République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 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 I 'obtention du diplome Master

Titre :

Sécurité Des Données Biomédicales Echangées en Télémédecine

Par :

- BEN CHEIKH Hana
- BOUZAINE Khaira

Soutenue publiquement le 14 Juin 2023

Devan le jury :

- Encadreur : A. KHALDI
- Président : Mr Kahlessenane Fares
- Examinateur : Mr Euschi Salah

Année Universitaire 2022/2023

DEDICACES

À celle que je préfère à moi-même, et pourquoi pas,

Elle s'est sacrifiée pour moi et n'a ménagé aucun effort pour toujours me rendre heureux.

Ma chère mère, que Dieu prolonge sa vie

À mes sœurs qui ont eu un grand impact sur de nombreux obstacles et difficultés

À mes amis, et à tous ceux qui se sont tenus à mes côtés et m'ont aidé avec tout ce qu'ils avaient, et sous de nombreux aspects,

Je vous présente cette recherche

Bouzaine

Khaira

DEDICACES

A celui qui m'a donné sa vie et m'a donné son sourire

Au plus grand homme de ma vie

Mon père bien-aimé

Aux yeux qui sont restés éveillés la nuit pour reposer mes yeux

A qui les mots ne remplissent pas leur droit

A la fleur de violette qui embellissait ma vie et parfumait mes matins

Ma chère mère

À ceux d'entre eux plus grands et sur eux s'appuyaient

Aux partenaires de la route dans mes peines

Et partage avec moi le bonheur de ma réussite

A ceux dont la présence dans ma vie était comme un millier amis

A mes chers frères : Djamel Eddine, Abdelhak

et à mon cher : Achraf.

Et mes sœurs : Fatima, Asma, la femme de mon frère : Bouchra

A toute ma famille élargie : BEN CHEIKH et BETTAYEB

En fin de compte, je le dédie aux personnes qui ont contribué

De près ou de loin pour développer ce travail

BenCheikh

Hana

Remerciements

Tout d'abord, nous voulons remercier Allah le tout puissant de nous avoir donné la force, la connaissance,

La capacité et l'opportunité d'entreprendre ces. Louange à Allah.

Nous tiendrons à exprimer mes vifs remerciements à mon directeur de thèse,

Dr KHALDI AMINE, MERCI.

Nous tiendrons à remercier sincèrement les membres du jury pour l'honneur qu'ils me font en Acceptant de juger et d'évaluer mon travail, ainsi qu'aux professeurs du département d'informatique.

Résumé

La télémédecine s'appuie sur une infrastructure d'échange d'informations numériques. Bien que les progrès récents des technologies de l'information offrent de nouvelles façons d'accéder, de gérer et de transférer des informations médicales, ils constituent également une menace pour sa sécurité en raison de leur vulnérabilité à la manipulation et à la réplication. En outre, l'authentification et la protection du droit d'auteur sont nécessaires pour protéger la déformation et la reproduction illégales des données d'informations médicales. Dans cette mémoire, nous proposons une technique de tatouage numérique pour l'image médicale et pour sécuriser les données des patients lorsqu'elles sont transmises dans un canal non sécurisé. La technique semi-fragile proposée combine les transformations DWT et DCT avec Utiliser un code QR comme filigrane et l'intégrer par la technologie LSB. Cela permet d'obtenir un degré élevé de vérification et une meilleure sécurité des données médicales. Nous avons implémenté notre approche en utilisant le langage de programmation Python. En outre, discuter de différents résultats expérimentaux et les comparer avec les résultats d'autres techniques

Mots clés : images médicales, sécurité, tatouage numérique, Python.

Abstract

Telemedicine relies on an infrastructure for exchanging digital information. Although recent advances in information technology offer new ways to access, manage and transfer medical information, they also pose a threat to its security due to their vulnerability to manipulation and replication. In addition, authentication and copyright protection are necessary to protect the illegal distortion and reproduction of medical information data. In this thesis, we propose a digital watermarking technique for the medical image and to secure patient data when transmitted in an unsecured channel. The proposed semi-fragile technique combines DWT and DCT transformations with Using a QR code as a watermark and integrating it by LSB technology. This allows for a high degree of verification and better security of medical data. We implemented our approach using the Python programming language. Also, discuss different experimental results and compare them with the results of other techniques

Keywords: medical images, security, watermarking, Python.

الملخص

يعتمد الطب عن بعد على بنية تحتية لتبادل المعلومات الرقمية. على الرغم من أن التطورات الحديثة في تكنولوجيا المعلومات توفر طرقًا جديدة للوصول إلى المعلومات الطبية وإدارتها ونقلها ، إلا أنها تشكل أيضًا تهديدًا لأمنها بسبب ضعفها أمام التلاعب والتكرار. بالإضافة إلى ذلك ، فإن المصادقة وحماية حقوق النشر ضرورية لحماية التشويه والاستنساخ غير القانونيين لبيانات المعلومات الطبية. في هذه الرسالة ، نقترح تقنية العلامة المائية الرقمية للصورة الطبية ولتأمين بيانات المريض عند إرسالها في قناة غير آمنة. تجمع التقنية شبه الهشة المقترحة بين تحويلات DWT و DCT مع استخدام رمز QR كعلامة مائية ودمجها بواسطة تقنية LSB. هذا يسمح بدرجة عالية من التحقق وأمان أفضل للبيانات الطبية. طبقنا نهجنا باستخدام لغة برمجة بايثون. ناقش أيضًا النتائج التجريبية المختلفة وقارنها بنتائج التقنيات الأخرى

الكلمات المفتاحية: صور طبية ، أمن ، علامة مائية ، بايثون.

LISTE DES FIGURES

CHAPTER.I: Etude bibliographique de la télémédecine et les images médicales

CHAPTER.II : Le tatouage pour la sécurité des données médicales

CHAPTER III : Approche proposée et implémentation

LISTE DES TABLEAUX

CHAPTER.II : Le tatouage pour la sécurité des données médicales

CHAPTER III : Approche proposée et implémentation

GLOSSAIRE

dB	Decibels
bpp	Les bits par pixel
DCT	La transformée discrète en cosinus
DFT	La transformée de Fourier discrète
DME	Les dossiers médicaux électroniques
DOC	Document
DPI	Points par pouce
DSE	Dossiers de santé électroniques
DWT	La transformée discrète en ondelettes
Eq	Équation
FFT	La transformation de Fourier rapide
EHR	Electronic Health Record
GDPR	Règlement Général sur la Protection des Données
HF	Haute fréquence
HH	Des détails haute fréquence de l'image
HL	Des détails horizontaux de l'image
HIPAA	Loi sur la transférabilité et la responsabilité de l'assurance maladie
HIS	Les systèmes d'information hospitaliers
HVS	Les systèmes visuels humains
IDCT	L'inverse de transformée discrète en cosinus
IDFT	L'inverse de transformée de Fourier discrète
IDWT	L'inverse de transformée discrète en ondelettes
ILSB	L'inverse de bit le moins significatif (LSB)
LF	Basse fréquence
LH	Des détails verticaux de l'image
LL	Des détails basse fréquence de l'image
LSB	Bit le moins significatif
MF	Moyenne fréquence
MSB	Bit le plus significatif
NC	Analyse de corrélation normalisée
PACS	Les systèmes d'archivage et de communication d'images
PDF	Portable Document Format
PHI	Les informations de santé protégées
PPCM	Les pixels par centimètre
PPI	Pixels par pouce
PSNR	Peak signal noise ration
RIS	Les systèmes d'information radiologique
RVB	Rouge-Vert-Bleu
SS	L'étalement de spectre
QR	Code à réponse rapide

TABLE DES MATIÉRES

TABLE DES MATIÉRES

INTRODUCTION GÉNÉRALE

Au cours des dernières années, la technologie des réseaux a connu un grand développement et une amélioration dans différents domaines. Le domaine principal qui influence l'avancement des personnes est Internet. Internet devient une colonne vertébrale dans notre vie quotidienne. C'est une solution simple et rapide pour accéder, fournir, utiliser des services et échanger des données multimédias (textes, images, audios et vidéos) entre différents sites. Cependant, le déplacement des services et des données via Internet a révélé de nombreux problèmes de sécurité, en particulier sur l'intégrité et l'authenticité des données de l'utilisateur. D'autre part, l'une des principales préoccupations dans le monde est de développer la qualité des soins de santé. La santé humaine est considérée comme le point le plus important à travers le monde. La technologie de l'information contribue à l'amélioration des services médicaux qui sont fournis aux personnes.

Les applications de télémédecine sont de plus en plus utilisées en raison du développement rapide de l'imagerie numérique et des technologies de l'information et de la communication. L'échange de données médicales (images médicales et les informations des patients) entre des cliniques situées dans des lieux géographiques différents est un moyen très couramment utilisé de nos jours[1]. Mais malheureusement, cet échange passe par des réseaux non sécurisés et ouverts, pour de nombreuses raisons, telles que le télédiagnostic, les traitements, les téléconférences entre cliniciens, la consultation médicale, l'apprentissage et la formation à distance, qui créent une menace d'actes défavorables les données médicales peuvent être manipulées intentionnellement et non intentionnellement par des utilisateurs non autorisés. Pour ces raisons et ces menaces, la télémédecine doit assurer les conditions de sécurité des échanges afin de garantir l'intégrité et l'authenticité des images médicales lors de la transmission. La protection des données médicales est nécessaire, Car ces données jouent un rôle important et parfois même vital dans la santé des patients, et cela pourrait provoquer un diagnostic erroné.[2]

Parmi les solutions précédentes pour les menaces de sécurité qui peuvent être considérées comme l'un des puissants systèmes de protection se trouve la cryptographie. Il consiste à rendre les données illisibles pour le côté non autorisé. Cependant, il ne protège les informations que lors de leur transmission ; cela signifie qu'une fois les données décryptées, nous ne pouvons pas empêcher leur modification ou leur reproduction illégale. Le tatouage est proposé en complément de la cryptographie. Elle consiste à intégrer des données dans une image pour en garantir l'intégrité et l'authenticité ; où le médecin pourra détecter l'altération de l'image médicale et n'utilisera pas l'image pour le diagnostic si elle n'est pas autorisée. Cependant, la

condition principale qui doit être respectée est que le médecin doit être capable d'extraire parfaitement le filigrane intégré sans perte.

Dans l'e-santé, le tatouage est utilisé pour intégrer des informations liées à l'image médicale ; par exemple, les informations sur le patient composées du nom du médecin, du nom de l'hôpital, etc. ces informations sont très utiles en télémédecine ; et les données reçues ne doivent pas affecter, modifiées ou envoyées par l'expéditeur prévu. La transmission de données médicales nécessite la présence de trois éléments majeurs ; à savoir la confidentialité, l'authenticité et la fiabilité (intégrité et disponibilité). La confidentialité est assurée lorsqu'un utilisateur non autorisé ne peut pas accéder ou modifier les informations de l'image médicale. L'objectif principal de nos recherches est d'assurer et de prouver l'authenticité et l'intégrité des données médicales. D'où le but principal de ces recherches ; est d'accompagner le système de santé afin de mettre en place un système sécurisé, imperceptible et rapide basé sur des méthodes de tatouage.

Ce mémoire est subdivisé en trois chapitres :

- **Le premier chapitre :** c'est une introduction à la télémédecine, types de données biomédicales échangées. Plus précisément, nous expliquons certains termes et certains concepts dans le domaine des images numériques et des images médicales.
- **Le deuxième chapitre :** nous discutons d'abord des exigences de sécurité des données médicales et du système de sécurité des données. Ensuite, nous présentons le tatouage numérique, ses propriétés, ses contraintes et ses domaines d'insertions et de toutes les informations qui y sont liées.
- **Le troisième chapitre :** nous allons parler d'appliquer à la partie de conception et implémenter la technique proposée pour chiffrer les informations médicales et les résultats du système proposé avec toutes les analyses et discussions nécessaires

Enfin, Nous terminons notre travail par une conclusion générale avec des futures perspectives que nous envisageons est donnée à la fin de cette thèse.

CHAPITRE 1

Etude bibliographique de la télémédecine et les images médicales

I.1. Introduction

La sécurité des informations est l'une des préoccupations majeures de nos sociétés actuelles. Depuis plusieurs années, des efforts importants ont été faits dans le domaine de télémédecine afin de répondre aux demandes mondiales en termes de besoins de sécurité des données biomédicales échangées. La télémédecine permet aux fournisseurs de soins de santé d'atteindre les patients dans les régions éloignées, de fournir des soins plus opportuns et plus pratiques et de réduire le besoin de rendez-vous en personne[3].

Les données biomédicales sont générées chaque jour en grande quantité. Les informations sur les données biomédicales issues de sources biologiques liées à la santé et aux maladies humaines. Ces données peuvent être nécessaires à partir de diverses sources, notamment l'imagerie médicale, les dossiers de santé électroniques (DSE), les biocapteurs, les résultats de tests et d'autres informations médicales pertinentes[4]. L'échange de données biomédicales implique le partage de données médicales entre les prestataires de soins de santé dans d'améliorer les soins aux patients. L'échange de données biomédicales peut aider les intervenants à prendre des décisions plus éclairées concernant les soins aux patients, à réduire les erreurs médicales et à améliorer les résultats pour les patients. Cependant, l'échange de données médicales s'accompagne d'un risque de violation de données et d'une atteinte potentielle à la vie privée des patients. Par conséquent, il est important que les prestataires de soins de santé mettent en œuvre des mesures de sécurité des données solides pour protéger les données des patients.

L'objectif de ce chapitre est de définir la télémédecine, les types de données biomédicales échangées, les menaces auxquelles elle est confrontée et l'importance de la sécurité et de la protection des données dans les applications de télémédecine.

I.2. La télémédecine

La télémédecine est un système de prestation de soins de santé qui implique l'utilisation de la technologie pour fournir des consultations médicales virtuelles et des soins cliniques aux patients à distance. Il a gagné en popularité ces dernières années, en particulier avec le besoin croissant des services de soins de santé à distance lors de pandémies, de catastrophes naturelles et d'autres urgences. Il a également permis aux patients des zones reculées et mal desservies de recevoir des soins médicaux et d'avoir accès à des spécialistes médicaux qui peuvent ne pas être disponibles localement. Cependant, cela pose également des risques de sécurité qui doivent être pris en compte pour protéger les informations sensibles des patients.[5][6]

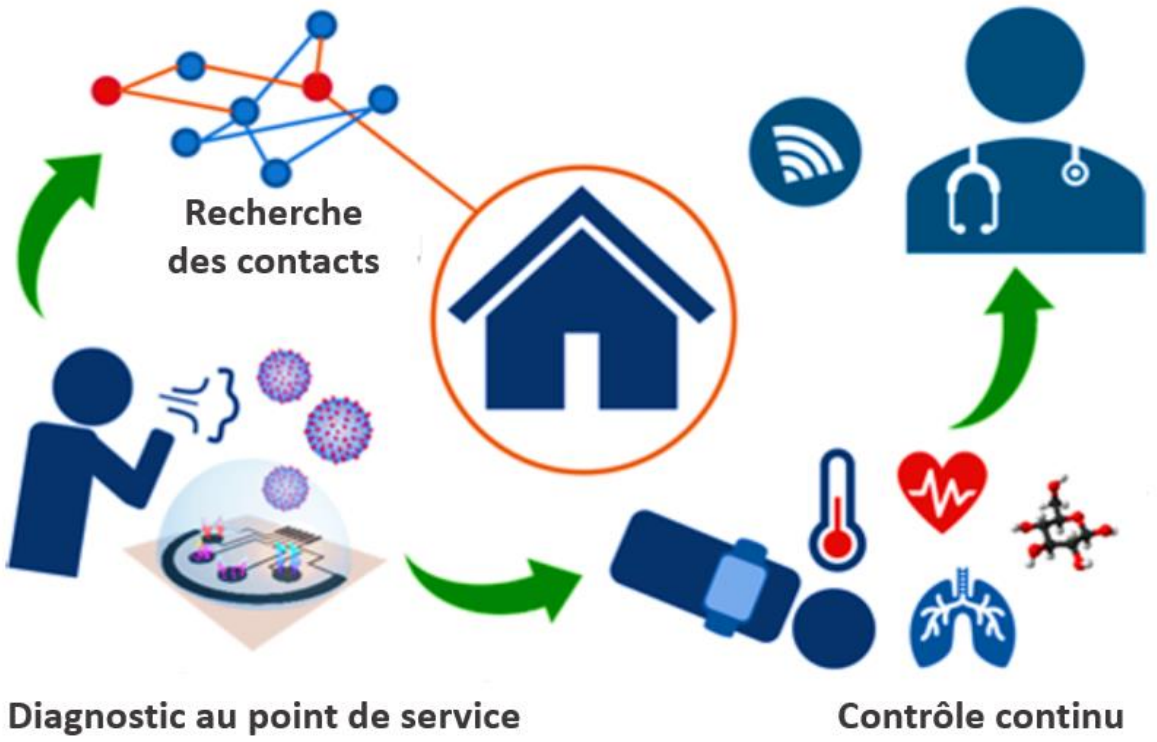


Figure I.1: Capteurs de télémédecine.

I.3. Échange de données biomédicales

L'échange de données biomédicales en télémédecine fait référence au transfert et au partage d'informations médicales sensibles entre les prestataires de soins de santé, les patients et d'autres parties concernées. Cela implique l'échange de dossiers médicaux, d'images, de résultats de tests et d'autres données cliniques en temps réel ou quasi réel pour faciliter le diagnostic, la surveillance et le traitement des problèmes de santé.[7]

L'échange de données biomédicales en télémédecine nécessite l'utilisation de technologies sécurisées et fiables et le respect des réglementations qui libèrent la vie privée et la confidentialité des patients.

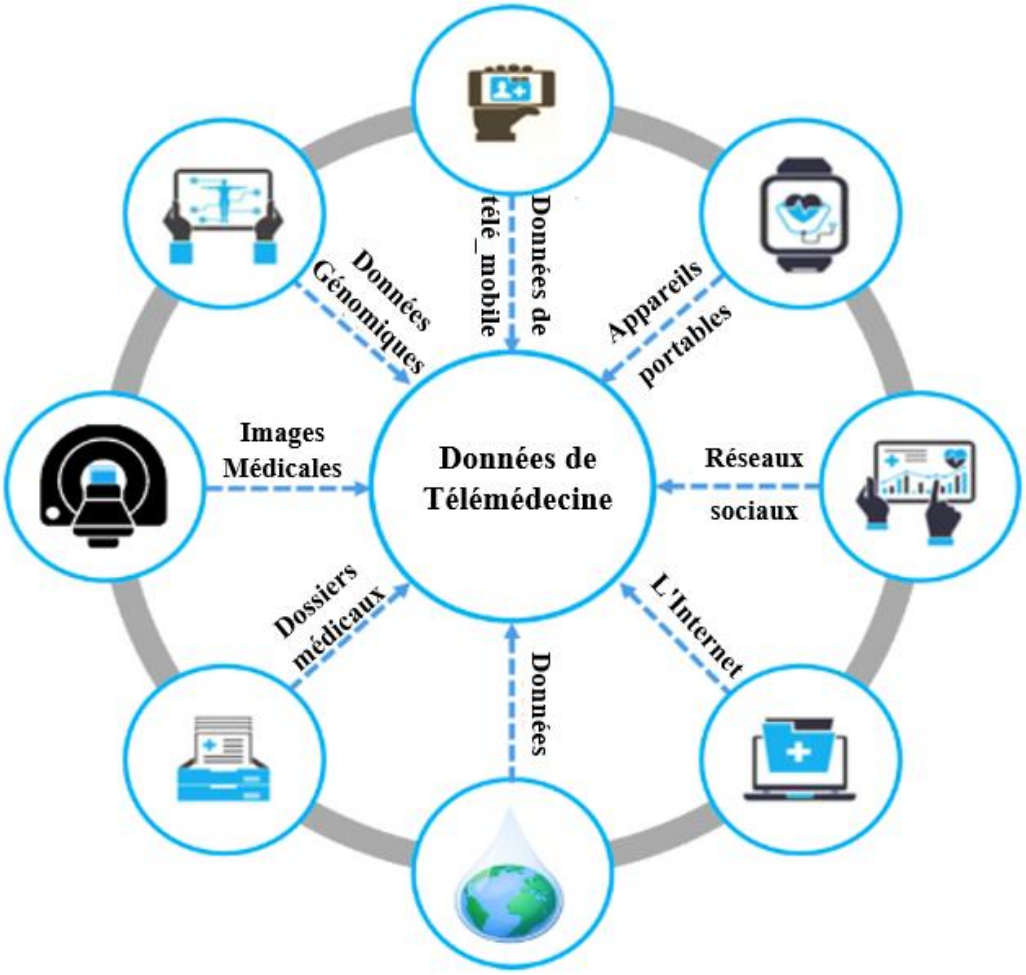


Figure I.2 : Illustration de sources hétérogènes contribuant aux données de télémédecine.

I.3.1. Types de données biomédicales

Il existe de nombreux types de données biomédicales qui sont partagées dans le secteur de la santé, notamment :

1. **Dossiers de santé électroniques (DSE) :** Auparavant, les médecins ou les infirmières devaient documenter tous les détails médicaux de leurs patients sur papier. Mais maintenant, ils peuvent remplir toutes les informations sur le système EHR. Il s'agit de versions numériques des informations médicales d'un patient, qui contiennent les antécédents médicaux du patient, les diagnostics, les médicaments, les résultats des tests de laboratoire et d'autres informations cliniques.[8]

Figure I.3 : Dossiers de santé électroniques (DSE).

2. **Images médicales :** Celles-ci contiennent les radiographies, les tomodensitogrammes, les IRM et d'autres études d'imagerie qui fournissent des informations visuelles sur la structure interne d'un patient.

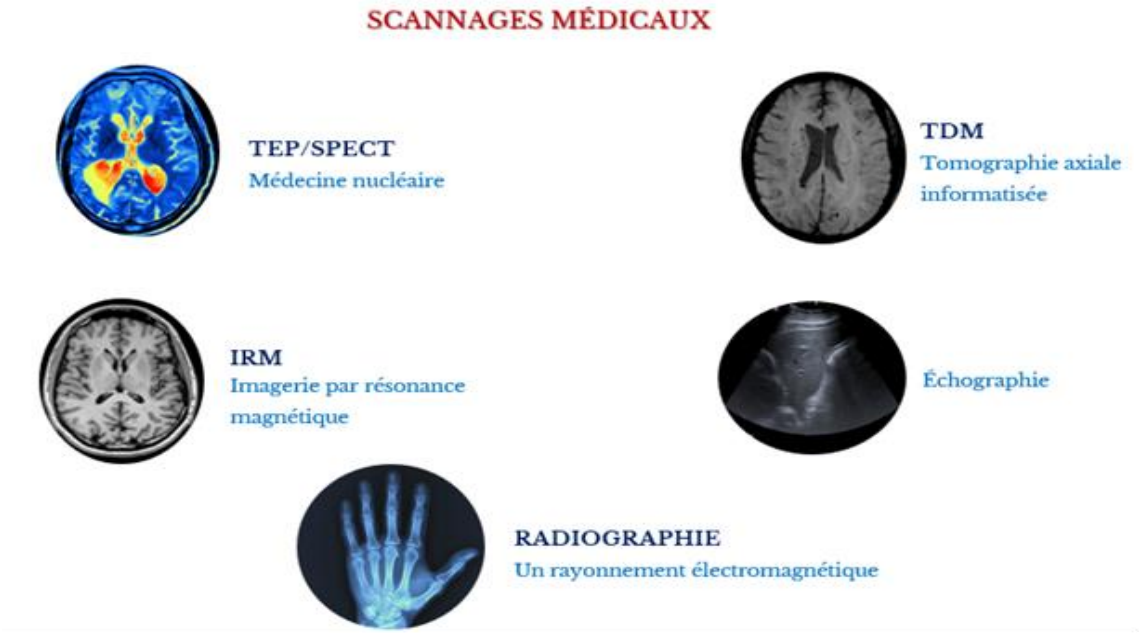


Figure I.4 : Cinq différents types d'imagerie scanne de médecine.

3. **Les analyses :** Les analyses médicales sont des examens réalisés par des professionnels de la santé pour identifier, diagnostiquer ou surveiller une maladie ou une condition médicale. Il existe différents types d'analyses médicales, chacune avec ses résultats propres. Par exemples : L'hémogramme, La glycémie, Le cholestérol, La créatinine, Les tests de dépistage du cancer...etc. Les résultats de ces analyses médicales peuvent être

exprimés sous forme de chiffres ou de pourcentages, et sont souvent comparés à des valeurs normales pour déterminer si le patient présente une condition médicale ou non.[9]

4. **Données de surveillance à distance des patients :** Cela inclut les données nécessaires à partir d'appareils portables, de capteurs et d'autres outils de surveillance à distance qui suivent les signes vitaux d'un patient et d'autres paramètres de santé. Les données recueillies sont ensuite transmises aux prestataires de soins qui peuvent évaluer l'état de santé du patient et modifier le plan de soins si nécessaire.[10]

Figure I.5 : Quelque capteurs médicaux

5. **Données personnelles de santé :** Cela inclut les données relatives au mode de vie et au comportement d'un patient, telles que son régime alimentaire et ses habitudes d'exercice. Y comprennent les antécédents médicaux, les diagnostics, les médicaments, les résultats des tests et d'autres informations relatives à la santé, ces données sont très sensibles. Il est important de s'assurer que tous ces types de données biomédicales sont protégés contre l'accès non autorisé, la divulgation et l'utilisation abusive grâce à des mesures de sécurité des données appropriées.[11]

I.4. Les techniques d'imagerie médicale

I.4.1. Radiologie

La radiologie est une technique d'imagerie médicale qui permet principalement d'obtenir des clichés en deux dimensions des structures osseuses et articulaires. Elle est notamment utilisée en orthopédie, en rhumatologie et en orthodontie pour étudier les traumatismes osseux tels que les fractures, les déformations du squelette ou les implantations dentaires. La pneumologie y a également recours pour la radiographie des poumons. Il est également possible de visualiser certains organes ou parties creuses habituellement invisibles aux rayons X en les "remplissant" d'un produit de contraste opaque aux rayons X, c'est la radiographie de contraste.

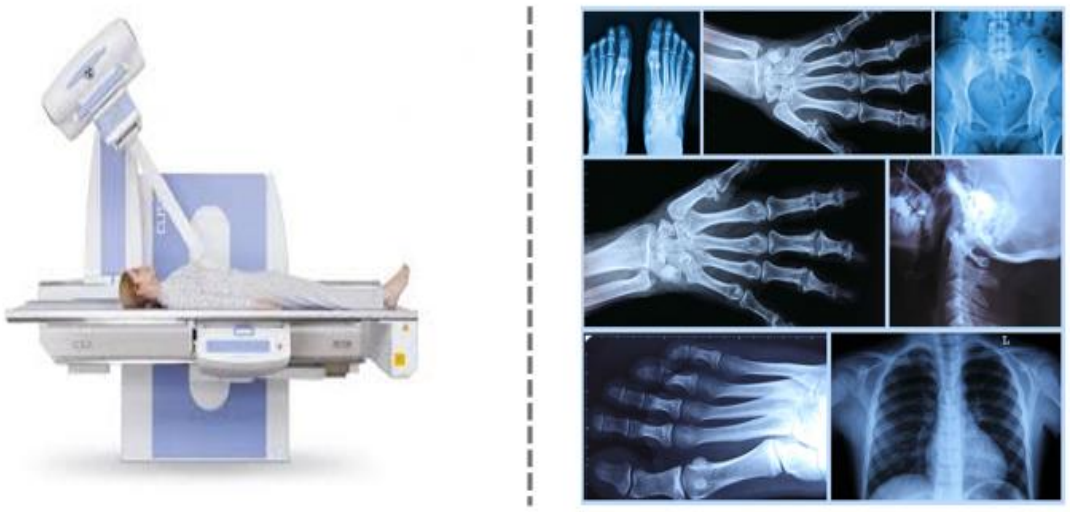


Figure I.6 : Appareil de radiologie et Imagerie aux rayons X de divers organes.

I.4.2. Scanner

Le scanner est une technique d'imagerie médicale qui permet de créer une image tridimensionnelle des organes ou des tissus qui composent les zones numérisées. Le scanner est un examen aux rayons X et est utilisé dans de nombreux domaines. Les résultats sont généralement stockés sur CD-ROM pour un accès facile. La figure I.7 ci-dessus illustre un schéma d'un tube à rayons X.

Figure I.7 : CT scan machine et Imagerie CT cerveau.

I.4.3. Résonance Magnétique

L'imagerie par résonance magnétique (IRM) est considérée comme l'un des meilleurs outils pour l'imagerie médicale en raison de sa capacité à produire des images de haute qualité avec un contraste automatique. Cela permet notamment d'identifier les lésions cérébrales, les tumeurs et les anomalies de la circulation sanguine. L'IRM utilise les propriétés magnétiques des protéines d'hydrogène pour produire des images précises des structures internes du corps, ce qui est particulièrement utile pour les organes internes tels que les poumons. [25]

Figure I.8 : Scanner d'IRM et Cerveau IRM.

I.4.4. Échographie

L'échographie est une technique d'imagerie médicale qui utilise des ondes sonores à haute fréquence pour obtenir une image anatomique des organes et des tissus corporels. Cette technique est largement utilisée pour les femmes enceintes, car elle est simple, efficace et peu coûteuse. Elle est également utilisée pour diagnostiquer d'autres affections, telles que les calculs rénaux ou les maladies cardiaques. La figure I.9 ci-dessus illustre un exemple d'échographie utilisée chez les femmes enceintes. [23]

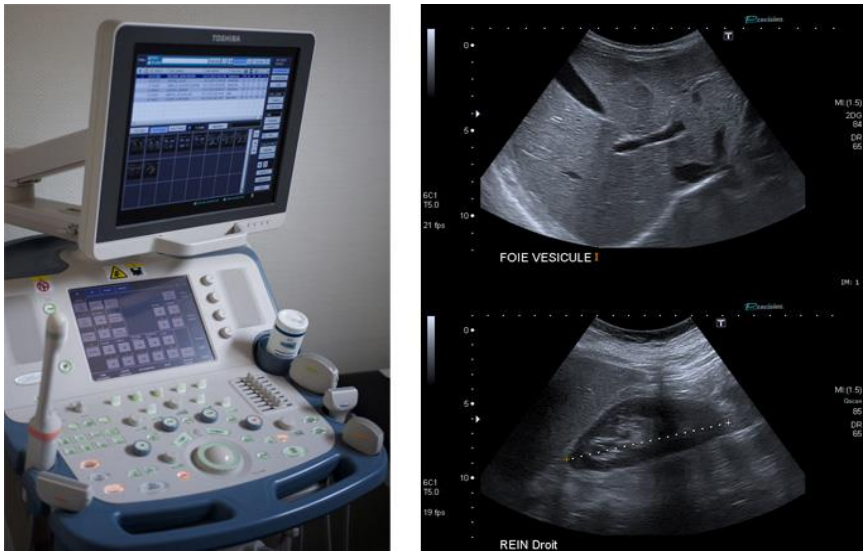


Figure 1.9 : Echotomographie abdominale.

I.5. Numérisation des images médicales

La numérisation de l'image médicale est un processus important qui permet de convertir une image analogique, telle qu'une radiographie ou une tomographie, en une image numérique qui peut être stockée, traitée et partagée électroniquement. Lorsque l'image est numérisée, elle est convertie en une série de pixels, chaque pixel représentant une petite partie de l'image. Chaque pixel est ensuite codé en utilisant un nombre binaire, qui représente l'intensité de la luminosité ou de la couleur du pixel. Ces codes binaires sont ensuite stockés dans un fichier numérique, qui peuvent être consultés et manipulés à l'aide de logiciels spécialisés.

De plus, Les images numériques peuvent également être intégrées dans les dossiers médicaux électroniques (DME), ce qui permet de les retrouver plus facilement et de suivre l'évolution de l'état du patient au fil du temps.

I.5.1. Pixel : Le pixel est le plus petit point de l'image, ce sont les nombres comme les éléments de colonnes de l'image qui multiplient son nombre de lignes. Fondamentalement, le pixel est

une unité de base, qui dénit la mesure d'une image matricielle, Chaque pixel de l'image véhicule des informations. où la valeur du pixel est représentée par des bits.[12]

Dans le cas d'une image monochrome (au niveau de gris), chaque pixel est codé sur un octet.

Dans une image couleur (RVB), un pixel peut être représenté sur trois octets : un octet pour chacune des couleurs : rouge (R), vert (V) et bleu (B)

I.5.2. Taille et résolution de l'image : La taille d'une image est déterminée directement à partir de la largeur M (nombre de colonnes) et de la hauteur N (nombre de lignes) de la matrice image I.

Généralement, la résolution est la capacité de distinguer des détails précis dans les images numériques, tandis que la résolution de l'image détermine le nombre de pixels affichés par l'image. Cela signifie que la résolution peut être rapportée au nombre de pixels, ce qui nous amène à la densité de pixels.

Dans ce contexte, la densité de pixels peut être mesurée à l'aide de pixels par pouce (PPI), de points par pouce (DPI) ou de pixels par centimètre (PPCM). Ce sont des termes courants utilisés pour exprimer les mesures de la résolution des images numériques. [12]

I.6. Les types d'images

Il y a 3 types d'images, des images binaires, des images au niveau de gris, et des images couleurs.

I.6.1. Images binaires

Une image binaire est une image pour laquelle chaque pixel peut avoir une valeur de 0 ou 1. En effet, ce type d'images est le plus simple, où typiquement zéro est pris pour noir, et 1 est pris pour blanc.[13]

I.6.2. Image au niveau de gris

Une image en niveaux de gris ne contient que des nuances de gris et aucune couleur. En outre, peut être désigné comme une image matricielle. Ici, la valeur du pixel est un nombre unique qui représente la luminosité du pixel. Le nombre de pixels est stocké sous la forme d'un entier 8 bits donnant une plage de valeurs possibles de 0 à 255. En règle générale, zéro est considéré comme noir et 255 est considéré comme blanc, et les valeurs des pixels constituent les différents nuances de gris.[13]

I.6.3. Couleur de l'image

La couleur de chaque pixel est d´efinie par 3 caractéristiques : Rouge, Vert et Bleu (système RVB ou RGB en anglais). D'autre part, RVB peut être représenté par trois matrices, chaque matrice détermine la quantité de rouge, de vert et de bleu qui constitue l'image. Pour plus d'illustrations, Figure 2.7 Ordre des couleurs de l'image RVB et image couleur RVB dans le composant.

Les pixels de ces matrices sont des entiers compris entre 0 et 255 qui déterminent l'intensité de la couleur de la matrice pour le pixel correspondant. Ainsi, avec l'espace colorimétrique RVB, il est possible de représenter.[13]

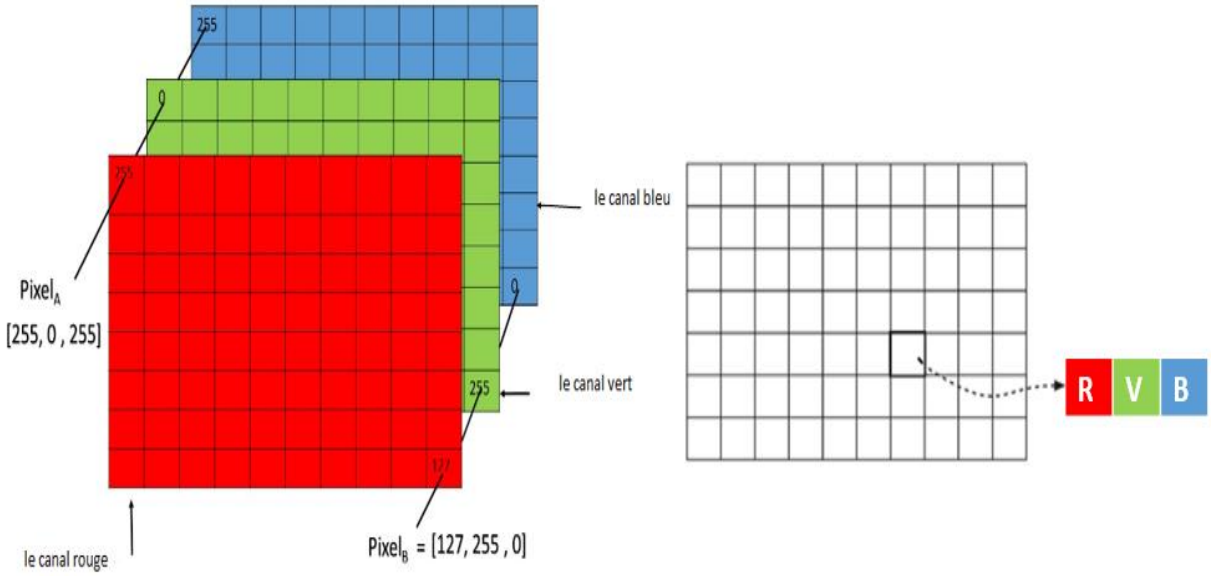


Figure I.10 : Présentation des pixels couleur

I.7. Risques pour les images médicales

La sécurité des données médicales est un sujet très important, car les données médicales sont des informations sensibles et confidentielles qui doivent être protégées contre les accès non autorisés, les pertes de données ou les fuites, voici quelques risques potentiels pour la sécurité des données :

1. **Accès non autorisé :** Les images médicales peuvent être soumises sur des serveurs ou des systèmes de stockage en réseau, qui peuvent être vulnérables aux attaques de pirates informatiques ou aux accès non autorisés. Si un tiers non autorisé accède aux images

médicales, cela peut avoir des conséquences graves, notamment la diffusion de données sensibles ou la violation de la vie privée des patients[14].

2. **Perte de données :**Les images médicales peuvent être perdues en raison d'une panne de matériel, d'une erreur humaine[15].
3. **Erreurs de stockage : Les** images médicales peuvent être portées de manière incorrecte, par exemple dans des dossiers incorrects ou avec des noms de fichiers incorrects. Cela peut rendre difficile la recherche ou la récupération des images médicales.
4. **Utilisation inappropriée :** Les images médicales peuvent être utilisées de manière inappropriée, par exemple pour la discrimination ou la stigmatisation des patients. Il est important de s'assurer que les images médicales sont utilisées uniquement à des fins médicales légitimes et que leur accès est limité aux personnes qui ont besoin de les consulter.
5. **Réseau domestique :** La transmission d'informations entre le terminal de télémédecine dans l'espace privé du patient (domicile ou bureau) et le système de télémédecine s'effectue principalement via un réseau sans fil. Dans de tels environnements, les données biomédicales sont exposées à des menaces de sécurité associées[15].

I.8. Importance de la sécurité des données en télémédecine

La sécurité des données biomédicales dans les applications de télémédecine est cruciale car elle implique la collecte, le stockage et la transmission d'informations sensibles sur les patients, y compris les informations de santé personnelles (PHI) et les dossiers de santé électroniques (DSE). Ces données contiennent des informations médicales privées et confidentielles qui diffusent des mesures strictes de sécurité et de confidentialité.

Les violations de données dans les applications de télémédecine peuvent entraîner de graves conséquences, notamment l'usurpation d'identité, la fraude médicale, les fautes professionnelles et les atteintes à la réputation des organisations de soins de santé. De plus, l'accès non autorisé aux données des patients peut entraîner des violations éthiques et juridiques pouvant entraîner des amendes et des poursuites judiciaires occasionnées.[16]

Par conséquent, il est essentiel de garantir des mesures de sécurité des données solides, telles que le cryptage, la transmission sécurisée et le contrôle d'accès, pour protéger la confidentialité des patients et maintenir la confiance dans les applications de télémédecine. Les professionnels

de la santé doivent se conformer aux réglementations de sécurité, y compris HIPAA et GDPR, pour protéger les données médicales de leurs patients.[17][18]

I.9. Conclusion

La sécurisation des données médicales dans les applications de télémédecine est de la plus haute importance en raison des informations sensibles et personnellement identifiables contenues dans les données. Les patients font confiance aux fournisseurs de soins de santé avec leurs informations personnelles, et il est de la responsabilité des organisations de soins de santé de protéger ces informations contre tout accès non autorisé, vol ou altération.

Cependant, le recours aux télécommunications et aux technologies Internet pour accéder aux données médicales pose des risques de sécurité. Les utilisateurs à la sécurité pourraient entraîner le vol d'identité, le chantage ou l'accès non autorisé aux renseignements personnels sur la santé. Des mesures de sécurité efficaces, telles que des mécanismes d'authentification solides et des audits de sécurité réguliers, sont nécessaires pour garantir la confidentialité, l'intégrité et la disponibilité des données médicales dans les applications de télémédecine. Les prestataires de soins de santé et les organisations doivent adopter les meilleures pratiques pour protéger les données des patients et instaurer la confiance avec les patients.

CHAPITRE 2

Le tatouage pour la sécurité des données médicales

II.1. Introduction

Les systèmes d'information numériques ont été de plus en plus déployés dans les environnements de soins de santé modernes au cours des dernières décennies. En fait, de nombreux hôpitaux et centres de santé dans le monde s'appuient dans leur fonctionnement sur les systèmes d'information hospitaliers (HIS), les systèmes d'information radiologique (RIS) et les systèmes d'archivage et de communication d'images (PACS).

Ces systèmes sont pour disponibiliseret et à faciliter le partage d'images médicales et de dossiers électroniques de patients entre cliniciens et radiologues pour des applications de télémédecine telles que la téléconsultation, le télédiagnostic et la téléchirurgie. Malgré ces progrès innovants, il est assez facile pour un adversaire malveillant d'intercepter et de falsifier les images transmises lorsque les réseaux publics sont utilisés. En raison de la facilité avec laquelle la manipulation des images est accomplie, l'authentification des images médicales est donc d'une grande importance dans ce domaine. Cependant, les approches proposées pour les images médicales sont limitées car ce type d'images présente des contraintes spécifiques à l'insertion. Le tatouage est proposé comme l'une des solutions pour garantir l'authenticité et l'intégrité de l'image médicale, il peut être défini comme suit : Le tatouage est le processus d'altération imperceptible d'une donnée afin d'y incruster une information. Cette définition révèle que les principaux objectifs du filigrane d'images médicales sont que les filigranes sont imperceptibles et agissent comme un moyen d'authentification et de contrôle d'intégrité. La confidentialité est obtenue en tant que sous-produit du masquage des données du patient dans l'image.

Dans ce chapitre, nous allons présenter d'abord les Exigences de sécurité des données médicales ainsi les différentes techniques de sécurité de l'information existantes comme la Stéganographie, tatouage et la cryptographie. Ensuite, nous présenterons le tatouage numérique comme une solution pour la sécurité et l'authentification des données médicales. Puis nous énumérons les différents schémas d'insertion.

II.2. Exigences de sécurité des données médicales

Le partage de données médicales via Internet devient très populaire de nos jours pour faire des télédiagnostics, des téléchirurgies et des téléconsultations. La sécurité des données médicales, donne des droits au patient et des devoirs aux professionnels de santé. Celle-ci impose trois caractéristiques obligatoires[19] :

II.2.1. Confidentialité :

La confidentialité signifie que seules les personnes autorisées ont accès aux données (les dossiers médicaux ne doivent être consultés que par des personnes autorisées)

II.2.2. Intégrité :

L'assurance que les données reçues sont exactement telles qu'elles ont été envoyées par une entité autorisée (ne contiennent aucune modification, insertion, suppression ou rejeu).

II.2.3. Authentification :

Les dossiers médicaux et/ou les images des patients doivent être envoyés et reçus de sources vérifiées aux destinataires.

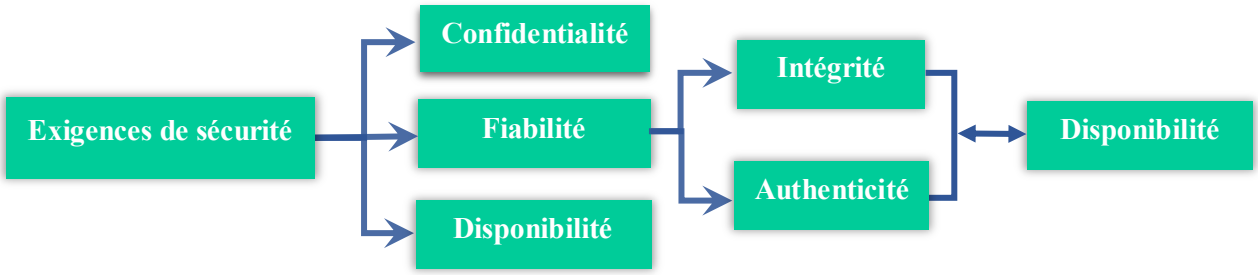


Figure II.1. Principales exigences de sécurité pour les données[20].

II.3. Techniques de protection des données

Le système de sécurité des données est divisé comme suit :

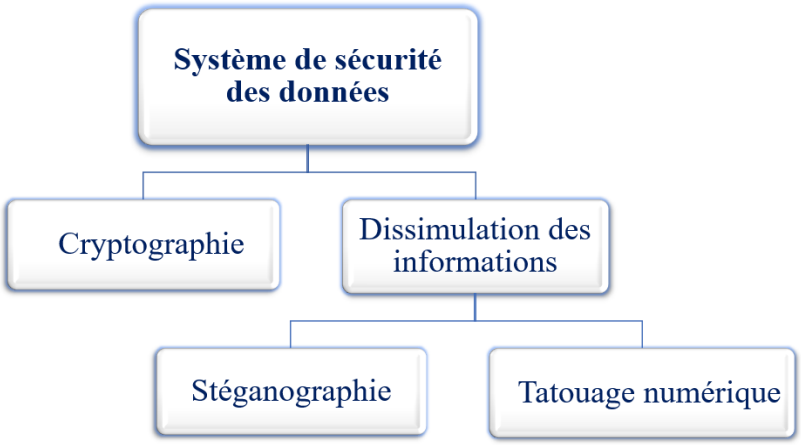


Figure II.2. Système de sécurité des données

II.3.1. La cryptographie

La cryptographie est une technique qui sécurise les données transférées, qui concerne la confidentialité, l'intégrité et la disponibilité des informations, pour transmettre les données en toute sécurité sur Internet en appliquant certains algorithmes cryptographiques en les rendant illisibles de sorte qu'il sera difficile pour un attaquant pour attaquer ou voler des informations confidentielles ou privées. Deux termes de base utilisés en cryptographie sont le chiffrement et le déchiffrement, de sorte qu'une clé est nécessaire à la fois pour le chiffrement et le déchiffrement du message.[21]

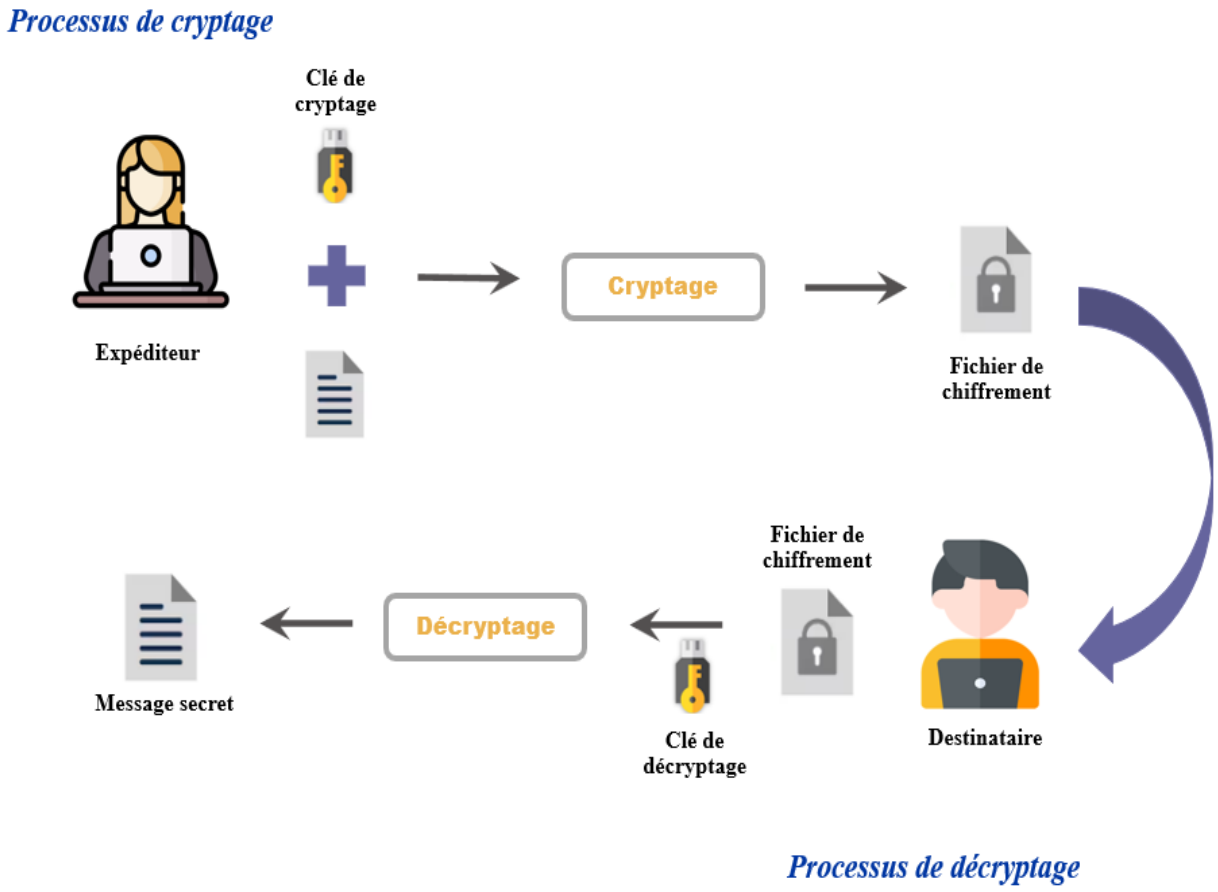


Figure II.3. Processus de données sécurisées : processus de cryptographie.

II.3.2. La stéganographie

La stéganographie est l'art de cacher des informations dans les médias numériques grâce aux techniques d'intégration de messages cachés de telle manière que personne, à l'exception de l'expéditeur et du ou des destinataires prévus, ne puisse détecter l'existence des messages.[22] La stéganographie permet de masquer l'existence d'un message au sein d'un autre objet (image, vidéo, audio) appelé data[23], pour créer une couverture qui contient les données secrètes appelées support de couverture qui

doit les protéger des attaques d'espionnage. C'est donc une technique pour créer une communication cachée. Les terminologies de base utilisées dans les systèmes de stéganographie proposés sont : le message ou l'information de couverture, le message secret, la clé secrète et l'algorithme d'intégration.

- ✓ **L'image du transporteur :** L'image porteuse est aussi appelée l'objet de couverture qui portera le message à masquer.
- ✓ **Le message :** Un message peut être n'importe quoi comme des données, un fichier ou une image, etc.
- ✓ **La Clé :** Une clé sert à décoder/déchiffrer/découvrir le message caché.

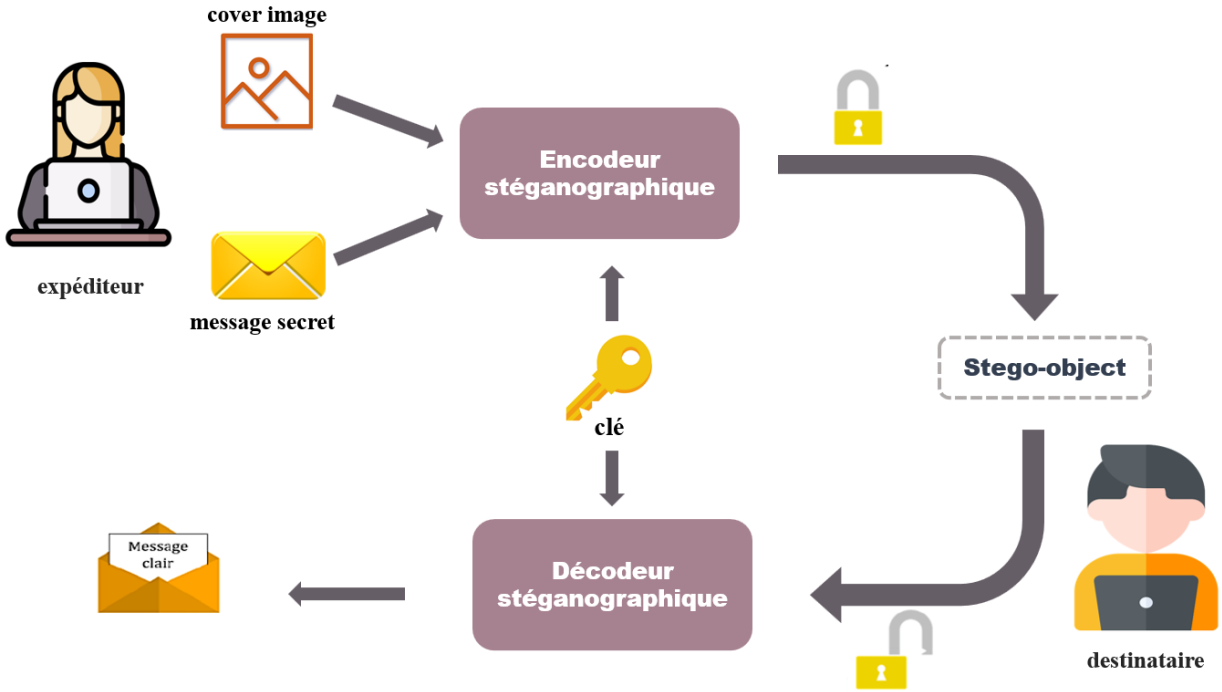


Figure II.4. Traitements de données sécurisés : processus de stéganographie

II.3.3. Cryptographie VS Stéganographie

Certaines évolutions des techniques ont amélioré les fonctionnalités de chaque champ dans les données sécurisées. Comme le montre le tableau 1, une étude comparative entre la cryptographie, les techniques de stéganographie largement utilisées pour assurer la sécurité des informations, les avantages et les inconvénients des techniques sur la cryptographie, la stéganographie. Cependant, les techniques proposées ne résolvent pas tous les problèmes, tandis que le tatouage confirme l'intégrité de l'information et afin d'être indétectable, tandis que l'objectif est d'intégrer un message de manière à ce qu'il ne peut pas être supprimé.[24]

Tableau II.1. Fonctionnalités générales pour les données sécurisées

	Cryptographie	**Stéganographie**	**Tatouage numérique**
But	Assurer la sécurité des informations et les transférer via des communications Protéger la confidentialité, l'intégrité et la non-répudiation (disponibilité) des données	Il s'agit d'une communication privée et de la protection des données contre l'altération à des fins d'authentification.	Protection des droits d'auteur, surveillance de la diffusion, authentification vidéo et sécurité des cartes d'identité
Force	Sécurisez les données et protégez la vie privée en utilisant la cryptographie avec une autre technique, par exemple, la stéganographie Fournir un processus d'autorisation sécurisé et de meilleures fonctionnalités de sécurité	Assurer la confidentialité des données de bout en bout pour les informations sensibles et une authenticité robuste	Améliorer l'imperceptibilité et la complexité de calcul pour les médias numériques
Fonctionnalités	Gestion complexe des clés, en particulier dans les infrastructures à clé publique	En utilisant uniquement la stéganographie du texte, le schéma sera plus naturel à interrompre ou à déchiffrer	Utilisation d'un logo universel sans cryptage dans l'algorithme d'intégration
Basé sur l'utilisation	Basé sur un algorithme	Basé sur le domaine	Basé sur les applications

II.4. Le tatouage numérique

La technique du tatouage numérique s'est imposée comme une alternative pouvant compléter la cryptographie[25]. Il consiste à intégrer les informations de données dans une image hôte pour améliorer l'intégrité des données, protéger les avantages du document et interdire la reproduction illégale le tatouage modifie les niveaux de gris des pixels de celle-ci pour y encoder un message. La « distorsion » induite ou le signal de différence entre l'image originale et sa version tatouée constitue le filigrane ou la marque associée au message inséré. Le message est ainsi accessible indépendamment du format de stockage de l'image.[26]

II.4.1. Comment fonctionne réellement le tatouage numérique

Tel que décrit en la figure 5 et 6 le modèle générique d'un framework de tatouage numérique, ce dernier se compose de deux parties principales[27]

A. Phase insertion : Cette étape permet d'insérer un message ou une marque dans l'image de manière imperceptible. Pour ce faire, une clé secrète de tatouage peut être utilisée pour sélectionner les pixels ou les coefficients à tatouer. Les modulations de tatouage seront évoquées en détails après.

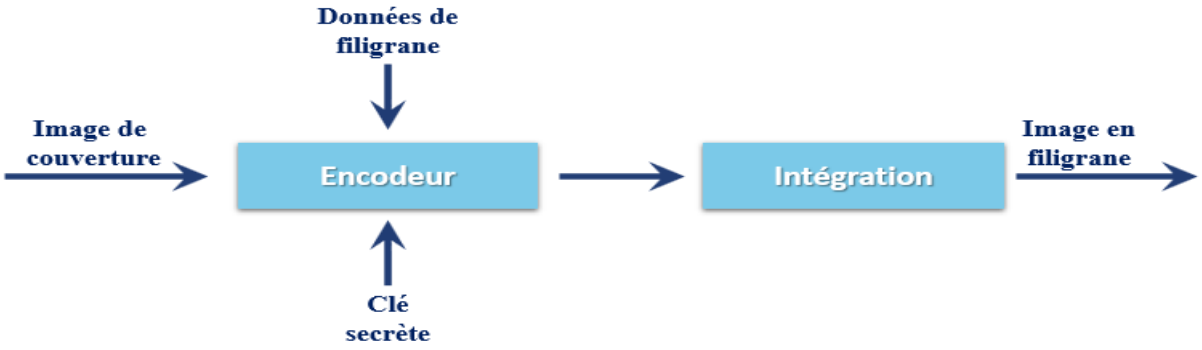


Figure II.5. Le processus d'intégration du filigrane

B. Phase Extraction/Détection :

- **Détection :** ce processus permet de détecter la présence d'une marque dans un signal hôte. Deux modèles sont distingués, le premier non aveugle nécessite l'image originale et la clé de tatouage. Quant à la détection aveugle seule la clé de tatouage est nécessaire
- **Extraction :** ce processus permet la lecture de la marque. Dans le cas des algorithmes caractérisés par la propriété de réversibilité. La marque est complètement extraite et l'image reconstruite sans perte de données.[26]

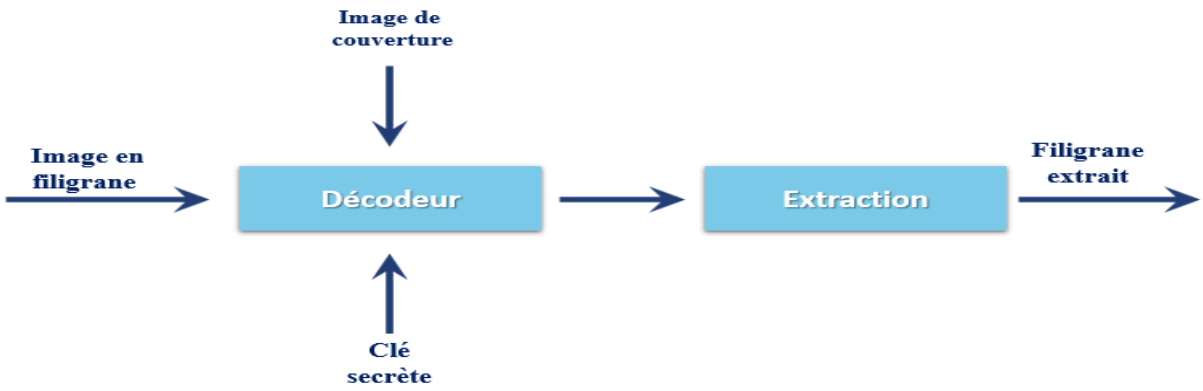


Figure II.6. Le processus d'extraction de filigrane.

II.4.2. Propriétés du tatouage numérique

Le système de tatouage numérique a des propriétés importantes qui doivent être atteintes, les propriétés les plus vitales pour le filigrane numérique sont décrites ci-dessous. L'importance de chaque propriété peut changer selon le domaine d'application[28].

II.4.2.1. Imperceptibilité

L'imperceptibilité est essentielle pour évaluer les performances d'un système de tatouage, elle fait référence à la dégradation de la qualité entre l'image originale et l'image tatouée. Ils doivent être perceptiblement indiscernables pour les humains, malgré une légère dégradation de la luminosité ou du contraste de l'image[29] La qualité de l'image filigranée peut également être évaluée à l'aide d'outils tels que le PSNR (Peak signal noise ration) il évalue la dégradation en db de l'image originale causée par l'insertion de la marque[30].

II.4.2.2. Robustesse

L'une des propriétés les plus importantes, c'est la capacité d'une méthode de tatouage à résister à différentes attaques comme l'attaque par suppression, les attaques par transformation affine telles que la translation, la rotation et l'échelle ou la compression, etc.[31]

II.4.2.3. Capacité

Il exprime le taux d'incorporation c'est-à-dire le nombre de bits de message incorporés par pixel (bpp) d'une image. Il donne une indication de la longueur du message qui peut être intégré dans une image. Plus la longueur du message est grande, plus les services de sécurité basés sur le tatouage peuvent être fournis.[32]

II.4.2.4. Sécurité

La sécurité des techniques de tatouage peut être interprétée de la même manière que la sécurité des techniques de chiffrement. Ainsi, une technique de tatouage est véritablement sécurisée si la connaissance de l'algorithme exact d'incorporation et d'extraction du tatouage n'aide pas une personne non autorisée à détecter la présence du filigrane ou à le supprimer sans connaître la clé secrète.[33]

II.5. Classification des tatouages numériques

Les tatouages numériques, leurs caractéristiques, leurs techniques et leurs applications sont classés en différentes catégories, chacune avec ses propres propriétés et caractéristiques distinctes. Cependant, il n'existe pas de critère uniforme pour la classification des schémas de tatouage d'image. Ils peuvent être classés de trois manières différentes, et selon divers paramètres comme le domaine d'insertion, la perception humaine ou la méthode de détection.

Ainsi, en se référant à divers articles d'enquête[31][34][35][36], il doit y avoir des exigences satisfaites lors de la mise en œuvre, comme illustré à la Figure 7.

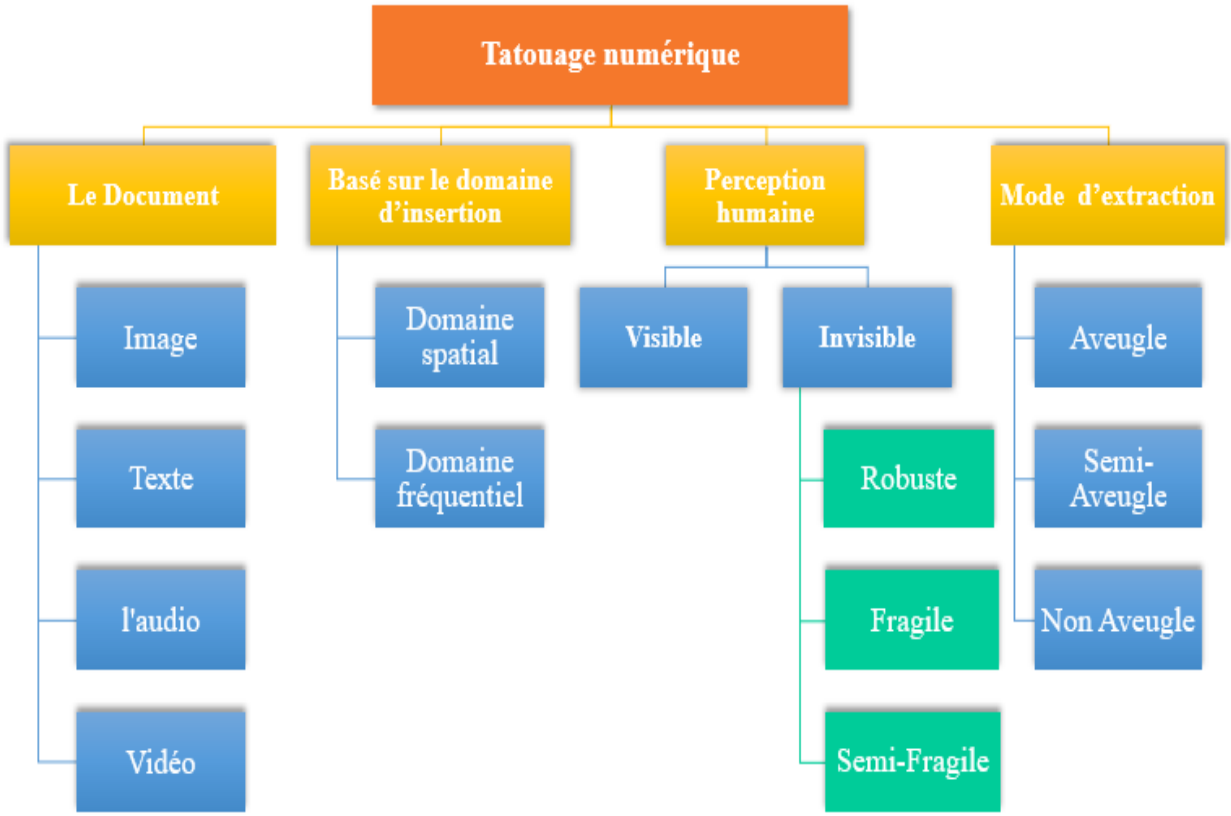


Figure II.7. Classification des schémas de tatouage

II.5.1. Classification basée sur le type de données

Les données peuvent être de type texte, image, audio ou vidéo qui font référence à l'insertion des marques dans un texte / une image / un audio / une vidéo afin de protéger le contenu des données contre la copie, la transmission ou la manipulation des données.

A. Tatouage de texte

Pour vérifier la modification apportée aux fichiers texte (par exemple Portable Document Format (PDF), DOC...), la forme de la police et les espaces entre les caractères ou en ligne sont utilisés pour insérer le tatouage. Ainsi, qu'en cas de modulation des polices, il ne peut pas être détecté[37][34]

B. Filigrane d'image

Cette classe de tatouage est la plus largement utilisée pour protéger les photos sur Internet, en profitant des propriétés d'images et des caractéristiques du système visuel humain, les données secrètes (Logo, Tampon, Étiquette...) sont cachées dans une image puis détectées plus tard[34][37]

C. Filigrane audio

La composition Internet d'audio (par exemple MP3) attire l'attention sur le filigrane audio. Comme d'autres catégories, cette approche nécessite la robustesse et l'inaudibilité des filigranes[38]

D. Filigrane vidéo

La vidéo fait référence à un signal tridimensionnel (3D), avec une image qui préserve la 2D dans l'espace et la 1D dans le temps. Ainsi, le tatouage vidéo est une extension du tatouage image, pour assurer le contrôle vidéo, il est intégré dans le flux vidéo. L'une des principales différences qui distinguent la vidéo du tatouage d'image est la synchronisation temporelle. Cette catégorie nécessite la robustesse et l'extraction en temps réel pour la compression.[38]

II.5.2. Classification basée sur le domaine d'intégration

L'algorithme de tatouage varie par rapport au domaine d'insertion, en effet, chaque domaine de tatouage se caractérise par certains avantages qui permettent son évaluation, c'est pour ça qu'on cite les différents domaines de tatouage.

A. Domaine spatial

Ces techniques de tatouage peuvent également être mises en œuvre en utilisant la séparation des couleurs. Ce domaine se concentre sur la modification des pixels d'un ou deux sous-ensembles d'images sélectionnés au hasard. Il charge directement les données dans les valeurs de pixel d'une image. Certains de ses algorithmes sont LSB, une technique basée sur la modulation à spectre étalé (SS). Les modifications peuvent inclure l'inversion du bit de poids faible de chaque pixel. Les informations insérées peuvent être facilement détectées à l'aide d'une analyse informatique.[39][40]

B. Domaine fréquentiel

L'utilisation de la transformée fréquentielle réversible est venue comme alternative du domaine spatial pour améliorer la robustesse de l'algorithme de tatouage. Les techniques du domaine fréquentiel sont plus largement mises en œuvre. L'objectif principal de cette classification est d'intégrer ou d'insérer les tatouages dans les coefficients spectraux de

l'image.[39] Parmi les transformées qui ont prouvé leur efficacité dans ce domaine, la transformée discrète de Fourier (DFT), la transformée discrète en cosinus (DCT) et la transformée discrète en ondelettes (DWT). Les méthodes fréquentielles sont plus robustes à la compression et moins sensibles aux attaques géométriques.[41]

II.5.3. Classification basée sur la robustesse

Les algorithmes de tatouage numérique des images peuvent être classés selon leur robustesse. On peut distinguer dans cette classification trois catégories de tatouage numérique :

A. Robuste

La robustesse est une capacité de détection du filigrane après des opérations de modifications (traitements), le tatouage intégré peut résister au traitement d'édition, au traitement d'image et à la compression avec perte. Cette classe de schémas a trouvé ses applications dans de nombreux domaines, notamment la preuve de propriété, l'identification, le suivi des transactions, le contrôle de la copie et la surveillance de la diffusion. Ainsi, la robustesse à tous les traitements possibles n'est pas requise pour toutes les applications de tatouage[42][43]. Ce type de tatouage est généralement préféré dans la protection du droit d'auteur.

B. Fragile

Dans certaines applications, la robustesse est considérée comme une propriété indésirable et complètement hors de propos. En fait, une importante catégorie de recherche sur les tatouages se concentre sur les filigranes fragiles. Contrairement au filigrane robuste, ils sont conçus pour être vulnérables à toutes les modifications, n'importe les quelles pouvant être dues à des petites manipulations de l'image tatouée, Dans ce cas, les filigranes peuvent être facilement détruits par toute tentative de falsification, en d'autres termes, fragile mark est conçu pour prendre en compte tous les types d'attaques malveillantes, telles que le copier-coller, la quantification vectorielle et les attaques non malveillantes.[36][34] Les tatouages fragiles sont plus faciles à concevoir que les robustes et sont généralement appliqués dans des scénarios d'authentification et de vérification de l'intégrité du contenu[42].

C. Semi-fragile:

Ces tatouages sont un juste milieu entre les tatouages fragiles et les filigranes fragiles. Le tatouage semi-fragile vis à résister à certains traitements du document, tant que son contenu sémantique n'est pas altéré. Cette classe fournit une robustesse sélective à un certain ensemble

de manipulations qui sont considérées comme légitimes et autorisées, tout en étant vulnérables (fragiles) aux autres. Il est conçu pour s'arrêter sous toutes les modifications qui dépassent un seuil spécifié par l'utilisateur[43][13]. Cela peut également être utilisé dans l'authentification et le contrôle effilé des images, afin d'améliorer davantage la robustesse et d'augmenter le niveau de sécurité, les schémas de tatouage sont généralement contrôlés par des clés cryptographiques.

II.5.4. Classification basée sur le mode d'extraction

Dans la classification des schémas de tatouage, un critère important est le type d'informations nécessaires au détecteur. En ce qui concerne le processus de détection, il peut être divisé en trois catégories principales :

A. Aveugles (publics)

Ce type de détection ne nécessite ni l'image d'origine (ou d'autres informations la concernant) ni les données de tatouage. Ici, le récepteur n'a pas accès aux données de marque et à l'image d'origine car elles ne sont pas disponibles, mais l'approche principale qui appartient à cette catégorie est la détection basée sur la corrélation, où la présence du tatouage est décidée en fonction de la corrélation entre le filigrane et le signal (nécessite une technologie de filigrane plus élevée) [42][37]. En raison de leur champ d'application plus large, aveugle (également connu sous le nom de filigrane public).

B. Non aveugles (privés)

Ici, le récepteur a besoin soit du signal d'origine, soit de certaines informations dérivées de celui-ci pendant la phase de détection (à la fois l'utilisation de l'image d'origine et la ou les clés secrètes pour l'intégration du tatouage). Ces schémas peuvent être considérés comme une catégorie plus générale de détection informée. Malgré leurs applications limitées, ces schémas sont considérés comme les méthodes de tatouage les plus robustes[28].

C. Semi-aveugle (Semi Privé)

Ces schémas ne nécessitent pas les données d'origine pour la détection de filigrane. Mais, les schémas nécessitent la ou les clés secrètes et la séquence de bits du filigrane et/ou les paramètres utilisés pour intégrer les données (le filigrane d'origine et la clé sont nécessaires pour extraire le bon tatouage)

II.6. Techniques de tatouage numérique

En général, il existe deux approches principales du tatouage numérique, à savoir le domaine spatial et le domaine de transformation (fréquence) :

II.6.1. Domaine spatial

Dans les méthodes de tatouage qui utilisent cette représentation de l'image, la marque est insérée dans l'image originale en modifiant directement les valeurs des pixels de l'image (en modifiant certains de ses aspects tels que la luminosité, la bande de couleur, etc.). Ces méthodes sont plus simples, plus rapides et moins couteuses en temps d'exécution. De plus, une marque peut être masquée plusieurs fois [24]. Le nombre de bits modifiés dans les pixels doit être soigneusement pris en compte pour éviter que le tatouage ne devienne visible, afin de l'utiliser pour l'authentification de document et la détection de falsification. Le LSB est la méthode le plus utilisées dans le domaine spatial.

A. Bit le moins significatif (LSB) Méthode

L'algorithme LSB est considéré comme l'approche la plus simple, que nous pouvons modifier le dernier bit de chaque pixel, en les remplaçant par le bit de données du message secret[44][29]. À partir de l'image ci-dessus, nous pouvons observer que si nous modifions le bit le plus significatif (ou MSB), cela aura un impact plus important sur les valeurs finales ; cependant, si nous modifions le peu le moins significatif (ou LSB), l'impact sur la valeur finale est minime. Le filigrane est inséré dans les bits les moins significatifs de l'image hôte et peut être extrait de la même manière. Bien que le nombre eût été intégré dans les 8 premiers octets de la grille, les 1 à 4 bits les plus petits doivent être modifiés en fonction du message secret intégré. Les avantages sont leur robustesse contre les changements de luminance, le réglage du contraste et leur fragilité contre d'autres attaques telles que le filtrage et le flou.

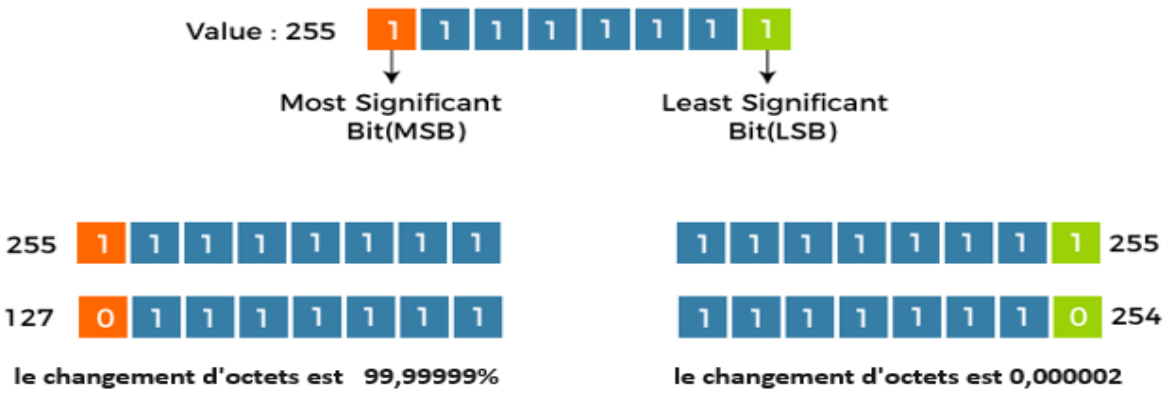


Figure II.8. Impact le bit le plus significatif (MSB) et le bit le moins significatif (LSB)

Avant d'incruster le tatouage, celui-ci est d'abord crypté puis des pixels aléatoires de l'image de couverture sont sélectionnés à l'aide d'une clé, qui détermine les pixels qui seront modifiés par le processus d'incrustation. Cette technique de tatouage consiste à remplacer le LSB des valeurs de pixel dans l'image porteuse par les valeurs du tatouage, cela nous permettra de modifier les valeurs du pixel de +1 ou -1 seulement, ce qui n'est pas du tout perceptible.[45]

Ainsi, le tatouage peut être masqué partiellement ou totalement. Pour extraire le filigrane, l'algorithme d'incorporation est inversé. La figure 9 illustre l'exemple de méthode LSB d'incorporation de filigrane (pour extraire le tatouage, les mêmes étapes sont appliquées dans l'ordre inverse.)[29].

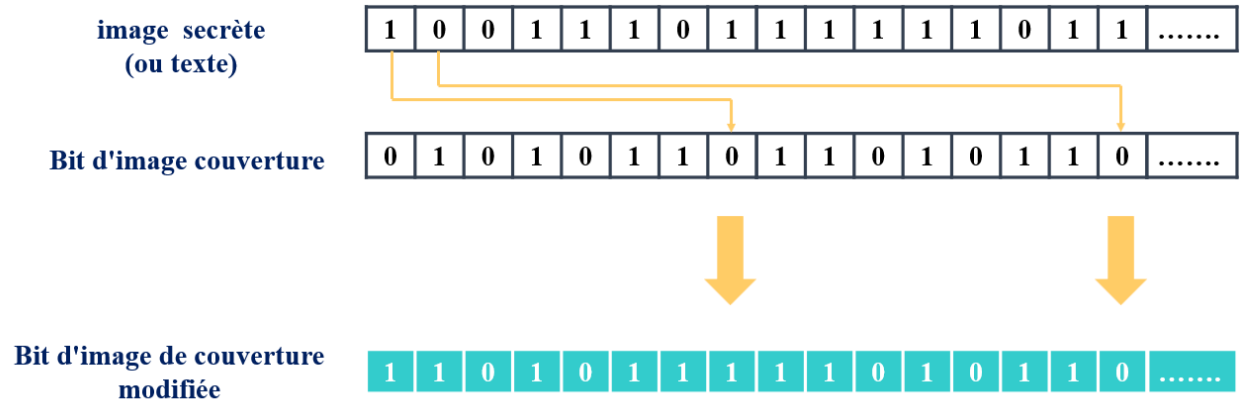


Figure II.9. Schéma de la méthode LSB.

Cependant , le tatouage dans le domaine spatial n'offre pas de bonne performance en terme de robustesse contre la compression et les attaques de tatouage et géométriques, une légère modification de l'image tatouée est suffisante pour supprimer la marque, d'où l' idée des algorithmes agissant dans le domaine fréquentiel[46]

II.6.2. Domaine fréquentiel

Ce type d'incorporation utilise les coefficients de transformation pour incorporer le tatouage. De plus, les techniques de domaine de transformation sont très robustes contre les attaques

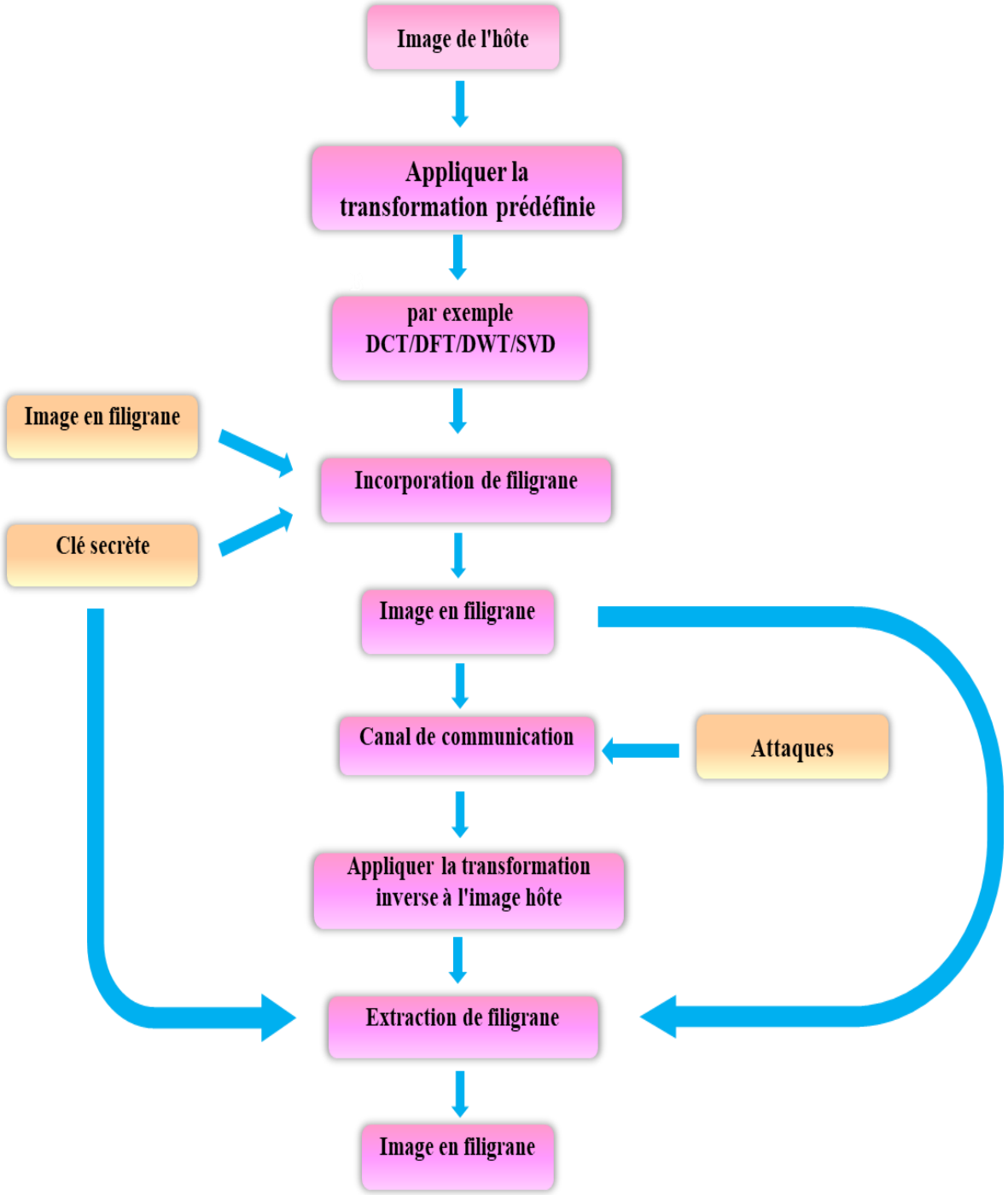


Figure II.10. Incorporation et extraction de tatouage dans le domaine de transformation.

A. Technique basée sur la transformée discrète en cosinus (DCT)

La DCT est une transformée de fréquence appliquée dans plusieurs domaines, tels que le traitement du signal, la compression des données et le tatouage numérique. DCT transforme l'image du domaine spatial au domaine fréquentiel pour obtenir les coefficients de cosinus. Ces coefficients sont classés en coefficients basse fréquence (LF), moyenne fréquence (MF) et haute

fréquence (HF), comme illustré à la figure 11. Chaque bande présente des informations spécifiques, telles que les coefficients basse fréquence, qui contiennent les informations importantes de cette image, et les coefficients haute fréquence représentent les détails nets de l'image[41].

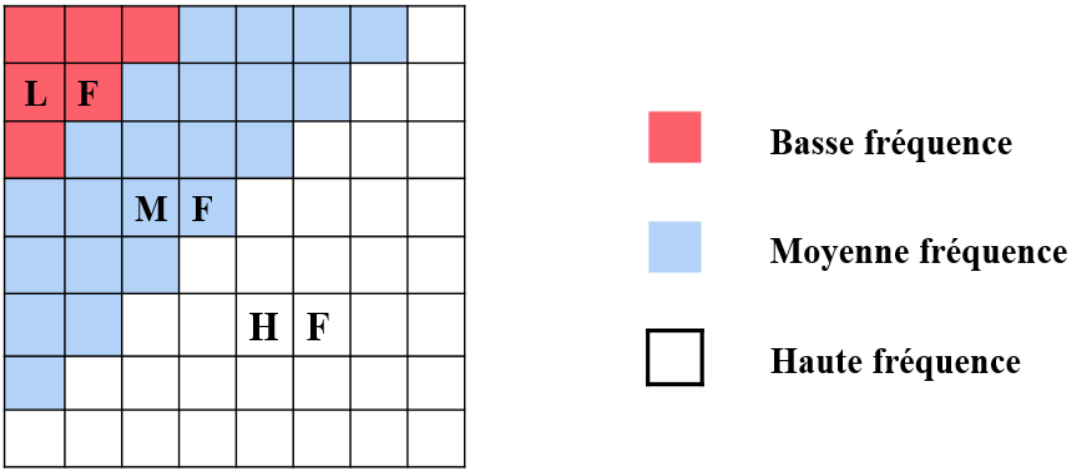


Figure II.11. Décomposition DCT.

Les principales étapes utilisées dans le DCT sont[47][28]:

- Tout d'abord, prenez l'image et divisez-la en blocs 8*8 non superposés.
- Calculer la DCT directe de chacun des blocs sans chevauchement.
- Utiliser les critères de sélection des blocs HVS.
- Utilise maintenant les critères de sélection des coefficients les plus élevés.
- Ensuite, intégrez le tatouage dans le coefficient sélectionné.
- Prenez maintenant la transformée DCT inverse de chaque bloc.

Le DCT formule l'ensemble sélectionné de points de données comme une somme de fonctions cosinus oscillant à différentes fréquences (Les équations mathématiques de la transformation directe et inverse voir Eq.1.1 et 1.2) :

$$F(u,v) = \frac{2}{\sqrt{N*M}} C(u)C(v) \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} f(i,j) \csc\left[\frac{\pi(2i+1)}{2N}u\right] \csc\left[\frac{\pi(2j+1}{2M}v\right]$$

$$0 \le u \le N-1\,;\;\; 0 \le v \le M-1$$

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

$$f(i,j) = \frac{2}{\sqrt{N * M}} \sum_{u=0}^{N-1} \sum_{V=0}^{M-1} F(u,v) C(u) C(v) \csc\left[\frac{\pi(2i+1)}{2N} u\right] \csc\left[\frac{\pi(2j+1)}{2M} v\right]$$

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

B. Technique basée sur la transformée de Fourier discrète (DFT)

La DFT est considérée comme un outil de traitement d'image important dans le domaine du tatouage car elle contrôle la fréquence d'un signal hôte et la décompose en ses composantes sinus et cosinus, ce qui donne des valeurs généralement complexes. Le DFT peut fournir la sélection des parties d'image adéquates pour intégrer le tatouage avec la plus grande invisibilité et robustesse, cette caractéristique rend le DFT adapté aux applications de tatouage. Comme Les schémas de tatouage basés sur DCT et DFT utilisent l'amplitude de ses coefficients pour intégrer le tatouage. Ainsi, les fréquences moyennes sont le meilleur emplacement pour intégrer le tatouage car la modification des coefficients de basse fréquence peut endommager la visibilité tandis que les coefficients de hautes fréquences peuvent être supprimés par compression JPEG. Il est utilisé dans le filigrane numérique car il a une bonne robustesse contre les attaques géométriques telles que le recadrage, la rotation et la mise à l'échelle. Elle offre plus de robustesse contre les attaques géométriques. Pour une image carrée de taille N x N, la DFT et l'IDFT sont données respectivement par les équations 2.1 et 2.2[48]. Pour ce faire, la transformée de Fourier rapide (FFT) est l'algorithme utilisé pour calculer la (DFT) et sa transformée inverse

$$F(k,I) = \frac{1}{M * N} \sum_{M-1}^{m=0} \sum_{N-1}^{n=0} F(m,n) e^{-j2\pi\left[\frac{km}{M} + \frac{nl}{N}\right]}$$

L'inverse de DFT est défini comme

$$F(m,n) = \sum_{M-1}^{k=0} \sum_{N-1}^{I=0} F(k,I) e^{j2\pi\left[\frac{mk}{M}+\frac{nl}{N}\right]}$$

C. Transformée discrète en ondelettes (DWT)

La transformée discrète en ondelettes (DWT) est une fonction mathématique qui associe à la fonction image, I(x, y) une autre fonction dont le domaine est exprimé en ondelettes. Dans le cas de l'image, cette fonction fournit une localisation spatiale appropriée et possède des caractéristiques multi-résolution, cette représentation fournit un cadre simple pour interpréter la formation de l'image, qui décompose l'image en un ensemble de composants à bande limitée qui peut être réutilisé pour reconstituer exactement l'image d'origine[1][47][28]. DWT décompose une image en composants basse fréquence et haute fréquence qui sont présentés en 4 sous-bandes notées LL, LH, HL et HH, où L = bas et H = haut. Si nous appliquons une DWT à 1 niveau sur une image bidimensionnelle, elle la divise en quatre parties[47]:

- **LL :** Il s'agit des détails basse fréquence de l'image originale. On peut dire que l'approximation de l'image réside dans cette partie.
- **LH :** Il s'agit des détails verticaux de l'image originale.
- **HL :** Il s'agit des détails horizontaux de l'image originale.
- **HH :** Il s'agit des détails haute fréquence de l'image d'origine

La sous-bande LL pourrait être décomposée en un autre niveau de 4 sous-bandes, comme le montre la figure 12 et 13, et cette décomposition pourrait persister jusqu'à ce que nous atteignions le nombre de niveaux souhaité, puisque la majorité de l'énergie de l'image se concentre ici. On peut reconstruire simplement l'image en appliquant la DWT inverse[41]. Dans les systèmes de tatouage numérique, les niveaux de décomposition les plus faibles de l'image, sont les plus utilisés pour l'insertion de la marque.[49]

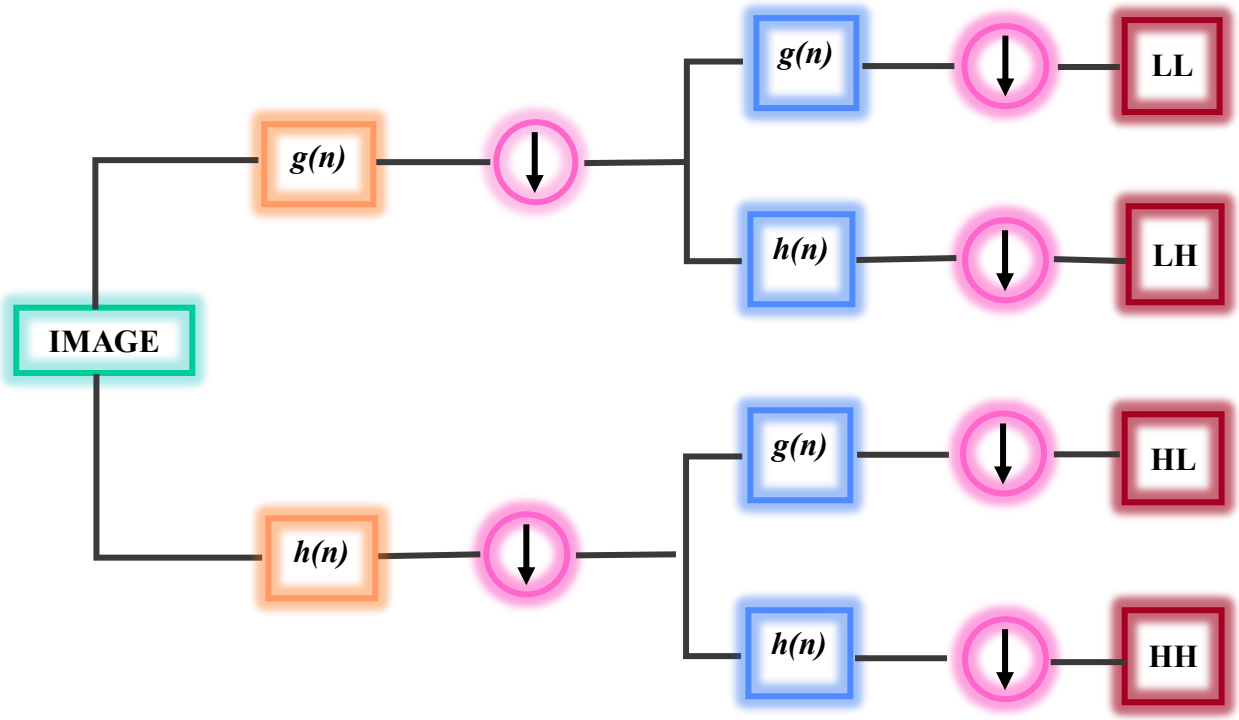


Figure II.12. Décomposition 2D-DWT d'une image.

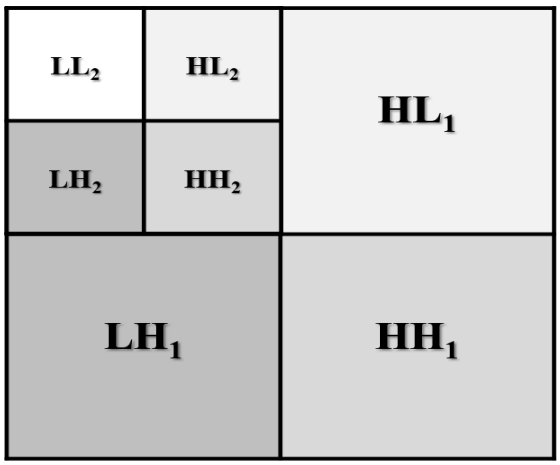


Figure II.13. La décomposition en ondelettes à 2 niveaux de résolution.

DWT effectue (Eq.3)[50]

$$Y_{\text{haute}}[k] = \sum_n x[n].g[2K-n] \qquad Y_{\text{faible}}[k] = \sum_n x[n].h[2K-n]$$

II.6.4. Domaine spatial vs Domaine fréquentiel

Pour comprendre la différence entre le domaine spatial et le domaine fréquentiel, une étude comparative est effectuée dans cette sous-section. Chacune de ces deux techniques a ses propres avantages et inconvénients (Voir Tableau.2)[51], donc privilégier un domaine n'est pas possible, un compromis entre plusieurs exigences qui sont définies par l'application de tatouage doit être considéré. Commençant par la technique d'insertion de la marque dans le domaine spatial, la marque est insérée directement dans les pixels de l'image tandis que dans le domaine fréquentiel, la marque est insérée dans les transformés des coefficients de l'image. En termes de robustesse, prenez le domaine fréquentiel, la marque est plus robuste que dans le domaine spatial. L'imperceptibilité dans le domaine spatial est plus élevée et contrôlable dans le domaine spatial alors que dans le domaine fréquentiel l'imperceptibilité est faible et contrôlable. Parlant de la capacité, nous remarquons que la capacité est plus élevée dans le domaine fréquentiel que dans le domaine spatial. Ainsi que pour la complexité de tatouage dans le domaine fréquentiel, nous remarquons qu'elle est plus élevée que la complexité dans le domaine spatial. En termes de temps d'exécution, le temps d'exécution dans le domaine spatial est plus faible que le temps d'exécution dans le domaine fréquentiel. Le tableau 3 montre la différence entre le domaine spatial et le domaine fréquentiel. Cette enquête capture également les limites et les avantages de chaque transformation[34][47].

Tableau II.2. Comparaison entre domaine spatial et domaine fréquentiel

Paramètre	Domaine spatial	Domaine fréquentiel
Avantage	Simplicité	Robuste contre le traitement d'image général
Désavantage	Échec du filigrane aveugle Faible résistance à certains	Échec du filigrane aveugle Faible résistance à certains
Capacité	Haut	Faible
Complexité informatique	Faible	Haut
Temps de traitement	Moins	Plus
Imperceptibilité	Faible	Haut
Robustesse	Faible	Haut

Tableau II.3. Enquête sur les techniques de tatouage dans le domaine spatial

Méthode	Idée basique	Avantages	Désavantages
LSB	-Les approches basées sur le domaine spatial sont conçues pour modifier des sous-ensembles de pixels sélectionnés d'images. - Elles intègrent directement le filigrane dans les pixels de l'image de couverture	•Facile à mettre en œuvre. •Faible complexité de calcul. •Ne génère pas de distorsion importante pour couvrir l'image. •Résistance aux attaques géométriques telles que la suppression de la distance intérieure, la mise à l'échelle, la rotation	• Restriction de robustesse. • Vulnérable au bruit, à la compression, au filtre passe-bas et à l'attaque par recadrage.
DCT	Dans ces techniques, l'image de couverture est d'abord transformée dans le domaine fréquentiel par l'utilisation de toute méthode de transformation, puis les valeurs de certaines fréquences sont modifiées pour intégrer le filigrane.	• Faible sensibilité du système visuel humain. • Difficile à détruire. • Tolérant aux manipulations du traitement du signal telles que la luminosité, le filtrage passe-bas, le flou et le réglage du contraste, etc.	• Difficile à mettre en œuvre. • Calcul plus pensif. cher. • Ils sont vulnérables aux attaques géométriques comme la rotation, la mise à l'échelle, le recadrage, etc.
DFT		• Plus robuste contre les manipulations géométriques comme le recadrage. • DFT est invariant RST. • Utile pour récupérer l'outil des distorsions géométriques.	• Mise en œuvre complexe. • Coût de calcul plus élevé. • Certaines composantes de fréquence plus élevée ont tendance à être supprimées pendant l'étape de quantification.
DWT		• Le HVS est plus étroitement traité. • Taux de compression plus élevé. • Bonne localisation à la fois dans le domaine des fréquences temporelles et spatiales.	• Plus grande complexité de calcul. • Temps de compression plus long. • Bruit/flou près des bords des images

II.7. Conclusion

En conclusion, la technologie du tatouage est une solution prometteuse pour renforcer la sécurité et la protection des données médicales. Avec la possibilité d'intégrer des marques invisibles et uniques dans les images numériques, la technologie de filigrane offre un moyen fiable d'identifier et de suivre les données médicales, ainsi que de détecter toute modification non autorisée ou tentative de falsification. De plus, le filigrane médical peut renforcer la vie privée et la confidentialité des patients, car il permet aux professionnels de la santé de partager des informations sensibles de manière plus sécurisée sans risquer des violations de données ou des violations de la confidentialité. Bien que la technologie de filigrane ne soit pas à l'abri des attaques ou des tentatives de piratage, elle offre une approche évolutive et rentable pour renforcer la sécurité des données dans les applications de télémédecine.

CHAPITRE 3
APPROCHE PROPOSEE ET IMPLEMENTATION

III.1. Introduction

L'infrastructure de télémédecine est basée sur la gestion numérique de l'information. Alors que les développements récents des technologies de l'information offrent de nouvelles façons d'accéder, de gérer et de déplacer les informations médicales. En raison de leur facilité de manipulation et de réplication, ils compromettent également leur sécurité. Ces dernières années, cacher des informations dans des images médicales est la plus grande utilisation pour sécuriser ces informations ou garantir l'intégrité du propriétaire, la stéganographie peut déformer l'image médicale et modifier les informations de santé nécessaires sur le patient.

Dans ce chapitre, nous proposons une méthode robuste de tatouage pour sécuriser les données des patients lorsqu'elles transitent dans un canal non sécurisé. L'utilisation des QR codes et des techniques de transformation d'ondelettes (DWT), la transformation en cosinus discret (DCT) et le bit le moins significatif (LSB) a renforcé la sécurité de ces données et images. Les codes QR sont des codes-barres bidimensionnels qui peuvent stocker une grande quantité d'informations. Pour sécuriser les données et images médicales à l'aide de codes QR, Converter les données ou images médicales dans un format compatible avec les codes QR (par exemple, PNG ou JPEG). Nous encodons les données médicales dans un QR code à l'aide d'un générateur de QR code. Le tatouage utilisant la technologie DWT et DCT peut être utilisé dans les dossiers médicaux et les images pour garantir leur authenticité et empêcher tout accès non autorisé ou falsification. Il peut également s'agir de protéger les données contre les cyber-attaques et la copie non autorisée, en cela d'aider à maintenir la confidentialité, l'intégrité et l'authenticité des données médicales. Enfin, nous avons décrit des résultats obtenus.

III.2. Implémentation

Nous avons utilisé le langage Python dans l'éditeur Microsoft Visual Studio pour l'implémentation de notre approche.

1- **Python :** Le langage Python est un langage de programmation open source multi-plateformes et orienté objet. Grâce à des bibliothèques spécialisées, Python s'utilise pour de nombreuses situations comme le développement logiciel, l'analyse de données, ou la gestion d'infrastructures. En effet, parmi ses qualités, Python permet notamment aux développeurs de se concentrer sur ce qu'ils font plutôt que sur la manière dont ils le font. Il a libéré les développeurs des contraintes de formes qui occupaient leur temps avec les autres langues. Ainsi, développer du code avec Python est plus rapide qu'avec d'autres langages.[52]

2- **Studio visuel Microsoft :** Microsoft Visual Studio est un environnement de développement intégré (IDE) disponible sur Windows, Linux et macOS. Il est doté de toutes les fonctionnalités d'un IDE moderne et prend en charge plusieurs langages de programmation, tels que C++, .NET, Java, Python, et PHP, ainsi que des environnements de développement Web, tels que ASP.NET MVC, entre autres. Il offre des outils et des fonctionnalités pour simplifier le développement de logiciels, d'applications Web. Il propose également des fonctionnalités avancées de débogage, des outils de test, des capacités de gestion de code source et des intégrations avec des systèmes de contrôle de version tels que Git. Il est largement utilisé par les développeurs professionnels et les amateurs et est considéré comme l'un des meilleurs environnements de développement intégrés disponibles.

III.3 Bibliothèque

1- **Opencv**(OpenSource Computer Vision) : Bibliothèques plus avancées de manipulation et de traitement d'images que PIL. Est aussi utilisé dans le cadre de la reconnaissance automatique en IA.[53]

2- **Pywt :**PyWavelets est un module de transformation d'ondelettes Python. il est très facile à utiliser et comprend la transformation d'ondelettes discrètes directes et inverses (DWT et IDWT), le calcul d'approximations des fonctions d'ondelettes et de mise à l'échelle....[54]

3- **Oreiller ouDIP:**Pillow est une bibliothèque de traitement d'image, elle dispose de capacités de traitement d'images relativement puissantes, Elle est conçue de manière à offrir un accès rapide aux données contenues dans une image, et offre un support pour différents formats de fichiers tels que PPM, PNG, JPEG, GIF, TIFF et BMP.[55]

4- **Numpy (Python numérique) :**est une bibliothèque de python qui comporte des fonctions permettant de manipuler des matrices ou des tableaux multidimensionnels, Les tableaux NumPy utilisent moins de mémoire et d'espace de stockage, ce qui le rend plus optimisé que les tableaux traditionnels de python.[56]

5- **Matplotlib :** Inspiré de Matlab, Matplotlib est une bibliothèque conçue pour tracer et visualiser des graphiques via le langage de programmation Python. Elle peut être combinée avec la bibliothèque python de calcul scientifique NumPy. Elle fournit également une API orientée objet, permettant d'intégrer des graphiques dans des applications.[57]

III.4. Notre Approche

Nous avons initialement basé notre méthode sur des articles existants, à la recherche de nouvelles méthodologies pour intégrer un tatouage de manière robuste et invisible. La principale différence avec la majorité des articles analysés était qu'ils utilisaient un cryptage ou la stéganographie pour extraire et intégrer le texte, une solution de contournement conforme aux règles était donc nécessaire. Dans l'ensemble, l'idée de base de la méthode proposée est de combiner les avantages du schéma de tatouage du domaine spatial et du domaine fréquentiel, nous avons utilisé pour mettre en œuvre une stratégie hybride impliquant la transformée discrète en ondelettes (DWT), et la transformée discrète en cosinus (DCT), qui est une méthode pour diviser l'image en blocs de taille N x N sont deux techniques couramment utilisées et le bit le moins significatif (LSB) du domaine spatial, qui ont été étudiés au chapitre 2. compte tenu de la comparaison visée au[58][59], l'imperceptibilité du tatouage et la résistance aux attaques sont plus importantes en DWT par rapport aux autres techniques, et comme en DCT. La méthode proposée consiste à intégrer le code QR ou l'image en tant que filigrane dans le domaine fréquentiel, résultant en quatre sous-bandes, servant de limiteur d'emplacement pour le filigrane. Cette technique est plus difficile à détecter et à supprimer, et préserver la qualité visuelle de l'image.

4.1. Schéma de tatouage de code QR proposé

Le schéma de tatouage de code QR proposé prend un code QR, qui contient les informations de tatouage, et l'intègre dans une image de couverture. Un aperçu du processus d'intégration du code QR dans l'image de couverture est illustré à la FigIII.1.

A. Le processus d'intégration

1. Appliquez la transformée discrète en ondelettes (DWT) à l'image de couverture pour obtenir les coefficients d'ondelettes. Cela décomposera l'image originale est décomposée en quatre sous-bandes LL1, HL1, LH1 et HH1
2. Choisissez la sous-bande LL1, qui contient les coefficients basse fréquence et représente l'approximation la plus grossière de l'image.
3. Ensuite, la sous-bande LL1 est divisée en blocs 8X8 sans chevauchement
4. Appliquez une transformée en cosinus discrète (DCT) aux coefficients de sous-bande LL1, pour obtenir les transactions DCT. Cela transformera les données d'image du domaine spatial au domaine fréquentiel.

5. Entrez du texte pour que le tatouage soit généré sous forme de code QR.
6. Convertissez le code QR en image binaire
7. Appliquez un DCT similaire à l'image du code QR du filigrane pour le convertir dans le domaine fréquentiel.
8. Nous calculons la valeur moyenne des DCT sélectionnés pour chaque bloc. La valeur moyenne est utilisée pour déterminer le seuil de quantification pour chaque bloc.
9. Nous traversons les éléments de la matrice de données d'image de code QR et comparons séquentiellement chaque élément avec le LSB de [8 8] de la matrice de coefficients DCT de l'image de couverture. S'ils sont égaux, réglez le LSB de [8 8] de la matrice de coefficients DCT de l'image de couverture sur 0, sinon réglez-le sur 1.
10. Appliquez une DCT inverse à la sous-bande LL1 modifiée pour obtenir la sous-bande LL1 filigranée.
11. Remplacez la sous-bande LL1 d'origine par la sous-bande LL1 filigranée.
12. Enfin, des DWT inverses sont appliqués pour obtenir l'image filigranée résultante

B. Le processus d'extraction

1. Nous appliquons une transformée DWT à l'image tatouée pour obtenir les coefficients d'ondelettes.
2. Nous choisissons le sous-domaine LL1 qui a été utilisé pour insérer le tatouage.
3. Divisez la sous-échelle LL1 en blocs 8x8 non superposés.
4. Appliquez une transformation DCT à chaque bloc de transactions dans le sous-domaine LL1.
5. Effectuez une opération XOR sur le LSB de [8X8] de la matrice de coefficients DCT de l'image de couverture et des images tatouée, puis nous pouvons obtenir l'image QR extraite.

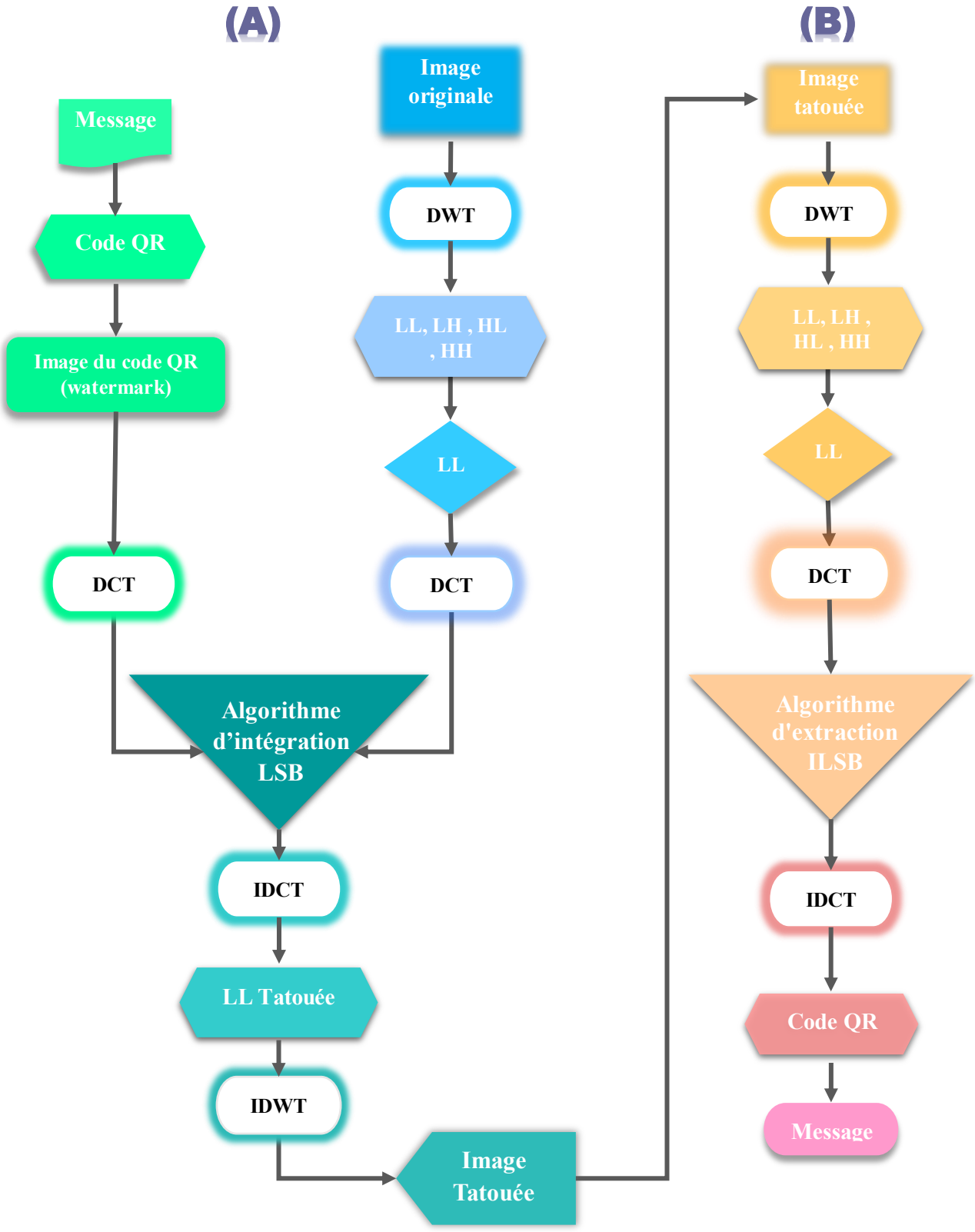


Figure.III.1. Schéma fonctionnel du tatouage du code QR (algorithme d'intégration A et d'extraction B).

4.2. Schéma de tatouage image en image

A. Le processus d'intégration

De la même manière, une image dans l'image est intégrée, comme illustré à la fig III.2.A

1. Nous convertissons l'image du tatouage et l'image de couverture en images en niveaux de gris pour obtenir deux matrices de données d'image.
2. Appliquez un DWT à la photo de couverture.
3. Définissez les paramètres du sous-domaine LL en sélectionnant les coefficients LL à partir des coefficients DWT de la photo de couverture.
4. Appliquez un DCT aux coefficients LL de la photo de couverture.
5. Intégrez le tatouage dans les coefficients DCT du sous-domaine LL de la photo de couverture.
6. Appliquez le DCT inverse pour obtenir le sous-domaine LL filigrané.
7. Appliquez le DWT inverse pour obtenir la photo de couverture en filigrane.
8. Enregistrer l'image tatouée.

B. Le processus d'extraction

Pour la section algorithme d'extraction, les étapes de l'extraction du tatouage sont représentées comme suit dans (fig III. 2.B) :

1. Lire l'image en tatouage.
2. Appliquez un DWT à l'image en tatouage.
3. Définir le sous-domaine LL.
4. Appliquer un DCT aux coefficients LL de l'image tatouée.
5. Extrayez le tatouage des coefficients DCT du sous-domaine LL. Les coefficients DCT modifiés sont comparés aux coefficients DCT d'origine, et les valeurs binaires du filigrane sont extraites sur la base des différences entre les deux ensembles de coefficients.
6. Reformatez les valeurs binaires extraites dans une matrice avec les mêmes dimensions que l'image du tatouage.

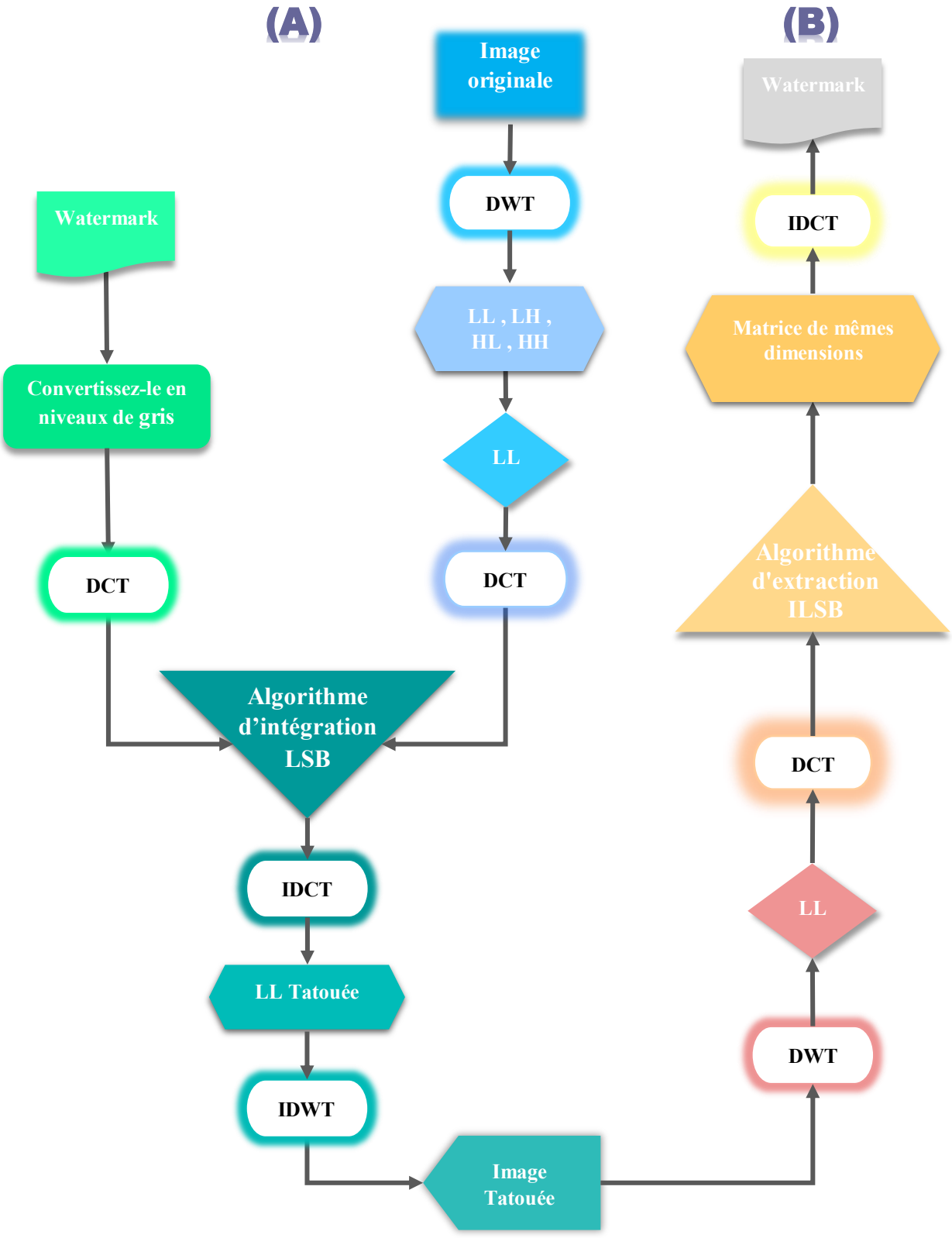


Figure.III.2. Schéma fonctionnel du tatouage de l'image (algorithme A- intégration et B-Extraction).

III.5. Métriques de mesures

5.1. Rapport signal-bruit de crête (PSNR)

L'imperceptibilité est mesurée par le paramètre Peak Signal to Noise Ratio (PSNR). La qualité des images originales et tatouées est comparée à l'aide de ce rapport, qui est mesuré en décibels. Un PSNR plus grand indique que l'image tatouée ressemble plus étroitement à l'image originale, ce qui signifie que le tatouage est plus imperceptible. Le PSNR et l'erreur quadratique moyenne (MSE) sont utilisés, où MSE est la différence des erreurs quadratiques cumulées entre les images tatouées et originales, tandis que le PSNR est la proportion de l'image originale qui est tatouée. En général, l'image tatouée avec une valeur PSNR supérieure à 28 dB est acceptable[60].

$$PSNR(I, Iw) = 10 * log_{10}\left(\frac{(255^2)}{MSE}\right)$$

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(xi - yi)^2$$

5.2. Analyse de corrélation normalisée (NC)

La robustesse d'un algorithme de tatouage est mesurée en termes de corrélation normalisée (NC) et de taux d'erreur sur les bits (BER). Cette métrique indique le facteur de ressemblance entre le tatouage inséré et extrait. Sa valeur est généralement de 0 à 1. Cependant, idéalement, il devrait être de 1, mais la valeur de 0,7 est acceptable[61]. Il est calculé par l'équation suivante:

$$NC(w, w') = \frac{\sum_{i=1}^{m}\sum_{j=1}^{m}[w(i,j).w'(i,j)]}{\sum_{i=1}^{m}\sum_{j=1}^{m}[w(i,j)]^2}$$

Où : W, W' sont respectivement le tatouage original et extrait.

Lorsque : NC=1, c'est la valeur maximale atteignable qui spécifie que tatouage inséré et extrait sont impossibles à différencier. NC=0, c'est la valeur minimale atteignable qui spécifie que le tatouage original et extrait sont exclusivement dissemblables.

III.6. Présentation de l'application

6.1. Interface graphique

L'interface de notre application trois boutons, le premier est "QR INSIDE IMAGE" pour nous convertir à l'interface le processus d'insertion ou d'extraction de texte sous forme de QR code, la seconde est "Image inside image" pour incorporer ou extraire une image dans une image. Aussi "Calculs" pour calculer PSNR et NC. In Figure III.3.

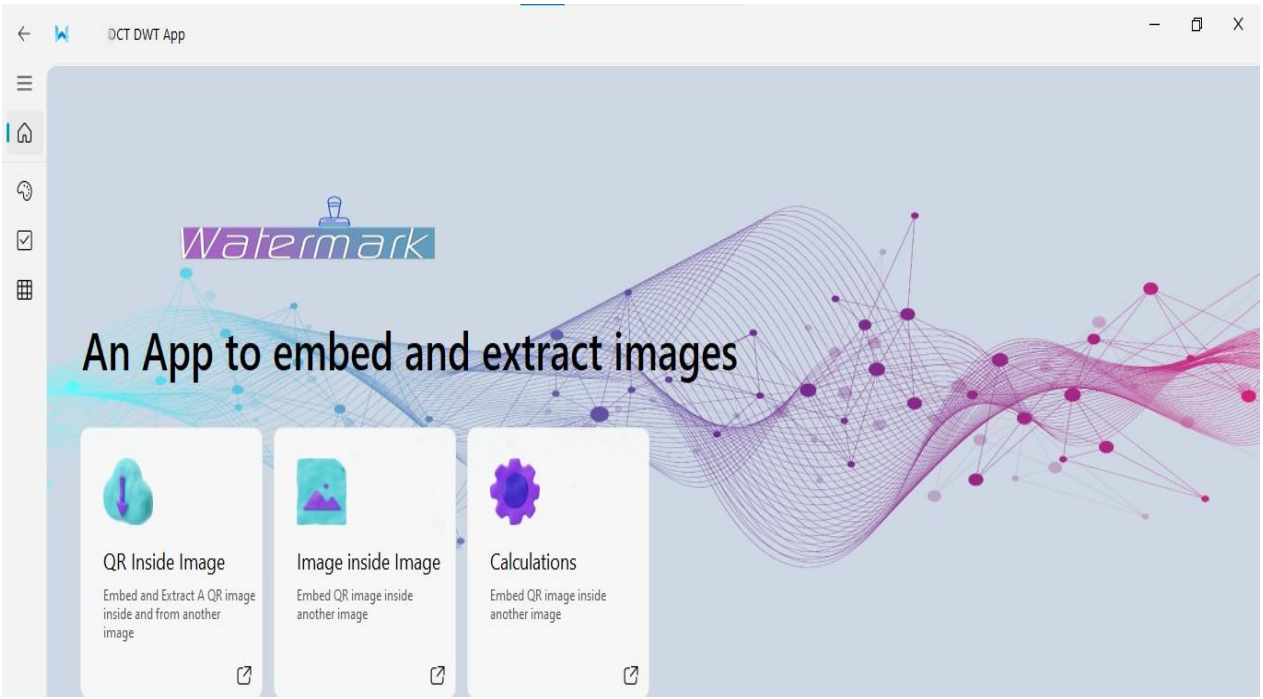


Figure III.3 : Interface graphique de l'application.

6.2. Processus d'insertion et d'extraction du code QR

Le processus d'insertion commence par la sélection du fichier dans lequel enregistrer les résultats, Écrivez ensuite la balise dans la zone de texte et affichez-la sous forme de code QR. Option d'image de couverture pour afficher une image avec un filigrane et l'enregistrer dans le fichier sélectionné. In Figure III.4.

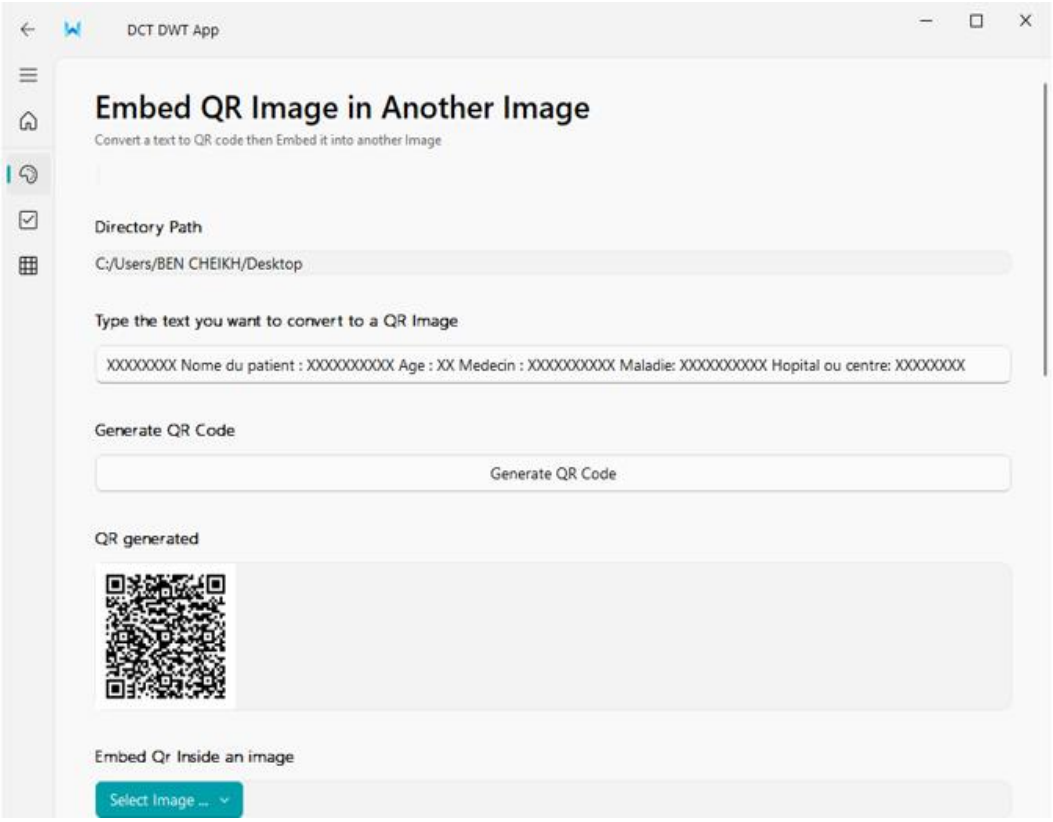


Figure III.4 : Interface processus d'insertion du code QR

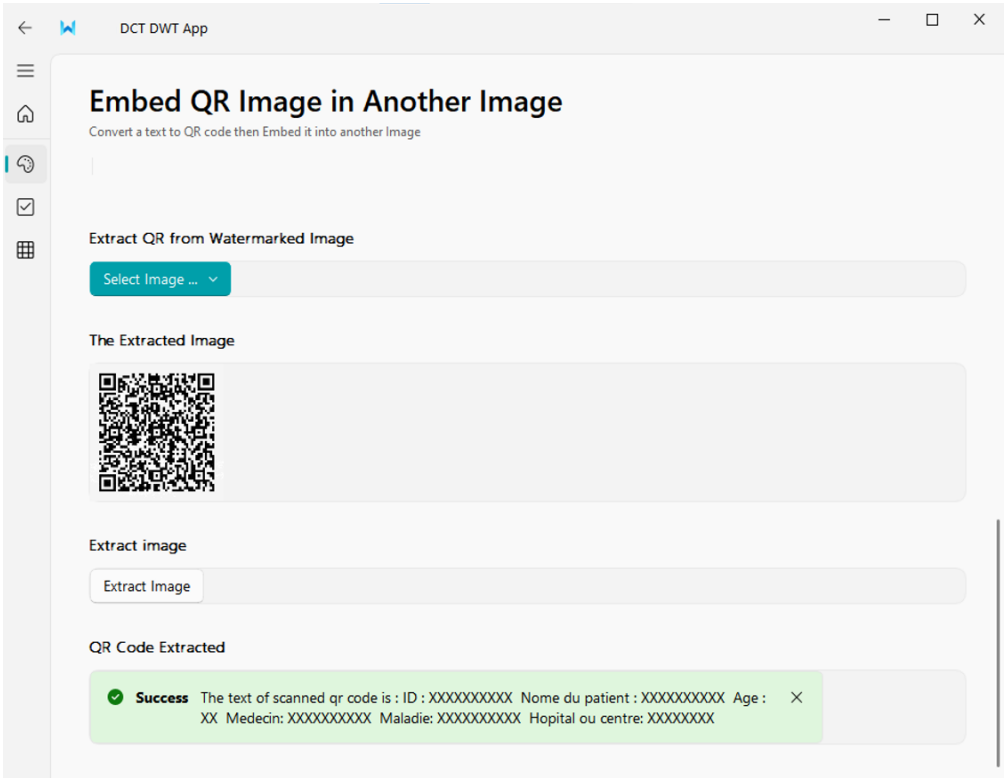


Figure III.5 : Interface processus d'extraction du code QR.

6.3. Processus d'insertion et d'extraction de l'image

De la même manière, une image est insérée dans une image en considérant d'abord l'image de couverture, puis l'image en tatouage, de sorte qu'une image avec un tatouage est enregistrée dans un fichier sélectionné.

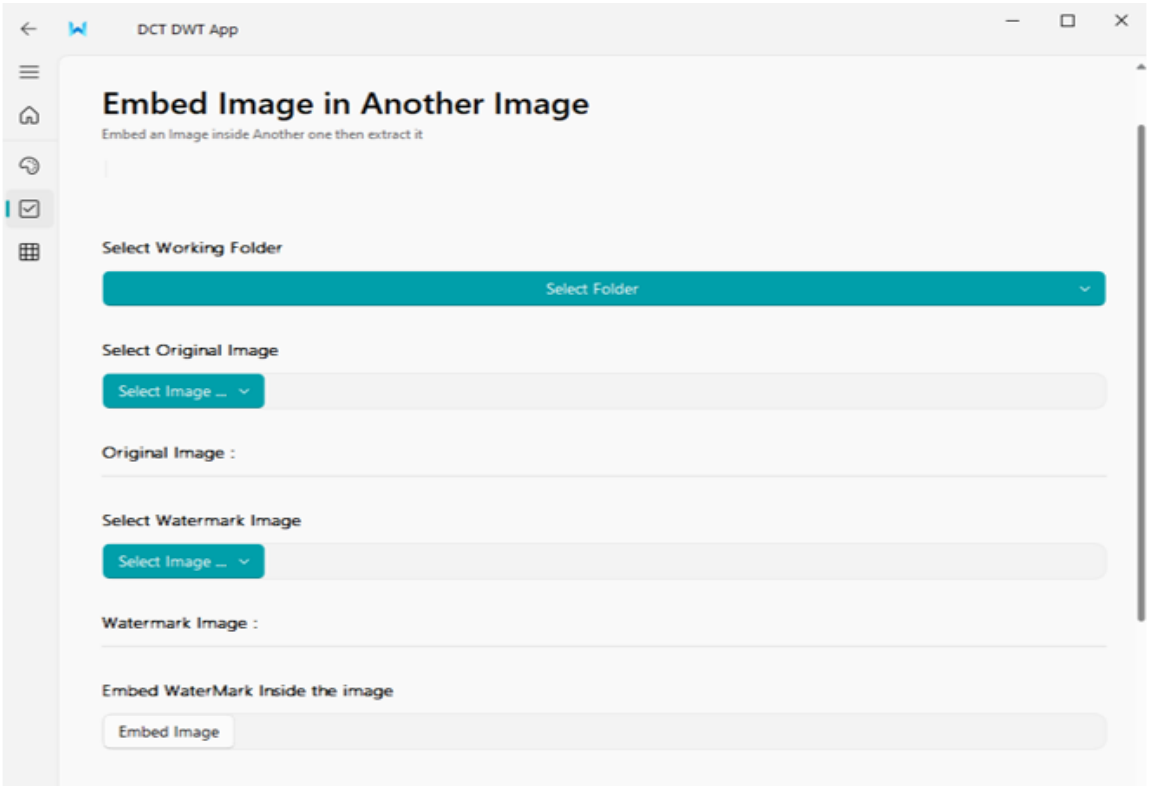


Figure III.6 : Interface processus d'insertion du tatouage de l'image.

Figure III.7 : Interface processus d'extraction du tatouage de l'image.

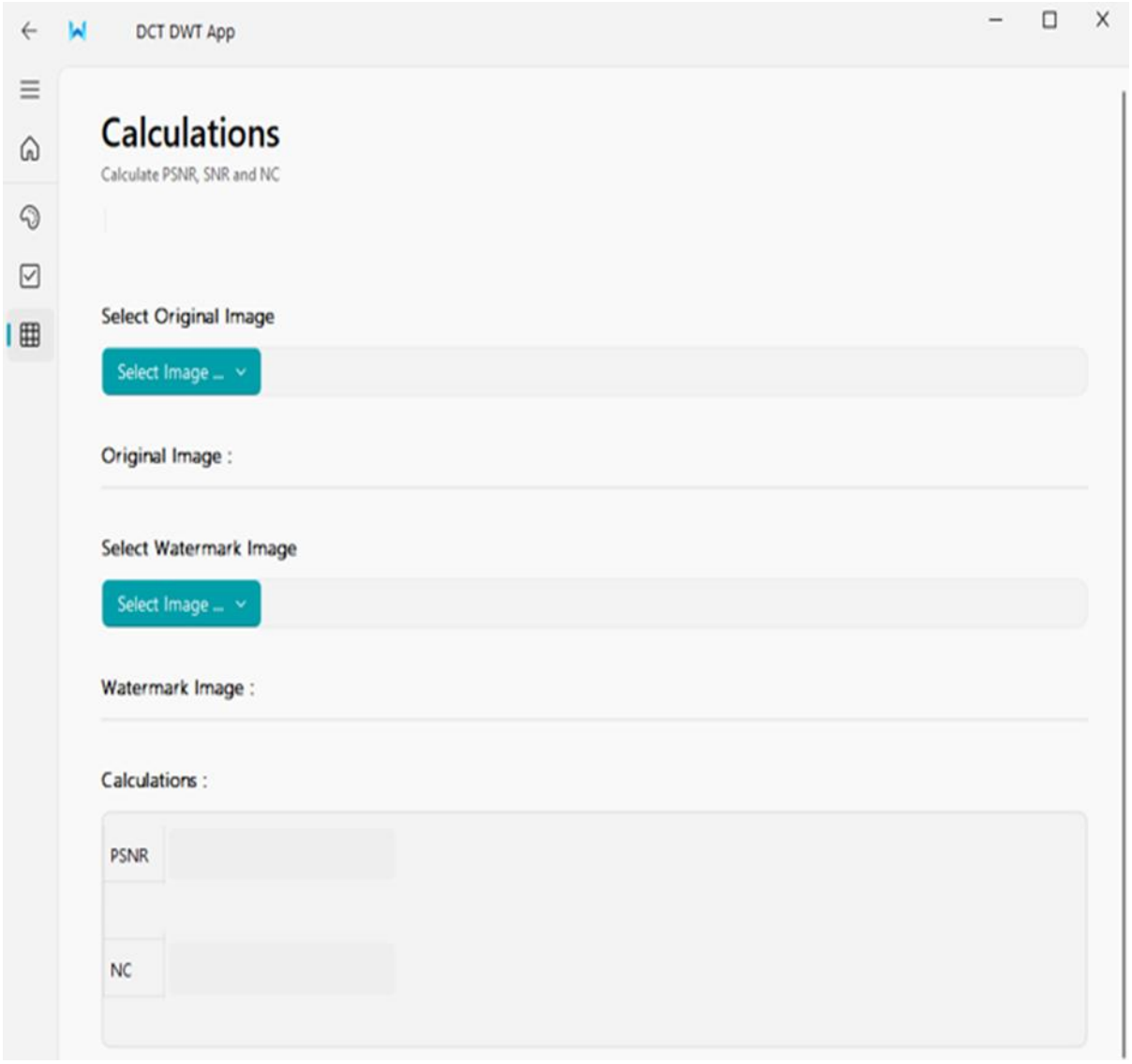


Figure III.8 : Interface d'affichage des résultats PSNR et NC.

III.7. Résultats Expérimentaux

Dans cette section, nous présentons Les résultats sont obtenus.

La figure III.9 et 10 montre les images en tatouage utilisées pour les résultats expérimentaux dans le tableau 1. Code QR texte, logo de l'hôpital et image médical

ID : XXXXXXXXXX

Nome du patient : XXXXXXXXXX

Age : XX

Médecin: XXXXXXXXXX

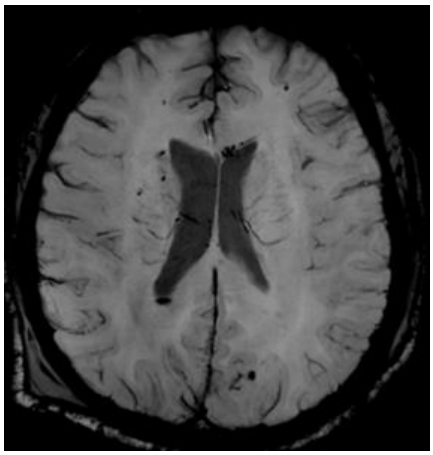
Maladie: XXXXXXXXXX

Hôpital ou centre: XXXXXXXX

(a)

(b)

Figure III.9 : (a) : texte, (b) : code QR de texte



(a)

(b)

Figure III.10 : Image en tatouage (a) : Image médical, (b) : Logo de l'hôpital

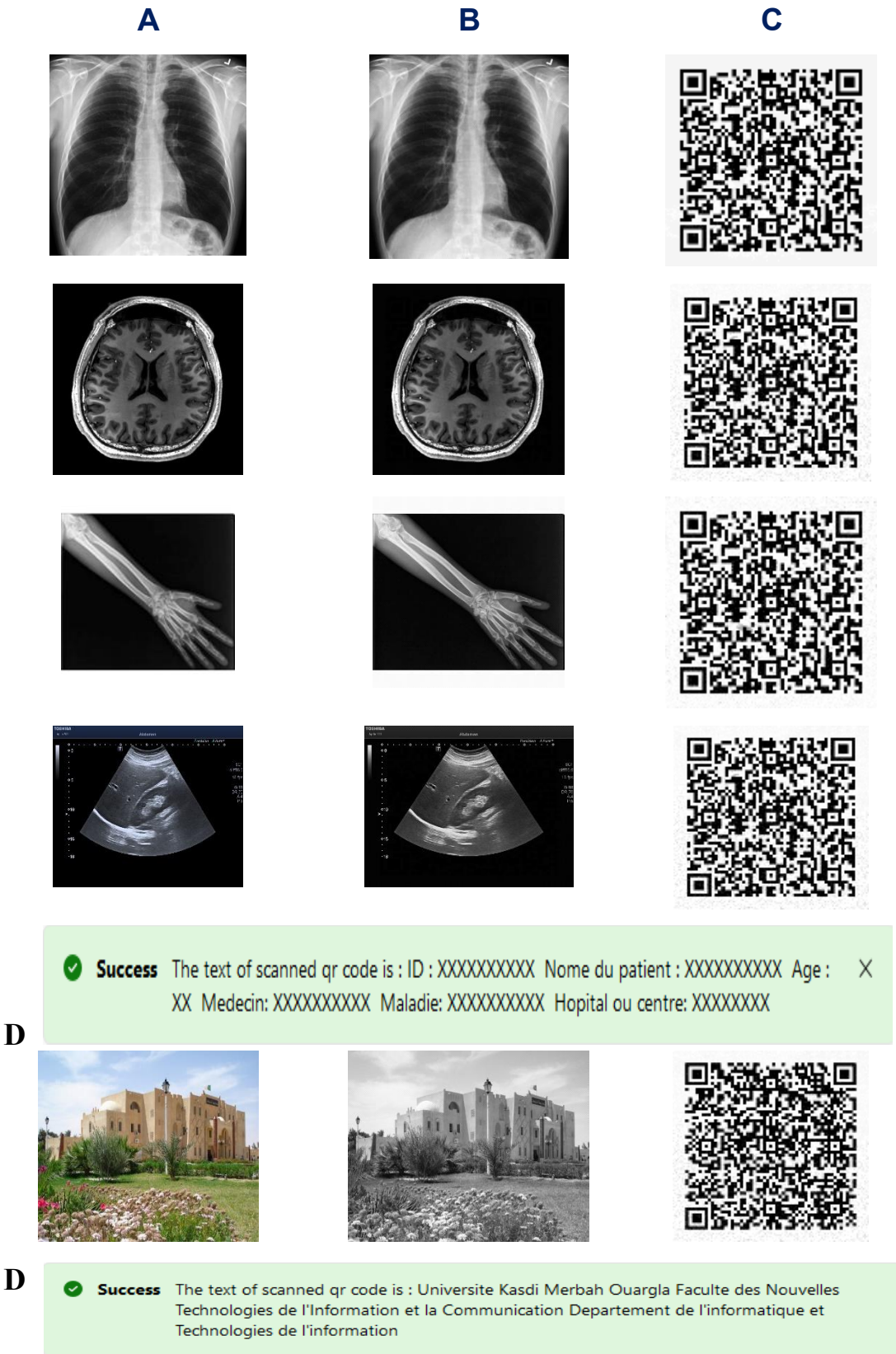


Figure III.11 : A Image de couverture, B image tatouage, C image tatouage récupérée et D Texte extrait du QR code.

III.8. ANALYSE COMPARATIVE

Les performances d'imperceptibilité du schéma proposé sont étudiées pour différents types d'images médicales, comme le montre la figure 9. Les images tatouées ne présentent aucune distorsion significative perçue. En outre, les performances d'imperceptibilité sont étudiées en termes de PSNR, et les résultats sont tabulés dans le tableau 1.

On peut étudier à partir du tableau 1 que les valeurs PSNR pour toutes les images sont supérieures à 35 dB. En général, la qualité visuelle de l'image tatouée est considérée comme bonne, si PSNR 35 dB[62][63]. De plus, les valeurs PSNR moyennes se situent entre 37,44dB et 42,61dB. Comme discuté, tatouage extrait d'images médicales tatouées. La robustesse du schéma proposé d'image différente est présentée dans, on peut observer à partir du tableau 1 que pour image médical, le logo de l'hôpital et le code QR sont proches des valeurs idéales

TABLEAU 1. PSNR, NC (Image médical, logo de l'hôpital et code QR)pour 4 images de couverture de test.

Images médicale	Image médical		Logo de l'hôpital		QR CODE	
	PSNR	NC	PSNR	NC	PSNR	NC
IRM	43,26	0,9987	43,40	0,9994	37,82	0,9988
CT Scan	43,10	0,9987	43,21	0,9994	37,51	0,9989
X-ray- main	41,46	0,9993	41,53	0,9995	36,96	0,9992
Ultrason	41,00	0,9984	42,30	0,9990	37,45	0,9978
Moyenne	42,21	0,9988	42,61	0,9993	37,44	0,9987

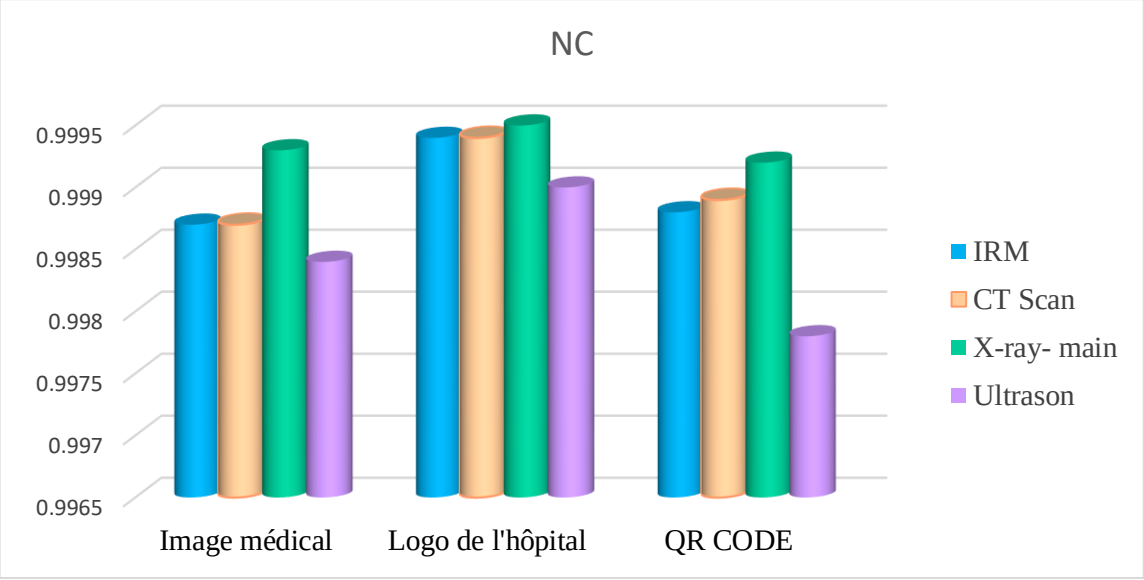


Figure III.12 : Performances NC de la méthode proposée en utilisant différentes images de couverture

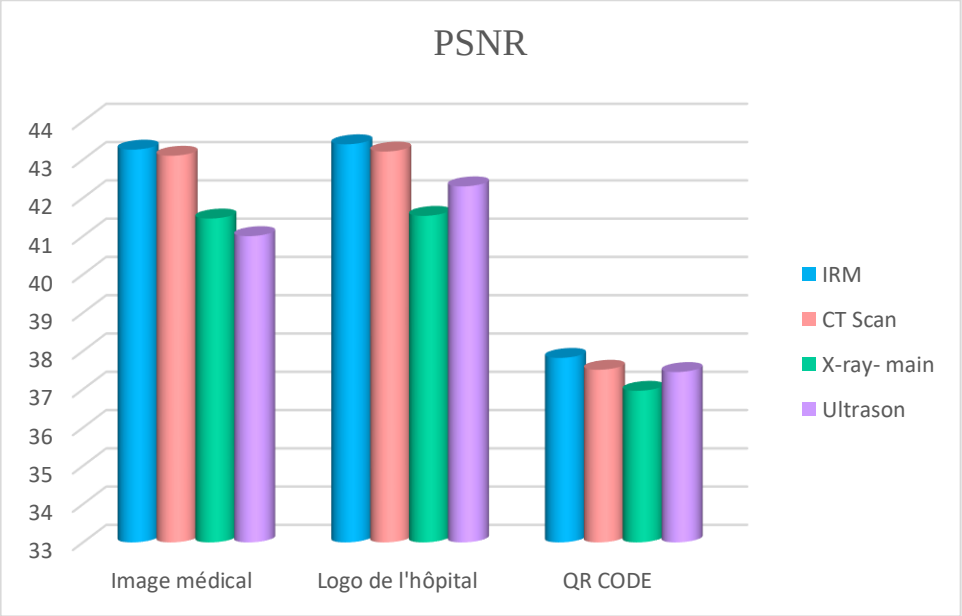


Figure III.13 : Performance PSNR de la méthode proposée en utilisant différentes images de couverture

III.9. Comparaison avec d'autres études

La comparaison de l'imperceptibilité et de la robustesse pour différentes images médicales, c'est-à-dire IRM thoracique, radiographie et scanner cérébral et échographie, est présentée dans le tableau 2. On peut observer à partir du tableau 2 que les valeurs PSNR du schéma proposé sont supérieures à N. Pulgam et S. Shinde [64], S.Thakur et al [65]et R.Thanki et al [66]. Il est également observé à partir des figures 14 et 15. Le tableau 2 montre que le schéma proposé a une valeur NC plus élevée que les autres schémas en comparaison. La comparaison de la valeur NC pour tous les schémas a également été illustrée à la figure 14. De cette observation, il est conclu que le schéma proposé à une imperceptibilité pour différentes modalités d'image que ses homologues.

TABLEAU 2. Analyser l'objectif des performances du système proposé.

Schème	IRM		X-ray		Image CT		Ultrason	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
N. Pulgam et S. Shinde[64]	33,67	0,97	30,24	0,92	28,58	0,95	/	/
S.Thakur et al [65]	35,52	0,9989	35,52	0,9665	35,52	0,9572	35,52	0,8082
R.Thanki et al [66]	37,81	0,9660	/	/	38,01	0,8668	37,92	0,9638
Proposer	43,26	0,9987	41,46	0,9993	43,10	0,9987	41,00	0,9984

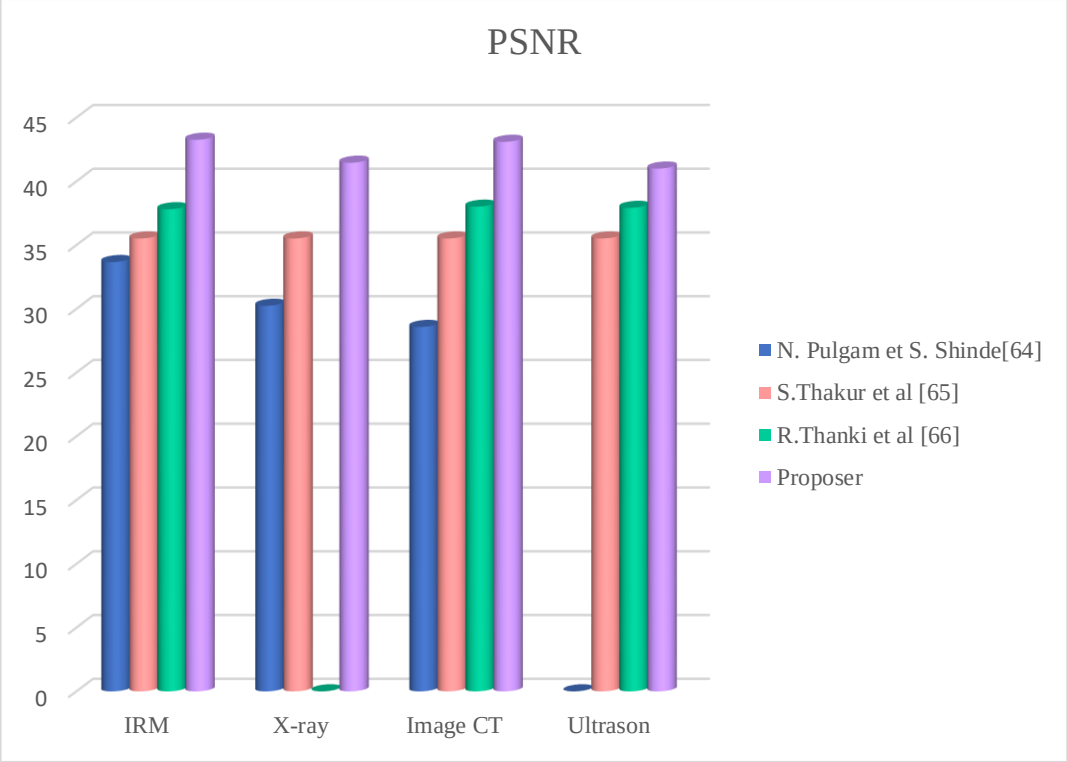


Figure III.14 : Comparaison des performances de l'imperceptibilité du schéma proposé avec d'autres études.

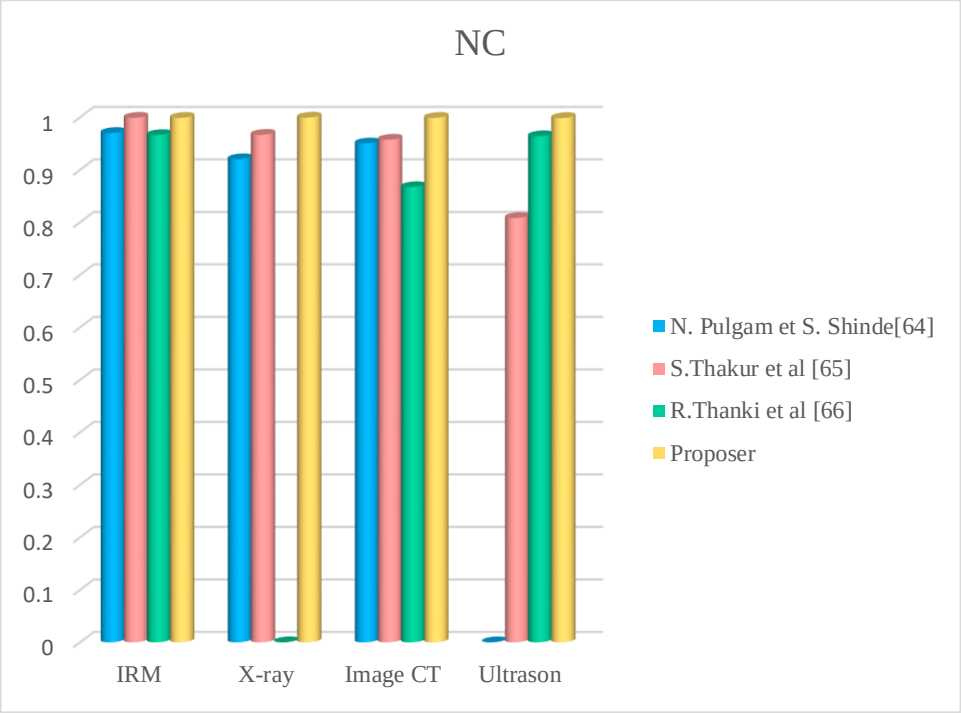


Figure III.15 : Comparaison des performances de la robustesse du schéma proposé avec d'autres études.

Dans le tableau 3, les performances PSNR et NC de la méthode hybride proposée pour différentes tailles de filigrane ont été évaluées sans aucune attaque de bruit. Avec le code QR, la valeur PSNR maximale est de 37,50 dB. Ici, la valeur NC est de 0,9986. Cependant, la valeur NC maximale est de 0,9987. Ce tableau montre également la comparaison des performances PSNR, NC de la méthode proposée avec d'autres techniques rapportées A.Mohan [67] A.Singh [60]. Ici, la valeur NC maximale avec la méthode proposée a été obtenue à 0,9987 avec des valeurs PSNR acceptables. Cependant, la valeur NC maximale obtenue avec A.Mohan [67] A.Singh [60]méthode sont respectivement de 0,9808 et 0,9937. La valeur PSNR maximale a été obtenue avec A.Mohan [67] A.Singh [60]sont respectivement de 36,19dB et 29,65dB. Cependant, la valeur PSNR maximale obtenue per la méthode proposée est de 37,13 dB en utilisant la même taille de texte.

TABLEAU 3. Analyse comparative du schéma proposé avec les techniques de pointe.

Schème	30 caractères		50 caractères	
	PSNR	**NC**	**PSNR**	**NC**
A.Mohan[67]	36,19	0,9808	35,84	0,9808
A.Singh[60]	29,65	0,9937	28,51	0,993
Proposer	37,13	0,9987	36,49	0,9986

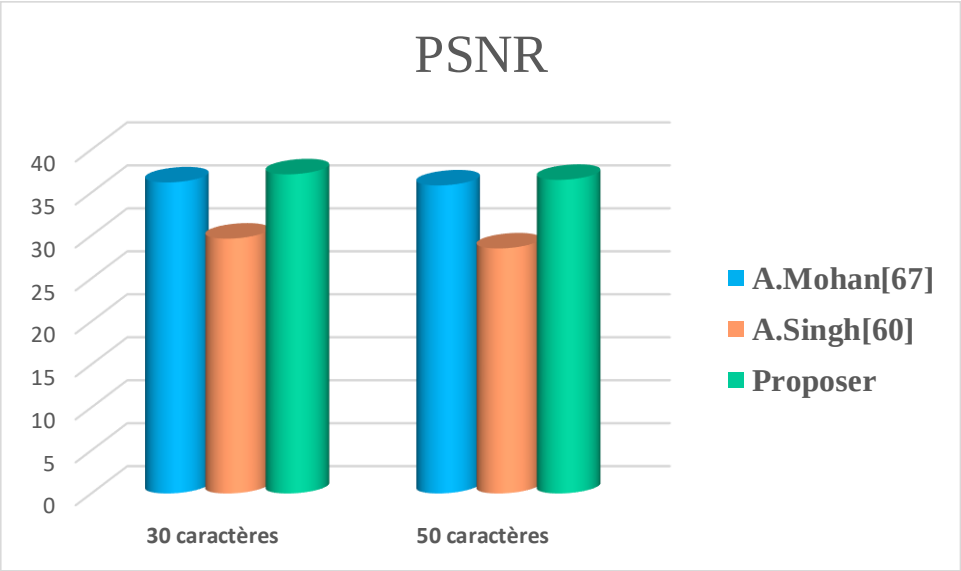


Figure III.16 : Comparaison des performances de l'imperceptibilité du schéma proposé avec d'autres études.

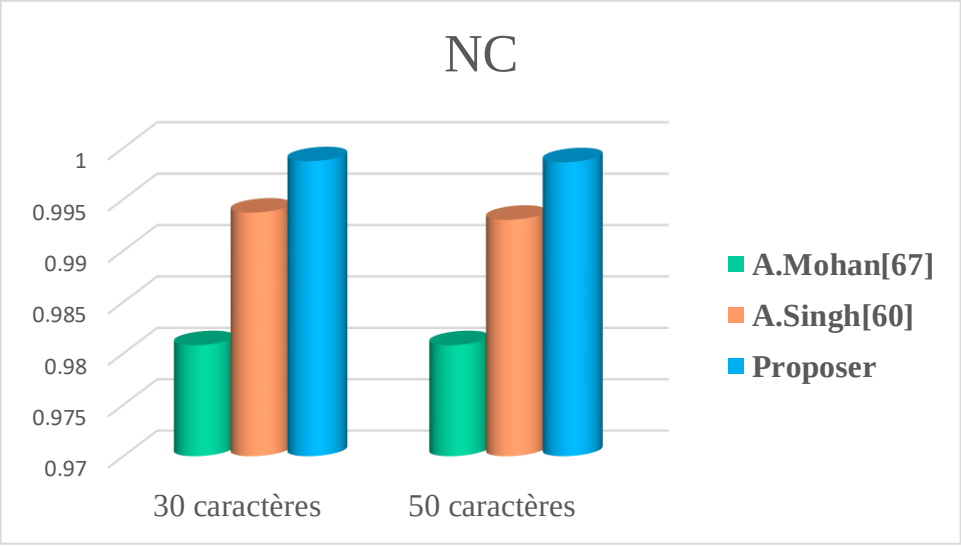


Figure III.17 : Comparaison des performances de la robustesse du schéma proposé avec d'autres études.

III.10. Conclusion

Dans ce chapitre, nous présentons nos contributions dans le domaine du tatouage d'images médicales fragiles. Pour assurer l'intégrité et l'identification de sabotage. Dans proposée technique, combine DWT, DCT et LSB, avec nous avons utilisé le code QR pour coder les données en utilise la sous-bande LL comme zone d'intégration, elle offre une meilleure capacité d'intégration, une sécurité de haut niveau, cependant, elle nécessite et doit encore être améliorée dans les travaux futurs. Les résultats expérimentaux sur différentes images médicales prouvent une imperceptibilité remarquable et une bonne authenticité des images médicales.

CONCLUSION GÉNÉRALE

CONCLUSION GÉNÉRALE

De nos jours, la sécurisation des données médicales (notamment les images médicales), dans la télémédecine, devient une activité complexe et déboursée.

Et pour cause, la plupart des techniques de tatouage existantes souffrent de trouver un consensus entre les exigences de tatouage telles la robustesse, l'imperceptibilité et la sécurité. Par robustesse, on désigne une forte similarité visuelle entre le tatouage original et celui extrait après avoir été attaqué. L'imperceptibilité signifie que le tatouage ne doit pas modifier de manière significative l'image hôte et doit être invisible. Alors que la sécurité doit garantir la protection de l'image contre tout type de tentative de modification.

Le travail présenté dans cette thèse consiste à proposer de nouvelles approches de tatouage sécurisé qui offrent une bonne robustesse (pour les méthodes robustes) en gardant une bonne qualité de l'image tatouée.

Au cours de ce mémoire, nous avons proposé un schéma de sécurisation des données médicales basé sur l'algorithme DWT, DCT et LSB de tatouage numérique avec l'algorithme de cryptage représenté par le code QR, qui a été utilisé pour chiffrer le tatouage. Le but principal de ce chiffrement c'est de garantir la confidentialité de l'information de l'image après l'envoie.

Il est également possible de se passer du QR code, d'inclure une image dans une image, puis de l'extraire

Finalement, Les comparaisons montrent que la technique proposée offre des performances très favorables

Comme perspective à ce travail, nous allons améliorer notre approche en utilisant d'autres techniques de tatouage.

TRAVAUX FUTURS

Le travail présenté dans cette thèse a porté sur la technique de tatouage médical concernant la préservation de la qualité des images médicales et l'authentification des images dans un

environnement non sécurisé. A cet effet, des perspectives qui semblent pertinentes à l'avenir afin d'améliorer ses performances.

- Tatouages d'images médicales avec détection, localisation et récupération d'effraction : il existe un besoin important pour une technique de tatouage qui pourrait détecter l'altération et localiser la zone altérée, puis la récupérer. La raison en est que l'image médicale est très sensible et pourrait même être modifiée involontairement (par exemple, un paquet de données corrompu via Internet), à cette fin, nous essayons d'utiliser certaines techniques d'intelligence pour trouver les caractéristiques les plus importantes pour l'intégration du tatouage.

RÉFÉRENCES

[1] M. Tayachi, “Sécurité des images par tatouage numérique et cryptographie dans les applications médicales,” L’UNIVERSITÉ DE BRETAGNE OCCIDENTALE ET L’UNIVERSITE DE TUNIS EL MANAR, 2022.

[2] M. AL-SHAIKH, “Protection des contenus des images médicales par camouflage d’informations secrètes pour l’aide à la télémédecine,” 2016.

[3] S. M. et B. N. Eddine, “Tatouage d ’ image médicale avec des données biométriques pour la confidentialité des dossiers de santé électroniques,” Université Larbi Tébessi, 2021.

[4] B. Teknolojileri, B. Enformatik, B. Enformatik, B. Enformatik, and A. Kelimeler, “Büyük Veri Açısından Biyomedikal Enformatik : Beklentiler ve Karşılaşılan Güçlükler Biomedical Informatics from Big Data Perspective : Expectations and Challenges,” p. 4, 2018.

[5] M. Albert, “Band 17,” 2019.

[6] C. O. Alenoghena *et al.*, “Telemedicine: A Survey of Telecommunication Technologies, Developments, and Challenges,” *J. Sens. Actuator Networks*, vol. 12, no. 2, p. 20, 2023, doi: 10.3390/jsan12020020.

[7] I. B. Aydilek, “Examining Effects of the Support Vector Machines Kernel Types on Biomedical Data Classification,” *2018 Int. Conf. Artif. Intell. Data Process. IDAP 2018*, p. 4, 2019, doi: 10.1109/IDAP.2018.8620879.

[8] M. R. Cowie *et al.*, “Electronic health records to facilitate clinical research,” *Clin. Res. Cardiol.*, vol. 106, no. 1, pp. 1–9, 2017, doi: 10.1007/s00392-016-1025-6.

[9] “The state of the art in health data analytics.” https://www.scnsoft.com/blog/health-data-analytics-overview (accessed Apr. 28, 2023).

[10] F. A. C. D. De Farias, C. M. Dagostini, Y. D. A. Bicca, V. F. Falavigna, and A. Falavigna, “Remote patient monitoring: A systematic review,” *Telemed. e-Health*, vol. 26, no. 5, pp. 576–583, 2020, doi: 10.1089/tmj.2019.0066.

[11] É. Debiès, “Health, big data and informational self-determination: Which articulation for a protective innovation of personal data?,” *Rev. Fr. d’Administration Publique*, vol. 167, no. 3, pp. 565–574, 2018, doi: 10.3917/rfap.167.0565.

[12] W. Kou, *Principles of Digital Image Compression*. 2013. doi: 10.1007/978-1-4757-2361-8_1.

[13] C. F. Ezzahra and K. Soumia, “Intitulé Sécurité des données médicales en appliquant le tatouage numérique,” UNIVERSITE MOHAMED BOUDIAF – M’SILA, 2020.

[14] A. M. Williams, U. F. Bhatti, H. B. Alam, and V. C. Nikolian, “The role of telemedicine in postoperative care,” pp. 1–9, 2018, doi: 10.21037/mhealth.2018.04.03.

[15] D. Kim, J. Choi, and K. Han, “Risk management-based security evaluation model for telemedicine systems,” vol. 7, pp. 1–15, 2020, doi: https://doi.org/10.1186/s12911-020-01145-7.

[16] N. H. Salem, D. Ouelha, M. Gharbaoui, S. Saadi, and M. Ben Khelil, “Medico-legal aspects

related to telemedicine in tunisia in the context of the COVID-19 pandemic," *Tunisie Medicale*, vol. 98, no. 6, pp. 423–433, 2020.

[17] "Data protection in the EU." https://commission.europa.eu/law/law-topic/data-protection/data-protection-eu_en (accessed Apr. 29, 2023).

[18] "The Security Rule | HHS.gov." https://www.hhs.gov/hipaa/for-professionals/security/index.html (accessed Apr. 29, 2023).

[19] M. B. Souad, "Etude et implémentation des techniques de tatouage numérique," UNIVERSITE DJILLALI LIABES, 2017.

[20] Amit Kumar Singh; Basant Kumar; Ghanshyam Singh; Anand Mohan, *Medical Image Watermarking: Techniques and Applications*. 2017.

[21] M. Khalid, K. Arora, and N. Pal, "A Crypto-Steganography: A Survey," *Int. J. Adv. Comput. Sci. Appl.*, vol. 5, no. 7, pp. 149–155, 2014, doi: 10.14569/ijacsa.2014.050722.

[22] M. Sasmal and D. Mula, "An enhanced method for information hiding using LSB steganography," *J. Phys. Conf. Ser.*, vol. 1797, no. 1, 2021, doi: 10.1088/1742-6596/1797/1/012015.

[23] K. Amarendra, V. N. Mandhala, B. C. Gupta, G. G. Sudheshna, and V. V. Anusha, "Image steganography using lsb," *Int. J. Sci. Technol. Res.*, vol. 8, no. 12, pp. 906–909, 2019.

[24] F. Q. A. Al-Yousuf and R. Din, "Review on secured data capabilities of cryptography, steganography, and watermarking domain," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 17, no. 2, pp. 1053–1059, 2019, doi: 10.11591/ijeecs.v17.i2.pp1053-1058.

[25] A. BENHOCINE, "Protection des contenus des images médicales dans le Cloud par camouflage d'informations secrètes pour aide à la télémédecine," Université Ferhat Abbas Sétif-1, 2021.

[26] M. Karasad, "Tatouage des images médicales partagées," L'ÉCOLE NATIONALE SUPERIEURE MINES-TELECOM ATLANTIQUE, 2020.

[27] S. Moataz, "Watermarking Medical Scans : Saliency Filter Pixels," *ResearchGate*, no. June, 2022, doi: 10.13140/RG.2.2.33193.67680.

[28] A. A. Embaby, M. A. W. Shalaby, and K. M. Elsayed, "Digital Watermarking Properties, Classification and Techniques," *Int. J. Eng. Adv. Technol.*, vol. 9, no. 3, pp. 2742–2750, 2020, doi: 10.35940/ijeat.c5773.029320.

[29] M. Begum and M. S. Uddin, "Digital image watermarking techniques: A review," *Inf.*, vol. 11, no. 2, 2020, doi: 10.3390/info11020110.

[30] A. Shell, "Les séquences chaotiques pour la sécurité des images : application des systémes de tatouage numérique robuste basé sur les séquences chaotiques pour la protection des droits d'auteurs," Untuersité Mohamed sadik Benyahia de jijel, 2016.

[31] A. H. Allaf and M. A. Kbir, *A Review of Digital Watermarking Applications for Medical Image Exchange Security*, no. January. Springer International Publishing, 2019. doi:

10.1007/978-3-030-11196-0_40.

[32] S. Haddad, “Protection of encrypted and / or compressed medical images by means of watermarking,” 2021.

[33] E. EL-Shazly, E.-S. M. El-Rabaie, M. A. Ashour, A. M. Abbas, and H. Kazemian, “Digital Image Watermarking in Transform Domains,” Minufiya University, 2012.

[34] W. BELFERDI, “A Robust Watermarking Approach for Images Authentication and Traceability,” University of Batna 2.

[35] M. Patel, P. S. Sajja, and J. Patel, “Enhancement of DWT based Watermarking Technique for Images,” vol. 2, no. 12, pp. 4750–4756, 2013.

[36] S. Patel, A. Katharotiya, and M. Goyani, “A detailed Study of Digital Image Watermarking Techniques,” no. October, 2022, doi: https://www.researchgate.net/publication/364307567 A.

[37] B. Kaur and S. Sharma, “Digital Watermarking and Security Techniques: A Review,” *Ijcst*, vol. 8, no. 2, pp. 44–47, 2017, [Online]. Available: http://www.ijcst.com/vol8/8.2/9-baljit-kaur.pdf

[38] D. Patel, N. Chitaliya, M. Pandya, P. Trivedi, M. B. Potdar, and P. Thakkar, “Digital Video Watermarking : A Retrospective,” *Int. J. Sci. Eng. Res.*, vol. 5, no. 12, pp. 1–11, 2014.

[39] M. A. Otair, “Security in digital images: From information hiding perspective,” *Handb. Res. Threat Detect. Countermeas. Netw. Secur.*, no. March, pp. 381–394, 2014, doi: 10.4018/978-1-4666-6583-5.ch021.

[40] M. Mustaqim Abrar, A. Pal, and T. M. Shahriar Sazzad, “Bit Plane Slicing and Quantization-Based Color Image Watermarking in Spatial Domain,” no. August 2022, pp. 371–383, 2021, doi: 10.1007/978-981-16-0586-4_30.

[41] M. Hatoum, “Digital watermarking for PDF documents and images : security, robustness and AI-based attack,” 2021.

[42] P. Singh and R. S. Chadha, “A Survey of Digital Watermarking Techniques , Applications and Attacks,” vol. 2, no. 9, pp. 165–175, 2013.

[43] P. B. Deshmukh, M. V. A. Metre, and M. Shradhha, “An Overview : Watermarking Approach for Digital Images,” vol. 11, no. 3, pp. 33–36, 2018, doi: http://dx.doi.org/10.21172/ijiet.113.06.

[44] M. Abdullatif, A. M. Zeki, J. Chebil, and T. S. Gunawan, “Properties of digital image watermarking,” *Proc. - 2013 IEEE 9th Int. Colloq. Signal Process. its Appl. CSPA 2013*, pp. 235–240, 2013, doi: 10.1109/CSPA.2013.6530048.

[45] S. M. Mousavi, A. Naghsh, and S. A. R. Abu-Bakar, “Watermarking Techniques used in Medical Images: a Survey,” *J. Digit. Imaging*, vol. 27, no. 6, pp. 714–729, 2014, doi: 10.1007/s10278-014-9700-5.

[46] R. Souadek, “Techniques sécurisantes par watermarking,” UNIVERSITÉ FERHAT

ABBAS - SETIF1, 2021. doi: 10.13140/RG.2.2.28201.67686.

[47] S. Tyagi, H. V. Singh, R. Agarwal, and S. K. Gangwar, “Digital watermarking techniques for security applications,” *Int. Conf. Emerg. Trends Electr. Electron. Sustain. Energy Syst. ICETEESES 2016*, pp. 379–382, 2016, doi: 10.1109/ICETEESES.2016.7581413.

[48] Z. Yuan, Q. Su, D. Liu, and X. Zhang, “A blind image watermarking scheme combining spatial domain and frequency domain,” *Vis. Comput.*, vol. 37, no. 7, pp. 1867–1881, 2021, doi: 10.1007/s00371-020-01945-y.

[49] T. Pardhu and B. R. Perli, “Digital Image Watermarking in Frequency Domain,” pp. 208–211, 2016.

[50] V. A. Pimpalkhute, R. Page, A. Kothari, S. Member, K. M. Bhurchandi, and V. M. Kamble, “Using DWT Coefficients,” vol. 30, pp. 1962–1972, 2021.

[51] M. Boreiry and M. R. Keyvanpour, “Classification of watermarking methods based on watermarking approaches,” *7th Conf. Artif. Intell. Robot. IRANOPEN 2017*, pp. 73–76, 2017, doi: 10.1109/RIOS.2017.7956446.

[52] “Définition | Python | Futura Tech.” https://www.futura-sciences.com/tech/definitions/informatique-python-19349/ (accessed Apr. 21, 2023).

[53] C. E. Widodo, K. Adi, and R. Gernowo, “Medical image processing using python and open cv,” *J. Phys. Conf. Ser.*, vol. 1524, no. 1, pp. 4–8, 2020, doi: 10.1088/1742-6596/1524/1/012003.

[54] “PyWavelets - Wavelet Transforms in Python — PyWavelets Documentation.” https://pywavelets.readthedocs.io/en/latest/ (accessed Apr. 21, 2023).

[55] “Python Imaging Library (PIL) — Documentation Bibliothèques Python 1.0.0.” https://he-arc.github.io/livre-python/pillow/index.html (accessed Apr. 21, 2023).

[56] “Maîtrisez l’analyse des données avec NumPy Python.” https://www.data-transitionnumerique.com/numpy-python/ (accessed Apr. 21, 2023).

[57] “Matplotlib : maîtriser la bibliothèque Python de data visualisation.” https://www.journaldunet.fr/web-tech/guide-de-l-intelligence-artificielle/1501867-matplotlib/ (accessed Apr. 21, 2023).

[58] K. S. B. Radhika v. Totla, “Comparative Analysis of Watermarking in Digital Images Using DCT & DWT,” vol. 3, no. 2, pp. 3–6, 2013.

[59] A. Benyoucef and M. ’H Hamadouche, “RONI-Based Medical Image Watermarking Using DWT and LSB Algorithms,” *Lect. Notes Networks Syst.*, vol. 413 LNNS, no. April, pp. 468–478, 2022, doi: 10.1007/978-3-030-96311-8_43.

[60] A. K. Singh, “Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images,” *Multimed. Tools Appl.*, vol. 76, no. 6, pp. 8881–8900, 2017, doi: 10.1007/s11042-016-3514-z.

[61] A. Singh and M. K. Dutta, “Lossless and Robust Digital Watermarking Scheme for Retinal

Images," *Int. Conf. "Computational Intell. Commun. Technol. CICT 2018*, no. Cict, pp. 1–5, 2018, doi: 10.1109/CIACT.2018.8480151.

[62] M. Moosazadeh and G. Ekbatanifard, "A new DCT-based robust image watermarking method using teaching-learning-Based optimization," *J. Inf. Secur. Appl.*, vol. 47, pp. 28–38, 2019, doi: 10.1016/j.jisa.2019.04.001.

[63] D. Liu, Z. Yuan, and Q. Su, "A blind color image watermarking scheme with variable steps based on Schur decomposition," *Multimed. Tools Appl.*, vol. 79, no. 11–12, pp. 7491–7513, 2020, doi: 10.1007/s11042-019-08423-1.

[64] N. D. Pulgam and S. K. Shinde, "Robust Digital Watermarking using Pixel Color Correlation and Chaotic Encryption for Medical Image Protection," 2022.

[65] S. Thakur, A. K. Singh, S. P. Ghrera, and M. Elhoseny, "Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications," *Multimed. Tools Appl.*, vol. 78, no. 3, pp. 3457–3470, 2018, doi: 10.1007/s11042-018-6263-3.

[66] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "A RONI Based Visible Watermarking Approach for Medical Image Authentication," *J. Med. Syst.*, vol. 41, no. 9, 2017, doi: 10.1007/s10916-017-0795-3.

[67] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible multiple watermarking using medical images," *Multimed. Tools Appl.*, vol. 75, no. 14, pp. 8381–8401, 2016, doi: 10.1007/s11042-015-2754-7.