République Algérienne Démocratique et Populaire

Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université de kasdi merbah ouargla

Faculté des Nouvelles Technologies de l'information et la Communication

Département de l'informatique et Technologies de l'information

Mémoire présente en vue de l'obtention du diplôme Master

Tatouage numérique des données biomédicales dans le domaine des transformée

Réalisé par :

Melouah Messaouda

Driche Imane

Encadré par :

Mr A. KHALDI

Mr F.Kahlessenane	Président	Univ ouargla
Mr A. KHALDI	Encadrant	Univ ouargla
Mr Salah Euschi	Examinateur	Univ ouargla

Année Universitaire 2022/2023

Remerciement

Avant tous, nous tenons à remercier Allah de pour nous avoir donné la santé, le courage, la patience et surtout la raison Pour réaliser ce modeste travail qui consiste en l'achèvement d'un mémoire de fin d'études à l'Université Kasdi Merbah de Ouargla.

Remerciements à :

Notre encadreur ,Monsieur **KHALDI AMINE** pour avoir dirigé ce travail, ainsi que pour sa supervision constante et efficace tout au long du développement de cette recherche , nous a beaucoup aidé avec ses idées, ses conseils .Nous remercions sincèrement les membres du jury pour l'honneur qu'ils nous ont accordé en approuvant notre travail et en l'évaluant, ainsi que tous nos professeurs du département d'informatique.

Un grand merci à notre famille et en particulier à celui dont je porte fièrement le nom Merci beaucoup, cher père. À mes anges dans la vie pour le sens de l'amour et de l'affection Merci beaucoup, ma chère mère.

Enfin, nous adressons nos remerciements les plus sincères à toutes les personnes qui de prés ou de loin nous ont aidé et soutenu pendant cette période .

Résumé

Le partage d'informations médicales en ligne peut être risqué car les gens pourraient essayer de les pirater. Même s'il existe des moyens de le protéger, ils ne suffisent pas toujours. Certains programmes informatiques peuvent aider à protéger les informations, mais ils ne sont pas toujours assez performants. Ainsi, une autre façon de le garder en sécurité consiste à ajouter une marque cachée aux images, appelée "watermark". Le tatouage numérique s'est imposé comme une solution complémentaire qui contribue à la sécurité des images partagées sur les réseaux. En effet, dans le domaine de l'imagerie médicales, le tatouage des données biomédicales représente une méthode importante pour protéger les données sensibles et privées et confidentielles face à diverses attaques pour maintenir son intégrité.

L'objectif de notre travail est de développer une méthode de tatouage des images médicales en y incorporant un marqueur invisible, et extraire cette marque de manière fiable. Nous nous sommes principalement concentrés sur deux aspects : la robustesse du tatouage et son imperceptibilité.

En effet, pour qu'un tatouage numérique soit efficace, il doit être suffisamment solide pour résister à diverses attaques et en même temps visuellement indétectable. De plus, il est important que le tatouage soit statistiquement invisible afin de ne pas dégrader l'image originale.

Mots clés : Tatouage numérique, Images médicales, sécurité des données, confidentialité, robustesse, imperceptibilité.

Abstract

Sharing medical information online can be risky as people may try to hack into it. Even though there are ways to protect it, they are not always sufficient. Some computer programs can help protect the information, but they are not always effective enough. Therefore, another way to keep it secure is by adding a hidden mark to the images, called a "watermark." Digital watermarking has emerged as a complementary solution that contributes to the security of shared images on networks. In the field of medical imaging, data watermarking represents an important method to protect sensitive, private, and confidential data from various attacks in order to maintain its integrity.

The objective of our work is to develop a method for watermarking medical images by incorporating an invisible marker and reliably extracting this mark. We primarily focused on two aspects : the robustness of the watermark and its imperceptibility. Indeed, for a digital watermark to be effective, it must be strong enough to withstand various attacks while remaining visually undetectable. Additionally, it is important for the watermark to be statistically invisible in order to not degrade the original image.

Key words : Digital watermarking, Medical images, data security, confidentiality, robustness, imperceptibility.

الملخص

قد تكون مشاركة المعلومات الطبية عبر الإنترنت محفوفة بالمخاطر حيث قد يحاول الناس اختراقها. في حين أن هناك طرقًا لحمايته، إلا أنها ليست كافية دائمًا. يمكن أن تساعد بعض برامج الكمبيوتر في حماية المعلومات، لكنها قد لا تكون دائمًا فعالة بما يكفي. لذلك، هناك طريقة أخرى للحفاظ عليها آمنة وهي إضافة علامة مخفية إلى الصور تسمى «العلامة المائية».

ظهرت العلامات المائية الرقمية كحل تكميلي يساهم في أمن الصور المشتركة على الشبكات. في مجال التصوير الطبي، يمثل وضع العلامات المائية على البيانات طريقة مهمة لحماية البيانات الحساسة والخاصة والسرية من مختلف الهجمات .من أجل الحفاظ على سلامتها

الهدف من عملنا هو تطوير طريقة لوضع علامات مائية على الصور الطبية من خلال دمج علامة غير مرئية واستخراج هذه العلامة بشكل موثوق. ركزنا بشكل أساسي على جانبين: متانة العلامات المائية وعدم محسوسيتها. في الواقع، لكي تكون العلامة المائية الرقمية فعالة، يجب أن تكون قوية بما يكفي لتحمل الهجمات المختلفة مع البقاء غير قابل للكشف بصريًا بالإضافة إلى ذلك، من المهم أن تكون العلامة المائية غير مرئية إحصائيًا حتى لا تتحلل الصورة الأصلية.

.**الكلمات الرئيسية:** العلامات المائية الرقمية، الصور الطبية، أمن البيانات، السرية، المتانة، عدم القدرة على التحمل.

Table des matières

Table des figures

Liste des tableaux

Introduction générale

Le domaine de l'Internet et des médias numériques connaît actuellement un développement considérable, ce qui permet la circulation de données numériques à grande échelle dans différents domaines, notamment l'enseignement et les soins de santé à distance, ainsi que de nombreux autres domaines.

L'importance de préserver la confidentialité, la sécurité et l'intégrité des images et des données médicales dans les applications d'enseignement médical et de soins de santé à distance réside dans la nécessité de les protéger contre les menaces et les violations électroniques qui pourraient entraîner la divulgation d'informations sensibles telles que les détails de traitement, de diagnostic et de tests médicaux, ainsi que d'autres informations personnelles.

Pour surmonter ces problèmes, plusieurs technologies sont utilisées pour assurer la sécurité et la vérification des données, notamment des technologies avancées telles que le tatouage numérique. Cette technologie est innovante et claire dans la garantie de la sécurité et de la confidentialité des informations médicales, ainsi que dans la fourniture d'une gestion précise et sécurisée des dossiers médicaux.

Dans ce mémoire, nous nous concentrerons principalement sur le tatouage des images médicales à l'aide de la transformée en ondelettes discrètes (DWT) et le chiffrement AES dans l'application du watermarking. Contrairement à la stéganographie où la capacité est considérée comme assez importante mais la qualité et la robustesse peuvent être compromises, cette méthode garantit une qualité et une robustesse accrues tout en offrant une capacité de stockage suffisante. Le but de ce mémoire est donc d'élaborer une méthode de tatouage d'images médicales numériques efficace pour répondre aux besoins de la télémédecine et de garantir la sécurité des données médicales échangées à travers les réseaux.

Dans le chapitre 1, nous présenterons un état de l'art sur les images numériques, en mettant l'accent sur leurs caractéristiques, formats et types.

Dans le chapitre 2, nous décrirons les différents éléments d'un système de tatouage numé-

rique, ainsi que les contraintes, les types et les domaines d'application de ces systèmes. Nous aborderons également les attaques potentielles sur les systèmes de tatouage et l'évaluation des algorithmes de tatouage d'images.

Le troisième chapitre sera consacré exclusivement à la présentation de notre méthode de tatouage d'images médicales numériques, où nous démontrerons les outils et les méthodes utilisées et présenterons notre application de tatouage ainsi que les résultats obtenus.

Chapitre 1

Image numérique

1.1 Introduction

L'image est devenue le support principal de l'information. Le traitement des images fixes ou animées est par conséquent un domaine de recherche en pleine expansion et aux applications toujours plus nombreuses.
Dans Ce Chapitre, nous avons présenté les notions de bases liées à la représentation des images, leurs types et leurs propriétés, tout en définissant le domaine de traitement d'images.

1.2 Définition

Une image peut être représentée sous forme d'une matrice à deux dimensions avec des coordonnées spatiales x et y. Les dimensions de cette matrice peuvent être ajustées pour modifier l'image. Si l'image est numérique, cela signifie qu'elle a été traitée et stockée sous forme binaire, avec une série de 0 et de 1 représentant des valeurs numériques. Les pixels de l'image numérique sont les points individuels qui la composent et sont abrégés en "pixels", qui signifie " Picture Élément".[26]

1.2.1 Les images matricielles (bitmap)

Également connues sous le nom de bitmap, sont définies comme un ensemble de points carrés individuels appelés pixels. Elles sont généralement obtenues à l'aide d'un appareil photo ou d'un scanner.
Lorsqu'une image est agrandie en ajustant la matrice, les pixels individuels peuvent devenir plus visibles, ce qui peut entraîner une apparence floue ou pixélisée de l'image, avec des boîtes

apparentes à l'écran. Les fichiers image sont généralement stockés dans des formats tels que le TIFF, BMP, PNG et JPG. [1]

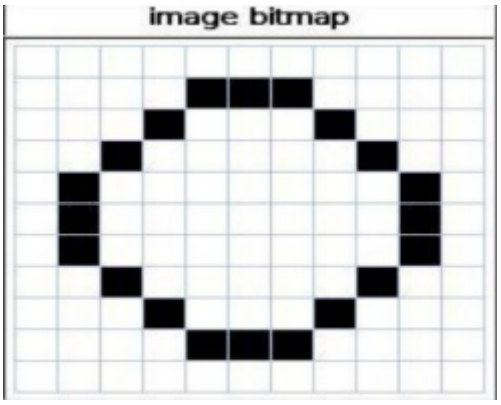

FIGURE 1.1 – Images matricielles (Bitmap) composées de pixels.

1.2.2 Les images vectorielles

Les images vectorielles sont créées à partir de lignes et de segments qui sont connectés entre eux à l'aide de formules mathématiques. Cette méthode permet de redimensionner l'image sans aucune perte de qualité. En effet, contrairement aux images bitmap, les images vectorielles ne sont pas basées sur des pixels, mais sur des équations mathématiques qui définissent la forme et les propriétés de l'image. On peut représenter une image vectorielle à l'aide de formules mathématiques, ce qui permet de la redimensionner sans perdre en qualité.[30]

1.3 Les caractéristique d'une image numérique

1.3.1 Le pixel

Le pixel représente l'unité de base d'une image numérique, le plus petit point de l'image. Ces points sont communément appelés " Picture éléments" en anglais, abrégé sous le terme "pixels". Ils sont organisés sur une grille régulière, et chacun est associé à une couleur ou une nuance de gris, définissant ainsi l'apparence de l'image dans son ensemble.[19]

1.3.2 La Dimension d'une image

La dimension d'une image fait référence au nombre de pixels qui la composent et est généralement exprimée sous la forme [largeur] × [hauteur]. Elle est mesurée en pixels (px) et représente le nombre total de pixels dans une image.[4]

1.3.3 Résolution d'une image

La résolution d'une image est la densité de pixels dans une unité de longueur. Elle est généralement exprimée en ppp (pixels par pouce) ou en dpi (points par pouce). Un pouce correspond à $2,54$ cm. La résolution est importante pour définir la qualité et la netteté de l'image. Plus la résolution est élevée, plus l'image est fine et détaillée.[6]

$$\text{Résolution en ppp } = \frac{\text{nombre de pixels(en pixels)}}{\text{Dimension (en pouces)}}$$

FIGURE 1.2 – Les différentes résolutions d'une image.

1.4 Les différents types d'images numériques

Pour stocker et transmettre une image numérique, il est nécessaire de la coder en binaire, c'est-à-dire de la décrire par une séquence de 0 et de 1. Cette représentation binaire permet de manipuler et de traiter l'image de manière numérique, en utilisant des algorithmes et des outils spécifiques.

1.4.1 Les images binaires

Une image binaire est une image qui ne contient que deux couleurs, généralement le noir et le blanc, chaque pixel ne peut avoir pour valeur que 0 (noir)ou 1 (blanc).[19]

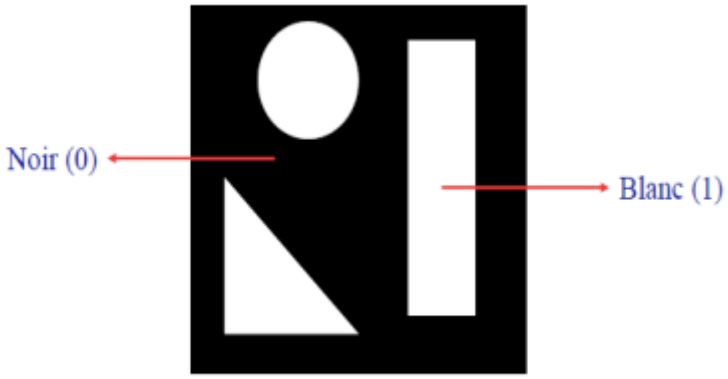

FIGURE 1.3 – Exemple image binaire.

1.4.2 Image en niveaux de gris

Les images en niveaux de gris ne contiennent pas de couleurs, mais seulement des nuances de gris. Chaque pixel est représenté par une valeur numérique allant de 0 (noir) à 255 (blanc), avec une gamme de niveaux de gris intermédiaires. Pour stocker ces valeurs numériques, chaque pixel est codé sur un octet, soit 8 bits, ce qui permet de stocker précisément sa valeur de gris. [7]

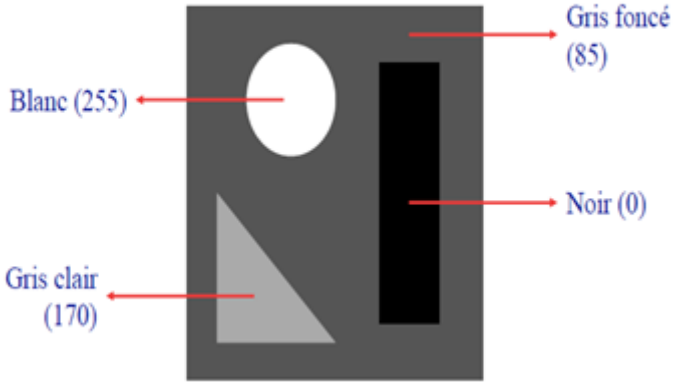

FIGURE 1.4 – exemple image en niveaux de gris.

1.4.3 Image couleur (ou RGB)

Dans une image couleur en mode RVB(RGB), chaque pixel est représenté par trois canaux de couleurs : rouge (R), vert (G) et bleu (B). Chaque canal est codé sur un octet, ce qui signifie

que chaque canal peut prendre 256 valeurs différentes, allant de 0 à 255. Ainsi, chaque pixel est représenté par trois valeurs numériques, chacune sur un octet, soit un total de 24 bits (trois octets). Cela permet de représenter 256^3, soit 16777216 couleurs différentes. Il est important de noter que le nombre de couleurs effectivement affichées dépend également de la capacité d'affichage de l'appareil et des limites de la vision humaine.[25]
Dans le modèle RVB, les images sont composées de trois plans indépendants, un pour chaque couleur primaire.

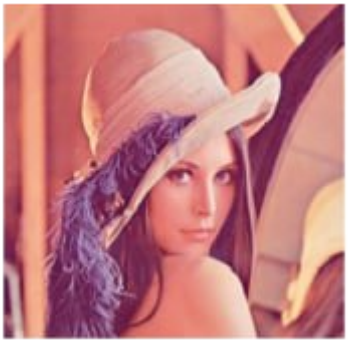

FIGURE 1.5 – Image Lina en codage RVB.

FIGURE 1.6 – Composante R(a),Composante V(b),Composante B(c).

1.5 Les différents espaces couleurs

Les espaces de couleur, également appelés espaces colorimétriques, sont des modèles mathématiques en trois dimensions représentant toutes les couleurs perceptibles, utilisables ou reproductibles par l'œil humain ou un appareil. Chaque couleur est associée à des coordonnées spécifiques qui correspondent approximativement aux trois longueurs d'onde auxquelles l'œil humain est sensible. Les espaces de couleur sont utilisés pour gérer la couleur dans les images numériques, l'impression, la vidéo, la télévision et d'autres domaines où la précision des couleurs

est importante. Parmi les nombreux espaces de couleur, on trouve notamment : RGB, YUV, HSV et YCM.

1.5.1 Le modèle RGB

Le modèle colorimétrique RGB (Red, Green, Blue) est constitué de trois composantes qui permettent de représenter les couleurs primaires. dans l'image chaque pixel est caractérisé par une combinaison des trois couleurs primaires En combinant différentes proportions de rouge, de vert et de bleu, on peut créer toutes les autres couleurs. Le modèle RGB est largement utilisé dans les images numériques affichées sur les écrans d'ordinateurs et de téléphones portables, ainsi que dans les graphiques et les jeux vidéo.

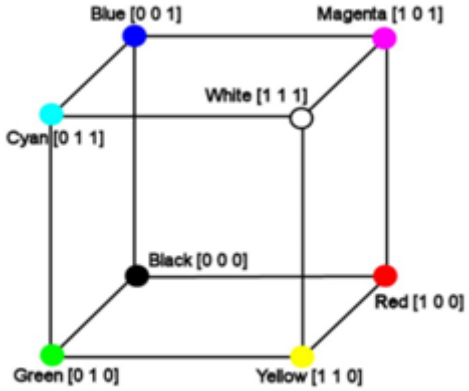

FIGURE 1.7 – Représentations de couleur de l'espace de couleur RGB.

1.5.2 Le modèle YUV

Le modèle YUV est un espace colorimétrique en trois composantes Le composant Y représente la luminance, c'est-à-dire l'information en noir et blanc, tandis que les composants U et V représentent la chrominance, c'est-à-dire l'information sur la couleur. Ce modèle est utilisé dans les systèmes de diffusion télévisuelle PAL, SECAM et NTSC pour transmettre des informations colorées aux téléviseurs couleur tout en garantissant la compatibilité avec les téléviseurs noir et blanc. Le modèle YUV est très utile pour la compression vidéo et la vidéo numérique car il permet de séparer la luminance et la chrominance pour une meilleure compression.[9]

1.5.3 Le modèle HSV

Le modèle HSV (Hue, Saturation, Value) est un espace colorimétrique en trois dimensions qui représente les couleurs selon leur teinte (Hue), leur saturation (Saturation) et leur valeur (Value ou luminosité). Contrairement au modèle RGB, qui représente les couleurs primaires en termes de quantités de rouge, de vert et de bleu e modèle HSV représente les couleurs en termes de teinte (couleur de base), de saturation (intensité de la couleur) et de valeur (luminosité ou brillance de la couleur). La saturation est une mesure de la différence de couleur d'un gris de la même luminosité. La saturation zéro n'indique aucune teinte, juste une échelle grise.[10]

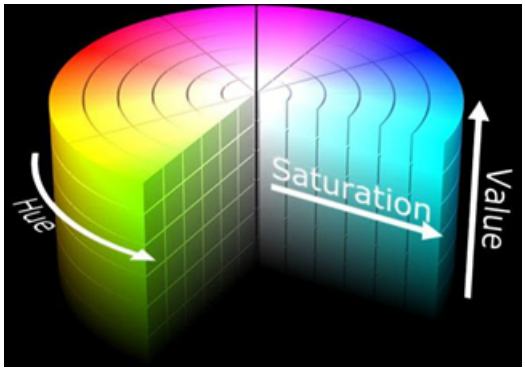

FIGURE 1.8 – Représentations de couleur de l'espace de couleur HSV.

1.5.4 Le modèle CMY

Le modèle de couleur soustractif CMY (Cyan, Magenta, Jaune) utilise une représentation de l'espace de couleur où le blanc est codé par $(0.0, 0.0, 0.0)$ et le noir par $(1.0, 1.0, 1.0)$. Ce modèle fonctionne en soustrayant des couleurs de la lumière blanche pour obtenir la couleur désirée. Ainsi, l'absence de soustraction de couleurs donne du blanc, tandis que la soustraction de toutes les couleurs donne du noir. Les modèles de couleurs CMY sont fréquemment employés dans l'industrie d'impression de couleurs, car ils offrent la possibilité de créer une grande variété de teintes en utilisant simplement trois couleurs primaires : cyan, magenta et jaune. En combinant ces couleurs dans différentes proportions, il est possible d'obtenir une grande diversité de couleurs. Toutefois, il est important de souligner que le modèle CMY n'est pas aussi précis que le modèle RGB pour représenter les couleurs, car il peut produire des couleurs indésirables ou des nuances de gris qui peuvent altérer la qualité de l'image imprimée.[10]

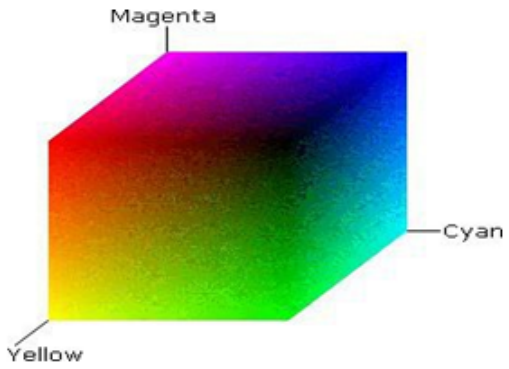

FIGURE 1.9 – Représentations de couleur de l'espace de couleur CMY.

1.6 Les formats d'images numériques

1.6.1 Format BMP (bitmap)

Format BMP (bitmap) : Le format d'image BMP (bitmap) est l'un des formats les plus simples, ayant été développé conjointement par Microsoft et IBM. Ce format est ouvert et non compressé, ce qui permet de stocker les pixels de l'image sous forme de tableau de points. Chaque fichier BMP est donc constitué de pixels individuels qui sont définis par leur couleur et leur position dans l'image. Bien que sa taille importante puisse rendre son utilisation en ligne difficile, le format BMP reste efficace pour travailler sur les fichiers image en raison de sa grande compatibilité.[26]

1.6.2 Tagged Image File Format (TIFF)

Le format TIFF est idéal pour stocker des documents numérisés tels que des images et du texte. Il peut stocker des fichiers de grande taille sans compromettre leur qualité, ce qui en fait un choix populaire pour l'archivage de documents. Les algorithmes de lecture du format TIFF garantissent que la qualité de l'image originale est préservée sans perte de qualité, même après la numérisation et le stockage. En somme, le format TIFF est un choix optimal pour stocker des documents numérisés de haute qualité, sans dégradation de la qualité d'image. [7]

1.6.3 Graphiques Inter change Format (GIF)

Le format GIF est largement reconnu comme un standard sur internet. Les fichiers GIF sont de petite taille, car ils sont limités à enregistrer uniquement 256 couleurs. Cependant, cette limitation est considérée comme l'un des avantages clés de ce format. En plus de stocker des

images, le format GIF permet également la création d'animations et de détourages, ce qui en fait un choix polyvalent pour de nombreux types de contenus en ligne.[8]

1.6.4 Portable Network Graphique (PNG)

Le format PNG est un standard du W3C (Consortium World Wide Web) et est largement répandu sur Internet. Ce format de fichier propriétaire permet une compression optimale de la taille des images en utilisant un système de couleurs indexées et en permettant l'utilisation de valeurs de couleur précises. En outre, il offre la possibilité d'utiliser 13 profondeurs de couleurs différentes allant de 1 à 48 bits et prend en charge la transparence.[25]

1.6.5 Joint Photographique Expert Group (JPEG)

La norme JPEG (ISO 10918-1) est la norme internationale pour la compression d'images fixes, en particulier pour les images photographiques. Bien que complexe et nécessitant des connaissances mathématiques solides, cette méthode de compression "avec pertes" basée sur l'algorithme DCT offre des taux de compression très intéressants. Bien qu'un mode "sans perte" ait été développé, il n'a pas été largement utilisé. Cette norme a été développée par le comité JPEG (Joint Photographique Experts Group) et normalisée par l'ISO/JTC1 SC29.[26]

1.7 Conclusion

Dans ce chapitre, nous avons essayé de présenter quelques notions de bases liées au domaine de l'image numérique ,nous avons décrit les différentes caractéristiques d'une image, et En donnant quelques définitions élémentaires sur les images numériques, ce sont des points essentiels dans la suite de notre travail sur le sujet de tatouage numérique, son état de l'art, ainsi que les différentes techniques utilisées.

Chapitre 2

tatouage numérique

2.1 Introduction

La protection des données numériques et les droits de propriété intellectuelle sont des enjeux importants dans le monde numérique. Le tatouage d'images suscite un intérêt croissant dans ce contexte.
Ce chapitre présente un état de l'art sur les méthodes de tatouage numérique et le concept général et les méthodes de tatouage numérique, ainsi que les différents domaines d'application et les principales attaques considérées.

2.2 Définition

Le tatouage numérique est une méthode utilisée pour intégrer une information appelée marque dans un support numérique, qu'elle soit visible ou invisible. La marque peut prendre la forme d'une image, d'un texte, d'une vidéo, d'un audio ou d'une autre donnée numérique. L'objectif est d'insérer la marque de manière à ce qu'elle soit perceptible ou imperceptible, sans altérer la qualité visuelle de l'image dans son ensemble.[28]

Le tatouage numérique est une technologie utilisée pour protéger les données multimédia contre la violation du droit d'auteur dans des environnements non sécurisés où la cryptographie ne peut pas être appliquée efficacement .[3]

La technique du tatouage numérique, qui est souvent utilisée avec d'autres techniques, vise à résoudre divers problèmes de sécurité liés aux données numériques, tels que la protection des droits d'auteur, la prévention de la redistribution non autorisée, l'intégrité du contenu d'une donnée, etc.

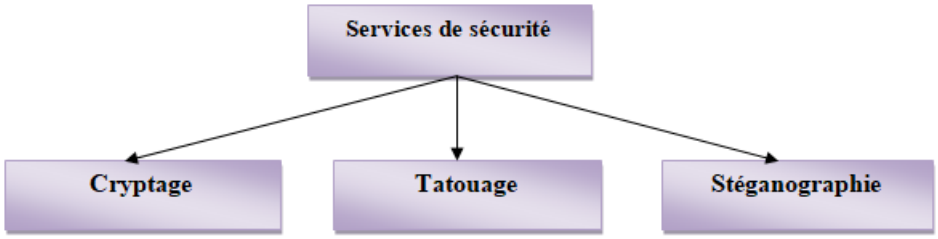

FIGURE 2.1 – Services de sécurité.

2.3 Schéma générale de l'implémentation de tatouage

Toutes les techniques de tatouage utilisent le même principe général, qui implique l'utilisation de services de sécurité pour insérer une marque dans les données à protéger.
Le schéma ci-dessous illustre ce principe.
En général, un système de tatouage est divisé en deux phases de base : la phase d'insertion de la marque et la phase d'extraction de la marque.

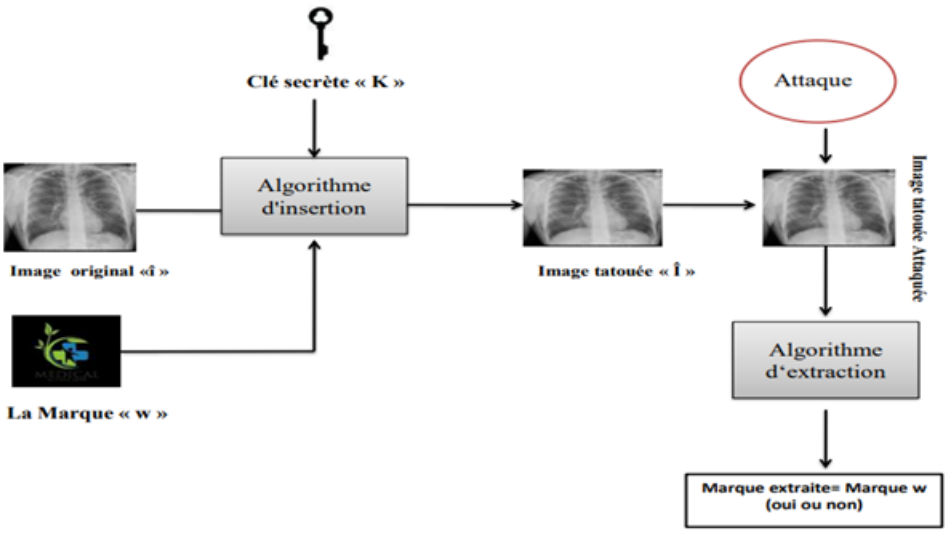

FIGURE 2.2 – Schéma générale d'insertion et d'extraction de la marque.

2.3.1 Phase d'insertion

Le sous-système d'insertion (Embedding) est une étape importante dans le processus de tatouage numérique. Il implique l'entrée d'un watermark W, d'un document hôte (porteur) I, et d'une clé secrète K spécifique au tatoueur pour renforcer la sécurité du système. La marque, qui représente le message d'information à cacher dans le document hôte, est généralement transformée en une séquence de N bits. Ces bits sont ensuite ajoutés au document hôte sous forme de séquences aléatoires qui peuvent être considérées comme du bruit ou intégrées de manière

transparente. Cette étape d'insertion est cruciale pour garantir que la marque ne soit pas détectable et ne perturbe pas la qualité du document hôte.
L'insertion de la marque s'effectuera en générale dans le domaine spatiale ou le domaine fréquentiel, un troisième paramètre peut être ajouté c'est la clé secrète de marquage pour encodée la marque qui permet d'assure un certain niveau de sécurité au tatouage.[3]

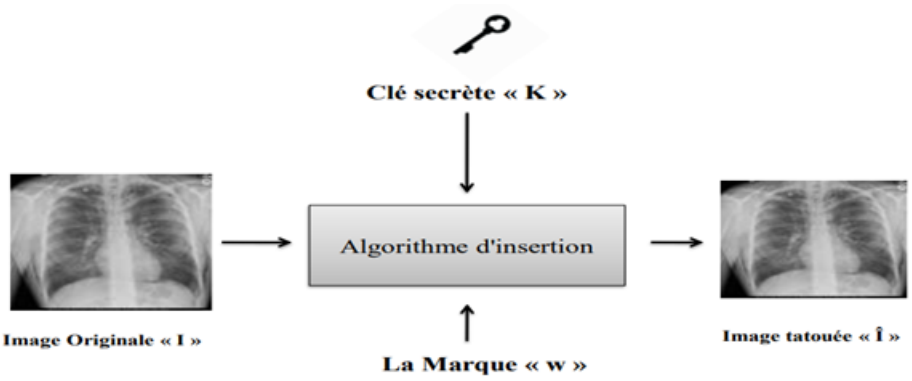

FIGURE 2.3 – phase d'insertion.

- Il existe deux types d'insertion :

2.3.1.1 Insertion additif

La technique d'insertion additive consiste à insérer un bruit dans l'image hôte pour y intégrer la marque générée directement dans l'image originale. [16]

2.3.1.2 Insertion par substitution

Avec la technique d'insertion par substitution, la marque à insérer ne sera pas simplement ajoutée, mais plutôt remplacera des composantes de l'image originale I. Cette insertion peut se faire de plusieurs façons, notamment en substituant les bits de poids faible (LSB) de l'image originale avec les bits de la marque. [3]

2.3.2 Phase d'extraction

La phase d'extraction permet de détecter la présence du marquage dans les données hôtes en utilisant la clé secrète K qui a été utilisée lors de la phase d'insertion. Elle permet également de récupérer la marque qui a été insérée dans les données hôtes.[20]

- Les schémas de tatouages peuvent être classés en trois catégories Selon les éléments nécessaires pour l'extraction de la marque

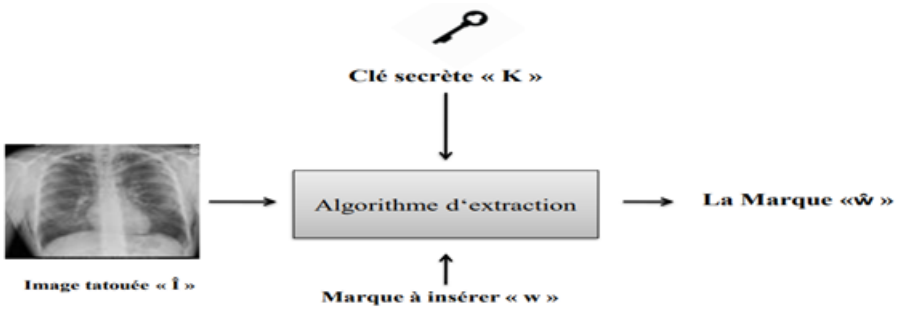

FIGURE 2.4 – phase d'extraction.

2.3.2.1 Les schémas aveugles

Les schémas aveugles se réfèrent aux systèmes où l'image originale n'est pas nécessaire lors de la phase d'extraction. Si la clé privée est également absente, alors la détection se fait à l'aide de la clé publique.[20]

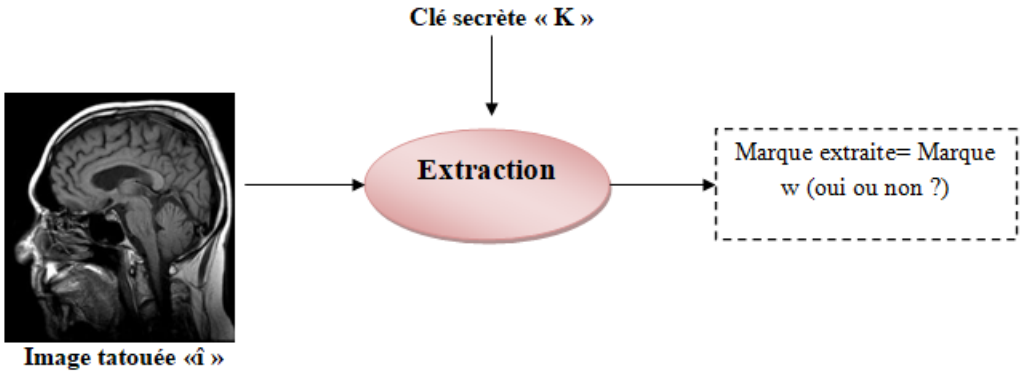

FIGURE 2.5 – Schéma général d'extraction aveugle d'une marque.

2.3.2.2 Les schémas non-aveugles

Les schémas non-aveugles de détection d'un tatouage numérique nécessitent l'image originale ainsi que la clé secrète (privée).[20]

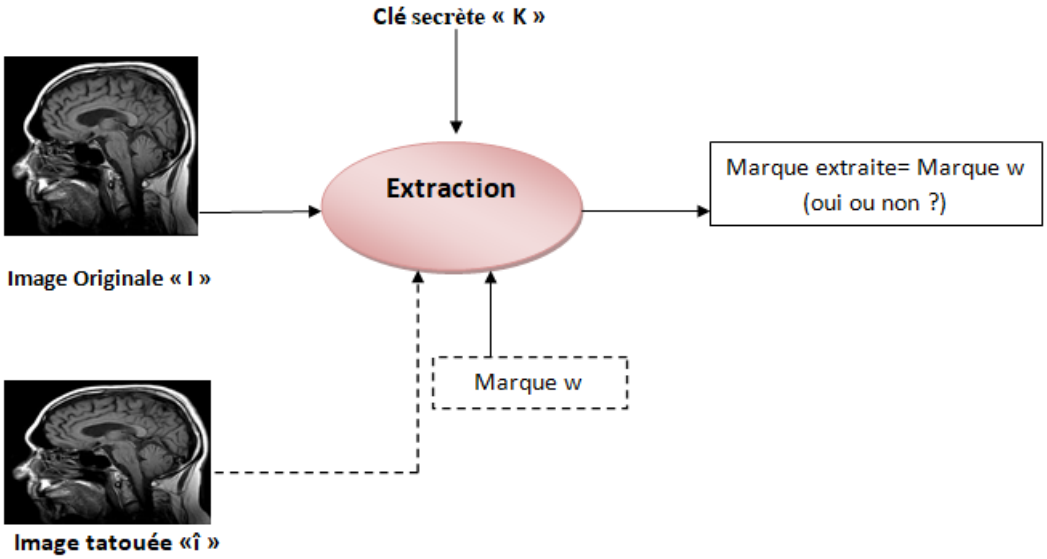

FIGURE 2.6 – Schéma général d'extraction non-aveugle d'une marque.

2.3.2.3 Les schémas semi-aveugles

Les schémas semi-aveugles utilisent des caractéristiques dérivées de l'image originale pour détecter la présence du marquage, contrairement aux schémas non-aveugles qui nécessitent à la fois l'image originale et la clé secrète.[20]

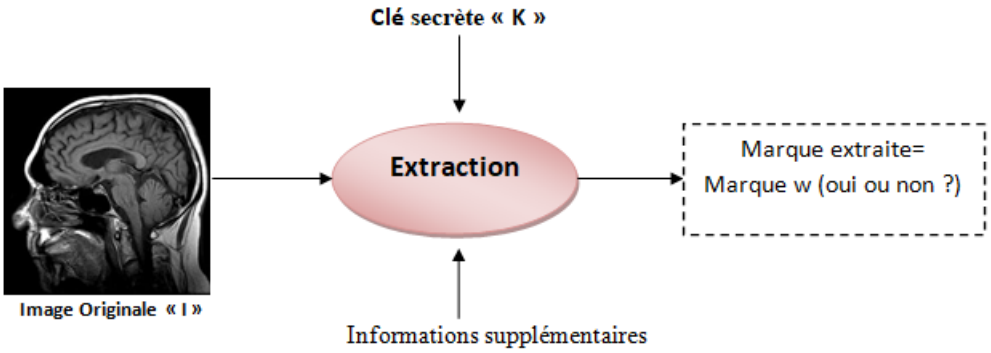

FIGURE 2.7 – Schéma général d'extraction Semi-aveugle d'une marque.

2.4 Contraintes du tatouage d'image

Pour quantifier la performance d'une technique de tatouage ou concevoir un algorithme performant, il est important de prendre en compte plusieurs facteurs essentiels tels que l'imperceptibilité, la robustesse et la capacité. Ces facteurs sont représentés schématiquement dans la figure suivante

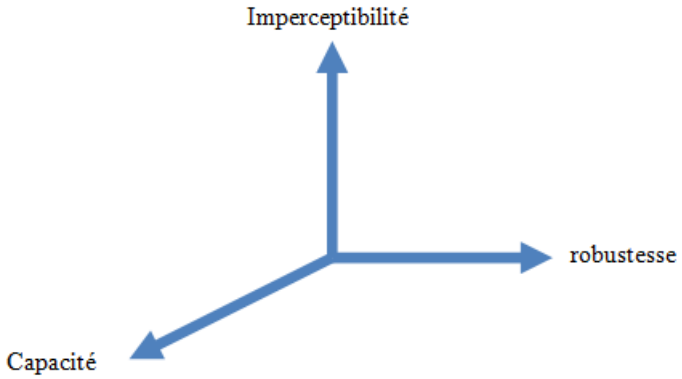

FIGURE 2.8 – Contrainte de tatouage d'image.

2.4.1 Imperceptibilité

L'imperceptibilité est un facteur essentiel pour l'efficacité d'un algorithme de tatouage numérique. En effet, lors de l'insertion du tatouage, des distorsions peuvent être introduites dans l'image hôte. Cependant, ces distorsions doivent être minimales pour garantir que l'image tatouée reste visuellement similaire à l'image originale. [8]

2.4.2 robustesse

La robustesse d'un système de tatouage fait référence à sa capacité à résister à différentes attaques de traitement d'image. Ces attaques sont conçues pour supprimer ou détruire la marque insérée, voire même empêcher la marque d'accomplir son objectif prévu. Cox et al. définissent également la robustesse comme la capacité de détecter la marque après des opérations de modification (traitement). Cela implique que le système de tatouage doit être capable de maintenir l'intégrité de la marque même en présence de modifications ou de manipulations sur l'image.[28]

2.4.3 Capacité

Représente la quantité d'information que l'on veut insérer dans l'image. Cette quantité varie selon l'algorithme utilisée et l'application visée par le tatouage, En générale en a besoin que de quelques bits pour la protection des droits d'auteurs, mais pas pour insérer un logo de société. En revanche, il est nécessaire de cacher plusieurs bits d'information pour permettre l'authentification des images [1].

2.4.4 Sécurité

Le tatouage numérique a pour but principal de protéger les données insérées en utilisant une clé d'insertion soigneusement sélectionnée. Une technique de tatouage fiable doit être capable d'empêcher l'extraction de la marque insérée par des personnes non autorisées, même si elles ont une connaissance de l'algorithme d'insertion et d'extraction.

2.5 Robustesses d'algorithme

2.5.1 Tatouage robuste

Un système de tatouage est qualifié de robuste lorsque la détection de la marque demeure efficace même en présence d'une altération ou d'une attaque du document tatoué. Pour être considéré comme robuste, un tel système doit être capable de résister à la fois aux opérations légales telles que la compression et le filtrage sur le document numérique, ainsi qu'aux attaques malveillantes des pirates. [19]

2.5.2 Tatouage fragile

Le tatouage dit "fragile" se caractérise par une marque sensible et fragile qui ne doit pas résister aux modifications apportées à l'image tatouée. Cette technique est utilisée pour détecter toute manipulation ou modification du contenu numérique.[4]
Cette technique sert à prouver l'authenticité et l'intégrité l'image tatouée.[19]

2.5.3 Tatouage semi-fragile

il combine les caractéristiques des tatouages robustes et fragiles pour créer une situation intermédiaire . Il permet de créer une marque qui est capable de résister à un ensemble défini de dégradations, tout en étant vulnérable à d'autres types de modifications. Cette technique est utilisée pour vérifier l'intégrité du contenu numérique et détecter toute tentative de manipulation ou de modification non autorisée.[19]

2.5.4 Classification des algorithmes de tatouage numérique selon la préservation de l'image originale

Les techniques de tatouage peuvent être classées en deux catégories, réversible et irréversible.

2.5.4.1 Le tatouage réversible

Le tatouage "réversible" est une technique de tatouage numérique qui permet de garantir l'intégrité de l'image, tout en ayant l'avantage de pouvoir restaurer l'image originale. Cette propriété de réversibilité est très recherchée dans les secteurs d'imagerie sensible, en particulier dans le domaine médical. [8]

2.5.4.2 Le tatouage non réversible

Le tatouage "non réversible" est une technique de tatouage numérique dans laquelle il est impossible de retrouver l'image originale à partir de l'image tatouée. [8]

2.6 technique de tatouage d'image

2.6.1 Tatouage visible

Dans les techniques de tatouage visible, la marque est facilement perceptible à l'œil humain. En d'autres termes, elle est clairement visible. Les logos et les images sont couramment utilisés comme filigranes pour les systèmes de filigrane visible.
Il y a au moins deux inconvénients liés aux techniques de tatouage visible :

- La marque insérée peut être facilement retirée par une simple découpe.
- La visibilité de la marque insérée peut détériorer la qualité visuelle de l'image hôte.

FIGURE 2.9 – Exemple d'un tatouage visible.

2.6.2 Tatouage invisible

Le tatouage "invisible" est une technique de tatouage numérique dans laquelle l'image tatouée est très similaire à l'image originale, ce qui rend difficile leur distinction. Il est donc

difficile de retirer ou de détruire la marque insérée sans altérer significativement la qualité visuelle de l'image tatouée. [2]

FIGURE 2.10 – Exemple d'un tatouage invisible.

2.7 Les Domaines d'application du tatouage

2.7.1 Protection des droits d'auteur

Le tatouage numérique est couramment utilisé dans le but de protéger les droits d'auteur, en insérant une signature unique qui permet d'identifier de manière fiable le propriétaire de l'œuvre. Il s'agit de l'application la plus évidente du tatouage numérique dans le domaine de la protection des droits d'auteur. Les deux caractéristiques primordiales à respecter sont l'invisibilité et la robustesse de la marque. En effet, la marque doit être invisible pour préserver l'intégrité de l'œuvre originale, tout en étant suffisamment résistante pour contrer les tentatives de piratage et de violation des droits d'auteur. [8]

2.7.2 L'authentification des données

Le tatouage numérique est une technique cruciale pour l'authentification des données, en particulier dans le domaine des images médicales. Il permet d'insérer une marque dans l'image qui sert de preuve que le contenu n'a pas été altéré depuis l'insertion de la marque. Cette application utilise des marques fragiles qui deviennent invisibles dès qu'une valeur des données est modifiée dans le document. Cette fonctionnalité de l'authentification des données est essentielle pour garantir l'intégrité et la fiabilité des informations médicales. [15]

2.7.3 Contrôle d'accès

Dans certains systèmes, des privilèges différents peuvent être offerts aux utilisateurs en fonction de leur mode de paiement. Afin d'éviter la copie illégale du contenu ou de limiter le nombre de copies, un mécanisme de contrôle de copie et d'utilisation est souhaitable. Dans ce cas, l'utilisation d'un filigrane robuste peut être une solution efficace pour identifier l'auteur du document et retracer son utilisation.[8]

2.7.4 L'intégrité des données multimédias

Le tatouage numérique est une méthode utilisée pour garantir l'authenticité du contenu d'un document en insérant une marque fragile dans l'image. Cette marque subit des distorsions si le document est altéré, ce qui la détériore instantanément. Cette technique permet ainsi de détecter toute modification apportée au document et de s'assurer de l'intégrité des données. Cette application est utile pour assurer la sécurité et la fiabilité des données dans diverses industries, y compris dans le domaine médical et financier. [11]

2.7.5 Les Empreintes

L'application de tatouage numérique est couramment utilisée pour tracer les copies illégales de médias et pour suivre les pirates. Cette application génère un marquage unique, généralement sous forme d'un numéro de série, pour chaque copie distribuée. Cependant, la distribution de copies comportant différentes marques peut entraîner des problèmes de collusion. Par conséquent, il est important que les marques utilisées répondent à des critères de sécurité pour prévenir les collusions. Les marques doivent être conçues de manière à garantir l'unicité de chaque marquage et à empêcher toute manipulation frauduleuse de l'information.[20]

2.7.6 Sécurité médicale

Il est important d'insérer un "identifiant" confidentiel assurant la correspondance entre le patient et la radio, afin d'éviter toutes confusions. Cela garantit la sécurité et la confidentialité des informations médicales.[31]

2.7.7 Information sur le support

Le tatouage numérique peut inclure des informations globales sur l'œuvre, telles que le nom de l'auteur, le titre, la date d'édition, l'adresse électronique, etc. Ces informations sont

intégrées à la même marque numérique, sans nécessiter une seconde marque distincte. Cette application peut être utilisée en complément d'une protection de la propriété intellectuelle pour renforcer la sécurité et l'authenticité des données. La présence de ces informations supplémentaires peut aider à identifier facilement les propriétaires de l'œuvre et à prévenir la contrefaçon et l'utilisation illégale.[1]

2.7.8 L'indexation des images

Le tatouage numérique est une méthode utilisée pour indexer les images en y insérant une signature. Cette technique facilite l'indexation et le classement des images dans une base de données. La signature peut contenir des informations sur l'image telles qu'un sommaire, un descripteur ou un lien vers d'autres informations pour permettre une recherche rapide et un classement efficace. Grâce à cette méthode, il est possible de gérer plus facilement de grandes quantités d'images et d'améliorer l'accessibilité aux informations. [16]

2.8 Le Domaine d'insertion du tatouage

2.8.1 Domaine spatial

Les méthodes agissant dans le domaine spatial modifient directement les valeurs des pixels de l'image pour y inclure le message caché Il existe plusieurs méthodes pour cela, telles que l'insertion des bits du message dans les bits de poids faible de chaque pixel (LSB), la modification des propriétés statistiques de petites régions de l'image (patchwork) . Ces méthodes sont utilisées pour assurer l'invisibilité de la signature et consistent en général à effectuer des modifications subtiles des pixels pour intégrer le message de façon efficace. Cependant, ces méthodes ont tendance à manquer de robustesse.[7]
cette méthode est vulnérable face à de nombreuses attaques telles que l'ajout de bruit ou la compression avec perte, ce qui peut altérer la qualité de l'image et même supprimer complètement le tatouage. [22]

2.8.2 Domaine Fréquentiel

Le domaine fréquentiel est une approche en traitement d'images et de signaux qui transforme une image ou un signal du domaine spatial en un autre domaine appelé domaine fréquentiel, représentant l'image ou le signal sous forme de coefficients de fréquence plutôt que de

pixels. Les transformations fréquentielles les plus courantes sont la Transformation de Fourier discrète (DFT) , la Transformation en Cosinus Discrète (TCD) et la Transformation en Ondelette (DWT) [13]. Les méthodes qui utilisent le domaine fréquentiel sont plus résistantes à la compression et moins vulnérables aux altérations géométriques.[16]

2.8.2.1 Transformée de Fourier Discrète

La transformée de Fourier (FT) est une technique largement utilisée en tatouage d'images et l'une des transformées les plus utilisées dans le traitement de signal , elle permet de contrôler les fréquences du signal et de choisir les parties de l'image qui doivent être marquées de manière appropriée, afin d'obtenir un compromis optimal entre la visibilité et la robustesse. Cette transformation est également employée pour intégrer la signature avec le support lors de la phase de modulation, ainsi que pour diviser les images en bandes perceptuelles.[7]
En général, la transformation de Fourier discrète est représentée par deux composantes : une amplitude et une phase. La modulation de la phase de la DFT est utilisée dans plusieurs articles pour l'insertion d'une marque, car la phase contient les composantes les plus importantes de l'image. En modulant la phase, on peut accroître la robustesse du schéma, et une attaque opérant dans la phase du spectre dégraderait rapidement la qualité de l'image. [8]

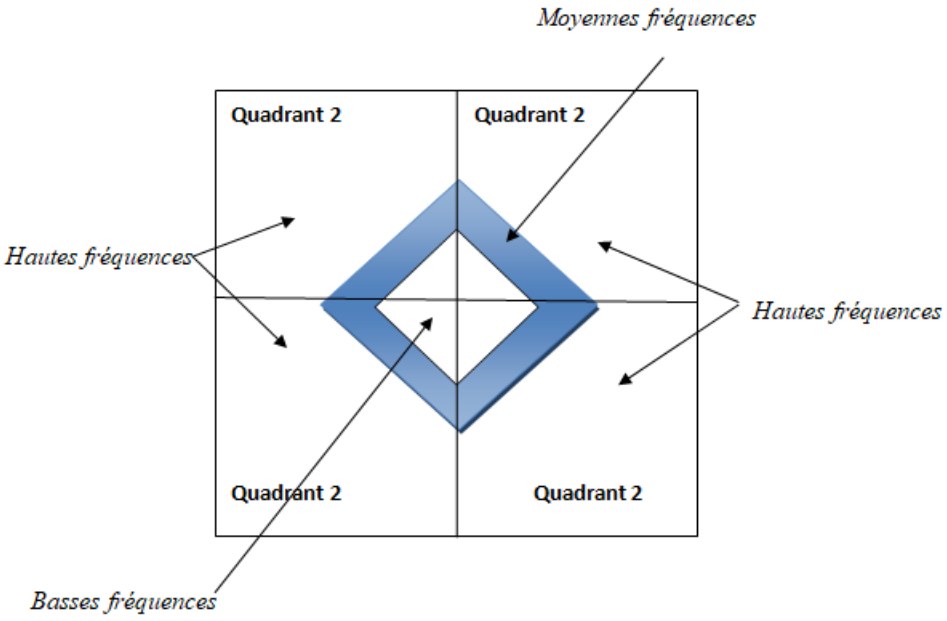

FIGURE 2.11 – Représentation fréquentielle des coefficients de module d'une DFT.

La transformée de Fourier discrète (DFT) (n) d'une séquence réelle $DFT(n)$ de longueur $x(k)$ est définie comme suit :

La définition de la TF est donnée par la formule suivante :

$$X(n) = \sum_{k=0}^{N-1} x(k) W_N^{nk}, \quad 0 \leq n \leq N-1$$

La transformée DFT inverse est calculée comme suit.

$$x(k) = \frac{1}{N} \sum_{n=0}^{N-1} X(n) W_N^{-nk}, \quad 0 \leq k \leq N-1$$

avec $W_N = e^{-j\frac{2\pi}{N}}$ et $j = \sqrt{-1}$

2.8.2.2 La transformée en ondelettes discrète

La Transformée en Ondelettes Discrète (DWT) est une technique de description multi-résolution qui permet de décomposer une image en bandes de fréquences. Ce processus de transformation repose sur deux étapes principales : l'échantillonnage et le filtrage. Le filtrage divise l'image en sous-bandes à haute fréquence et à basse fréquence, tandis que l'échantillonnage réduit la résolution de chaque sous-bande à l'aide de filtres passe-bas et passe-haut en quadrature.[28]

La décomposition horizontale de l'image génère quatre sous-bandes de représentation fréquentielle : LL (approximative), LH (verticale), HL (horizontale) et HH (diagonale). La sous-bande LL représente une version approximative de l'image originale, tandis que les sous-bandes LH, HL et HH captent les détails dans les directions verticale, horizontale et diagonale, respectivement. elle permet de capturer à la fois les informations de fréquence et de localisation dans le temps. Cette capacité est essentielle pour l'analyse des images, car elle permet de représenter avec précision les détails à différentes échelles temporelles.

Pour réduire la résolution de l'image, on procède au sous-échantillonnage des quadrants approximatifs. Cela signifie qu'on réduit la taille des quadrants approximatifs en conservant uniquement les pixels situés aux positions paires.

Par conséquent, on réduit de moitié la résolution horizontale et verticale de ces quadrants. Après l'insertion de la marque d'eau, la DWT inverse est appliquée à la nouvelle image modifiée pour obtenir l'image finale. La DWT inverse est utilisée pour reconstruire l'image à partir des sous-bandes de fréquence décomposées précédemment.[3]

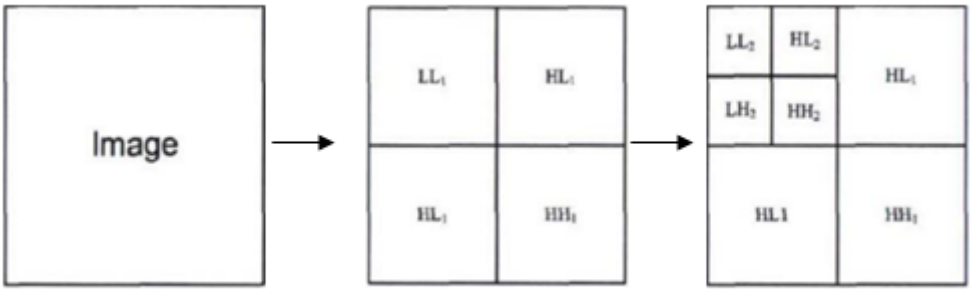

FIGURE 2.12 – Deux niveaux de décomposition en utilisant la DWT.

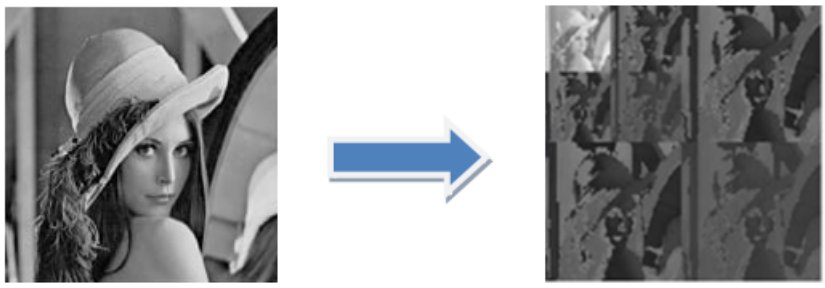

FIGURE 2.13 – Décomposition en ondelette au 2 ème niveau de l'image de Lena.

Il existe différentes formes d'ondelettes disponibles :

2.8.2.2.1 Les ondelettes de Haar

Le filtre Haar est une fonction d'ondelettes largement utilisée dans DWT qui est spécifiquement conçue pour calculer les disparités entre les valeurs de pixels adjacents. Cela permet de séparer l'image en composants approximatifs et détaillés, qui peuvent ensuite être divisés en quadrants. En diminuant la résolution de l'image, un sous-échantillonnage est effectué sur les quadrants approximatifs, en ne retenant que les pixels aux positions paires. Ce processus peut être répété de manière récursive pour créer une pyramide d'images avec des résolutions variables.[32]

2.8.2.2.2 Les ondelettes de Daubechies

Les ondelettes de Daubechies sont des instruments très performants pour l'analyse des signaux et des images. Ils permettent la segmentation d'un signal ou d'une image à différentes échelles, exposant ainsi des informations à différents niveaux de détail. Grâce à la décomposition en ondelettes, le signal est divisé en deux composants principaux : les approximations (représentant les caractéristiques et les tendances globales du signal) et les détails (capturant les fluctuations locales et les informations nuancées).[32]

2.8.2.3 Domaine de la DCT

De nombreux algorithmes de compression d'image et de vidéo utilisent la transformation en cosinus discrète (DCT) pour convertir une image dans le domaine fréquentiel, puis appliquent une quantification pour comprimer les données. Ce processus permet de diviser l'image en sous-bandes spectrales qui ont une importance hiérarchique en termes de qualité visuelle de l'image.[17]

La DCT est une technique utilisée dans la technologie JPEG pour comprimer les images. Elle est également connue pour sa robustesse face à certaines attaques telles que les ajustements de luminosité, de teinte, de contraste, de filtrage et de lissage.[5]

L'algorithme DCT est généralement appliqué sur des blocs d'images de taille fixe, tels que 8x8 ou 64x64 pixels. Les coefficients de la transformation sont ensuite répartis sur trois bandes de fréquences : basses, moyennes et hautes fréquences. Cela permet de représenter l'image dans le domaine fréquentiel et de capturer différentes caractéristiques de l'image à différentes échelles de fréquences, ce qui contribue à la compression efficace des données tout en conservant la qualité visuelle de l'image.[17]

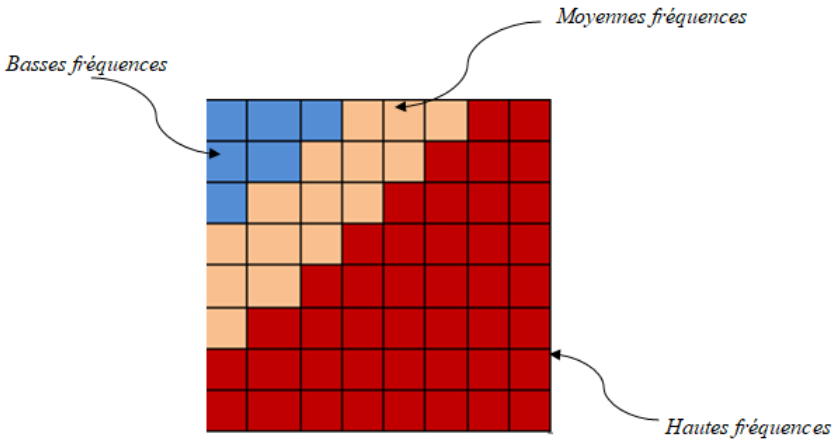

FIGURE 2.14 – Répartition des coefficients d'un bloc DCT de taille 8×8 sur trois bandes de fréquence.

La formule générale de la transformée DCT est :

$$F(u,v) = C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \times \cos\left(\frac{u\pi(2x+1)}{2N}\right) \times \cos\left(\frac{v\pi(2y+1)}{2N}\right)$$

Avec :

$$C(u) = C(v) = \begin{cases} \sqrt{\frac{1}{N}} & \text{si } u = v = 0 \\ \sqrt{\frac{2}{N}} & \text{sinon} \end{cases}$$

2.9 Les attaques et la robustesse

Pour évaluer la robustesse des algorithmes de tatouage, il est nécessaire de simuler des attaques sur les images après la phase d'insertion.[7]
Il existe deux types d'attaques contre le tatouage numérique les attaques non intentionnelles et les attaques intentionnelles.
Les attaques non intentionnelles résultent généralement des traitements usuels de l'image, tels que la réduction des dimensions ou la compression, et ne visent pas spécifiquement à supprimer, identifier ou isoler le tatouage numérique. Les attaques intentionnelles, quant à elles, sont menées dans le but de détruire le tatouage numérique, afin de falsifier l'image ou de voler les droits de propriété.
dans cette section, nous allons expliquer certaines attaques.

2.9.1 Le Filtrage

Le filtrage est une technique utilisée pour améliorer la qualité visuelle d'une image en supprimant le bruit qui peut s'y trouver. Cette méthode peut être appliquée lorsque de l'information supplémentaire (comme une marque) a été ajoutée à l'image, ou lorsqu'un bruit a été introduit dans le processus de capture de l'image. Le filtrage peut également être utilisé pour rendre une image plus douce en effectuant une opération de lissage.[21]

2.9.2 La compression

Pour garantir l'efficacité d'un système de tatouage d'image, il est important qu'il puisse résister à un certain niveau de compression. En effet, la plupart des données échangées sur les réseaux sont compressées, avec ou sans perte de données. Parmi les algorithmes de compression d'images les plus couramment utilisés se trouve le JPEG. Par conséquent, les systèmes de tatouage doivent être conçus pour être compatibles avec les algorithmes de compression courants et résister aux pertes de données potentielles engendrées par ces algorithmes.[10]

2.9.3 Rotation

Lorsque de légères rotations sont appliquées à une marque ou à un motif, cela peut rendre la marque pratiquement invisible ou difficile à détecter. Ces petites variations d'angle peuvent altérer suffisamment la forme ou l'orientation de la marque, ce qui rend plus difficile son identification ou sa reconnaissance par des techniques de détection automatique.[20]

2.9.4 L'ajout de bruit

Lorsque des images tatouées sont transmises à travers un canal bruité, du bruit peut être ajouté à l'image. Si le niveau de bruit ajouté est important, cela peut masquer la marque et rendre difficile son extraction ou sa détection.

- Les attaques qui cherchent à insérer une autre signature dans une image tatouée ne visent pas à supprimer la signature existante, mais à la remplacer par une autre pour fausser l'identification du véritable propriétaire de l'image.[21]

2.10 Évaluation des algorithmes de tatouage

2.10.1 L'erreur quadratique (MSE)

L'erreur quadratique moyenne (MSE) est une mesure qui compare deux images pixel par pixel : l'image hôte (I) et l'image tatouée (Iw).est définie par :

$$\mathrm{m_s} = \frac{1}{MN} \sum_i \sum_j \left(\mathrm{I(i,j)} - \mathrm{I_w(i,j)}\right)^2$$

Chaque pixel est comparé, avec $I(i, j)$ représentant la valeur de la luminance du pixel (i.j) de référence et Iw(i, j) la valeur du même pixel dans l'image à tester. Les deux images doivent avoir la même taille (MxN). Cette mesure nous donne une indication sur le niveau de dégradation introduit au niveau du pixel. Plus le MSE est élevé, plus la dégradation est importante.[11]

2.10.2 Le rapport signal / bruit de crête (PSNR)

Le PSNR (Peak Signal-to-Noise Ratio) est une mesure de qualité d'image qui est fonction du MSE (Mean Squared Error). Le PSNR permet de déterminer l'imperceptibilité de la signature tatouée dans l'image. En d'autres termes, il évalue la dégradation en décibels (dB) de l'image originale causée par l'insertion de la marque, ainsi que par d'autres attaques éventuelles.

Plus le PSNR est élevé, plus la qualité de l'image est proche de l'originale et moins la marque est perceptible.

- Le PSNR est définit comme suit :

$$PNSR = 10 * \log 10[(MAX^2)/MSE]$$

Le PSNR est une mesure qui compare la qualité de l'image originale à la qualité de l'image compressée ou dégradée. Une image est considérée comme robuste si elle conserve une très bonne qualité de perception visuelle, avec un PSNR supérieur à 30. En d'autres termes, plus le PSNR est élevé, plus la qualité de l'image est proche de celle de l'image originale.[18]

2.10.3 Indice de similarité structurelle (SSIM)

En ce qui concerne le domaine du tatouage numérique, Le SSIM est une mesure de similarité utilisée pour évaluer la qualité visuelle d'une image ou d'une vidéo dégradée par rapport à l'image ou la vidéo originale. et Elle prend en compte les aspects perceptifs importants tels que la luminance et le contraste, et les combine en une seule valeur appelée indice. L'indice SSIM est exprimé sous forme d'une valeur décimale comprise entre 0 et 1, où 0 représente la pire qualité visuelle possible, indiquant que le dessin de tatouage est très différent de l'original, et 1 représente une correspondance parfaite entre le design original et le dessin de tatouage dégradé.[23]
Le SSIM est calculé comme suit :

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

2.10.4 Le taux de changement des pixels (NPCR)

Le taux de changement des pixels (NPCR) est une mesure utilisée pour évaluer le nombre de pixels qui changent entre deux images, l'image tatouée par rapport à l'image originale. NPCR est une valeur normalisée entre 0 et 1.

- Un NPCR de 0 indique qu'il n'y a aucun changement entre les deux images, ce qui implique que l'image tatouée est identique à l'image originale.
- Un NPCR proche de 1 indique que la plupart des pixels ont changé, ce qui peut être un indicateur d'une bonne qualité de tatouage.[14]

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

W et H les dimension de l'image.

$$D(i,j) = \begin{cases} 0 & \text{si } (C_1(i,j) = C_2(i,j)) \\ 1 & \text{si } (C_1(i,j) \neq C_2(i,j) \end{cases}$$

2.10.5 Le coefficient de corrélation normalisé (NCC)

Le NCC (Normalized Cross-Correlation) est une métrique utilisée pour mesurer la fidélité de la marque extraite dans un système de tatouage numérique. Elle permet de quantifier la corrélation entre la marque de référence et la marque extraite, qu'il y ait eu des attaques ou non. Si la valeur de NCC est égale à 1 , cela signifie que la méthode de tatouage est valide et que la marque insérée peut être extraite fidèlement. [12]

$$\text{NCC} = \frac{\Sigma_{i=1}^{N_m} \Sigma_{j=1}^{M_m} m(i,j) * m(i,j)^*}{\Sigma_{i=1}^{N_m} \Sigma_{j=1}^{M_m} (m(i,j))^2}$$

$N_m \times M_m$: représente la taille de la marque

$m(i,j)$: les pixels de la marque d'origine

$m(i,j)^*$: les pixels de la marque extraite

2.11 Conclusion

En conclusion de ce chapitre, nous avons introduit le tatouage numérique en présentant ses concepts de base, les outils d'évaluation de performances ainsi qu'une taxonomie des techniques du tatouage selon différents critères. Ces éléments seront des éléments clés pour la suite de notre travail.

Chapitre 3

Tatouage numérique des données biomédicales dans le domaine des transformée

3.1 Introduction

Le tatouage des donnés biomédicales est très important pour assurer la confidentialité de ces images lorsqu'elles sont transmises ou stockées sur des réseaux non sécurisés.

Dans ce chapitre, nous présentons la conception et la mise en place de notre application de tatouage numérique, en offrant une vue d'ensemble détaillée des techniques et des outils utilisés dans notre travail , ainsi qu'une étude expérimentale pour évaluer les performances de notre algorithme de tatouage.

3.2 Outils utilisés

Nous avons développé notre application de tatouage numérique en utilisant le langage de programmation Python, ainsi que les bibliothèques PyWavelets, OpenCV ,PIL,Numpy ,cryptography ,Base64 et le QT Pour l'interface graphique.

3.2.1 Python

C'est le langage de programmation open source le plus utilisé dans le domaine du traitement d'images. Le langage est à la pointe de la gestion des infrastructures, de l'analyse des données et du développement de logiciels. L'un des avantages de Python est qu'il permet aux

développeurs de se concentrer sur la tâche à accomplir au lieu de la terminer. Cette approche a libéré les développeurs des limitations de syntaxe qui tourmentaient chaque jour les langages plus anciens. Par conséquent, le développement de code en Python est plus rapide que les autres langages.[8]

3.2.2 QT

Qt est une boîte à outils de widgets gratuite et open source largement utilisée pour le développement d'interfaces graphiques et d'applications multiplateformes. Qt offre une gamme complète de fonctionnalités, y compris la gestion des fenêtres, des boutons, des boîtes de dialogue, des graphiques, des contrôles de saisie, etc.[24]

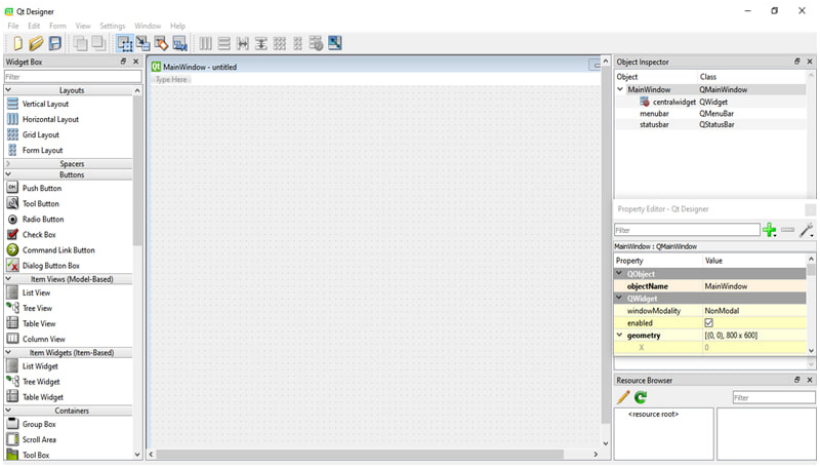

FIGURE 3.1 – Environnement QT.

3.2.3 PyWavelets

Pywt (PyWavelets) est une bibliothèque open source de transformation en ondelettes pour Python. Elle offre une interface haut niveau simple à utiliser, tout en fournissant des performances optimisées grâce à l'utilisation de codes en C et en Python de bas niveau.[8]

Pywt permet aux utilisateurs d'effectuer diverses opérations liées aux transformations en ondelettes, telles que la décomposition et la reconstruction d'une image ou d'un signal en utilisant différentes familles d'ondelettes.

3.2.4 Open cv

Open CV (Open Source Computer Vision)Cette bibliothèque fournit des fonctions avancées pour la manipulation et le traitement d'images en tant que PIL. Il est également largement

utilisé dans le domaine de la détection automatique de l'intelligence artificielle.

3.2.5 PIL

PIL (Python Imaging Library) est une bibliothèque logicielle utilisée pour manipuler et traiter efficacement des images en langage Python.[8]

PIL permet aux utilisateurs d'effectuer des opérations telles que le redimensionnement d'images, la manipulation des couleurs d'une image, l'amélioration de la qualité d'une image, la conversion de formats, l'application d'effets sur une image, et bien d'autres opérations encore.

3.2.6 Numpy

Numpy est une bibliothèque de bas niveau écrite en C (et FORTRAN) pour les fonctions mathématiques de haut niveau. Elle fournit des fonctionnalités avancées pour manipuler des tableaux et des matrices multidimensionnels, ainsi que pour effectuer des opérations mathématiques complexes.[8]

3.2.7 Cryptographie

Cryptographie est une bibliothèque de cryptographie open source. dans Python pour la sécurisation des données Elle offre des fonctionnalités pour la génération de clés, le chiffrement et le déchiffrement de données, la vérification de signatures numériques, l'authentification de messages, la gestion de certificats et bien plus encore.

3.2.8 Base64

Ce module offre des fonctionnalités permettant de convertir des données binaires en caractères ASCII imprimables, ainsi que de décoder ces encodages pour retrouver les données binaires d'origine. Il propose des fonctions d'encodage et de décodage conformes aux spécifications de la RFC 4648, qui définissent les algorithmes Base16, Base32 et Base64, ainsi qu'aux encodages Ascii85 et Base85, largement utilisés dans la pratique.[27]

3.2.9 Pycharm

Pycharm, qui a été développé par JetBrains, est un IDE spécialement conçu pour Python. Il offre une gamme d'outils utiles aux développeurs Python, tels qu'une interface conviviale, un

système de débogage avancé, un éditeur de code intelligent et des fonctionnalités de test et de débogage.

De nombreux développeurs Python expérimentés comptent sur Pycharm pour améliorer leur productivité et rendre leur travail plus efficace lors de la création d'applications Python complexes.

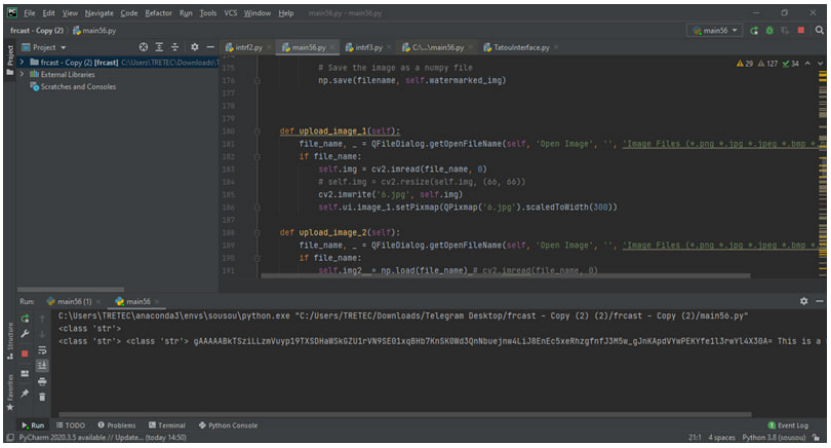

FIGURE 3.2 – Environnement de développent pycharm.

3.3 Méthode utilisé

Dans notre travail, nous avons utilisé une méthode de domaine transformé sur les images médicales numériques. Cette méthode combine la transformée en ondelettes discrètes (DWT) avec l'algorithme de chiffrement AES (Advanced Encryption Standard) pour sécuriser la marque insérée.

Dans la phase d'insertion, les marqueurs (sous forme de texte ou d'image) sont incorporés dans l'image hôte. Avant leur placement, ils sont préalablement encodés à l'aide de l'algorithme de chiffrement AES pour renforcer la sécurité. Ensuite, la DWT est appliquée à l'image hôte pour obtenir une image tatouée. Notre méthode est considérée comme semi-fragile, ce qui signifie qu'elle est robuste à certaines opérations telles que la compression, qui ne devraient pas altérer la marque.

Cependant, elle est vulnérable aux attaques malveillantes qui pourraient tenter de supprimer ou de modifier la marque pour compromettre l'intégrité des données.

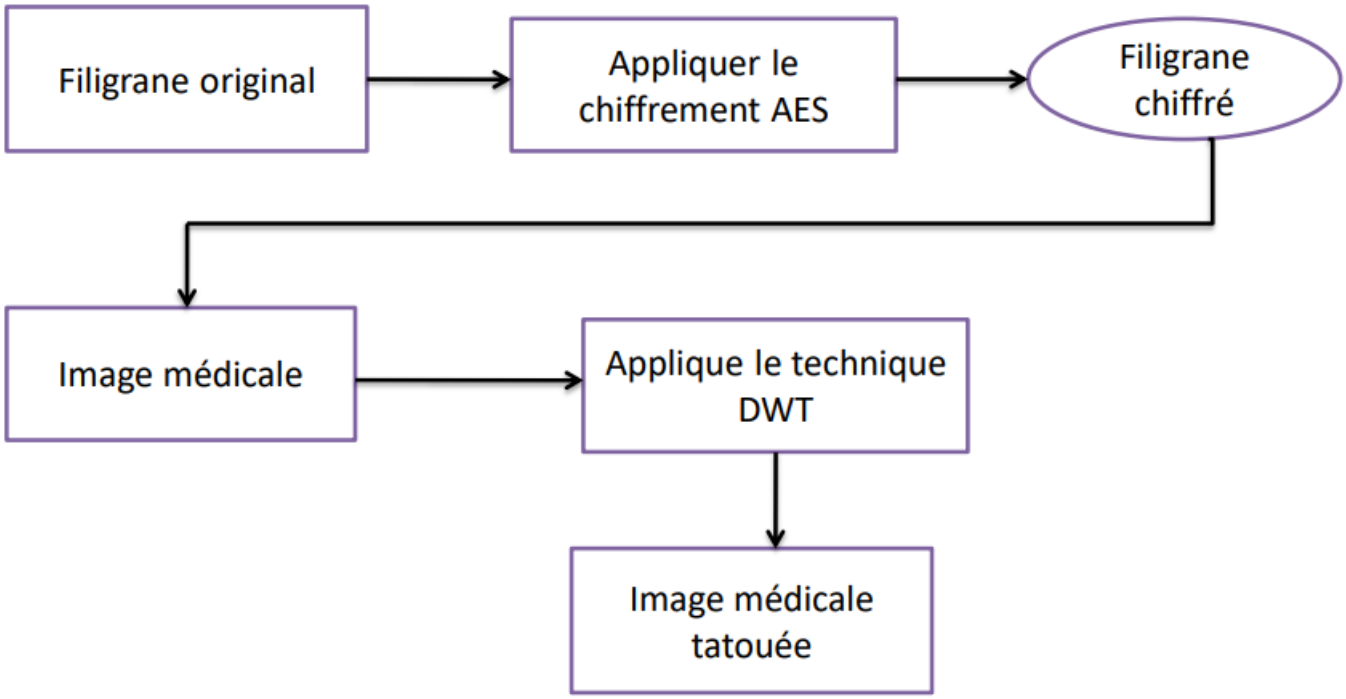

FIGURE 3.3 – Schéma explicatif pour intégration de Filigrane par DWT.

3.4 Algorithme de Chiffrement et Déchiffrement AES

Le chiffrement AES (Advanced Encryption Standard) est un algorithme de chiffrement par bloc. Il s'agit d'un algorithme de chiffrement symétrique, ce qui signifie qu'une même clé est utilisée pour chiffrer et déchiffrer les données [12]. Il utilise des clés de 128 à 256 bits pour assurer un chiffrement hautement sécurisé des données sensibles. Le chiffrement AES est essentiel pour garantir la sécurité informatique et la protection des données. [15]

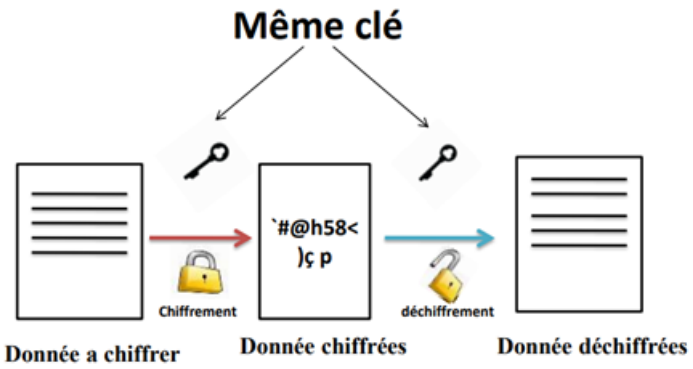

FIGURE 3.4 – cryptographie symétrique méthode AES.

3.4.1 processus de chiffrement

Pour utiliser l'algorithme AES afin de chiffrer du texte ou des images, vous pouvez suivre les étapes suivantes :

1. Génération de la clé AES : Vous devez choisir une clé secrète AES de 128, 192 ou 256 bits, en fonction du niveau de sécurité souhaité. Assurez-vous de générer une clé aléatoire et suffisamment robuste.

- Nous avons utilisé dans notre application une taille de clé 128 bit.

2. Préparation des données : Si vous chiffrez du texte, convertissez-le en une représentation binaire appropriée, comme l'encodage UTF-8. Si vous chiffrez une image, convertissez-la en un format binaire approprié, tel que PNG ou JPEG et Divisez ensuite les données que vous souhaitez chiffrer en blocs de taille fixe. La taille du bloc pour AES est de 128 bits.

3. Chiffrement des blocs de données : Appliquez l'algorithme AES à chaque bloc de données en utilisant la clé générée précédemment. Le chiffrement AES utilise différentes opérations, telles que la substitution de bytes, le décalage des lignes, le mélange des colonnes et l'ajout de clé, pour mélanger les données et les rendre crypto graphiquement sécurisées.

Les opérations de chiffrement dans AES reposent sur les quatre fonctions suivantes :

1. Block to state :est une étape supplémentaire dans le processus de chiffrement AES, qui consiste à convertir un bloc en une matrice. Après avoir divisé les données en blocs de taille fixe, chaque bloc doit être converti en une matrice d'état avant d'appliquer l'algorithme de chiffrement. L'état de la matrice est composé de lignes et de colonnes qui sont utilisées dans les opérations internes pour réaliser le chiffrement.

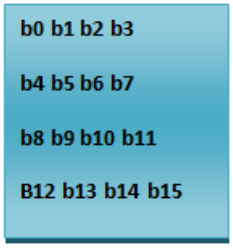

FIGURE 3.5 – state block de taille 128 bit en hexadécimale.

2. AddRoundKey :C'est une opération de OU exclusif (XOR) entre la clé de chiffrement et l'état de la matrice. Cette opération permet de combiner les bits de la clé avec les bits de l'état de manière sécurisée.

3. SubBytes :est une substitution dans laquelle chaque octet est remplacé par un autre octet sélectionné à partir d'une table particulière appelée la "Boîte-S" (S-Box en anglais). est une table de substitution fixe qui associe chaque octet d'entrée à un octet de sortie correspondant.[25]

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

FIGURE 3.6 – passage de la matrice $B_{i,j}$ dans une S-Box : transformation non-lineaire (confusion).

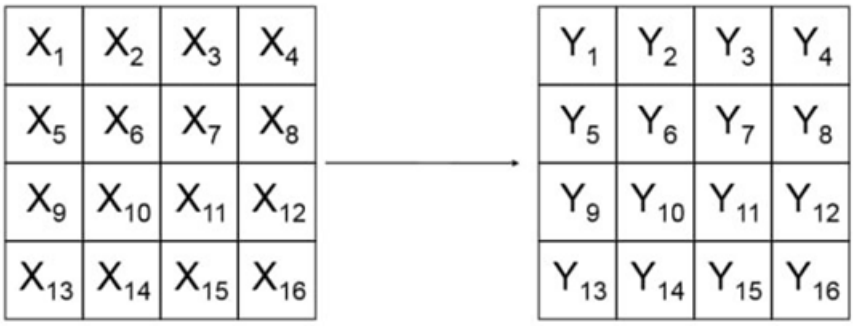

FIGURE 3.7 – passage de la matrice S-Box.

4. ShiftRows :Dans la transformation ShiftRows Shift Row (), les octets dans les trois dernières lignes de l'état sont décalés de manière cyclique sur différents nombres d'octets (offsets).[26]

   Le décalage des octets est effectué selon les règles suivantes :

   - La première ligne reste inchangée.
   - La deuxième ligne est décalée d'un octet vers la gauche.
   - La troisième ligne est décalée de deux octets vers la gauche. La quatrième ligne est décalée de trois octets vers la gauche.

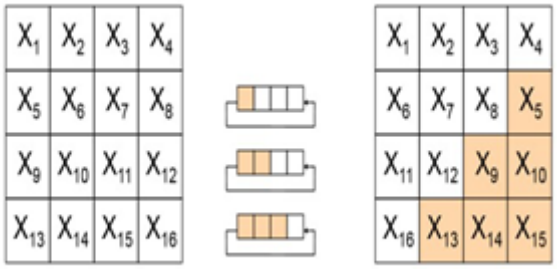

FIGURE 3.8 – décalage cyclique des trois dernières rangées de l'état.

5. MixColumns :La phase "MixColumns" dans le chiffrement AES consiste à calculer chaque colonne de sortie en multipliant une matrice constante par la colonne d'entrée correspondante. [25] qui crée un nouveau mélange des octets Chaque octet d'une colonne est remplacé par une autre valeur et chaque colonne de la matrice d'état est traitée individuellement.

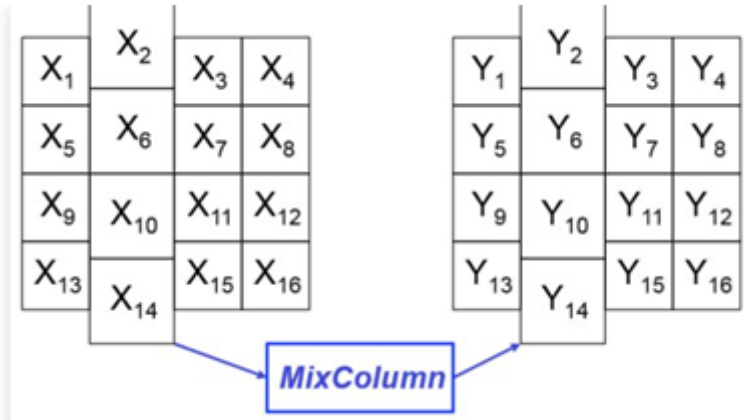

FIGURE 3.9 – matrice ShiftRows MixColumns.

Pour chaque colonne on applique une multiplication par une matrice circulante. échiffre final est obtenu en exécutant les neuf premiers tours de l'algorithme AES, qui incluent l'opération "MixColumns", suivis du dixième tour sans l'opération "MixColumns". Cette étape finale permet d'obtenir le texte chiffré qui peut ensuite être utilisé pour le déchiffrement. [25]

3.4.2 processus de déchiffrement AES

Après le chiffrement d'un message avec l'algorithme AES, le processus de déchiffrement consiste à appliquer les opérations inverses des fonctions de chiffrement dans l'ordre inverse .

en commençant par "InvMixColumns", suivi de "InvSubBytes" et "InvShiftRows".

La fonction "AddRoundKey" reste inchangée.

Ce processus inverse permet de récupérer les données d'origine à partir du texte chiffré.

- InvSubBytes : la Transformation InvSubBytes() dans AES est l'inverse de la transformation de substitution d'octets. Elle utilise la S-Box inverse, obtenue en appliquant l'inverse de la transformation affine suivie de l'inverse multiplicatif, pour remplacer chaque octet de l'état par un octet spécifique. Cela permet de restaurer les valeurs d'octets d'origine avant le chiffrement.

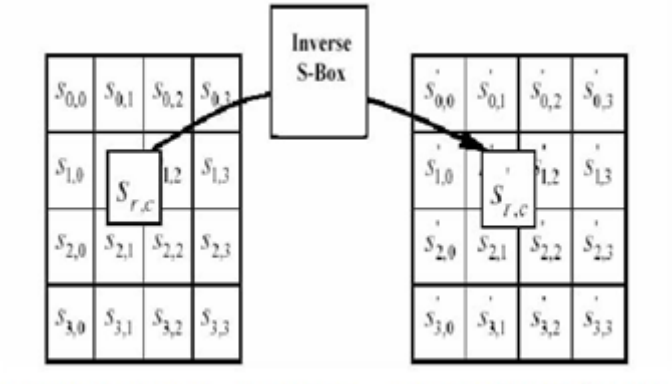

FIGURE 3.10 – Application de la boite S inverse à chaque octet de l'État.

Inverse S-box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
70	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

FIGURE 3.11 – valeurs S-BOX inverses pour toutes les 256 combinaisons en format hexadécimal.

- InvShiftRows : les octets des trois dernières lignes de l'état subissent un décalage cyclique sur différents nombres d'octets. La première rangée (r = 0) n'est pas décalée. Les trois rangées inférieures sont décalées.

  La transformation InvShiftRows() est réalisée comme suit :

  — La première rangée ($r = 0$) n'est pas décalée, elle reste inchangée.

  — La deuxième rangée ($r = 1$) subit un décalage cyclique de Nb-shift(1, Nb) octets vers la droite.

— La troisième rangée ($r = 2$) subit un décalage cyclique de Nb-shift(2, Nb) octets vers la droite.

— La quatrième rangée ($r = 3$) subit un décalage cyclique de Nb-shift(3, Nb) octets vers la droite.

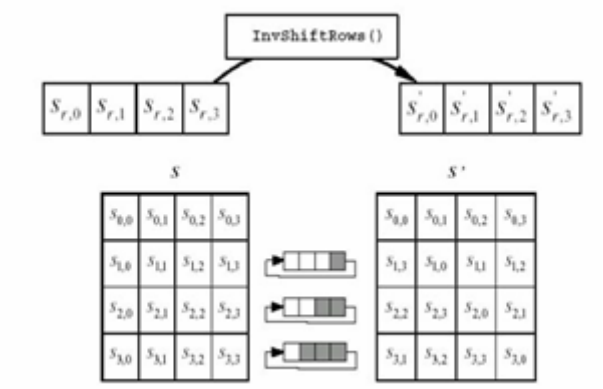

FIGURE 3.12 – décalage cyclique inverse des trois dernière rangées de l'État.

Voici le résultat de chiffrement du texte :

FIGURE 3.13 – Capture d'écran du résultat de chiffrement du texte.

3.5 Algorithme d'insertion

1. Lire l'image hôte et la marque insérée (qu'elle soit un texte ou une image).
2. Chiffrer la marque insérée avec le chiffrement AES.
3. Appliquer la transformation d'ondelette discrète (DWT).
4. Calculer la taille de bloc LL pour insérer la chaîne binaire.

5. Le message est ensuite converti en une séquence binaire (chaîne binaire) de bits (chaque caractère étant représenté par 8 bits).

   • Si la marque est une image, on convertit l'image en binaire avec la fonction image-to-binary et on l'insère dans les coefficients d'approximation (LL) de l'image hôte.

6. Les bits du message sont insérés en modifiant le bit de poids faible de chaque pixel de l'image.

7. Appliquer la transformée inverse de la DWT pour reconstruire l'image.

8. la résultante est une image tatouée .

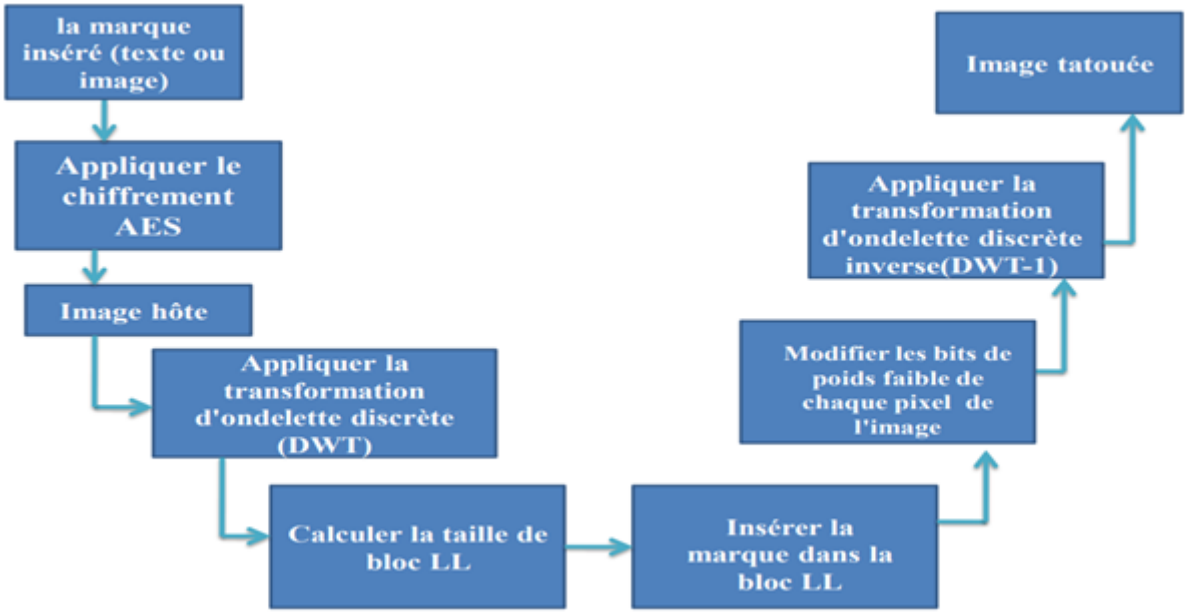

FIGURE 3.14 – Organigramme d'insertion du tatouage.

Pour insérer le watermark, nous avons utilisé la fonction Embed-watermark.

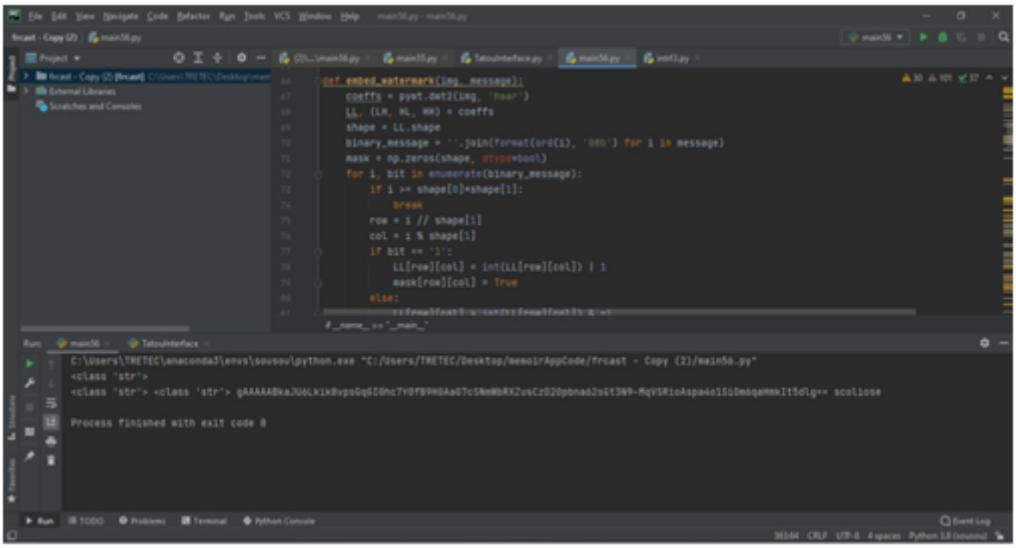

FIGURE 3.15 – Capture d'écran de la fonction utilisée 'Embed-watermark'.

3.5.1 Embed-watermark

La fonction permet d'intégrer un message ou une image dans une image donnée. Elle prend deux paramètres en entrée : "img", qui représente l'image de base, et "watermark", qui représente le message ou l'image à intégrer Pour commencer, la fonction applique la transformation en ondelettes discrètes (DWT) à l'image "img" en utilisant le filtre de Haar, à l'aide de la fonction pywt.dwt2.L'image hot décomposée comprend plusieurs niveaux, comprenant les approximations de résolution (LL) à différents niveaux et les détails (HL, LH, HH) correspondants. Ensuite, le message est converti en une représentation binaire en utilisant le format (ord(i), '08b'), où chaque caractère ou pixel est représenté par une séquence de 8 bits. La fonction parcourt ensuite la représentation binaire de chaque caractère ou pixel du watermark. Si un bit est égal à 1, la fonction modifie la valeur correspondante de l'élément "LL" en utilisant l'opération int(LL[row][col]) | 1. De plus, la fonction enregistre la valeur True à l'emplacement correspondant dans une matrice appelée "mask", qui a la même taille que "LL". Une fois que "LL" a été modifié et que "mask" a été créé, les coefficients modifiés sont reconstruits en utilisant l'inverse de la transformation en ondelettes discrètes (IDWT), avec la fonction pywt.idwt2, à nouveau en utilisant la transformation de Haar. Enfin, la fonction renvoie l'image modifiée ainsi que le masque "mask". Cela permet de récupérer l'image avec le watermark intégré et de savoir quelles parties de l'image ont été modifiées

3.6 Algorithme d'extraction

Voici les étapes de l'algorithme d'extraction de manière claire.

1. Lire l'image originale et l'image tatouée.
2. Appliquer la transformation en ondelettes discrètes (DWT).
3. Identifier le niveau LL (approximatifs) qui contient le tatouage en examinant les coefficients d'ondelettes.
4. Pour extraire la marque de l'image, il y a deux cas :
   - Si le watermark est un texte, alors le dernier bit de l'image tatouée doit être égal à "1". en extrayant le bit de poids le moins significatif LSB de chaque pixel. Déchiffrer les bits extraits en utilisant l'algorithme de chiffrement AES avec la clé secrète. Le texte caché peut ensuite être extrait en utilisant le code ASCII.
   - Si le watermark est une image, alors le dernier bit de l'image tatouée doit être égal à "0". Extraire les bits du watermark à partir de LL en extrayant le bit de poids le moins significatif LSB de chaque pixel. Ensuite, on obtient une chaîne binaire qu'on déchiffre avec AES et qu'on transforme en image avec la fonction "binary-to-image".

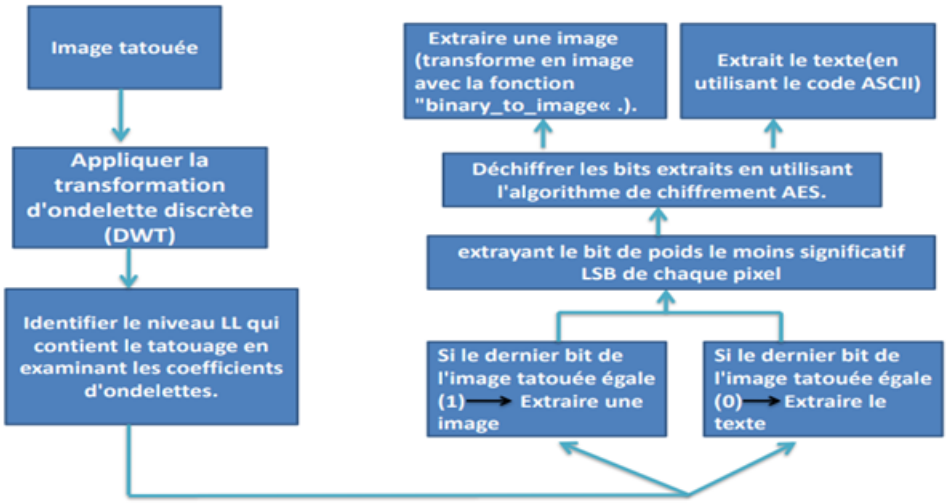

FIGURE 3.16 – Organigramme d'extraction du tatouage.

- Pour extraire le watermark, nous avons utilisé la fonction extract-watermark .

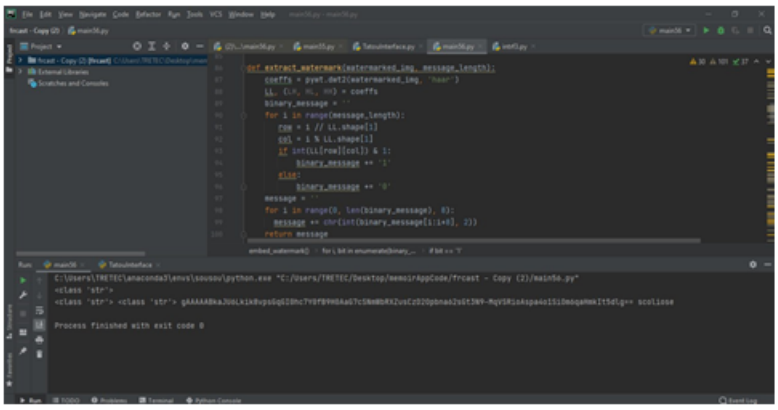

FIGURE 3.17 – Capture d'écran de la fonction utilisé ' Extract-watermark'.

3.6.1 Extract-watermark

La fonction "extract-watermark" est utilisée pour extraire le watermark d'une image tatouée en utilisant la transformée en ondelettes (Wavelet Transform) . cette fonction Elle prend deux paramètres en entrée :

— "watermarked-img", qui représente l'image modifiée à partir de laquelle le watermark doit être extrait.

— "message-length", qui indique la longueur du message à extraire en nombre de caractères.

Dans un premier temps, la fonction applique la DWT à l'image "watermarked-img" en utilisant la fonction pywt.dwt2. pour la décomposition de l'image tatouée on quatre sous-bandes de représentation fréquentielle (LL,LH,HL,HH) Ensuite, la fonction initialise une chaîne de caractères appelée "binary-message" qui servira à stocker la représentation binaire du watermark extrait. Elle parcourt les premiers éléments du tableau "LL" en fonction de la taille de celui-ci. Pour chaque élément, la fonction vérifie si le dernier bit est égal à 1 en utilisant l'opération int(LL[row][col]) & 1, et ajoute '1' à la chaîne "binary-message" si le bit est égal à 1, sinon elle ajoute '0'. Par la suite, la fonction initialise une autre chaîne de caractères appelée "message" qui servira à stocker le message extrait. Elle parcourt la chaîne "binary-message" par groupes de 8 bits et les convertit en caractères en utilisant la fonction chr(int(binary-message $[i : i+8], 2)$). Ces caractères sont ajoutés à la chaîne "message".

Enfin, la fonction renvoie la chaîne "message" qui correspond au watermark extrait.

3.7 Présentation de l'application réalisée

3.7.1 Interface graphique

FIGURE 3.18 – Interface graphique de l'application.

Notre application dispose d'une interface simple et conviviale comprenant 6 boutons.

Les boutons "Select image" et "upload " permettent d'importer une image qui sera affichée dans une zone dédiée. Deux zones de texte sont également présentes, l'une pour entrer le watermark à insérer et l'autre pour afficher le résultat d'extraction.

Si le watermark est un texte, il peut être saisi directement. Si le watermark est une image, il suffit de cliquer sur le bouton "Add image", puis sur le bouton "Add Watermark" pour intégrer le watermark à l'image. En cliquant sur le bouton "Save", il est possible de sauvegarder le résultat.Le bouton "Extract

3.7.2 Processus d'insertion du tatouage

Pour insérer une marque, nous débutons par sélectionner une image, puis écrire le texte dans la zone de texte ou ajouter une image en cliquant sur le bouton "Add image". Nous poursuivons ensuite en choisissant l'option "Add watermark" pour démarrer l'opération.

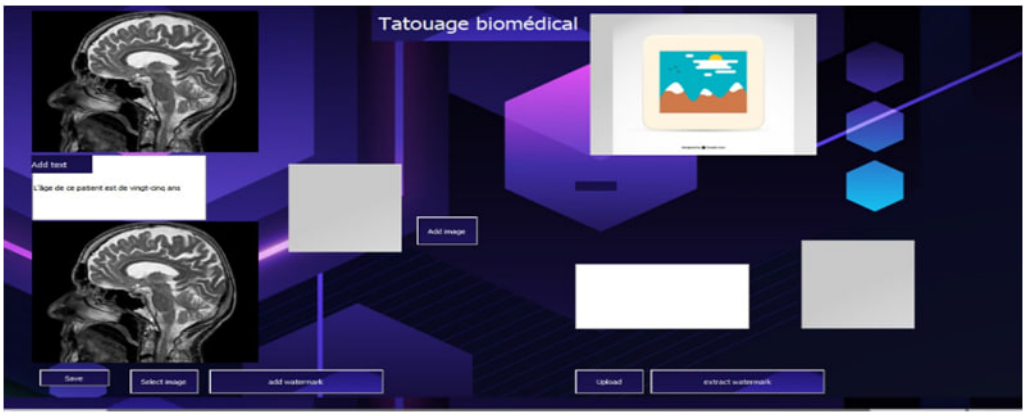

FIGURE 3.19 – Interface graphique de l'application lors l'insertion du tatouage (text dans une image).

FIGURE 3.20 – Interface graphique de l'application lors l'insertion du tatouage(image dans une image).

3.7.3 Processus d'extraction du tatouage

Pour extraire la marque, commencez par télécharger l'image tatouée à l'aide du bouton de "upload ", puis cliquez sur "Extracte watermark " si celle-ci est du texte. Le début de l'opération et le message seront affichés dans la zone de texte. Si la marque est une image, une petite vignette sera affichée.

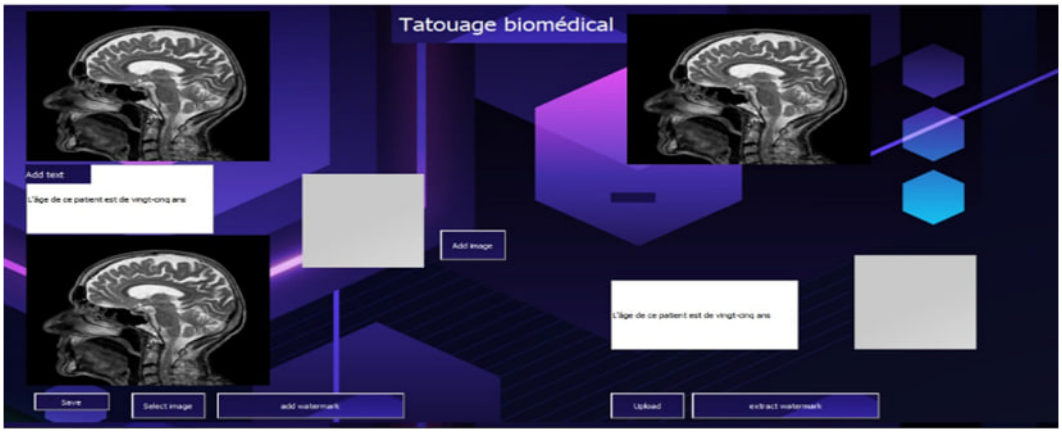

FIGURE 3.21 – Interface graphique de l'application lors l'extraction du tatouage(text dans une image).

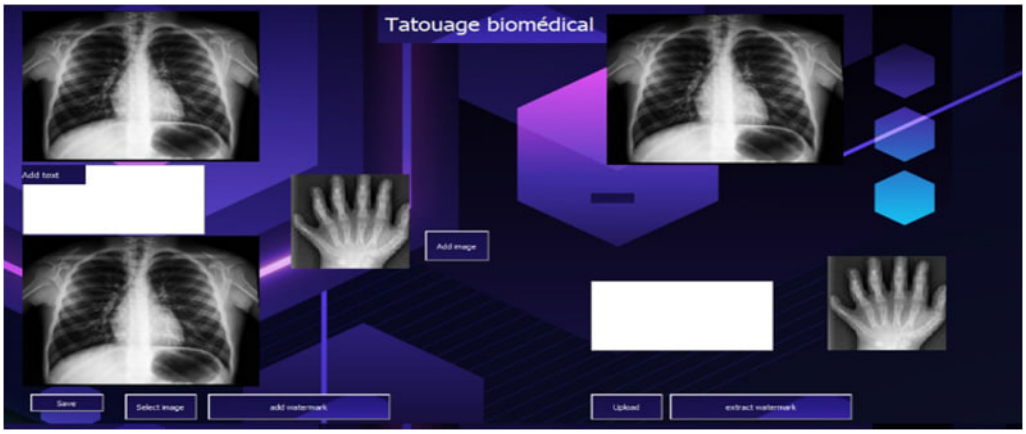

FIGURE 3.22 – Interface graphique de l'application lors l'extraction du tatouage(image dans une image).

3.8 Résultat obtenu

Nous avons appliqué une technique de tatouage numérique invisible pour dissimuler un texte à l'intérieur d'une image, ou une autre image à l'intérieur de l'image d'origine. Cette technique offre un compromis entre l'imperceptibilité et la robustesse du système de tatouage, garantissant ainsi la sécurité et l'intégrité des données. De plus, elle assure la préservation de la qualité de l'image sans altération visible. Enfin, il est possible d'extraire en toute sécurité la marque de reconnaissance afin de vérifier son imperceptibilité et sa robustesse.

3.8.1 Propriété d'imperceptibilité

Notre méthode garantit l'imperceptibilité en testant plusieurs images médicales de tailles différentes qui sont tatouées avec du texte et des images similaires. Les résultats obtenus

confirment l'imperceptibilité de notre technique de tatouage numérique.

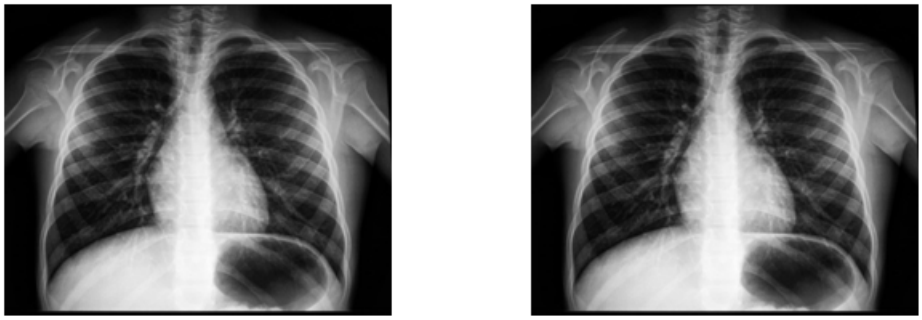

FIGURE 3.23 – Comparaison entre Images (texte dans une image).

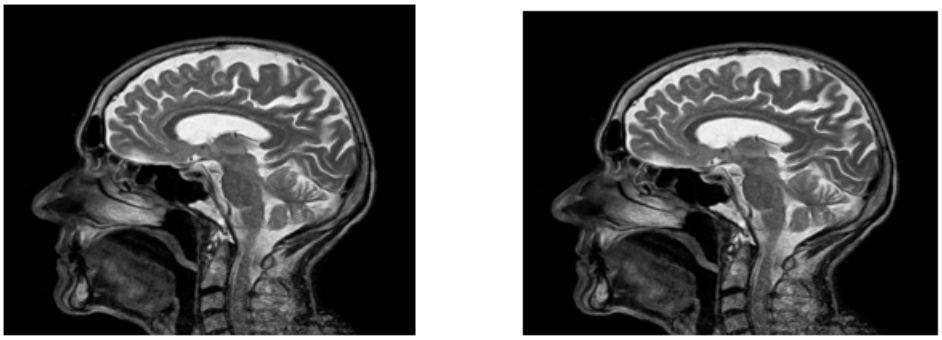

FIGURE 3.24 – Comparaison entre Images(image dans l'image).

En se basant sur notre observation de l'image hôte et de l'image tatouée, il est difficile de faire la distinction entre l'image originale et l'image tatouée. De plus, le marquage n'est pas visible et l'image d'origine demeure identique à l'image initiale grâce à leur similitude, sans qu'aucune différence ne soit perceptible à l'œil humain. Nous utilisons la métrique d'évaluation PSNR pour quantifier la qualité et la similarité entre les deux images.

Image médicale pour	Taille	PSNR
le système nerveux	$1280 * 1024$	58.33
L'épaule	$1280 * 24$	52.46
La main	$761 * 1280$	49.11
Cage thoracique	$60 * 60$	INFINI
Colonne vertébrale	$60 * 60$	INFINI
Le dos	$60 * 60$	36.53

TABLE 3.1 – Mesures de la qualité d'images tatouée

3.9 Intégrité

Dans notre méthode de tatouage pour les images médicales, nous visons à assurer l'intégrité des données, qu'elles soient sous forme d'images ou de texte. Cela se reflète dans le calcul du PSNR (Peak Signal-to-Noise Ratio), où nous observons une valeur de PSNR qui tend vers l'infini. Cela garantit la sécurité des données insérées et confirme leur intégrité.

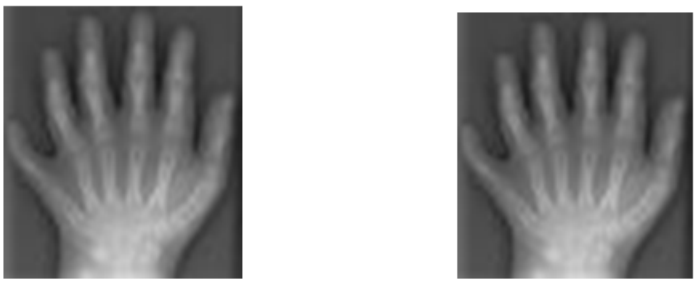

FIGURE 3.25 – Comparaison entre Images (image (A) entrées et image (B) sorties).

3.10 Capacité

En général, La capacité de notre approche corresponds aux nombre de coefficients LL modifiables divisé par 8 vu que noue ne modifions que le dernier bits le moins significatif du coefficients.

$$\text{Capacité} = (Nombre\ de\ coefficients\ LL\ modifiables)/8$$

.

Il est important de noter que cette formule suppose que chaque coefficient LL est représenté par 8 bits (1 octet) et que nous ne modifions qu'un seul bit par coefficient. Si les coefficients LL sont représentés par un nombre différent de bits, la formule devrait être adaptée en conséquence. De plus, d'autres facteurs tels que la taille de l'image et les contraintes de codage peuvent également affecter la capacité réelle du tatouage.

3.11 Conclusion

Ce chapitre traite des outils et des méthodes utilisés dans le développement de notre application. Nous avons ensuite détaillé la phase de listage et la phase d'extraction, qui dépend

de la technologie DWT utilisée pour sécuriser les images médicales et la technologie de cryptage AES utilisée pour chiffrer le filigrane. Enfin, nous avons discuté et présenté les résultats obtenus.

Conclusion générale

Avec le développement des réseaux de communication et des technologies Internet, les risques auxquels les données, les fichiers et les images médicale numériques sont confrontés ont augmenté, ce qui rend leur protection indispensable. Parmi les mesures pouvant être prises pour améliorer la sécurité des données et les protéger, l'utilisation de la technique de tatouage numérique est une méthode efficace pour protéger les données numériques et les sécuriser contre les intrusions non autorisées.

Cependant, parfois les données sont compromises et l'accès au tatouage numérique est obtenu. Notre objectif est de protéger les données médicales en suivant quelques étapes nécessaires : le tatouage numérique doit être solide et répondre aux normes de résistance et d'imperceptibilité pour garantir la sécurité et l'intégrité et la confidentialité des images et des données médicales.

Notre travail prend en compte l'importance de l'équilibre entre la qualité visuelle des images tatouées et leur résistance aux attaques potentielles, tout en mettant l'accent sur le maintien et l'amélioration de la qualité des images tatouées pour qu'elles puissent résister à une utilisation quotidienne et à des facteurs externes qui pourraient les affecter.

Nous avons concentré nos efforts sur le développement de la technologie de tatouage numérique en utilisant la transformation en ondelettes discrètes (DWT) pour décomposer les images médicales et utiliser l'algorithme de cryptage symétrique AES pour crypter le watermark. Cette technique de cryptage est principalement utilisée pour garantir la confidentialité des informations figurant dans l'image après son envoi et la protéger contre toute divulgation non autorisée.

Les résultats de l'évaluation ont montré des résultats satisfaisants, ce qui signifie que notre approche est hautement sécurisée et efficace. Les objectifs futurs de notre travail pourraient être les suivants :

- Améliorer et développer les techniques de cryptage d'images pour les rendre plus efficaces

et plus sûres.

- Améliorer notre algorithme pour permettre son utilisation dans la technologie de tatouage vidéo.

Bibliographie

[1] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, "A robust blind medical image watermarking approach for telemedicine applications," Cluster Comput, vol. 24, no. 3, pp. 2069–2082, Sep. 2021, doi : 10.1007/s10586-020-03215-x.

[2] Bekkouche.S,Tatouage appliqué à l'Imagerie Médicale,Faculté des Sciences,Département d'Informatique,UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE d'ORAN Mohamed Boudiaf,2011/2012.

[3] Mohamed Belahreche,Application des Ondelettes pour le Tatouage Numérique des Images, FACULTE DE TECHNOLOGIE,DEPARTEMENT D'ELECTRONIQUE,UNIVERSITE FERHAT ABBAS DE SETIF - 01,juin 2015.

[4] K. Amine, K. Fares, K. M. Redouane, and E. Salah, "Medical Image Watermarking for Telemedicine Application Security," J CIRCUIT SYST COMP, vol. 31, no. 05, p. 2250097, Mar. 2022, doi :10.1142/S0218126622500979.

[5] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, "A lossless DWT-SVD domain watermarking for medical information security," Multimed Tools Appl, vol. 80, no. 16, pp. 24823–24841, Jul. 2021, doi : 10.1007/s11042-021-10712-7.

[6] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, "A DWT-SVD based robust digital watermarking for medical image security," Forensic Science International, vol. 320, p. 110691, Mar. 2021, doi : 10.1016/j.forsciint.2021.110691.

[7] KISSOUM Farida,ROUIFED Chahira,Watermarking et compression d'images numériques : Applications aux images médicales,FACULTE DE GENIE ELECTRIQUE ET DE L'INFORMATIQUE DEPARTEMENT D'ELECTRONIQUE UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU,2011/2012.

[8] K. Amine, K. Redouane, and M. Bilel, “A redundant wavelet based medical image watermarking scheme for secure transmission in telemedicine applications,” Multimed Tools Appl, Aug. 2022, doi : 10.1007/s11042-022-13649-7.

[9] A.Khaldi, M. R. Kafi, and M. S. Moad, “Wrapping based curvelet transform approach for ECG watermarking in telemedicine application,” Biomedical Signal Processing and Control, vol. 75, p. 103540, May 2022, doi : 10.1016/j.bspc.2022.103540.

[10] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, “A DWT based watermarking approach for medical image protection,” J Ambient Intell Human Comput, vol. 12, no. 2, pp. 2931–2938, Feb. 2021, doi : 10.1007/s12652-020-02450-9.

[11] BOUCHAMA Samira,Le tatouage des images Appliqué à l’imagerie médicale ,DEPARTEMENT D’ELECTRONIQUE,ECOLE NATIONALE POLYTECHNIQUE,2007.

[12] TRACHE Nadjia,Sécurisation de la transmission de l’information par les techniques du tatouage robuste et applications,Faculté : Génie Electrique ,Département : Electronique,Université des sciences et technologies d’Oran Mohamed Boudiaf.

[13] K. Fares, A. Khaldi, K. Redouane, and E. Salah, “DCT DWT based watermarking scheme for medical information security,” Biomedical Signal Processing and Control, vol. 66, p. 102403, Apr. 2021, doi : 10.1016/j.bspc.2020.102403.

[14] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, “A lossless DWT-SVD domain watermarking for medical information security,” Multimed Tools Appl, vol. 80, no. 16, pp. 24823–24841, Jul. 2021, doi : 10.1007/s11042-021-10712-7.

[15] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane, and S. Euschi, “A DWT-SVD based robust digital watermarking for medical image security,” Forensic Science International, vol. 320, p. 110691, Mar. 2021, doi : 10.1016/j.forsciint.2021.110691.

[16] Bekkouche Souad,Tatouage appliqué à l’Imagerie Médicale ,Faculté des Sciences, Département d’Informatique, UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE d’ORAN Mohamed Boudiaf,2011/2012.

[17] E.-H. GOLEA, “Tatouage numérique des images couleurs rgb.” Ph.D. dissertation, Université de Batna 2, 2010.

[18] Chokri Chemak,"Algorithme de Tatouage Robuste et Aveugle pour la Déontologie et le Transfert des Informations Médicales : "Le Tatouage Combinée " ATRADTIM",Université de Franche-ComtéU.F.R Sciences et Techniques,2006.

[19] M. S. Moad, M. R. Kafi, and A. Khaldi, “Medical image watermarking for secure e-healthcare applications,” Multimed Tools Appl, May 2022, doi : 10.1007/s11042-022-12004-0.

[20] BELILITA Sarra,"Développement et Implémentation d’algorithmes de tatouage robustes des images fixes et vidéo",FACULTÉ DE TECHNOLOGIE,Filière : Electronique ,UNIVERSITÉ FERHAT ABBAS - SETIF1,2019.

[21] M. Farouk ZEHDA,Tatouage d’images basé sur des transformées discrètes entières ,Faculté de Technologie ,Département dÉlectronique,UNIVERSITE FERHAT ABBAS – SETIF 1–UFAS (ALGERIE),2014.

[22] A. Khaldi, M. R. Kafi, and B. Meghni, “Electrocardiogram signal security by digital watermarking,” J Ambient Intell Human Comput, Jul. 2022, doi : 10.1007/s12652-022-04101-7.

[23] Mustafa OTHMAN,Objective video quality metric aware Adaptation mechanisms for video streaming based on DASH,’Université Sorbonne Paris Nord,2021.

[24] Wikipédia, “Qt — wikipédia, l’encyclop´edie libre,” 2023, [En ligne ; Page disponible le 30-mai-2022]. [Online]. Available : http ://fr.wikipédia.org/w/index.php ?title=Qt &oldid=170935077.

[25] M. M. Sayah, K. M. Redouane, and K. Amine, “Secure transmission and integrity verification for color medical images in telemedicine applications,” Multimed Tools Appl, May 2022, doi : 10.1007/s11042-021-11791-2.

[26] M. S. Moad, M. R. Kafi, and A. Khaldi, “A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications,” Microprocessors and Microsystems, vol. 90, p. 104490, Apr. 2022, doi : 10.1016/j.micpro.2022.104490.

[27] https ://docs.python.org/fr/3/library/base64.html.

[28] Mayssa Tayachi, Sécurité des images par tatouage numérique et cryptographie dans les applications médicales.Cryptographie et sécurité [cs.CR], Université de Bretagne occidentale - Brest ; Université de Tunis El Manar, 2021. Français.

[29] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, “Robust SVD-based schemes for medical image watermarking,” Microprocessors and Microsystems, vol. 84, p. 104134, Jul. 2021, doi : 10.1016/j.micpro.2021.104134.

[30] F. Kahlessenane, A. Khaldi, M. R. Kafi, and S. Euschi, “A color value differentiation scheme for blind digital image watermarking,” Multimed Tools Appl, vol. 80, no. 13, pp. 19827–19844, May 2021, doi : 10.1007/s11042-021-10713-6.

[31] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane, and S. Euschi, "An SVD Values Ordering Scheme for Medical Image Watermarking," Cybernetics and Systems, vol. 53, no. 3, pp. 282–297, Feb. 2022, doi :10.1080/01969722.2021.1983700.

[32] CHIKH- A.B et A.E,La Méthode des ondelettes et ses applications,DEPARTEMENT DE CONSTRUCTION,UNIVERSITE SAAD DAHLAB - BLIDA 1,Octobre 2014.