasis on code readability, and its syntax allows programmers to express concepts in fewer lines of code. [28]

figure 4.1.:python logo.

4.1.2. QT

Qt is a widget toolkit for creating graphical user interfaces as well as cross-platform applications that run on various software and hardware platforms such as Linux, Windows, macOS, Android. Qt supports various compilers including GCC C++ compiler and Jupyter Notebook. [5]

figure 4.2:Qt logo.

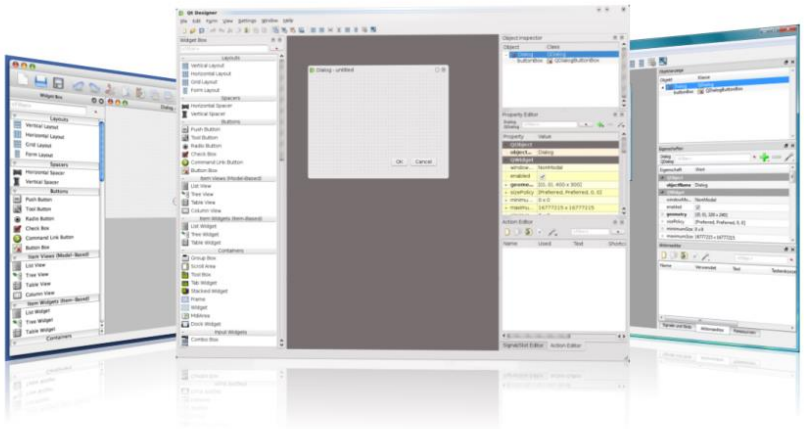


figure 4.3: Qt environment.

4.1.3. Jupyter

Jupyter is an integrated development environment (IDE) for Windows, Linux and macOS. It includes all the features of a modern IDE and supports over 40 programming languages, including Python, Julia, Ruby, R, and Scala2. It is a community project whose goal is to develop free software, open formats and services for interactive computing. Jupyter is an evolution of the IPython project. Jupyter allows the creation of notebooks, i.e. programs containing both markdown text and code. These notebooks are used in data science to explore and analyse data.

Figure 4.4:jupyter logo.

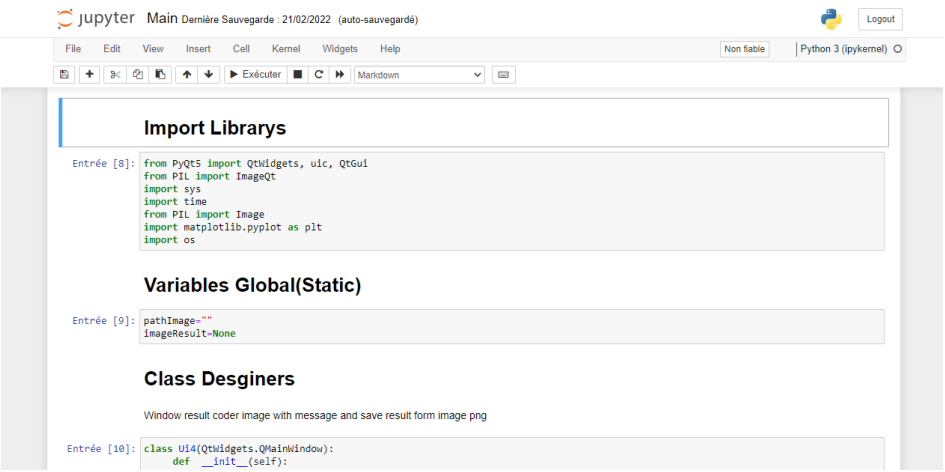


Figure 4.5:jupyter environment.

4.1.4. OpenCV

OpenCV (for Open Computer Vision) is a free graphics library, initially developed by Intel, specialized in image processing. OpenCV provides many features. OpenCV provides many diversified functionalities allowing to create programs starting from the data. programs from raw data to the creation of basic graphical interfaces.

4.2. Method used

We used a spatial domain LSB (least significant bit) method on the images. This method is a type of coding to increase the steganography and secrecy of data in telemedicine exchanges. In this process, one byte of the secret message is hidden in pixels with a single change of N bits. In this paper, we experiment with three versions of the revisited LSB matching approach after working with two, three bits.

- **The objective of using the LSB method:**

  - ✓ Method based on the least significant bit.
  - ✓ Simple to implement.
  - ✓ Does not change the size of the image.
  - ✓ Modifications invisible to the naked eye.

4.2.1. Presentation of method

The idea of our approach is to hide the message using a specific coding, the message will be hidden in the blocks of a color channel of the host image and grayscale image(monochrom), this coding is used to improve the security and robustness of our algorithm.

the proposed scheme contains two phases insertion and extraction of the message of this method.

4.2.1.1. Insertion algorithm

First of all, we choose the secret message that we want to hide and it is converted into binary system as shown in the figure below:

```
['01101101', '01100001', '01110010', '01101111', '01110101', '011
00001', '00100000', '01100010', '01100101', '01110010', '01110010
', '01100001', '01100011', '01101000', '01100101', '01100100', '0
0001010', '00110010', '00110000', '00110010', '00110010', '001011
11', '00110000', '00110101', '00101111', '00110001', '00110101',
'00001010', '01101100', '00100111', '01101000', '01101111', '0111
0000', '01101001', '01110100', '01100001', '01101100', '00100000'
, '01100010', '01101111', '01110101', '01100100', '01101001', '01
100001', '01100110', '00001010']
```

Figure 4.6 :a list of binary data.

- **Insertion watermark organigram:**

  The proposed scheme contains the steps to insert a watermark in a color image (RGB) and a grayscale image (monochrome) with the same data, so that the latter obtains an image with watermark.

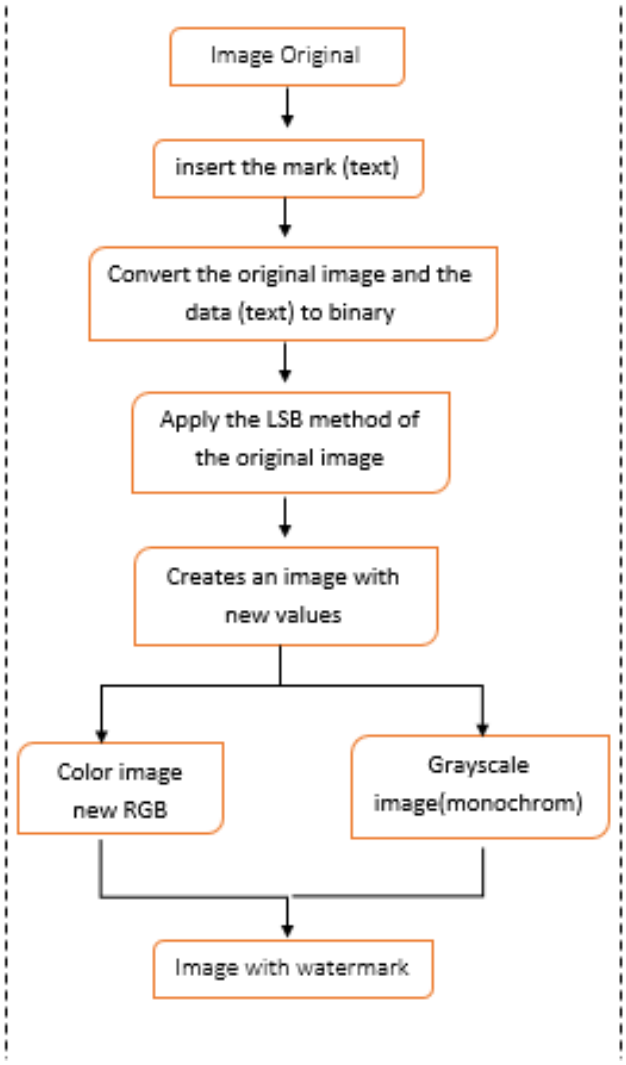


Figure 4.7 :insertion watermark organigram.

The algorithm of the proposed technique proceeds as follows:

1. Read host image and message.

2. First of all, we check if the image is a color image or a grayscale, so that the insertion process would be done in the RGB or the pixel
   - If a color image:
     - Transform the values of the matrix R G B in 8bit binary
     - The first RGB values are used to store length of data in 16 bits
   - If a grayscale image:
     - Transform the pixel's values of the matrix in 8bit binary
     - The first two pixel's values are used to store length of data in 16 bits.
3. First each character in the data the ASCII value is converted into an 8bit binary.
4. Then, the value (RGB or pixels) and the corresponding binary data are compared.

   If the first bit of the first character

   if the bit data is 1 and LB is 0 then

   LB → 1

   else

   if the bit data is 1 and LB is 1 then

   LB → 1

   else LB → 0

   the last bit will be replaced according to the substitutive method.

5. Repeat this process until all data is watermarked into the image.
6. finally show and save the new watermarking image.

4.2.1.2. Extraction algorithm

- **Extraction watermark organigram:**

  The proposed scheme contains the steps of the reverse phase (watermark extraction) applied to two types of images as mentioned before to obtain the watermark .

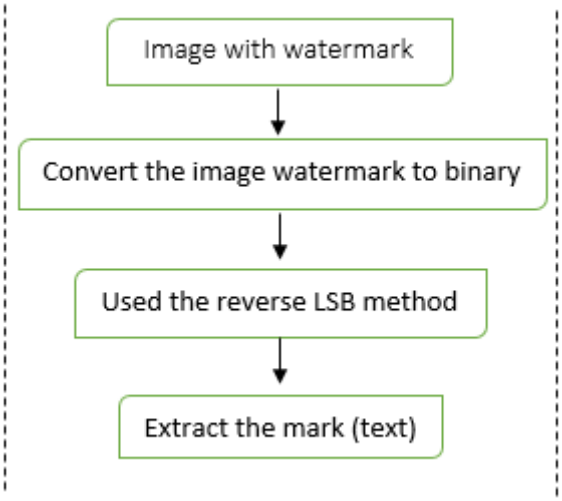


Figure 4.8 :extraction watermark organigram.

The extraction of the mark is done without recourse to the original image.

1. Read the watermarking image.
2. Again, the pixels are read at a time. The first (RGB in color image or pixel in grayscal image) values give us information about the secret data.
3. After converting the pixel values to binary (RGB or pixel), we extract the value of the last bit of each channel.
4. The bits are concatenated to a string, every block of pixels we get a byte of secret data, which means one character.
5. Now, if the Last value is even then we keep reading another block of pixels at a time, or otherwise, we stop.
6. finally, Extraction and save the watermark

4.3. Presentation of the realized application

Graphic interface

Part (01):

when you open the application, this interface will appear containing a Start button, when you press the Start button, we will move to the interface (02).

4.9:The first graphic interface of the application.

Part (02):

The Main interface of our application, which contains three buttons (the insert watermark button, the extract watermark button, and the return to the first destination button).

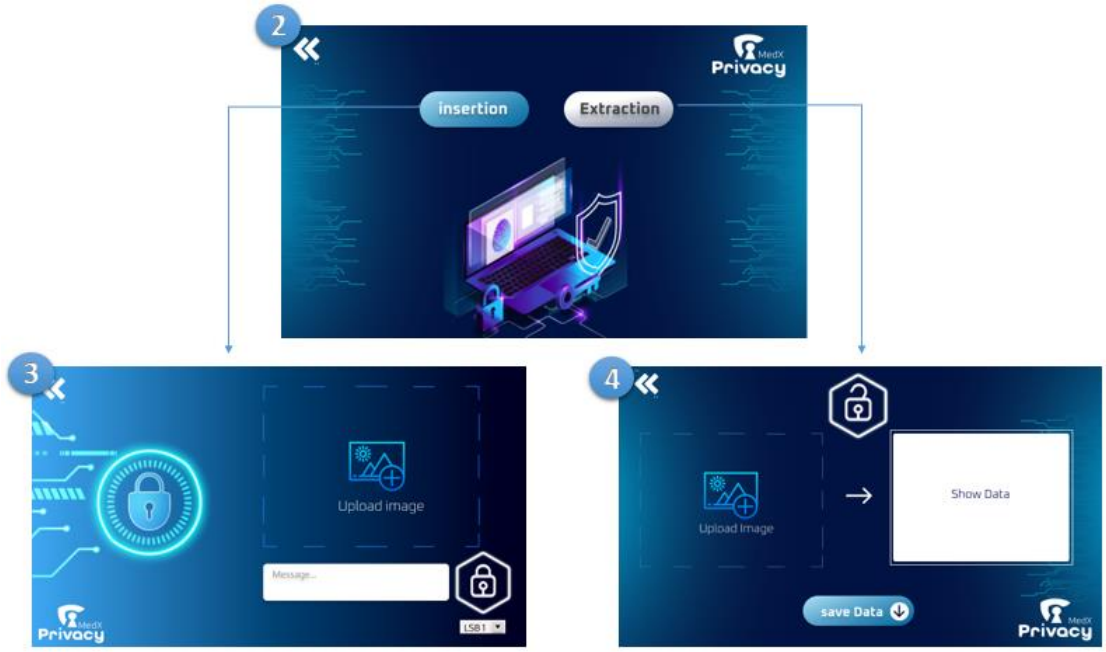


Figure 4.10 :The main graphical interface of our application.

Part (03):

Watermarking insertion process:

which contains four buttons (the upload original image, the insert watermark text, LSB button (check boxes) to choose any LSB to hide secret data in, and the return to the first destination button). When the insertion process is completed, we will go directly to an

interface that displays the original image and the image with the watermark, and a button that allows us to download the new image.

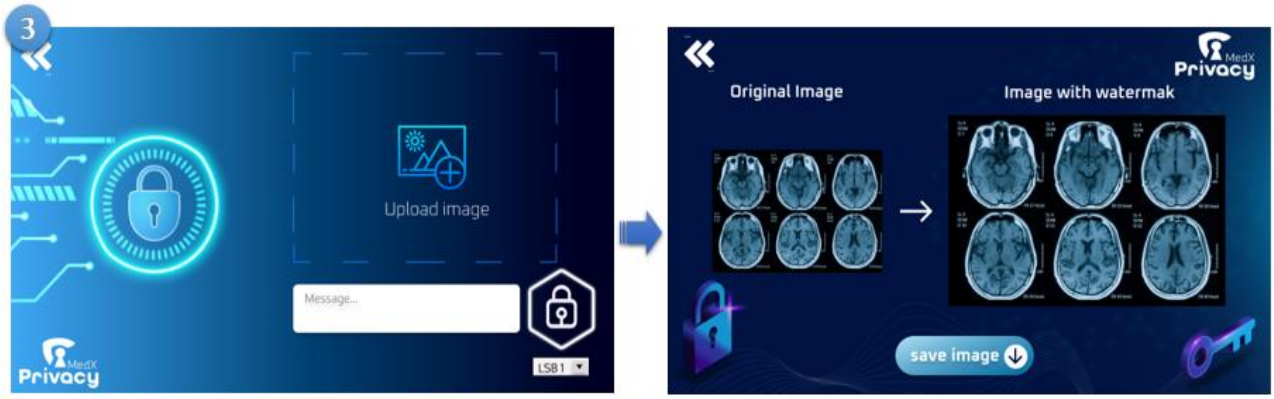


Figure 4.11:Graphical interface of the watermarking insertion process.

Part (04):

Watermarking extraction process:

When we click on the extract the watermark button, this interface (04) will appear to us, which contains a place to download the image with the watermark, a box to extract the text of the watermark, a button to perform the extraction process, and a button that allows us to download the extracted data.

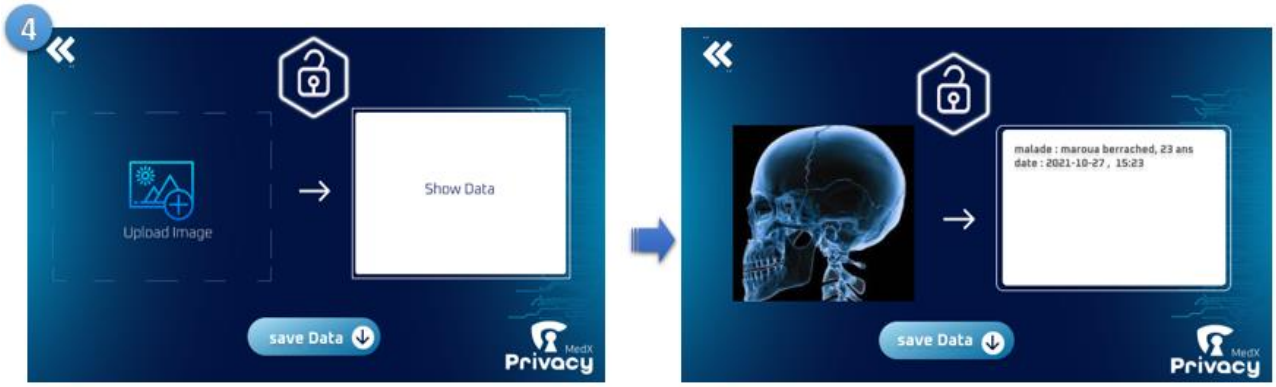


Figure 4.12:Graphical interface of the watermarking extraction process.

4.4. Obtained result

In this section, we evaluate the performance of our method in terms of imperceptibility, capacity and robustness. The experimental results are separated into three parts: the first is devoted to testing the property of imperceptibility while the second is devoted to the

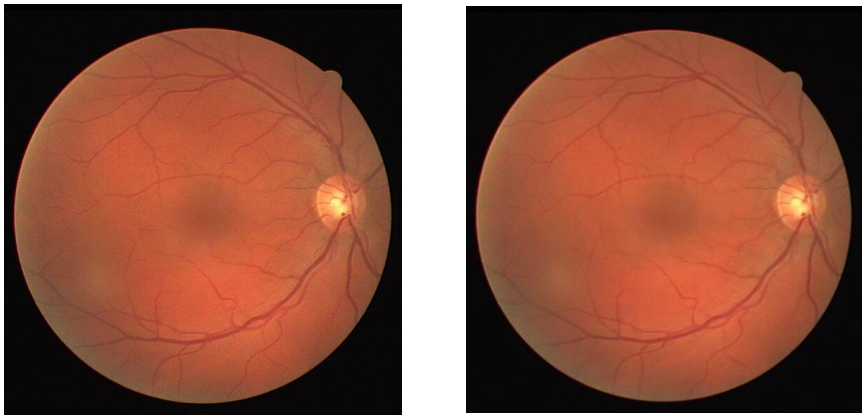
analysis of the robustness against some standard and more interesting types of attacks, and the third part shows the insertion capacity of our algorithm.

4.4.1. Imperceptibility property:

In order to test the imperceptibility property of our watermarking method, several RGB color images and grayscals images of different sizes are watermarked with a same text. A host image and the watermarked image are shown above:

Color image (RGB):

Original Image (01): watermarking Image (01):



(01) (1.1)

Figure 4.13 :Comparison between color images.

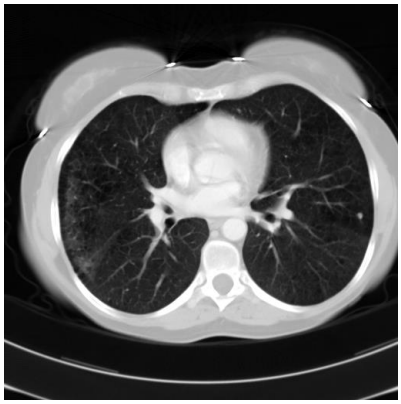
PSNR and SSIM:

Table 4.1: Measurements of the quality of watermarked color image.

IMAGE (01)	PSNR	SSIM
LSB(01)	**80.23**	**0.9999**
LSB (02)	**74.26**	**0.9999**
LSB (03)	**68.06**	**0.9998**

Grayscals image:

Original Image (02): watermarking Image (02):



(02) (2.1)

Figure 4.14 :Comparison between Grayscals image.

Table 4.2: Measurements of the quality of watermarked grayscal image.

IMAGE (02)	PSNR	SSIM
LSB(01)	**78.43**	**0.9999**
LSB (02)	**72.79**	**0.9998**
LSB (03)	**66.39**	**0.9998**

From the images we can see that it is difficult to differentiate between the original image and the watermarked image. To concretely evaluate the quality of our method, we use some m evaluation etrics among those previously explained (PSNR, SSIM).

- **PSNR:** we evaluate the performance of our method by experimenting with three methods: the first is for the last bit, then the last two bit, the last three bits, where we noticed that the closer we get to the most important bit, the PSNR gradually decreases, which indicates the increasing differences between the original image and the image with the watermark, which makes it gradually lose its quality.
- **SSIM**: Structural similarity (SSIM) was defined from what was previously reported as equation (3.7), SSIM has values between "0" and "1". Similar images have SSIM values closer to "1".

This means that the SSIM results we obtained are very good and the closer we get to the most important bit, the SSIM gradually decreases (the similarity between the images decreases).

4.4.2. Capacity

Regarding the capacity, when applying LSBs by the substitution method, it is necessary to preserve the capacity of the image after entering the watermark.

From what was previously mentioned about capacity, this means the amount of information or mark that can be included in the image, so we calculated the number of bits that can be included on the color and gray images in each of LSB 1, LSB 2 And LSB 3, we got the results shown in the table below:

the weight of (LSB1 =1/8, LSB2=2/8, LSB3=3/8).

Color image size: 565*584

LSB 1: ((565*584) *3) *1

LSB 2: ((565*584) *3) *2

LSB3: ((565*584) *3) *3

Grayscals image size: 512*512

LSB 1: (512*512) *1

LSB 2: (512*512) *2

LSB 3: (512*512) *3

Table 4.3: comparison of the two type images in terms of capacity.

CAPACITY	COLOR IMAGE	GRAYSCALS IMAGE
LSB (01)	**989 880**	**262144**
LSB (02)	**1979 760**	**524 288**
LSB (03)	**2969 640**	**786 432**

Among the results we get is concluded: The more we go to the important bits he more bits we can insert into the image (that is the capacity of the LSB increases).

4.5. Conclusion:

In this chapter, we presented the tools and method used to develop our application, then we explained the insertion phase and the extraction phase of our algorithm, lastly, we have shown the results obtained in terms of watermarking constrain.

GENERAL CONCLUSION

Digital watermarking has been implemented as an interesting technique for protecting the exchange of medical data on the Internet: integrity, confidentiality and authentication. Our goal is to check the three security properties together, in this case the watermark must meet a criterion: non-perception to ensure authentication and protect images.

During this thesis we examined the problem related to digital watermarking of images, as well as the idea of a digital image. We introduced a watermarking method that ensures the integrity of images. Our work focused on developing a technology for watermarking color and grayscale images. This work takes into account the blind detection of the watermark and the good compatibility between the visual quality of the watermark images and the robustness against known attacks. The watermark is entered into the spatial domain; this is done by applying the lsb method.

The continuation of our work aimed first to evaluate our method using evaluation metrics, which gave very good results showing the imperceptibility and that our approach allows to obtain a high quality of watermarked images.

The perspectives opened by our work can be summarized in the following points:

1. Encrypt the message or the mark before hiding it in the document to increase the security of the layer.

2.the proposed algorithm can be applied on other media such as video or sound.

REFERENCES

[1] Imane Assini, Laboratoire d'Electronique, Electrotechnique, Automatique & Traitement de l'Information -FST Mohammedia – Université Hassan II Casablanca - Conference Paper , June 2015.

https://www.researchgate.net/publication/309673966_TATOUAGE_D%27IMAGES_NUMERIQUES_PAR_CODAGE_APPLICATION_A_L%27IMAGERIE_MEDICALE

[2] Mohamed A. Belal Professor, Computer Science Dept., Faculty of Computers & Information, Helwan Univ., Cairo, Egypt,September – 2012.

[3] Baxes, Gregory H. "Digital Image Processing: Principles and Applications". New York: John Wiley and Sons, 1994.

[4] Wikip´edia, "Image num´erique — wikip´edia, l'encyclopedie libre," 2020, [En ligne; Page disponible le 8-janvier-2020].

[5] MARIF Oussama Benzid, "digital image watermarking JPEG," 2019.

[6] Y. NEDJAR and I. MOUSSI, "Application des methodes numeriques de traitement d'image sous android." Ph.D. dissertation.

[7] Application « des Ondelettes pour le Tatouage Numérique des Images »,dans UNIVERSITE FERHAT ABBAS DE SETIF - 01, 2015.

[8] M. Tkalcic and J. F. Tasic, "Colour spaces: perceptual, historical and applicational background". IEEE, 2003.

[9]http://www.eclairement.com/Image-numerique-quel format.2007.

[10] D. Lin grand. « Introduction au traitement d'images ». Vuibert, 2008.

[11] C. Rey, "Tatouage d'image: gain en robustesse et intégrité des images." Avignon, 2003.

[12] « Tatouage d'images par la décomposition en valeurs singulières et la transformée en cosinus discrète », dans UNIVERSITE MOHAMED BOUDIAF - M'SILA,2017

[13] BOUGOFFA Hiba AL-Rahman BEZZIOU Maissa “ A spatial domain watermarking approach for Fingerprint security “2020.

[14] D. Battikh, “S´ecurite de l’information par steganographie basee sur les sequences chaotiques,” Ph.D. dissertation, Rennes, INSA, 2015.

[15] Dagar, Ekta, and Sunny Dagar. "LSB based image steganography using x-box mapping." Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on. IEEE, 2014.

[16] Zhang, Hao, Tao Zhang, and Huajin Chen. "Variance Analysis of Pixel-Value Differencing Steganography." Proceedings of the 2017 International Conference on Cryptography, Security and Privacy. ACM, 2017.

[17] MOHAMMED MAHDI HASHIM, MOHD SHAFRY MOHD RAHIM, ALI ABDULRAHEEM ALWAN ,Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia,UTM-IRDA Digital Media Center, Faculty of Computing, University Technology Malaysia, Johor Bahru, Malaysia 3Uruk University, Baghdad, Iraq -A “REVIEW AND OPEN ISSUES OF MULTIFARIOUS IMAGE STEGANOGRAPHY TECHNIQUES IN SPATIAL DOMAIN”.

[18] F. Y. Shih, Digital watermarking and steganography: “fundamentals and techniques”. CRC press, 2017.

[19] N. Ahmed, T. Natarajan, and K. R. Rao, “Discrete cosine transform,” IEEE transactions on Computers, 1974.

[20] D. Marshall, “Transformation de cosinus discrete,” 2001.

[21] L. Diane, “Cours de traitement d’images,” Laboratoire I3S Informatique, Signaux et Systemes, Universite de Nice Sophia Antipolice, Rapport de recherche ISRN I3S/RR, vol. 22, 2005.

[22] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: “Steganography and Watermarking-Attacks and Countermeasures Springer Science & Business Media”, 2001.

[23] L. K. Saini and V. Shrivastava, “A survey of digital watermarking techniques and its applications,” ,2014.

[24] Y. A. Al-Najjar, D. C. Soong et al., “Comparison of image quality assessment: Psnr, hvs, ssim, uiqi,” ,2012.

[25] Rossum, Guido Van “The History of Python: A Brief Timeline of Python",The History of Python. Retrieved 5 March 2021.

[26] Y. Wu, J. P. Noonan, S. Agaian et al. Cyber journals: multidisciplinary journals in science and technology, “Npcr and uaci randomness tests for image encryption,”

[27] https://www.geeksforgeeks.org/history-of-python/ ,17:26 ,05-04-2022.