

Ministère de l'enseignement supérieure de la recherche scientifique

Université KASDI Merbah-Ouargla

Faculté des Nouvelles Technologies de l'Information et de la Communication
Département d'Informatique et de la Technologie de l'Information



Mémoire

Présenté en vue de l'obtention du diplôme de Master

Spécialité : Informatique Industrielle

**Présenté par : BACHA Melissa
BENISSAD Bouchra**

Thème

Protection du copyright des images Médicales par tatouage numérique

Membres de jury :

Dr.HAMROUNI Besma	Président	UKM Ouargla
Dr.KAHLESSENANE Fares	Encadreur	UKM Ouargla
Dr.BENBEZZIANE Mohamed	Examineur	UKM Ouargla

Année universitaire :2023/2024

REMERCIEMENTS

En premier, nous aimerions remercier le Dieu le tout puissant de nous avoir donné le courage et la volonté de réaliser ce projet.

Nous désirons remercier nos chers parents qui nous ont soutenus et encouragé durant toute notre vie et pendant notre cursus d'étude.

Nos remerciements les plus chaleureux vont à Mr F. KAHLESSENANE

Pour sa disponibilité et ses très précieux conseils ainsi que ses remarques qui nous ont permis d'améliorer la qualité de ce travail.

Nos vifs remerciements s'adressent également à tous nos enseignants de la faculté des nouvelles technologies de l'information et de la communication de l'université KASDI MERBAH Ouargla pour la formation qu'ils ont eu le soin de nous apporter le long de notre cursus universitaire.

DÉDICACE

Avec l'expression de ma sincère reconnaissance, je dédie humblement ce travail à ceux qui ont été mes piliers tout au long de ma vie. Leur amour, leur soutien et leur inspiration ont été un moteur pour moi, et je ne pourrai jamais assez les remercier.

À mes parents, la plus belle mère et au meilleur père au monde, pour leur amour inconditionnel, leur soutien indéfectible et leur confiance en moi. Je prie Dieu de vous protéger pour moi, de vous donner une longue vie heureuse et en bonne santé.

À mon frère Mohammed Haythem, ainsi qu'à mes sœurs, qui ont été ma force tout au long de ma vie.

À mes grands-pères et mes grand-mères et à toute ma famille, qui m'ont inspiré volonté et sagesse.

À mon oncle Amor et sa femme Malika, qui ont toujours été là pour moi.

À mes meilleures amies pour leur soutien constant et leurs encouragements à mon égard, et pour avoir rendu ma vie plus belle et plus joyeuse.

Et enfin, à ma meilleure binôme Melissa qui m'a accompagné tout au long de ce projet, pour notre collaboration fructueuse et notre amitié sincère. Cette dédicace est un hommage à toutes les personnes qui ont joué un rôle important dans ma vie et qui ont contribué à mon parcours académique et personnel. Je leur suis infiniment reconnaissant(e) pour tout ce qu'ils ont fait pour moi et je leur dédie ce mémoire avec amour et gratitude.

Bouchra Benissad

DÉDICACE

Je dédie ce mémoire :

À mes chers parents,

Je tiens à vous exprimer toute ma gratitude et ma reconnaissance pour le soutien constant que vous m'avez apporté tout au long de mon parcours d'études. Votre amour inconditionnel, vos encouragements et vos sacrifices ont été les piliers de ma réussite.

À mon frère salah, Merci d'avoir toujours cru en moi vous êtes mon meilleur compagnon de vie.

À ma grand-mère, ainsi que tous les membres de ma famille - oncles, tantes, cousins et cousines - qui ont toujours été présents pour moi.

À mes proches amies, vous êtes les sœurs que j'ai choisies. Votre présence joyeuse et vos mots d'encouragement ont illuminé mes journées les plus sombres. Vous avez été mes confidentes, mes conseillères et mes soutiens inconditionnels.

Enfin, à ma meilleure binôme Bouchra, merci d'avoir été à mes côtés tout au long de ce travail. Nous avons surmonté ensemble les défis, partagé nos idées et soutenu mutuellement. Ta présence et ta collaboration ont été inestimables, et je suis reconnaissant d'avoir pu compter sur toi pour achever ce projet avec succès.

Melissa Bacha

ملخص

أدت التطورات الأخيرة في الطب إلى ثورة رقمية، حيث تلعب الصور الطبية دورًا حاسمًا في التشخيص والبحث والتعليم. وقد جلب هذا التحول فوائد كبيرة: زيادة إمكانية الوصول، وتعاون أقوى بين المهنيين الصحيين ورعاية أكثر فعالية للمرضى. ومع ذلك، يأتي هذا العصر الرقمي مع مخاوف جدية بشأن الوصول غير المصرح به أو التلاعب أو سرقة المعلومات الطبية الحساسة. تهدد هذه المخاطر خصوصية المريض وأمن الرعاية، حيث تحتوي الصور الطبية غالبًا على بيانات شديدة الحساسية. لمواجهة هذه التحديات، تستكشف دراستنا تقنيات العلامات المائية الرقمية المتقدمة، مع التركيز على تكامل تحويل جيب التمام المنفصل (DCT) والجزء الأقل أهمية (LSB). يسمح DCT بإدخال العلامات المائية بحكمة في نطاقات تردد مختلفة، مما يزيد من عدم الإحساس والمتانة. في الوقت نفسه، تضمن طريقة LSB أن يظل التأثير الإدراكي ضئيلاً. هدفنا هو تحقيق التوازن بمهارة بين عدم الإحساس والقوة من خلال تقييم تأثير نطاقات تردد DCT على جودة العلامات المائية في الصور الطبية. من خلال الجمع بين هذه التقنيات المبتكرة، نهدف إلى تأمين معلومات نصية حساسة في الصور الطبية، وبالتالي تغيير مشهد حماية البيانات في قطاع الرعاية الصحية. يسعى نهجنا ليس فقط للحفاظ على سرية المريض، ولكن أيضًا لضمان مزيد من النزاهة والثقة في استخدام الصور الطبية في العصر الرقمي.

الكلمات الرئيسية: البت الأقل أهمية، تحويل جيب التمام المنفصل، الصورة الطبية، العلامات المائية

.الرقمية، مجال التردد، أمن البيانات، المتانة، عدم الإحساس

Résumé :

Les avancées récentes en médecine ont amorcé une révolution numérique, où les images médicales jouent un rôle crucial dans le diagnostic, la recherche et l'éducation. Cette transformation a apporté des avantages considérables : une accessibilité accrue, une collaboration renforcée entre les professionnels de santé et des soins plus efficaces pour les patients. Cependant, cette ère numérique s'accompagne de préoccupations sérieuses concernant l'accès non autorisé, la manipulation ou le vol d'informations médicales sensibles. Ces risques menacent la confidentialité des patients et la sécurité des soins, car les images médicales contiennent souvent des données extrêmement sensibles. Pour affronter ces défis, notre étude explore des techniques de tatouage numérique de pointe, en mettant l'accent sur l'intégration de la transformation en cosinus discrète (DCT) et du bit le moins significatif (LSB). La DCT permet une insertion judicieuse des tatouages dans différentes plages de fréquences, maximisant l'imperceptibilité et la robustesse. Parallèlement, la méthode LSB garantit que l'impact perceptuel reste minimal. Notre objectif est d'équilibrer subtilement l'imperceptibilité et la robustesse en évaluant l'influence des bandes de fréquences DCT sur la qualité du tatouage dans les images médicales. En mariant ces techniques innovantes, nous visons à sécuriser les informations textuelles sensibles dans les images médicales, transformant ainsi le paysage de la protection des données dans le secteur de la santé. Notre approche s'efforce non seulement de préserver la confidentialité des patients, mais aussi d'assurer une intégrité et une confiance accrues dans l'utilisation des images médicales à l'ère numérique.

Mots-clés : Transformation en cosinus discrète, image médicale, tatouage numérique, le bit le moins significatif, sécurité des données, robustesse, imperceptibilité.

Abstract:

Recent advances in medicine have ushered in a digital revolution, where medical images play a crucial role in diagnosis, research and education. This transformation has brought significant benefits: increased accessibility, stronger collaboration between health professionals and more effective patient care. However, this digital age comes with serious concerns about unauthorized access, manipulation or theft of sensitive medical information. These risks threaten patient privacy and care security, as medical images often contain highly sensitive data. To address these challenges, our study explores advanced digital watermark techniques, with an emphasis on the integration of discrete cosine transformation (DCT) and the least significant bit (LSB). The DCT allows for judicious insertion of watermarks in different frequency ranges, maximizing imperceptibility and robustness. At the same time, the LSB method ensures that the perceptual impact remains minimal. Our goal is to subtly balance imperceptibility and robustness by evaluating the influence of DCT frequency bands on watermark quality in medical images. By combining these innovative techniques, we aim to secure sensitive textual information in medical images, thus transforming the data protection landscape in the healthcare sector. Our approach strives not only to preserve patient confidentiality, but also to ensure greater integrity and confidence in the use of medical images in the digital age.

Keywords: DCT, medical image, digital watermarking, LSB, data security, robustness, imperceptibility.

Table des matières

Introduction générale	1
Chapitre 1 : IMAGE NUMÉRIQUE	3
1.1 Introduction :	4
1.2 Définition :.....	4
1.2.1 Les images matricielles (bitmap) :	4
1.2.2 Les images vectorielles :	4
1.3 Les caractéristiques d'une image numérique :	5
1.3.1 Pixel :.....	5
1.3.2 Dimension :.....	5
1.3.3 Résolution :.....	5
1.3.4 Luminance (Intensité) :.....	6
1.3.5 Contraste :	6
1.3.6 Contours :.....	7
1.3.7 Texture :.....	7
1.3.8 La couleur :.....	7
1.3.9 Bruit :.....	8
1.3.10 L'histogramme :.....	8
1.4 Les différents types d'image numérique :.....	9
1.4.1 Les images binaires :	9
1.4.2 Image en niveaux de gris :.....	9
1.4.3 Image en couleur :.....	10
1.5 Les différents espaces couleurs :.....	10
1.5.1 Le modèle RGB :.....	11
1.5.2 Le modèle YUV :.....	11
1.5.3 Le modèle HSV :	12
1.5.4 Le modèle CMY :.....	12
1.6 Les formats d'images numériques :.....	13
1.6.1 Format BMP (bitmap) :.....	13
1.6.2 Tagged Image File Format (TIFF):.....	13
1.6.3 Graphiques Inter change Format (GIF) :.....	13

Table des matières

1.6.4	Portable Network Graphique (PNG) :	14
1.6.5	Joint Photographique Expert Group (JPEG) :	14
1.7	Image médicale :	14
1.8	Conclusion :	14
Chapitre 2 : TATOUAGE NUMÉRIQUE		15
2.1	Introduction :	16
2.2	Définition :	16
2.3	Historique du tatouage numérique :	16
2.4	Applications du tatouage numérique :	18
2.4.1	Protection des droits d'auteur :	18
2.4.2	L'authentification des données :	18
2.4.3	Contrôle d'accès :	18
2.4.4	L'intégrité des données multimédias :	18
2.4.5	Les empreintes :	19
2.4.6	Sécurité médicale :	19
2.4.7	Information sur le support :	19
2.4.8	L'indexation des images :	19
2.5	Caractéristiques du tatouage numérique :	19
2.5.1	Robustesse :	19
2.5.2	Imperceptibilité :	20
2.5.3	Flexibilité :	20
2.6	Limites du tatouage numérique :	20
2.6.1	Capacité de tatouage :	20
2.6.2	Réversibilité :	20
2.6.3	Impact sur la qualité du fichier :	20
2.7	Techniques de tatouage d'image :	20
2.7.1	Tatouage visible :	20
2.7.2	Tatouage invisible :	20
2.8	Schéma générale de l'implémentation de tatouage :	20
2.9	Le Domaine d'insertion du tatouage :	21
2.9.1	Domaine spatial :	21
2.9.2	Domaine Fréquentiel :	21
2.10	Les attaques et la robustesse :	22
2.10.1	Le filtrage :	22
2.10.2	La compression :	22

Table des matières

2.10.3	La rotation :.....	23
2.10.4	L'ajout de bruit :.....	23
2.11	Le bit le moins significatif (LSB) :.....	23
2.12	Le ZigZag :.....	23
2.13	Évaluation des algorithmes de tatouage :.....	24
2.13.1	L'erreur quadratique (MSE) :.....	24
2.13.2	Le rapport signal sur bruit (PSNR) :.....	24
2.13.3	Indice de similarité structurelle (SSIM) :.....	25
2.14	Conclusion :.....	25
Chapitre 3 : APPROCHE PROPOSEE ET IMPLEMENTATION.....		26
3.1	Introduction :.....	27
3.2	Méthode utilisée :.....	27
3.3	Processus de tatouage :.....	27
3.3.1	L'insertion :.....	27
3.3.2	Processus d'extraction.....	29
3.4	Outils utilisés :.....	30
3.4.1	Python :.....	30
3.4.2	Tkinter :.....	30
3.4.3	OpenCV :.....	30
3.4.4	NUMPY :.....	30
3.4.5	PIL :.....	30
3.4.6	Visual Studio Code :.....	30
3.5	Présentation de l'application réalisée :.....	31
3.5.1	Interface graphique :.....	31
3.5.2	Interface d'Intégration de Texte :.....	32
3.5.3	Interface d'Extraction de Texte.....	33
3.6	Résultat obtenu :.....	34
3.7	Conclusion :.....	35
Conclusion générale.....		36
Bibliographie.....		37

Liste des figures

Figure 1.1 Images matricielles (Bitmap).....	4
Figure 1.2 Résolution D'image	5
Figure 1.3 Exemple de Luminance	6
Figure 1.4 Exemple de contraste.....	6
Figure 1.5 Exemple de contours	7
Figure 1.6 Exemple de texture	7
Figure 1.7 Exemple de bruit	8
Figure 1.8 Exemple de l'histogramme.....	9
Figure 1.9 Image binaire.....	9
Figure 1.10 Image en niveau de gris	10
Figure 1.11 Image en couleur	10
Figure 1.12 Représentations de couleur de l'espace de couleur RGB	11
Figure 1.13 Représentations de couleur de l'espace de couleur HSV	12
Figure 1.14 Représentations de couleur de l'espace de couleur CMY.....	13
Figure 2.15 Schéma générale de l'implémentation de tatouage	21
Figure 2.16 La méthode LSB.....	23
Figure 2.17 Parcours en zigzag.....	24
Figure 3.18 Schéma explicatif sur le processus de tatouage	28
Figure 3.19 Schéma explicatif sur le processus d'extraction	29
Figure 3.20 Environnement de développement Visual Studio Code	31
Figure 3.21 Interface graphique de l'application.....	32
Figure 3.22 Interface graphique de l'application lors l'insertion du tatouage.....	33
Figure 3.23 Interface graphique de l'application lors d'évaluation.....	33
Figure 3.24 Interface graphique de l'application lors l'extraction du tatouage.....	34
Figure 3.25 Comparaison entre Images (texte dans une image).....	35

Liste des tableaux

Tableau 1 Représente la moyenne de chaque métrique.....35

Table d'abréviations

JPEG	JointPhotographicExpertGroup)
GIF	GraphicsInterchangeFormat
PNG	PortableNetworkGraphic
SECAM	Système Électronique Couleur Avec Mémoire
NTSC	National Television System Committee
CT	ComputerizedTomography
MRT	Magnetic ResonanceTomography
PET	Positron Emission Tomography
US	UltraSound
TIFF	TaggedImageFileFormat
BMP	BitMap
PIL	Python Imaging Library
LSB	LeastSignificantBit
PSNR	PeakSignaltoNoiseRational
SSIM	StructuralSimilarityIndexMethod
MSE	MeanSquaredError
DCT	DiscreteCosineTransform
DWT	DiscreteWaveletTransform
DFT	Discrete Fourier Transform

Introduction générale

Les réseaux numériques de communication sont largement utilisés pour l'échange des informations comme texte, audio, vidéo etc. La sécurité de ces informations échangées est devenue une nécessité primordiale dans beaucoup d'applications des organismes civils ou militaires, citons par exemple, l'internet, la téléphonie mobile, les distributeurs de billets, les abonnements aux chaînes de télévision payantes, le commerce électronique et les cartes à puce, afin d'assurer la confidentialité et d'empêcher toute modification ou exploitation non autorisée des données. L'une des méthodes connues pour la réalisation efficace de cet objectif est le tatouage qui rend la marque insérée complètement illisible et imperceptible. En effet, le tatouage est l'un des moyens technologiques utilisés pour fournir la sécurité et l'authenticité aux données transmises sur des systèmes de communication.

Plusieurs techniques de tatouage ont été développées pour résoudre le problème de sécurité. Elles peuvent être classifiées de différentes manières. On distingue généralement deux types de systèmes de tatouage selon l'apparence ou non de la marque insérée : le tatouage visible et le tatouage invisible. Les systèmes de tatouage invisibles sont largement utilisés, puisqu'il est difficile de faire la distinction entre l'information originale (image, audio ou vidéo) et l'information tatouée d'une part, et d'autre part, une tentative de suppression de la marque insérée provoque une dégradation de manière significative de la qualité de la donnée tatouée.

Il existe dans la littérature des techniques de tatouage spatiales et fréquentielles. Les algorithmes traditionnels de tatouage comme ceux qui modifient les bits de poids faibles LSB (Least Significant Bit) des pixels de l'image hôte dans le domaine spatial[1], ne sont pas très robustes aux attaques comme la compression et l'ajout de bruit. Pour fournir une meilleure solution au problème de la robustesse des images tatouées, des techniques de tatouage d'images ont été proposées dans[2] - [3], où le tatouage se fait dans le domaine fréquentiel. La marque est insérée dans les coefficients obtenus par l'utilisation d'un processus de transformation sur l'image. Une partie de ces méthodes utilise des transformées discrètes, telles que la transformée de Fourier discrète DFT, la transformée en ondelettes discrète DWT, la transformée en cosinus discrète DCT, etc. La DCT et la DFT ont des algorithmes de calcul rapide, mais leur complexité reste élevée et ne répond pas aux exigences des applications modernes. En conséquence, il est préférable d'utiliser des transformées complètes dont la complexité est considérablement réduite. Cela est dû au fait que ces types de transformées ne nécessitent pas de multiplications, mais seulement des additions et des décalages de bits. La DCT possède une excellente capacité de compactage d'énergie, ce qui la rend plus attrayante que

Introduction générale

les autres transformées entières existantes. Ainsi, le but de ce mémoire est d'élaborer une méthode efficace de tatouage d'images médicales numériques pour répondre aux besoins de la télémédecine et garantir la sécurité des données médicales échangées à travers les réseaux.

Ce mémoire est composé de trois chapitres. Le premier chapitre traite de l'état de l'art des images numériques, en mettant en avant leurs caractéristiques, formats et types.

Dans le chapitre 2, nous décrivons les différents éléments d'un système de tatouage numérique, ainsi que les contraintes, les types et les domaines d'application de ces systèmes. Nous aborderons également l'évaluation des algorithmes de tatouage d'images.

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

Chapitre 1 : IMAGE NUMÉRIQUE

1.1 Introduction :

L'image numérique est devenue omniprésente dans notre quotidien, jouant un rôle essentiel dans la communication visuelle, la création artistique, la documentation et bien d'autres domaines. À la croisée de l'informatique et de la représentation visuelle, elle se définit comme une représentation graphique stockée sous forme de données numériques.

1.2 Définition :

Une image numérique est une image acquise, traitée et stockée en bits. Une image numérique est un tableau de pixel : chaque pixel est codé par un nombre binaire pour un niveau de gris, ou par trois nombres binaires qui correspondent à une nuance de rouge, de vert et de bleu (codage RVB).[4]

1.2.1 Les images matricielles (bitmap) :

Une image matricielle, également connue sous le nom d'image bitmap, est une image composée de pixels disposés dans une grille. Chaque pixel a une couleur spécifique et, lorsqu'on les regarde ensemble, ces pixels forment l'image entière.[5]

Il existe différents types d'images matricielles telles que le TIFF, BMP, PNG et JPG.



Figure 1.1 Images matricielles (Bitmap)

1.2.2 Les images vectorielles :

Les images vectorielles, s'appuient sur des formules mathématiques et des points pour définir les formes, les lignes et les courbes. Les vecteurs peuvent être mis à l'échelle à n'importe quelle taille sans perte de qualité et sont idéaux pour les graphiques tels que les logos, les icônes et les diagrammes.[5]

1.3 Les caractéristiques d'une image numérique :

1.3.1 Pixel :

Le pixel est une unité de mesure de la définition d'une image numérique. Abrégée en px, elle est souvent présentée comme un petit carré de couleur. Lorsqu'on zoome sur une image numérique matricielle (les images vectorielles ne sont pas basées sur les pixels), on aperçoit en effet que celle-ci se compose d'une multitude de petits carrés colorés. Il s'agit des pixels. À noter qu'il n'existe pas de plus petit élément d'une surface d'affichage que le pixel.[6]

1.3.2 Dimension :

C'est la taille de l'image. Cette dernière se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des intensités lumineuses (pixels). Le nombre de lignes de cette matrice multipliée par le nombre de colonnes nous donne le nombre total de pixels dans une image [7].

1.3.3 Résolution :

La résolution est définie par un nombre de pixels par unité de longueur de l'image à numériser en dpi (dots per inch) ou ppp (points par pouce). On parle de définition pour un écran et de résolution pour une image. Plus le nombre de pixels est élevé par unité de longueur de l'image à numériser, plus la quantité d'information qui décrit l'image est importante et plus la résolution est élevée (et plus le poids de l'image est élevé) [8].

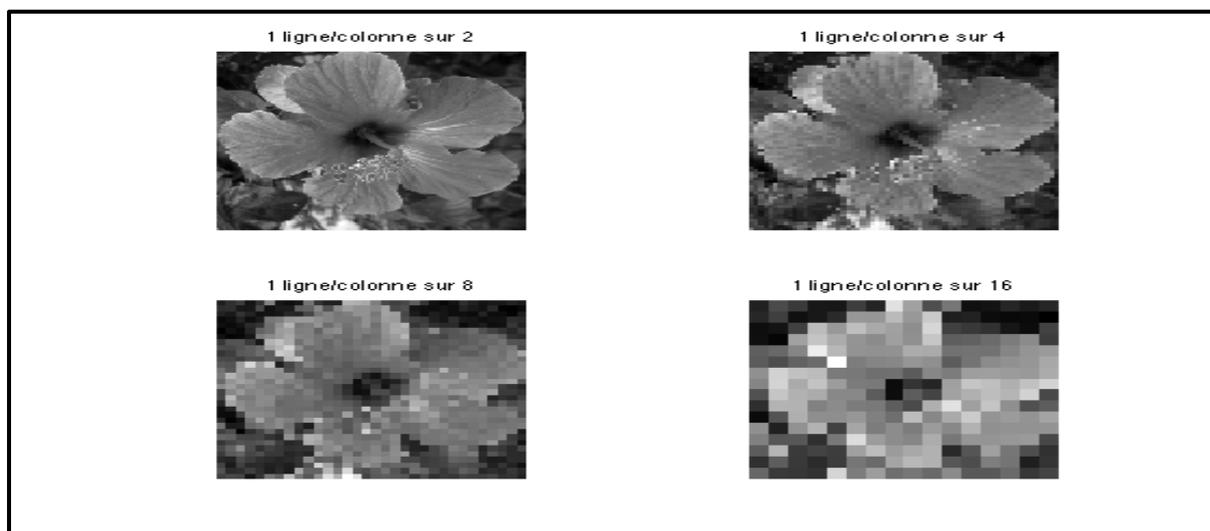


Figure 1.2 Résolution D'image

1.3.4 Luminance (Intensité) :

C'est le degré de luminosité des points (Pixels) de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface.



Figure 1.3 Exemple de Luminance

1.3.5 Contraste :

Le contraste dans une image fait référence à la différence de luminance ou de couleur entre les différents éléments de l'image. Un fort contraste signifie qu'il y a une grande différence entre les parties les plus sombres et les parties les plus claires de l'image, tandis qu'un faible contraste indique que cette différence est moins marquée.



Figure 1.4 Exemple de contraste

1.3.6 Contours :

Les contours d'une image se réfèrent aux bordures ou frontières qui délimitent les différentes régions ou objets présents dans l'image. Ces contours sont formés par des changements significatifs dans les niveaux de couleur, de luminosité ou de texture de l'image.

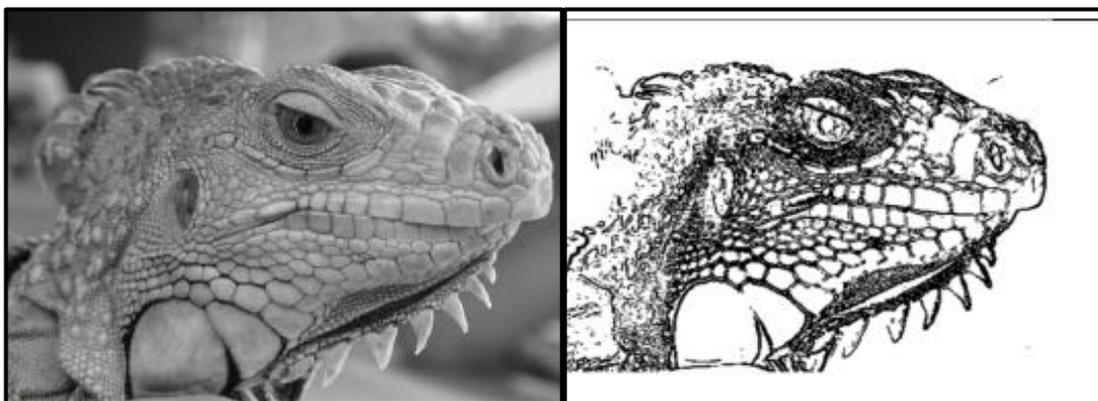


Figure 1.5 Exemple de contours

1.3.7 Texture :

Les textures décrivent la structure de l'image. L'extraction de contour consiste à identifier dans l'image les points qui séparent deux textures différentes [9]

La texture est modélisée comme une structure spatiale constituée de l'organisation de primitives ayant chacune un aspect aléatoire ou défini comme une microstructure de la surface. Une texture peut avoir un aspect périodique ou bien aléatoire.



Figure 1.6 Exemple de texture

1.3.8 La couleur :

La couleur est un des premiers descripteurs qui sont employés pour la recherche d'images. La couleur forme une partie significative de vision humaine, sans elle beaucoup de tâches journalières prouveraient très difficile. Nous pouvons distinguer efficacement les objets basés sur seule la couleur. Deux espaces de couleur le plus utilisée sont le RGB et HVS. La forme la plus simple de descripteur de couleur est l'histogramme de couleur [10].

1.3.9 Bruit :

On peut définir le bruit numérique comme étant l'apparition aléatoire de « traces » et de variations de la luminosité ou de la couleur de la photo numérique. Ces traces se présentent généralement dans la plupart des cas comme des points de taille variable mais on peut aussi inclure dedans d'autres défauts produits par les dégradés de couleur.[11]



Figure 1.7 Exemple de bruit

1.3.10 L'histogramme :

Un histogramme d'image est un type de graphique statistique distribution des intensités de couleur dans une image. Il utilise comme abscisse des couleurs et pour ordonnées le nombre de pixel pour chaque couleur ce qui permet d'évaluer rapidement la répartition des couleurs au sein de l'image image.

En pratique, les couleurs sont généralement limitées à 255 niveaux de gris, l'image est donc préalablement convertie en niveau de gris (luminance)[12].

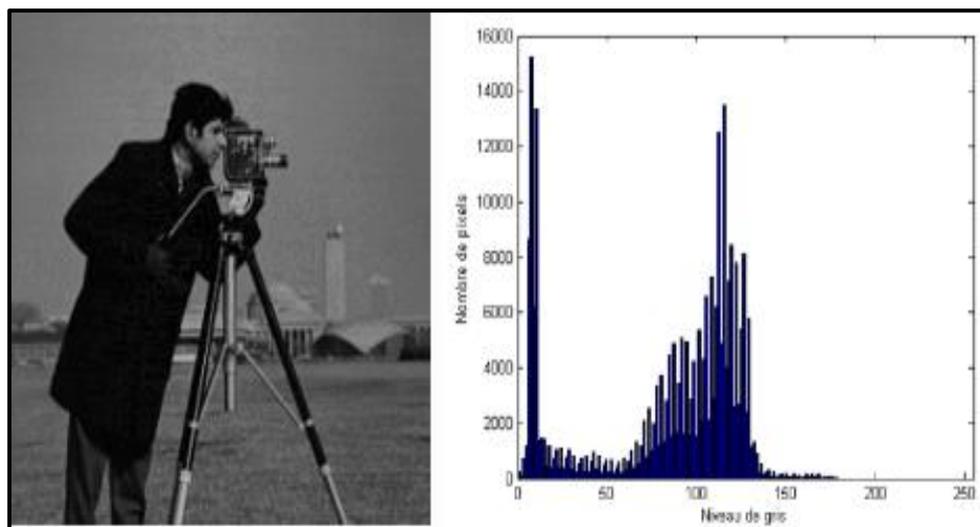


Figure 1.8 Exemple de l'histogramme

1.4 Les différents types d'image numérique :

Il existe différentes catégories d'image selon le nombre de bits sur lequel est codée la valeur de chaque pixel.

1.4.1 Les images binaires :

Une image binaire est une image qui ne contient que deux couleurs, généralement le noir et le blanc, chaque pixel ne peut avoir pour valeur que 0 (noir) ou 1 (blanc)[13].



Figure 1.9 Image binaire

1.4.2 Image en niveaux de gris :

Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur de pixel prend des valeurs allant de noir au blanc en passant par un nombre fini de niveaux intermédiaires. Les valeurs peuvent être comprises entre 0 et 255 ; les pixels sont alors codés non pas sur un bit mais sur un octet[14].



Figure 1.10 Image en niveau de gris

1.4.3 Image en couleur :

Peut-être codée elle aussi sur 4 bits (image en 16 couleurs), 8 bits (image en 256 couleurs) ou davantage : 24 bits pour une image en 16 millions de couleurs ($16777216=2^{24}$) On obtient ainsi $256 \times 256 \times 256 = 16777216$ (plus de 16 millions de couleurs différentes)[15].



Figure 1.11 Image en couleur

1.5 Les différents espaces couleurs :

Les espaces de couleur, également appelés espaces colorimétriques, sont des modèles mathématiques en trois dimensions représentant toutes les couleurs perceptibles, utilisables ou reproductibles par l'œil humain ou un appareil. Chaque couleur est associée à des coordonnées spécifiques qui correspondent approximativement aux trois longueurs d'onde auxquelles l'œil humain est sensible. Les

espaces de couleur sont utilisés pour gérer la couleur dans les images numériques, l'impression, la vidéo, la télévision et d'autres domaines où la précision des couleurs est importante. Parmi les nombreux espaces de couleur, on trouve notamment : RGB, YUV, HSV et YCM.

1.5.1 Le modèle RGB :

Le modèle colorimétrique RGB (Red, Green, Blue) est constitué de trois composantes qui permettent de représenter les couleurs primaires dans l'image chaque pixel est caractérisé par une combinaison de trois couleurs primaires. En combinant différentes proportions de rouge, de vert et de bleu, on peut créer toutes les autres couleurs. Le modèle RGB est largement utilisé dans les images numériques affichées sur les écrans d'ordinateurs et de téléphones portables, ainsi que dans les graphiques et les jeux vidéo [16].

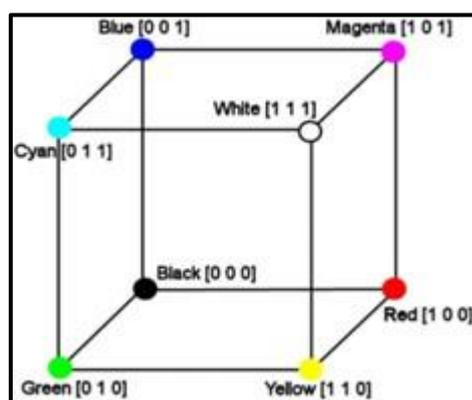


Figure 1.12 Représentations de couleur de l'espace de couleur RGB

1.5.2 Le modèle YUV :

Le modèle YUV est un espace colorimétrique en trois composantes. Le composant Y représente la luminance, c'est-à-dire l'information en noir et blanc, tandis que les composants U et V représentent la chrominance, c'est-à-dire l'information sur la couleur. Ce modèle est utilisé dans les systèmes de diffusion télévisuelle PAL, SECAM et NTSC pour transmettre des informations colorées aux téléviseurs couleur tout en garantissant la compatibilité avec les téléviseurs noir et blanc. Le modèle YUV est très utile pour la compression vidéo et la vidéo numérique car il permet de séparer la luminance et la chrominance pour une meilleure compression [16].

1.5.3 Le modèle HSV :

Le modèle HSV (Hue, Saturation, Value) est un espace colorimétrique en trois dimensions qui représente les couleurs selon leur teinte (Hue), leur saturation (Saturation) et leur valeur (Value ou luminosité). Contrairement au modèle RGB, qui représente les couleurs primaires en termes de quantités de rouge, de vert et de bleu, le modèle HSV représente les couleurs en termes de teinte (couleur de base), de saturation (intensité de la couleur) et de valeur (luminosité ou brillance de la couleur). La saturation est une mesure de la différence de couleur d'un gris de la même luminosité. La saturation zéro n'indique aucune teinte, juste une échelle grise[17].

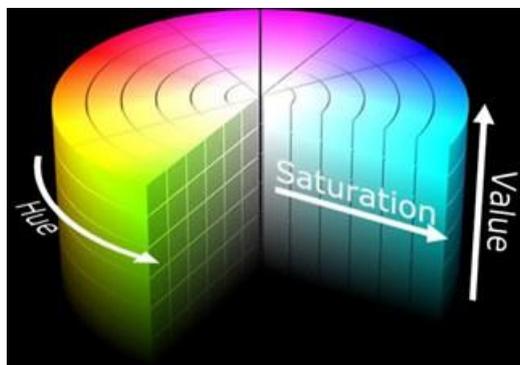


Figure 1.13 Représentations de couleur de l'espace de couleur HSV

1.5.4 Le modèle CMY :

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

imprimée.[18]

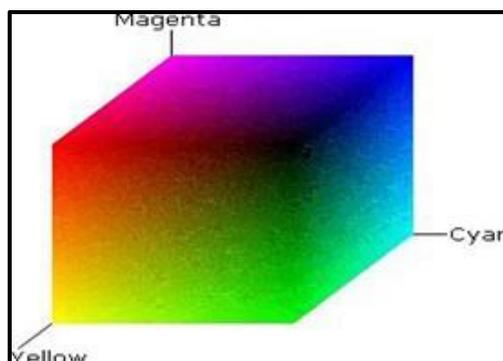


Figure 1.14 Représentations de couleur de l'espace de couleur CMY.

1.6 Les formats d'images numériques :

1.6.1 Format BMP (bitmap) :

Le format d'image BMP (bitmap) est l'un des formats les plus simples, ayant été développé conjointement par Microsoft et IBM. Ce format est ouvert et non compressé, ce qui permet de stocker les pixels de l'image sous forme de tableau de points. Chaque fichier BMP est donc constitué de pixels individuels qui sont définis par leur couleur et leur position dans l'image. Bien que sa taille importante puisse rendre son utilisation en ligne difficile, le format BMP reste efficace pour travailler sur les fichiers image en raison de sa grande compatibilité.[16].

1.6.2 Tagged Image File Format (TIFF):

Le format TIFF est idéal pour stocker des documents numérisés tels que des images et du texte. Il peut stocker des fichiers de grande taille sans compromettre leur qualité, ce qui en fait un choix populaire pour l'archivage de documents. Les algorithmes de lecture du format TIFF garantissent que la qualité de l'image originale est préservée sans perte de qualité, même après la numérisation et le stockage. En somme, le format TIFF est un choix optimal pour stocker des documents numérisés de haute qualité, sans dégradation de la qualité d'image. [14].

1.6.3 Graphiques Inter change Format (GIF) :

Le format GIF est largement reconnu comme un standard sur internet. Les fichiers GIF sont de petite taille, car ils sont limités à enregistrer uniquement 256 couleurs. Cependant, cette limitation est considérée comme l'un des avantages clés de ce format. En plus de stocker des 20 images, le format GIF permet également la création d'animations et de détourages, ce qui en fait un choix polyvalent pour de nombreux types de contenus en ligne. [19].

1.6.4 Portable Network Graphique (PNG) :

Le format PNG est un standard du W3C (Consortium World Wide Web) et est largement répandu sur Internet. Ce format de fichier propriétaire permet une compression optimale de la taille des images en utilisant un système de couleurs indexées et en permettant l'utilisation de valeurs de couleur précises. En outre, il offre la possibilité d'utiliser 13 profondeurs de couleurs différentes allant de 1 à 48 bits et prend en charge la transparence. [20].

1.6.5 Joint Photographique Expert Group (JPEG) :

La norme JPEG (ISO 10918-1) est la norme internationale pour la compression d'images fixes, en particulier pour les images photographiques. Bien que complexe et nécessitant des connaissances mathématiques solides, cette méthode de compression « avec pertes » basée sur l'algorithme DCT offre des taux de compression très intéressants. Bien qu'un mode « sans perte » ait été développé, il n'a pas été largement utilisé. Cette norme a été développée par le comité JPEG (Joint Photographique Experts Group) et normalisée par l'ISO/JTC1 SC29[16].

1.7 Image médicale :

Depuis que Wilhelm Conrad Roentgen a découvert les rayons X en 1895, l'imagerie médicale est devenue une discipline scientifique majeure. L'étude des informations obtenues par les techniques d'imagerie actuelles, comme la tomographie informatisée (CT), la tomographie par résonance magnétique (MRT), la tomographie par émission de positrons (PET) ou l'échographie (US), permet de réaliser des diagnostics novateurs, de planifier et d'évaluer la thérapie. Il est crucial de traiter les images médicales afin d'utiliser cette multiplication de données et d'explorer et de présenter les informations contenues de manière appropriée à la tâche médicale particulière[21].

1.8 Conclusion :

Dans ce chapitre, nous avons essayé de présenter quelques concepts de base liés au domaine de l'image numérique et décrit les différentes caractéristiques d'une image. Nous avons également donné quelques définitions fondamentales des images numériques, ce qui est important pour la suite de notre travail sur le sujet du tatouage numérique, son état de l'art et les différentes techniques utilisées

Chapitre 2 : TATOUAGE NUMÉRIQUE

2.1 Introduction :

La préservation des données numériques et la préservation des droits de propriété intellectuelle sont des préoccupations majeures dans l'ère digitale. Dans ce contexte, le tatouage d'images attire de plus en plus l'attention. Ce chapitre propose un examen approfondi des techniques de tatouage numérique, couvrant leur concept général, leurs diverses méthodes, ainsi que les domaines d'application et les principales formes d'attaques envisagées.

2.2 Définition :

Le tatouage numérique est une méthode utilisée pour intégrer une information appelée marque dans un support numérique, qu'elle soit visible ou invisible. La marque peut prendre la forme d'une image, d'un texte, d'une vidéo, d'un audio ou d'une autre donnée numérique. L'objectif est d'insérer la marque de manière à ce qu'elle soit perceptible ou imperceptible, sans altérer la qualité visuelle de l'image dans son ensemble[22].

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

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

2.3 Historique du tatouage numérique :

L'information est un élément essentiel et déterminant dans tous les domaines. Tout au long de l'histoire, l'humanité a essayé d'échanger les informations d'une façon sécurisée. Pour cette raison, la dissimulation d'information a été utilisée pour les stratégies militaires et l'échange de données secrètes. On distingue, principalement deux grandes catégories : la stéganographie et le tatouage. L'utilisation classique de la stéganographie prend place il y a plus de deux mille ans. Hérodote, l'historien grec, raconte que Xerxès, roi des Perses, décida d'envahir la Grèce. Lorsque l'offensive fut lancée, les Grecs étaient depuis longtemps au courant de ses intentions. Démarate, ancien roi de Sparte réfugié auprès de Xerxès, apprit ses intentions et décida de transmettre l'information à Sparte. Il prit une tablette double, en gratta la cire, puis écrivit sur le bois même les projets de

Xerxès, il recouvra ensuite de cire son message : ainsi le porteur d'une tablette vierge ne risquait pas d'ennuis.

Un autre exemple de dissimulation d'information est celui de Histiée qui incite son gendre Aristagoras, gouverneur de Milet, à se révolter contre son roi, Darius. Pour passer son message, Histiée fit raser la tête d'un esclave, et tatoua son message sur le crâne et attendit que les cheveux repoussent et envoya l'esclave à Milet [Tou06].

Dans les années 80, Margaret Thatcher, premier ministre britannique, soupçonna certains de ses ministres de transmettre des informations à la presse. Pour identifier le coupable, elle exigea que tous les documents de son cabinet aient un espacement entre les mots spécifiques pour chaque ministère afin d'identifier la source de la fuite des informations.

Cependant, l'art du tatouage a été inventé en Chine depuis plus de mille ans pour tatouer le papier (papermarking), mais le plus ancien papier marqué archivé date de 1292 et son origine est la ville Fabriano en Italie. Le but principal des premiers tatouages sont incertains, mais ils ont été utilisés pour des fonctionnalités pratiques telles que l'identification de l'origine de fabrication du papier ou pour l'identification du fabricant. Au 18^{ème} siècle, le tatouage fut utilisé en Europe et en Amérique, initialement pour identifier un fabricant ou une usine de papeterie. Il a servi par la suite à indiquer le format et la qualité du papier, et aussi comme base d'authentification du papier et une mesure anti-contrefaçon pour la monnaie et autres documents. Le terme watermark semble avoir été inventé vers la fin du 18^{ème} siècle et peut avoir été dérivé du mot Allemand wassermarke. Il est difficile de déterminer quand le tatouage numérique a été introduit pour la première fois, mais le premier article utilisant le terme Digital Watermark semble être celui de Komatsu et Tominaga [KT88] en 1988. À partir de 1995 cette technique a connu son plein essor.

En outre, à cette époque plusieurs organisations ont commencé à considérer le tatouage numérique pour l'inclure dans leurs normes. Le Copy Protection Technical Working Group a testé des systèmes de tatouage numérique pour la protection de la vidéo dans des disques DVD. Deux projets (Viva et Talisman) ont été sponsorisés par l'Union Européenne afin de tester le tatouage numérique pour le contrôle de diffusion. Vers la fin des années 90, plusieurs compagnies ont été établies pour lancer des produits de tatouage numérique sur le marché. Dans le domaine de l'imagerie, la société Adobe en collaboration avec la compagnie Digimarc a utilisé cette technique dans son logiciel Adobe Photoshop. Depuis, le tatouage numérique a été utilisé dans diverses applications comme le contrôle de diffusion (broadcast monitoring), l'identification du propriétaire (copyright identification), le suivi de transaction (transaction tracking),

l'authentification du contenu (content authentication), le contrôle de copie (copy control) et le contrôle de périphérique (device control)[23].

2.4 Applications du tatouage numérique :

Il existe plusieurs applications du tatouage numérique : parmi celle-ci on peut citer :

2.4.1 Protection des droits d'auteur :

Le tatouage numérique est couramment utilisé dans le but de protéger les droits d'auteur, en insérant une signature unique qui permet d'identifier de manière fiable le propriétaire de l'œuvre. Il s'agit de l'application la plus évidente du tatouage numérique dans le domaine de la protection des droits d'auteur. Les deux caractéristiques primordiales à respecter sont l'invisibilité et la robustesse de la marque. En effet, la marque doit être invisible pour préserver l'intégrité de l'œuvre originale, tout en étant suffisamment résistante pour contrer les tentatives de piratage et de violation des droits d'auteur[19].

2.4.2 L'authentification des données :

Le tatouage numérique est une technique cruciale pour l'authentification des données, en particulier dans le domaine des images médicales. Il permet d'insérer une marque dans l'image qui sert de preuve que le contenu n'a pas été altéré depuis l'insertion de la marque. Cette application utilise des marques fragiles qui deviennent invisibles dès qu'une valeur des données est modifiée dans le document. Cette fonctionnalité de l'authentification des données est essentielle pour garantir l'intégrité et la fiabilité des informations médicales[24].

2.4.3 Contrôle d'accès :

Dans certains systèmes, des privilèges différents peuvent être offerts aux utilisateurs en fonction de leur mode de paiement. Afin d'éviter la copie illégale du contenu ou de limiter le nombre de copies, un mécanisme de contrôle de copie et d'utilisation est souhaitable. Dans ce cas, l'utilisation d'un tatouage robuste peut être une solution efficace pour identifier l'auteur du document et retracer son utilisation[19].

2.4.4 L'intégrité des données multimédias :

Le tatouage numérique est une méthode utilisée pour garantir l'authenticité du contenu d'un document en insérant une marque fragile dans l'image. Cette marque subit des distorsions si le document est altéré, ce qui la détériore instantanément. Cette technique permet ainsi de détecter toute modification apportée au document et de s'assurer de l'intégrité des données. Cette application est utile pour assurer la sécurité et la fiabilité des données dans diverses industries, y compris dans le domaine médical et financier[25].

2.4.5 Les empreintes :

L'application de tatouage numérique est couramment utilisée pour tracer les copies illégales de médias et pour suivre les pirates. Cette application génère un marquage unique, généralement sous forme d'un numéro de série, pour chaque copie distribuée. Cependant, la distribution de copies comportant différentes marques peut entraîner des problèmes de collusion. Par conséquent, il est important que les marques utilisées répondent à des critères de sécurité pour prévenir les collusions. Les marques doivent être conçues de manière à garantir l'unicité de chaque marquage et à empêcher toute manipulation frauduleuse de l'information[26].

2.4.6 Sécurité médicale :

Il est important d'insérer un « identifiant » confidentiel assurant la correspondance entre le patient et la radio, afin d'éviter toutes confusions. Cela garantit la sécurité et la confidentialité des informations médicales[27].

2.4.7 Information sur le support :

Le tatouage numérique peut inclure des informations globales sur l'œuvre, telles que le nom de l'auteur, le titre, la date d'édition, l'adresse électronique, etc. Ces informations sont intégrées à la même marque numérique, sans nécessiter une seconde marque distincte. Cette application peut être utilisée en complément d'une protection de la propriété intellectuelle pour renforcer la sécurité et l'authenticité des données. La présence de ces informations supplémentaires peut aider à identifier facilement les propriétaires de l'œuvre et à prévenir la contrefaçon et l'utilisation illégale[1].

2.4.8 L'indexation des images :

Le tatouage numérique est une méthode utilisée pour indexer les images en y insérant une signature. Cette technique facilite l'indexation et le classement des images dans une base de données. La signature peut contenir des informations sur l'image telles qu'un sommaire, un descripteur ou un lien vers d'autres informations pour permettre une recherche rapide et un classement efficace. Grâce à cette méthode, il est possible de gérer plus facilement de grandes quantités d'images et d'améliorer l'accessibilité aux informations[2].

2.5 Caractéristiques du tatouage numérique :

Le tatouage numérique présente plusieurs avantages :

2.5.1 Robustesse :

Le tatouage numérique est généralement robuste et résistant aux modifications du fichier original.

2.5.2 Imperceptibilité :

Le tatouage numérique est généralement invisible à l'œil nu, ce qui rend difficile sa détection et sa suppression.

2.5.3 Flexibilité :

Le tatouage numérique peut être appliqué à différents types de fichiers numériques.

2.6 Limites du tatouage numérique :

Le tatouage numérique présente également quelques limites :

2.6.1 Capacité de tatouage :

La quantité d'informations pouvant être tatouée dans un fichier est limitée.

2.6.2 Réversibilité :

Le tatouage numérique peut être parfois réversible, ce qui soulève des questions de sécurité.

2.6.3 Impact sur la qualité du fichier :

Le tatouage numérique peut légèrement affecter la qualité du fichier original.

2.7 Techniques de tatouage d'image :

2.7.1 Tatouage visible :

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

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

2.7.2 Tatouage invisible :

Le tatouage « invisible » : Est une technique de tatouage numérique dans laquelle l'image tatouée est très similaire à l'image originale, ce qui rend difficile leur distinction. Il est donc difficile de retirer ou de détruire la marque insérée sans altérer significativement la qualité visuelle de l'image tatouée [2].

2.8 Schéma générale de l'implémentation de tatouage :

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

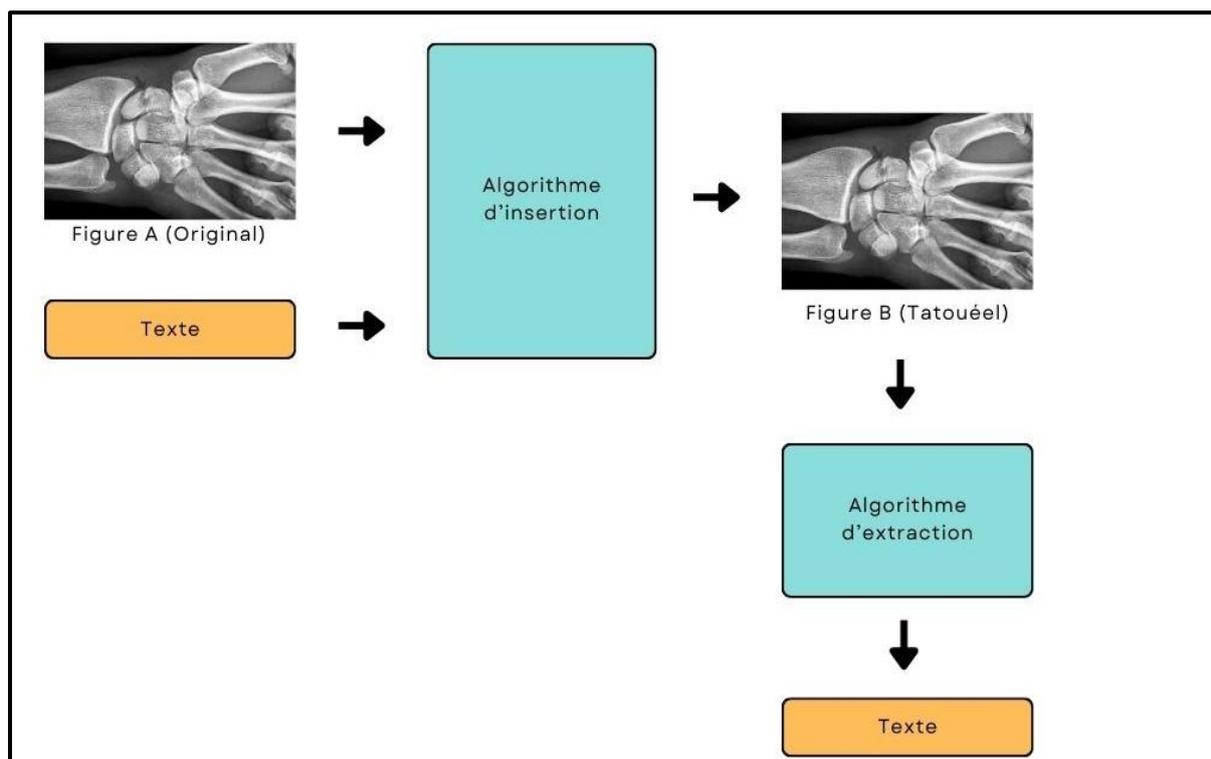


Figure 2.15 Schéma générale de l'implémentation de tatouage

2.9 Le Domaine d'insertion du tatouage :

2.9.1 Domaine spatial :

Les méthodes agissant dans le domaine spatial modifient directement les valeurs des pixels de l'image pour y inclure le message caché. Il existe plusieurs méthodes pour cela, telles que l'insertion des bits du message dans les bits de poids faible de chaque pixel (LSB), la modification des propriétés statistiques de petites régions de l'image (patchwork). Ces méthodes sont utilisées pour assurer l'invisibilité de la signature et consistent en général à effectuer des modifications subtiles des pixels pour intégrer le message de façon efficace. Cependant, ces méthodes ont tendance à manquer de robustesse [14].

Cette méthode est vulnérable face à de nombreuses attaques telles que l'ajout de bruit ou la compression avec perte, ce qui peut altérer la qualité de l'image et même supprimer complètement le tatouage. [28]

2.9.2 Domaine Fréquentiel :

Le domaine fréquentiel est une approche en traitement d'images et de signaux qui transforme une image ou un signal du domaine spatial en un autre domaine appelé domaine fréquentiel, représentant l'image ou le signal sous forme de coefficients de fréquence plutôt que de 32 pixels. Les transformations fréquentielles les plus courantes sont la Transformation de Fourier discrète (DFT), la Transformation en Cosinus Discrète (TCD) et la Transformation en Ondelette (DWT). Les méthodes qui utilisent le domaine fréquentiel sont plus résistantes à la compression et moins vulnérables aux altérations géométriques[2].

2.10 Les attaques et la robustesse :

Afin d'évaluer l'efficacité des algorithmes de tatouage, il est essentiel de réaliser des attaques sur les images après l'insertion[14].

Deux catégories d'attaques sont présentes contre le tatouage numérique. Les attaques non intentionnelles et les attaques intentionnelles.

En règle générale, les attaques non intentionnelles découlent des traitements habituels de l'image, comme la réduction des dimensions ou la compression, et ne cherchent pas spécifiquement à supprimer, identifier ou isoler le tatouage numérique. En ce qui concerne les attaques intentionnelles, elles sont réalisées dans le but de détruire le tatouage numérique, dans le but de falsifier l'image ou de dérober les droits juridiques.

Nous allons examiner certaines attaques dans cette partie.

2.10.1 Le filtrage :

Le filtrage permet d'améliorer la qualité visuelle d'une image en éliminant le bruit qui peut y être présent. Cette approche peut être utilisée lorsque des éléments supplémentaires (tels qu'une marque) ont été intégrés à l'image ou lorsque le bruit a été introduit lors de la capture de l'image. Il est aussi possible d'utiliser le filtrage afin de rendre une image plus douce en effectuant une opération de lissage[29].

2.10.2 La compression :

Afin d'assurer la performance d'un système de tatouage d'image, il est essentiel qu'il puisse supporter une certaine compression. Effectivement, la majorité des données transmises sur les réseaux sont compressées, qu'elles soient mal ou bien pertes. Le JPEG est l'un des algorithmes de compression d'images les plus utilisés. En conséquence, il est essentiel de concevoir les systèmes de tatouage de manière à être compatibles avec les algorithmes de compression courants et à résister aux éventuelles pertes de données causées par ces algorithmes[18].

2.10.3 La rotation :

Lorsque de légères rotations sont appliquées à une marque ou à un motif, cela peut rendre la marque pratiquement invisible ou difficile à détecter. Ces petites variations d'angle peuvent altérer suffisamment la forme ou l'orientation de la marque, ce qui rend plus difficile son identification ou sa reconnaissance par des techniques de détection automatique[26]

2.10.4 L'ajout de bruit :

Quand des images tatouées sont transmises par un canal bruité, le bruit peut être ajouté à l'image, et si le bruit ajouté est élevé, il peut masquer la marque et rendre difficile son extraction ou sa détection.

- Les attaques qui cherchent à ajouter une autre signature dans une image tatouée ne cherchent pas à supprimer la signature existante, mais à la remplacer par une autre afin de fausser l'identification du véritable propriétaire de l'image[29].

2.11 Le bit le moins significatif (LSB) :

Le LSB (Least Significant Bit) consiste à insérer des données uniquement au niveau des bits de poids faible de l'image, Pour une image codée sur 8 bits. Cette modification est en pratique invisible.

Une méthode d'insertion consiste alors à supprimer tous les bits de poids faible de l'image à marquer, puis à y insérer les données voulues. Il suffit en effet de mettre à zéro tous les bits de poids faible de l'image marquée pour effacer irrémédiablement la marque.

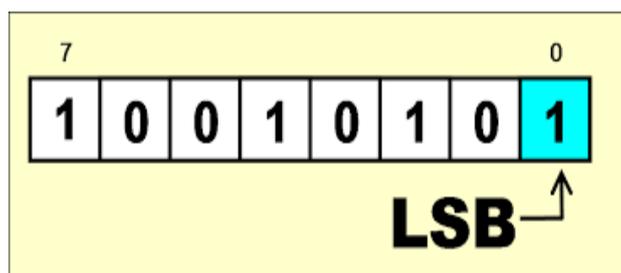


Figure 2.16 La méthode LSB

2.12 Le ZigZag :

Zigzag est un processus qui ordonne les coefficients de basse à haute fréquence de haut en bas et de gauche à droite, sans négliger aucun coefficient (Figure2.17), permettant ainsi un meilleur codage entropique (Basheera et al. 2011). Les coefficients sont balayés en ordre zigzag pour atteindre l'invisibilité perceptuelle de la marque, sans perte de robustesse face aux techniques de traitement du signal.[18]

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

2.13.3 Indice de similarité structurelle (SSIM) :

En ce qui concerne le domaine du tatouage numérique, Le SSIM est une mesure de similarité utilisée pour évaluer la qualité visuelle d'une image ou d'une vidéo dégradée par rapport à l'image ou la vidéo originale. Et elle prend en compte les aspects perceptifs importants tels que la luminance et le contraste, et les combine en une seule valeur appelée indice.

L'indice SSIM est exprimé sous forme d'une valeur décimale comprise entre 0 et 1, où 0 représente la pire qualité visuelle possible, indiquant que le dessin de tatouage est très différent de l'original, et 1 représente une correspondance parfaite entre le design original et le dessin de tatouage dégradé[31].

Le SSIM est calculé comme suit :

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c1)(2\varphi_{xy} + c2)}{(\mu^2 + \mu_y^2 + c1)(\varphi_x^2 + \varphi_y^2 + c2)}$$

2.14 Conclusion :

Pour conclure ce chapitre, nous avons abordé le sujet du tatouage numérique en décrivant ses fondements, les méthodes d'évaluation de performances, ainsi qu'une classification des techniques de tatouage en fonction de divers critères. Ces éléments seront essentiels pour la progression de notre travail à venir

Chapitre 3 : APPROCHE PROPOSEE ET IMPLEMENTATION

3.1 Introduction :

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

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

3.2 Méthode utilisée :

Dans notre travail, nous avons employé la Transformée en Cosinus Discrète (DCT) pour l'insertion de messages (ou tatouage) dans les images médicales numériques. Cette technique a été appliquée à trois niveaux de fréquence distincts : haute fréquence, moyenne fréquence et basse fréquence. Chaque niveau de fréquence a des caractéristiques spécifiques qui influencent la visibilité et la robustesse du tatouage.

Pour évaluer la performance et l'impact de notre méthode, nous avons utilisé plusieurs métriques de qualité d'image et de corrélation. Comme le MSE, PSNR et SSIM.

En comparant ces métriques à travers les trois niveaux de fréquence, nous avons pu analyser les compromis entre la visibilité du tatouage et la robustesse contre les altérations, en déterminant les conditions optimales pour le tatouage des images médicales numériques dans chaque niveau de fréquence.

3.3 Processus de tatouage :

- **préparation du texte** : la première étape consiste à coder le texte en binaire pour l'insertion.
- **préparation de l'image** : on a commencé par la transformation de l'image en une matrice. Puis on a divisé notre matrice en 8x8 sous matrice. Pour chaque sous matrice on a appliqué la DCT après on a codé les valeurs en binaire.

3.3.1 L'insertion :

Pour l'insertion on a 3 cas d'insertion : l'insertion dans les basses fréquence, l'insertion dans les moyennes fréquences et enfin l'insertion dans les hautes fréquences. Les 8x8 sous matrice sont de l'ordre zigzag.

- **L'insertion dans les basses fréquences** : Dans ce cas on a inséré le texte dans les premières cases des 8x8 sous matrices sous forme de zigzag.

Chapitre 3 : APPROCHE PROPOSEE ET IMPLEMENTATION

- **L'insertion dans les moyennes fréquences :** Dans ce cas on a inséré le texte dans le moyen case des 8x8 sous matrices sous forme de zigzag.
- **L'insertion dans les hautes fréquences :** Dans ce cas on a inséré le texte dans la dernière case des 8x8 sous-matrices sous forme de zigzag.
- L'insertion se déroule comme suit : on prend chaque bit du message codé en binaire et pour chaque pixel de chaque cas d'insertion on a remplacé le dernier bit avant la virgule par le bit du message.

- Après l'insertion de tous les bits du message, on a décodé les valeurs des sous matrices en décimale, ensuite on applique la IDCT pour chaque block.

- enfin on construit la nouvelle image en fusionnant les blocks.

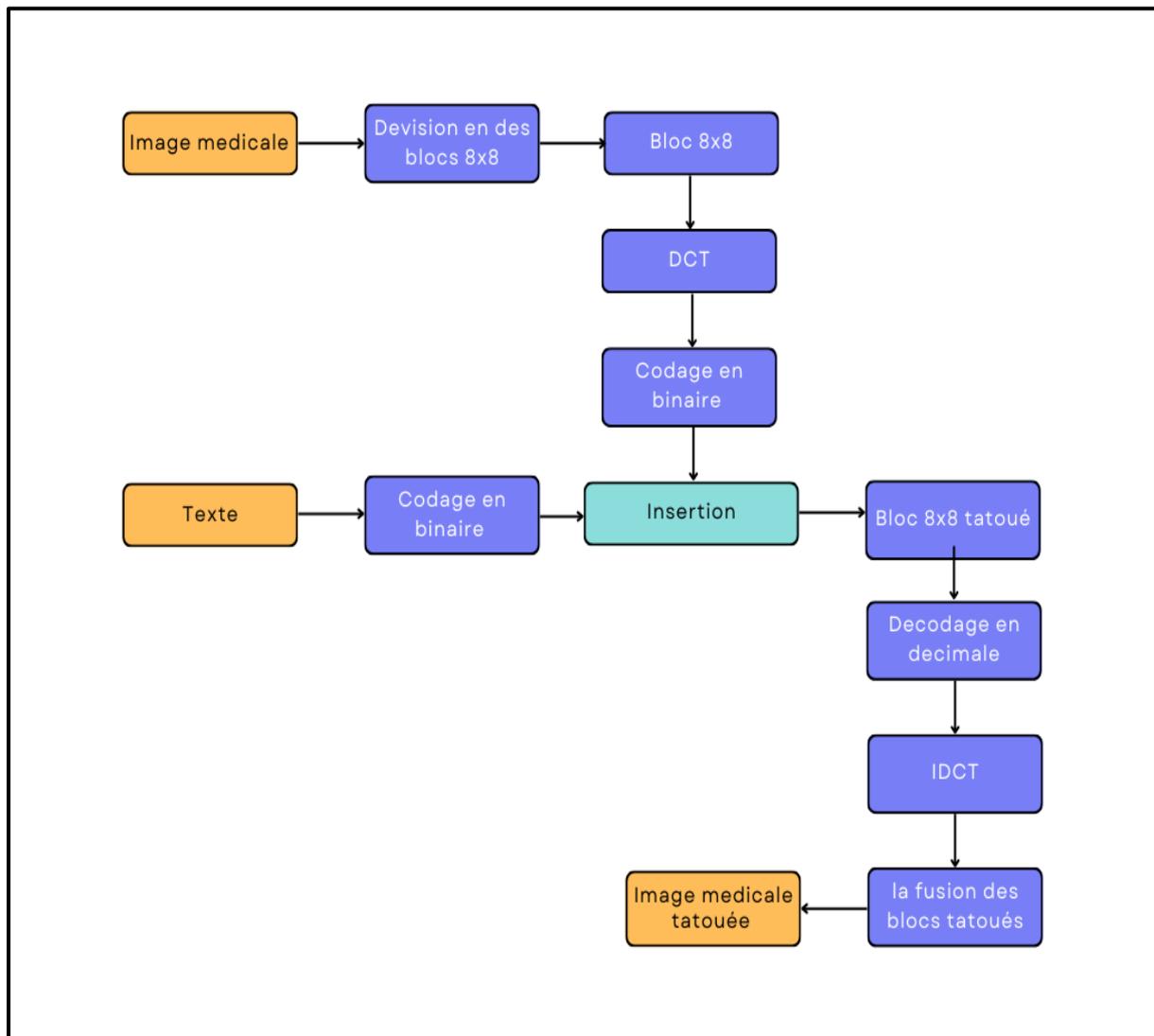


Figure 3.18 Schéma explicatif sur le processus de tatouage

3.3.2 Processus d'extraction

Voici les étapes de l'algorithme d'extraction du message :

- Découpage de l'image en blocs de taille 8x8.
- Application de la Transformée en Cosinus Discrète (DCT) à tous les blocs.
- Conversion de chaque pixel en binaire et extraction du bit caché.
- Regroupement des bits extraits.
- Reconstruction de chaque caractère.
- Reconstitution du message complet.

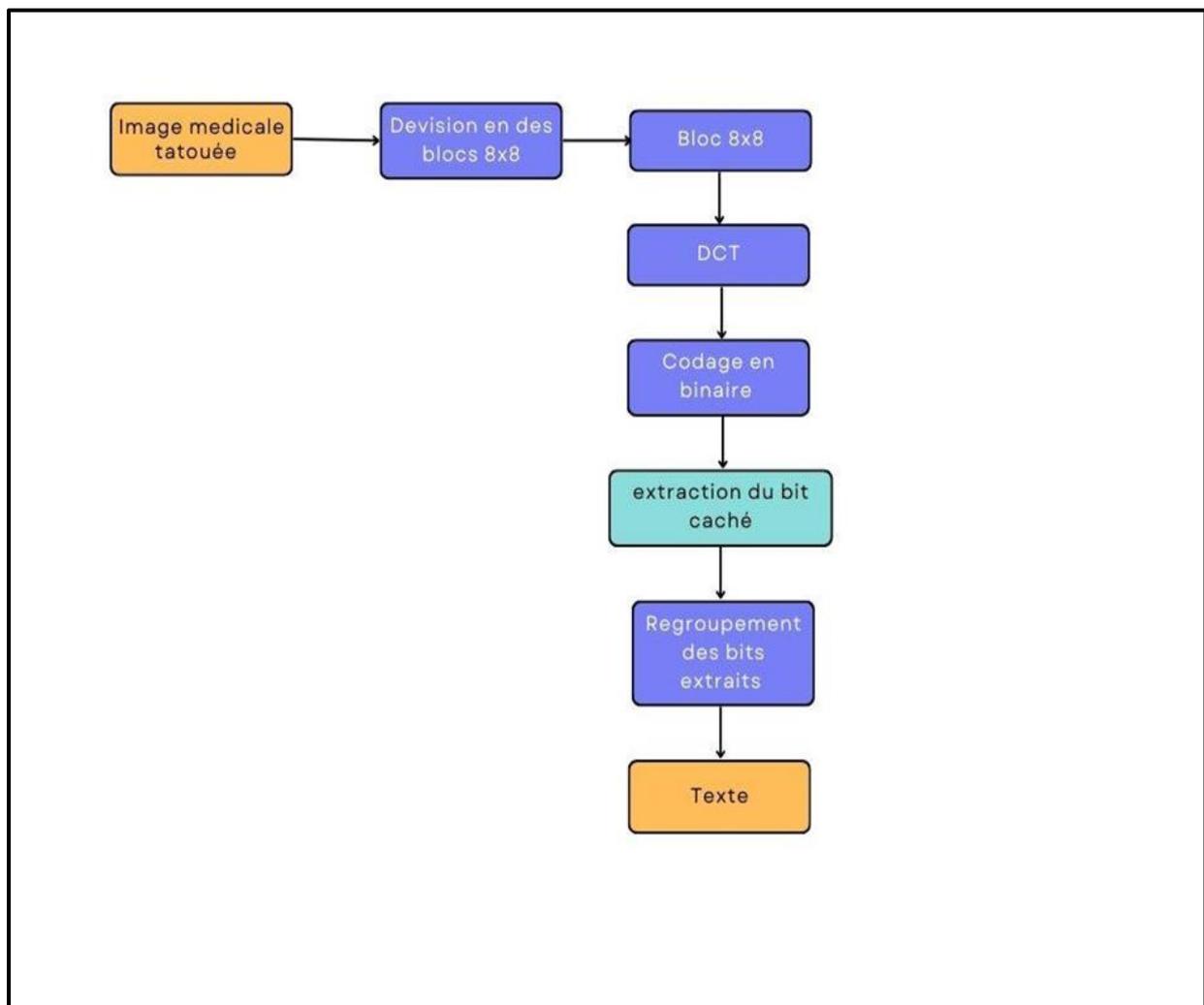


Figure 3.19 Schéma explicatif sur le processus d'extraction

3.4 Outils utilisés :

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

3.4.1 Python :

C'est le langage de programmation open source le plus utilisé dans le domaine du traitement d'images. Le langage est à la pointe de la gestion des infrastructures, de l'analyse des données et du développement de logiciels. L'un des avantages de Python est qu'il permet aux développeurs de se concentrer sur la tâche à accomplir au lieu de la terminer. Cette approche a libéré les développeurs des limitations de syntaxe qui tourmentaient chaque jour les langages plus anciens. Par conséquent, le développement de code en Python est plus rapide que les autres langages[19].

3.4.2 Tkinter :

Tkinter (de l'anglais Tool kit interface) est la bibliothèque graphique libre d'origine pour le langage Python, permettant la création d'interfaces graphiques. Elle vient d'une adaptation de la bibliothèque graphique Tk écrite pour Tcl.

3.4.3 OpenCV :

Open CV (Open Source Computer Vision) Cette bibliothèque fournit des fonctions avancées pour la manipulation et le traitement d'images en tant que PIL. Il est également largement utilisé dans le domaine de la détection automatique de l'intelligence artificielle.

3.4.4 NUMPY :

Numpy est une bibliothèque de bas niveau écrite en C (et FORTRAN) pour les fonctions mathématiques de haut niveau. Elle fournit des fonctionnalités avancées pour manipuler des tableaux et des matrices multidimensionnels, ainsi que pour effectuer des opérations mathématiques complexes[19].

3.4.5 PIL :

PIL (Python Imaging Library) est une bibliothèque logicielle utilisée pour manipuler et traiter efficacement des images en langage Python[19].

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

3.4.6 Visual Studio Code :

Visual Studio Code (VS Code) est un éditeur de code source développé par Microsoft. Il est léger, mais puissant, et prend en charge la plupart des langages de programmation. VS Code inclut des

Chapitre 3 : APPROCHE PROPOSEE ET IMPLEMENTATION

fonctionnalités telles que la coloration syntaxique, l'autocomplétions, le débogage intégré, le contrôle de version Git intégré, et une large gamme d'extensions pour ajouter des fonctionnalités supplémentaires.[32]

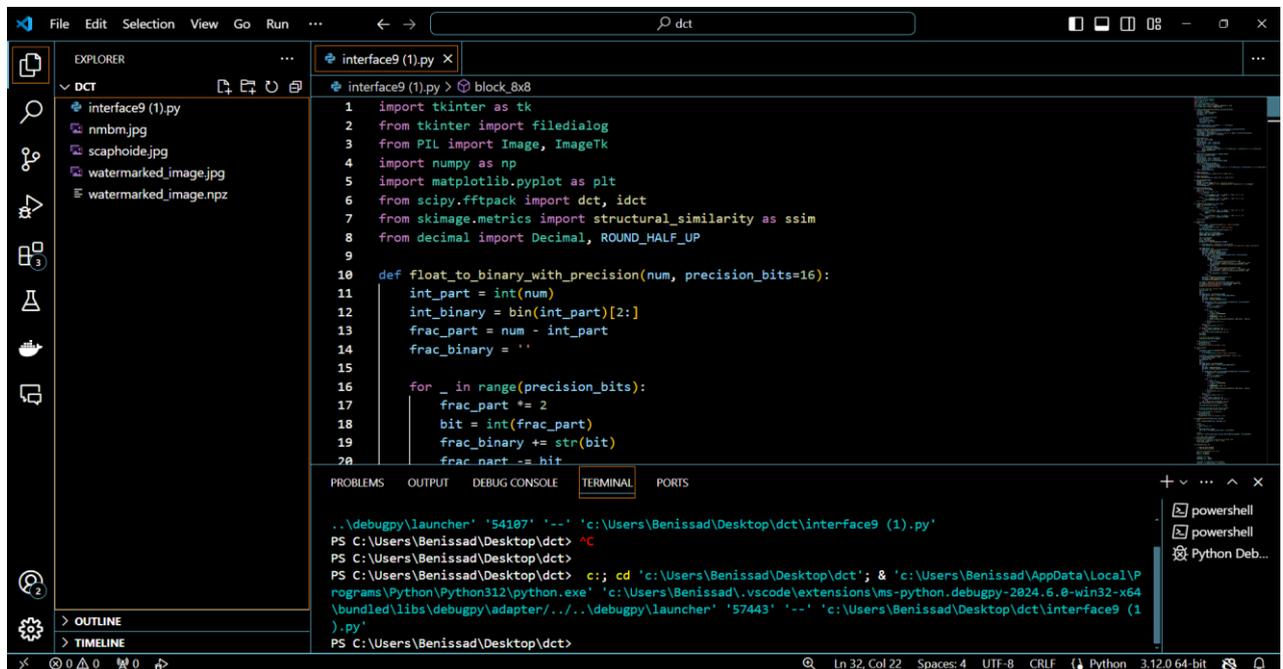


Figure 3.20 Environnement de développement Visual Studio Code

3.5 Présentation de l'application réalisée :

3.5.1 Interface graphique :

Notre application dispose d'une interface simple et conviviale. À l'ouverture de l'application, l'utilisateur est accueilli par un menu principal avec deux options :

Intégrer du texte : Permet à l'utilisateur d'accéder à l'interface d'intégration de texte dans une image.

Extraire du texte : Permet à l'utilisateur d'accéder à l'interface d'extraction de texte depuis une image précédemment sauvegardée.

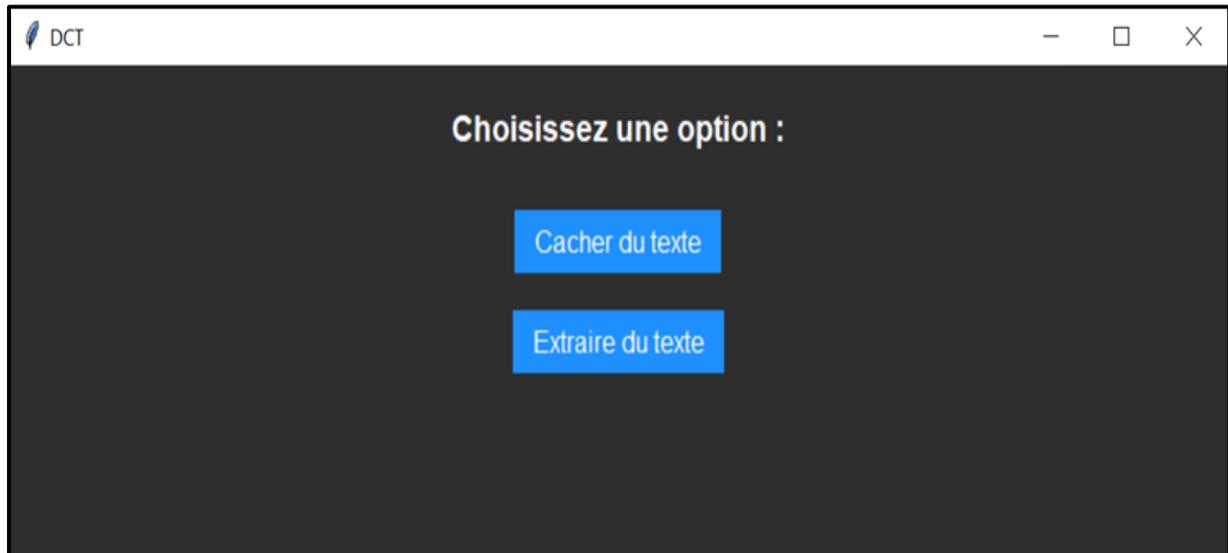


Figure 3.21 Interface graphique de l'application.

3.5.2 Interface d'Intégration de Texte :

Lorsque l'utilisateur choisit d'intégrer du texte :

- Champ de Texte : Un champ où l'utilisateur peut entrer le texte à cacher dans l'image.
- Bouton de sélection d'Image : Permet à l'utilisateur de sélectionner l'image dans laquelle le texte sera intégré.
- Aperçu de l'Image : Affiche l'image sélectionnée.
- Bouton "Intégrer le texte dans l'image" : Lance le processus d'intégration du texte dans l'image.
- Bouton "Retour au Menu" : Ramène l'utilisateur au menu principal.



Figure 3.18 Interface graphique de l'application lors l'insertion du tatouage

Nous avons également développé une interface utilisateur pour évaluer notre approche. Elle intègre des outils de mesure pour évaluer la qualité des images tatouées. Elle calcule automatiquement les métriques telles que l'erreur quadratique moyenne (MSE), le rapport signal sur bruit (PSNR) et l'indice de similarité structurelle (SSIM). Ces résultats sont présentés de manière claire.



Figure 3.19 Interface graphique de l'application lors d'évaluation

3.5.3 Interface d'Extraction de Texte

Lorsque l'utilisateur choisit d'extraire du texte :

- Message d'Extraction : Indique que l'extraction du texte se fera Bouton "Extraire le texte de l'image" : Lance le processus d'extraction du texte depuis l'image sauvegardée.
- Texte Extrait : Affiche le texte extrait de l'image.
- Bouton "Retour au Menu" : Ramène l'utilisateur au menu principal.

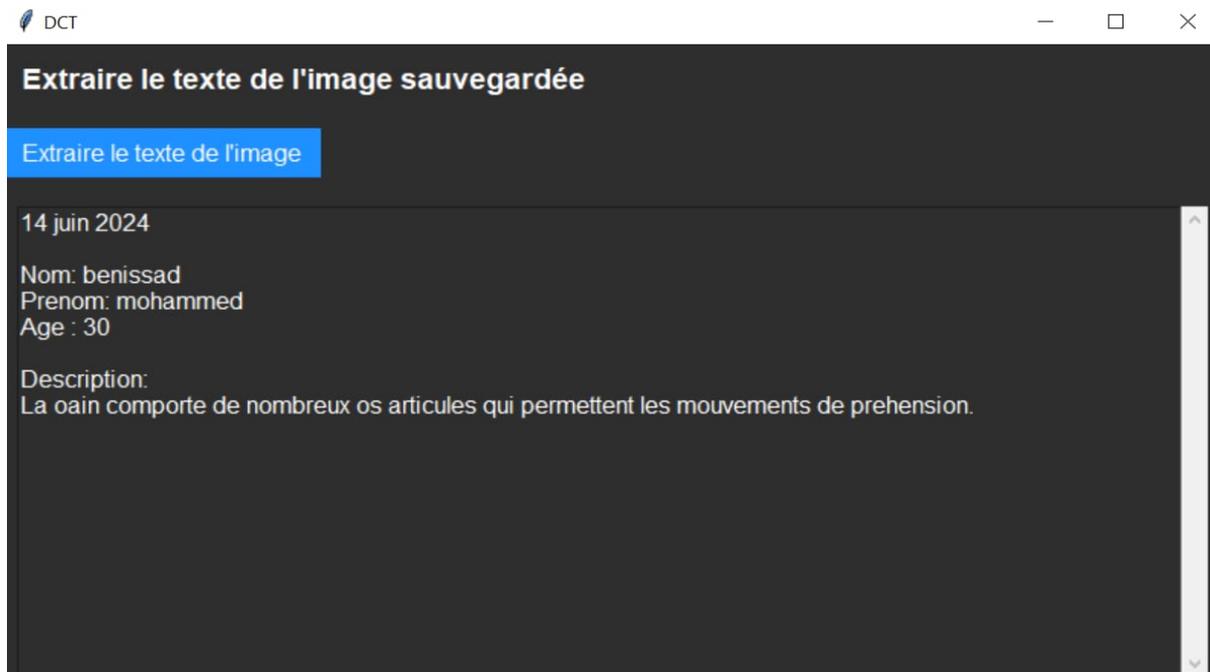


Figure 3.20 Interface graphique de l'application lors l'extraction du tatouage

3.6 Résultat obtenu :

Nous avons utilisé une méthode de tatouage numérique invisible pour intégrer discrètement un texte au sein d'une image. Cette approche équilibre imperceptibilité et robustesse, assurant ainsi la sécurité et l'intégrité des données. Elle maintient également la qualité visuelle de l'image sans altération apparente. En outre, la marque de reconnaissance peut être extraite en toute sécurité, permettant de vérifier son invisibilité et sa résistance.

Figure A(Original)

Figure B(Tatouée)

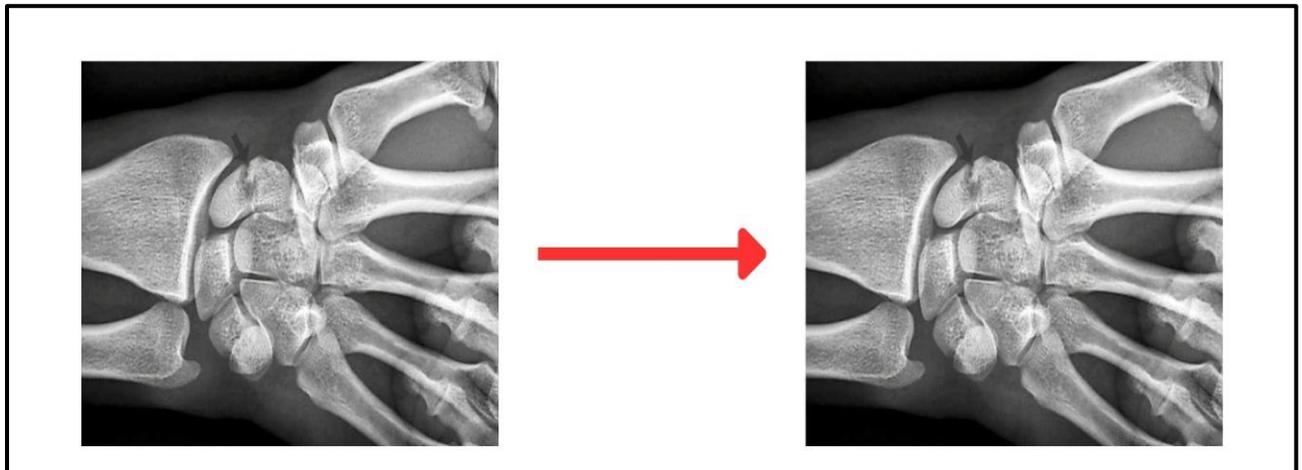


Figure 3.21 Comparaison entre Images (texte dans une image)

À partir de notre observation de l'image hôte et de l'image tatouée, il est presque impossible de différencier l'image originale de l'image tatouée. Le marquage est invisible, et l'image d'origine reste visuellement inchangée, sans aucune différence perceptible à l'œil nu. Nous employons les métriques MSE, PSNR et SSIM pour évaluer et quantifier la qualité et la similarité entre les deux images.

Nous avons appliqué notre approche sur 930 images médicales et nous avons calculé la moyenne de chaque métrique :

MSE (moyenne)	PSNR (moyenne)	SSIM (moyenne)
0,005227541573	45,16276186	0,9947724584

Tableau 1 Représente la moyenne de chaque métrique

3.7 Conclusion :

Ce chapitre explore les outils et les méthodes utilisés pour développer notre application. Ensuite, nous examinons en détail les phases d'insertion et d'extraction, qui dépendent de la technologie DCT utilisée pour sécuriser les images médicales. Enfin, nous discutons et présentons les résultats obtenus.

Conclusion générale

Avec l'avènement des réseaux de communication et des technologies Internet, la sécurisation des données, des fichiers et des images médicales numériques est devenue une priorité incontournable. Dans ce contexte, le recours à la technique de tatouage numérique s'avère être une méthode efficace pour protéger ces informations sensibles contre les intrusions non autorisées. Toutefois, même avec cette protection, il est crucial de prendre des mesures pour renforcer la sécurité des données.

Notre objectif principal est de garantir la sécurité, l'intégrité et la confidentialité des données médicales en suivant des étapes clés. Premièrement, le tatouage numérique doit être robuste, répondant aux normes de résistance et d'imperceptibilité pour assurer une protection optimale. Nous nous efforçons également de trouver un équilibre entre la qualité visuelle des images tatouées et leur capacité à résister aux attaques potentielles, tout en veillant à ce qu'elles restent de haute qualité malgré une utilisation quotidienne et des influences externes.

Notre approche se concentre sur le développement de la technologie de tatouage numérique en utilisant la Transformée en Cosinus Discrète (DCT) pour insérer le watermark. Cette méthode d'insertion est spécifiquement choisie pour préserver la confidentialité des informations dans l'image et les protéger contre toute divulgation non autorisée. Les évaluations de notre approche ont révélé des résultats satisfaisants, témoignant de son haut niveau de sécurité et d'efficacité.

En ce qui concerne nos objectifs futurs, nous visons à améliorer et à développer davantage les techniques de cryptage d'images pour les rendre encore plus efficaces et sécurisées. De plus, nous aspirons à étendre notre algorithme pour le rendre adaptable à la technologie de tatouage vidéo, ce qui permettrait une protection similaire pour les données médicales sous forme vidéo.

Bibliographie

- [1] F. Kahlessenane, A. khaldi et and S. Euschi, A robust blind medical image watermarking, vol. 24, no. 3, pp.: Cluster Comput, Sep.2021.
- [2] Bekkouche Souad, Tatouage appliqué à l'Imagerie Médicale, Oran, Faculté des Sciences, Département d'Informatique, UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE Mohamed Boudiaf, 2011/2012.
- [3] M. Belahreche, Application des Ondelettes pour le Tatouage Numérique des Images, SETIF, FACULTE DE TECHNOLOGIE DEPARTEMENT D'ELECTRONIQUE, UNIVERSITE FERHAT ABBAS DE SETIF, 01, juin 2015.
- [4] «Définition : image numérique,» [En ligne]. Available: <https://www.schoolmouv.fr/definitions/image-numerique/definition>. [Accès le 12 06 2024].
- [5] Antonio, «The Color Blog,» 4 septembre 2023 . [En ligne]. Available: <https://thecolor.blog/fr/image-matricielle/>. [Accès le 12 06 2024].
- [6] «journal du NET,» [En ligne]. Available: <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203295-pixel-definition/>. [Accès le 12 06 2024].
- [7] D. Chantegrel, Traitement numérique de l'image, L'Académie de Poitiers, 2004.
- [8] 2007. [En ligne]. Available: <http://www.eclairment.com/Image-numerique-quel-format.2007..> [Accès le 12 06 2024].
- [9] C. Lou, J. Liu et and T. Li, Digital Signature-based Image Authentication. Idea Group, I. G. Publishing, Éd., IEEE International Conference on Multimedia Computing and Systems (ICSMCS'99), 2004.
- [10] Y. Hu, J. Huang, S. Kwong et and Y. Chan, Image Fusion Based Visible Watermarking Using Dual-Tree Complex Wavelet Transform, 2003.
- [11] «photo24,» [En ligne]. Available: <blog.photo24.fr/bruit-numerique-quest-ce-que-cest/>. [Accès le 12 06 2024].
- [12] «Histogramme image,» [En ligne]. Available: <https://www.dcode.fr/histogramme-image>. [Accès le 12 06 2024].
- [13] M. S. Moad, M. R. Kafi et and A. Khald, Medical image watermarking for secure ehealthcare, 2022.
- [14] KISSOUM Farida et ROUIFED Chahira, Watermarking et compression d'images numériques, TIZI-OUZOU, FACULTE DE GENIE ELECTRIQUE ET DEL'INFORMATIQUE DEPARTEMENT D'ELECTRONIQUE UNIVERSITE MOULOUD MAMMERI, 2011/2012..

- [15] C. Lou, J. Liu et T. Li, Digital Signature-based Image Authentication, I. Group, Éd., Florence, 2004, p. [66].
- [16] M. S. Moad, M. R. Kafi et A. Khaldi, A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications *Microprocessors and Micro-systems*, vol. 90, Apr. 2022, p. 104490.
- [17] F. Kahlessenane,, A. Khaldi, R. Kafi et and S. Euschi, “A DWT based watermarking approach, vol. 12, no. 2, pp., *J Ambient Intell Human Comput*, Feb. 2021.
- [18] F. Kahlessenane, A. Khaldi, R. Kafi et S. Euschi, A DWT based watermarking approach for medical image protection, vol. 12, Feb. 2021, p. 2931–2938.
- [19] K. Amine, K. Redouane et M. Bilel, A redundant wavelet based medical image watermarking scheme for secure transmission in telemedicine applications, Aug. 2022.
- [20] M. M. Sayah, K. M. Redouane et d K. Amine, Secure transmission and integrity verification for color medical images in telemedicine applications,” *Multimed Tools Appl*, May 2022.
- [21] F.Ritter, T.Boskamp, A.Homeyer, H.Laue, M.Schwier, F.Link et and H.Peitgen, *Medical Image Analysis*, 2011.
- [22] M. Tayachi, Sécurité des images par tatouage numérique et cryptographie dans les applications médicales *Cryptographie et sécurité [cs.CR]*, Université de Bretagne occidentale - Brest ; Université de Tunis El Manar , 2021.
- [23] K. LOUKHAOUKHA, Tatouage numérique des images dans le domaine, la Faculté des études supérieures de l'Université Laval, 2010.
- [24] N. Zermi, A. Khaldi, R. Kafi, F. Kahlessenane et S. Euschi, A DWT-SVD based robust digital watermarking for medical image security, vol. 320, Mar. 2021, p. 110691.
- [25] BOUCHAMA Samira, Le tatouage des images Appliqué à l'imagerie médicale, DEPARTEMENT D'ELECTRONIQUE,ECOLE NATIONALE POLYTECHNIQUE, 2007.
- [26] BELILITA sarra, Développement et Implémentation d'algorithmes de tatouage robustes des images fixes et vidéo, SETIF, FACULTÉ DE TECHNOLOGIE,Filière : Electronique ,UNIVERSITÉ FERHAT ABBAS, 2019.
- [27] N. Zermi, A. Khaldi, M. R. Kafi, F. Kahlessenane et S. Euschi, An SVD Values Ordering Scheme for Medical Image Watermarking, vol. 53, Feb. 2022, p. 282–297.
- [28] A. Khaldi, M. R. Kafi et B. Meghni, Electrocardiogram signal security by digital watermarking, Jul. 2022.
- [29] M. Farouk ZEHDA, Tatouage d'images basé sur des transformées discrètes entières, SETIF, Faculté de Technologie ,Département d'Électronique,UNIVERSITE FERHAT ABBAS, 2014.

- [30] Chokri Chemak, *Algorithme de Tatouage Robuste et Aveugle pour la Déontologie et le Transfert des Informations Médicales*, Université de Franche-Comté U.F.R Sciences et Techniques, 2006.
- [31] Mustafa OTHMAN, *Objective video quality metric aware Adaptation mechanisms for video streaming based on DASH*, Université Sorbonne, 2021.
- [32] «visualstudio,» [En ligne]. Available: <https://code.visualstudio.com/>. [Accès le 12 06 2024].