

**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE MINISTERE DE
L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE MOHAMED BOUDIAF – M'SILA**

FACULTE : des Mathématiques et de
l'Informatique

DEPARTEMENT : de l'informatique

N° :



DOMAINE : Mathématiques et de
l'Informatique

FILIERE : Informatique

OPTION : Réseaux et Technologies de
l'Information et de la Communication

**Mémoire présenté pour l'obtention
Du diplôme de Master Académique**

Par : - Chennouf Fatima Ezzahra
- Kouidri Soumia

Intitulé

**Sécurité des données médicales en appliquant le
tatouage numérique**

Évalué par le jury composé de :

Mr. Adel Moussaoui	Président	Université de M'sila
Mr. Noureddine Chikouche	Rapporteur	Université de M'sila
Mr. Mohamed Bahache	Examineur	Université de M'sila

Année universitaire 2019/2020

Remerciements

Nous remercions ALLAH, Dieu qui nous a permis de nous guider dans nos études jusqu'à la préparation de cette présente mémoire, nous vous remercions de nous guider de la meilleure façon possible.

Nous remercions nos parents qui ont travaillé si dur pour nous voir réussir et arriver à ce point

Nous sommes heureux d'exprimer nos modestes remerciements à :

Tout d'abord, Dr. Noureddine Chikouche, notre encadreur dans ce domaine, nous le remercions pour ses conseils, sa compréhension, sa présence, son aide et sa patience.

Deuxièmement, tous les professeurs sans exception qui nous ont honorés pendant nos études en nous apportant des connaissances avec dévouement.

Troisièmement, les membres du jury, qui ont accepté de nous honorer, ont accepté d'examiner, de juger et d'évaluer le mémoire de maîtrise final.

Enfin, à nos familles et amis pour leur soutien affectif et financier tout au long de nos études qu'ils trouvent ici le témoignage de nos profondes gratitude.

Merci à ceux que nous avons toujours oubliés : notre école, notre collège et nos lycées. Nous apprécions vraiment cela.

Merci

Résumé

La protection des données d'images médicales confidentielles contre tout accès non autorisé est un domaine de recherche très important. Dans ce mémoire, nous avons proposé une approche améliorée pour la sécurité des images médicales avec une application de tatouage numérique, basée sur la combinaison de l'algorithme DWT, l'algorithme de cryptage AES, et la fonction de hachage (SHA-256).

Nous avons implémenté notre approche en utilisant le langage de programmation Python. De plus, nous avons discuté les différents résultats expérimentaux et les comparé avec les résultats de l'approche d'origine. Notre approche est plus sécurisée par rapport d'autres approchés étudiées.

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

ملخص

تعد حماية بيانات الصور الطبية السرية من الوصول غير المصرح به مجال بحث مهم للغاية. في هذه المذكرة، اقترحنا طريقة محسنة لأمان الصور الطبية باستخدام تطبيق الدمغ بالعلامات المائية الرقمية (watermarking) بالقيام بالدمج ما بين خوارزمية DWT وخوارزمية التشفير AES وخوارزمية التجزئة (SHA-256).

قمنا ببرمجة الطريقة المحسنة بإستعمال لغة البرمجة بايتون. بالإضافة إلى ذلك قمنا بمناقشة النتائج التجريبية المختلفة ومقارنتها بنتائج الطريقة الأصلية. الطريقة المقترحة أكثر أماناً مقارنة بالمناهج الأخرى التي تمت دراستها.

الكلمات المفتاحية: الصور الطبية، الأمان، الدمغ بعلامة مائية ، DWT، بايتون

Abstract

Protecting confidential medical image data from unauthorized access is a very important area of research. In this dissertation, we proposed an improved approach for the security of medical images with a digital watermarking application, based on combining of DWT technique, AES algorithm, and hash algorithm (SHA-256).

We implemented our approach by using programming language Python. In addition, we discussed the different experimental results and compared it with the results of original approach. Our improved approach is more secure compared to other approaches studied.

Keywords: medical images, security, watermarking, DWT, Python

TABLE DES MATIÈRES

Liste des Tableaux	i
Liste des Figures	ii
Liste des Notations	iii
Liste des Acronymes	iv
INTRODUCTION GÉNÉRALE	1
CHAPITRE 01 : IMAGES MÉDICALES	
1.1.Introduction	3
1.2.Image.....	3
1.3.La structure d'image	3
1.3.1. L'image matricielle	3
1.3.2. L'image vectorielle.....	4
1.4.Numérisation d'une image	5
1.4.1. Définition	5
1.4.2. Procédures de numérisation	5
1.5.Définitions relatives à l'image	6
1.5.1. Pixel	6
1.5.2. La taille d'une image	6
1.5.3. Résolution	7
1.6.Caractéristiques des images	7
1.6.1. La luminance	7
1.6.2. Le contraste	8
1.6.3. La notion de bruit	8
1.6.4. L'histogramme	8
1.7.Les types d'image	9
1.7.1. Image binaire	9
1.7.2. Image au niveau de gris	10
1.7.3. Image couleur	10
1.8.Format d'enregistrement d'une image	11

1.8.1. BMP	11
1.8.2. GIF	11
1.8.3. JPEG	11
1.8.4. TIFF	11
1.8.5. PNG	12
1.9. Les techniques d'imagerie médicale	12
1.9.1. Radiologie	12
1.9.2. Scanner	13
1.9.3. Echotomographie	14
1.9.4. La mammographie	14
1.9.5. Imagerie par résonnance magnétique	15
1.10. La sécurité d'une image médicale	16
1.11. Conclusion	16

CHAPITRE 02 : TATOUAGE NUMÉRIQUE.

2.1. Introduction	17
2.2. Historique	17
2.3. Définition	18
2.4. Propriétés du tatouage numérique	18
2.5. Le tatouage numérique des images	19
2.5.1. Phase d'insertion	20
2.5.2. Phase d'extraction	20
2.6. Les applications du tatouage numérique	21
2.6.1. Protection des droits d'auteur	21
2.6.2. La prévention de la copie illégale ou « fingerprinting »	21
2.6.3. Authentification des données	22
2.6.4. Contrôle d'accès	22
2.7. Classification des algorithmes de tatouage	22
2.7.1. Classification des algorithmes de tatouage numérique selon le domaine d'insertion	23
2.7.1.1. Insertion dans le domaine spatial	24
2.7.1.2. Insertion dans le domaine fréquentiel	24

2.7.1.3. Algorithme hybrides	27
2.7.2. Classification des algorithmes de tatouage numérique selon la robustesse	27
2.7.2.1. Algorithme de tatouage numérique robustes	27
2.7.2.2. Algorithme de tatouage numérique fragiles	27
2.7.2.3. Algorithme de tatouage numérique semi-fragiles	27
2.7.3. Classification des algorithmes de tatouage numérique selon la technique d'insertion	28
2.7.3.1. Insertion additive	28
2.7.3.2. Insertion par substitution	28
2.7.4. Classification des algorithmes de tatouage numérique selon le mode d'extraction	28
2.7.4.1. Le tatouage Aveugle	28
2.7.4.2. Le tatouage Semi-Aveugle	28
2.7.4.3. Le tatouage Non Aveugle	29
2.7.5. Classification des algorithmes de tatouage numérique selon la perception de la marque	29
2.7.5.1. Le tatouage invisible	29
2.7.5.2. Le tatouage visible	29
2.7.6. Classification des algorithmes de tatouage numérique selon la préservation de l'image originale	29
2.7.6.1. Le tatouage réversible	29
2.7.6.2. Le tatouage non réversible	30
2.8. Les attaques	30
2.8.1. Attaques de traitement d'image	30
2.8.2. Attaques géométriques	30
2.8.3. Attaques cryptographiques	30
2.8.4. Attaques de protocole	30
2.9. Conclusion	31

CHAPITRE 03 : TECHNIQUES DE TATOUAGE BASÉES SUR DWT.

3.1. Introduction	32
3.2. Technique transformée en ondelettes discrète (DWT)	32

3.2.1. Algorithme pour l'intégration de Filigrane	33
3.2.2. Algorithme pour l'extraction de Filigrane	34
3.3. Technique DWT-DCT	35
3.3.1. Algorithme d'intégration	36
3.3.2. Algorithme d'extraction	38
3.4. Technique DWT-SVD	39
3.4.1. Algorithme-intégration d'un Filigrane	40
3.4.2. Algorithme-extraire le Filigrane	42
3.5. Technique DWT-DCT-SVD	42
3.5.1. Procédure d'intégration	43
3.5.2. Procédure d'extraction	44
3.6. Comparaison	45
3.7. Conclusion.....	47

CHAPITRE 04 : APPROCHE PROPOSÉE ET IMPLÉMENTATION.

4.1. Introduction	48
4.2. Notre Approche	48
4.3. Implémentation	50
4.4. Bibliothèque	51
4.5. Environnement matériel	51
4.6. Résultats Expérimentaux	52
4.6.1. Filigrane avec DWT	52
4.6.2. Filigrane avec DWT améliorer.....	58
4.6.3. PSNR (peak signal-to-noise ratio)	63
4.6.4. SSIM (Structural Similarity Index)	64
4.7. Discussion	65
4.8. Conclusion	66
CONCLUSION GÉNÉRALE	67
BIBLIOGRAPHIE	68

Liste des tableaux

Table 3.1 : Comparaison des techniques des tatouage numérique	46
Table 4.1 : Les valeurs PSNR de l'approche proposée et l'approche existante.....	65
Table 4.2 : Les valeurs SSIM de l'approche proposée et l'approche existante.....	66

Liste des Figures

Figure 1.1 : Différences entre image vectorielle et matricielle	4
Figure 1.2 : Différences entre image vectorielle et matricielle	5
Figure 1.3 : Une image constitue d'un ensemble des pixels	6
Figure 1.4 : Le passage d'une image couleur à une image de luminance en niveaux de gris	7
Figure 1.5 : Contraste de la luminosité	8
Figure 1.6 : Histogrammes pour une même image " plus ou moins bien exposée "	9
Figure 1.7 : Convertir une image couleur en une image en niveaux de gris	10
Figure 1.8 : Schéma d'un tube à rayons X	13
Figure 1.9 : Géométrie d'un scanner	13
Figure 1.10 : Echotomographie abdominale	14
Figure 1.11 : Mammographie d'un sein de femme à cancer (la masse suspecte)	15
Figure 1.12 : Scanner d'IRM	15
Figure 2.1 : Propriétés du tatouage numérique	19
Figure 2.2 : Schéma général d'un système de tatouage numérique des images	19
Figure 2.3 : Schéma général de l'insertion d'une marque	20
Figure 2.4 : Schéma général d'extraction non aveugle d'une marque	21
Figure 2.5 : Organigramme de la classification des algorithmes de tatouage numérique	23
Figure 2.6 : Les régions de DCT	25
Figure 3.1 : Modèle de décomposition DWT en 2 niveaux	32
Figure 3.2 : Schéma explicatif pour l'insertion par la technique DWT	34
Figure 3.3 : Schéma explicatif pour l'extraction par la technique DWT	35

Figure 3.4 : Procédure combinée d'intégration du filigrane DWT-DCT	36
Figure 3.5 : Sous-bandes DWT multi-résolution de l'image originale	37
Figure 3.6 : Procédure d'extraction de filigrane DWT-DCT combinée	39
Figure 3.7 : Système proposé	40
Figure 3.8 : Schéma explicatif pour l'insertion par la technique DWT-DCT-SVD	43
Figure 3.9 : Schéma explicatif pour l'extraction par la technique DWT-DCT-SVD	45
Figure 4.1 : Schéma explicatif pour intégration de Filigrane par DWT amélioré.....	49
Figure 4.2 : Schéma explicatif pour extrait la Filigrane par DWT amélioré	50
Figure 4.3 : IRM avant et après le DWT.	52
Figure 4.4 : Scanner avant et après le DWT.	53
Figure 4.5 : Les résultats obtenus de IRM par DWT.	54
Figure 4.6 : Les résultats obtenus de Scanner par DWT.	55
Figure 4.7 : Les résultats obtenus de IRM par DWT inverse.	56
Figure 4.8 : Les résultats obtenus de Scanner par DWT inverse.	57
Figure 4.9 : IRM avant et après le DWT amélioré.	58
Figure 4.10 : Scanner avant et après le DWT amélioré.	59
Figure 4.11 : Les résultats obtenus de IRM par DWT amélioré	60
Figure 4.12 : Les résultats obtenus de Scanner par DWT amélioré.	61
Figure 4.13 : Les résultats obtenus de IRM par DWT inverse amélioré	62
Figure 4.14 : Les résultats obtenus de Scanner par DWT inverse amélioré.	63

Liste des Notations

I	Image originale.
M	Marque.
I_w	Image tatouée.
C_m	La clé secrète de marquage.
U	Matrice orthogonale.
S	Diagonal matrice.
V^T	La transposition d'une matrice orthogonale.
A	Matrice carrée.
X	Matrice des coefficients de bande.
H	Image hôte.
P	Matrice orthogonale (unitaire).
R	Matrice orthogonale (unitaire).
Q	Diag (F1, F2...Fr).
I	Image modifiée.
W	Watermark.
H	Band.
α	Intensité d'incorporation.
α	Facteur de gain.
PN_0	Incorporer le bit de filigrane 0.
PN_1	Incorporer le bit de filigrane 1.
DCT (m, n)	Coefficient DCT.
c(m)	Les coefficients calculés.
x (k, l)	La valeur du pixel du domaine spatial.
w_M	Watermark.
f0	Fonction Boolean 0.

f1	Fonction Boolean 1.
$\Sigma 0$	Fonction linéaire 0.
$\Sigma 1$	Fonction linéaire 1.

Liste des Acronymes

IRM	Imagerie par résonance magnétique.
SVG	SVG-Edit ou Inkscape.
ai	Adobe Illustrator.
Pixel	Picture élément.
R	Rouge.
V	Vert.
B	Bleu.
DPI	Dots Per Inch.
PPP/PPI	Points par pouce/inch.
SVH	Système Visuel Humain.
BMP	Bit Map.
GIF	Graphics Interchange format.
JPEG	Joint Photographic Experts Group.
TIFF	Tagged image file format.
PNG	Pour portable networks graphics.
SQUID	Superconducting quantum interference device.
CD-ROM	Disc read-only memory.
DWT	Discret Wavelet Transform.
DCT	Discret Cosine Transform.
SVD	Singular Value Decomposition.
IDWT	Inverse Discret Wavelet Transform.

IDCT	Inverse Discret Cosine Tronsform.
FL	Band frequency low.
FM	Band frequency middle.
FH	Band frequency high.
LL	Low low frequency band.
HL	High low frequency band.
LH	Low high frequency band.
HH	High high frequency band.
AES	Advanced Encryption Standard.
CBC	Cipher Block Chaining.
DES	Data Encryption Standard.
SHA	Secure Hash Algorithm.
NIST	National Institute of Standards and Technology.
IA	Intelligence Artificielle.
Pywt	Python Wavelets.
Py	Python.
PIL	Python Imaging Library.
Tcl/Tk	Tool Command Language/ToolKit.
PC	Personal Computer.

INTRODUCTION GÉNÉRALE

Contexte:

Le développement rapide de la technologie Internet et du multimédia dans tous les domaines conduit à la disponibilité des données numériques pour le public. L'utilisation d'Internet s'étend à plusieurs domaines tels que la télémédecine, la banque en ligne, le télé-achat, etc.

Dans les applications de télémédecine, il faut assurer la sécurité, la confidentialité et l'intégrité des images médicales. Les principaux aspects de la sécurité liées aux données médicales sont la confidentialité, l'authentification, l'intégrité et la disponibilité des images, car un jugement critique se fait sur les images médicales, ce qui conduit au traitement approprié.

Il est très important pour prévenir la manipulation non autorisée et l'appropriation illicite de ces images numérisées. À cela il existe plusieurs techniques pour la sécurité et la vérification de l'intégrité des données, parmi eux le tatouage numérique.

Le tatouage numérique est une technologie destinée à protéger le droit d'auteur et l'authentification de ces images médicales, cette technique comprend deux étapes : l'incorporation et l'extraction. Pendant le processus d'intégration, certaines informations confidentielles sont incluses dans les photos médicales. Au cours du processus d'extraction, le message secret est extrait qui est incorporé dans l'image médicale. La falsification d'image peut être détectée lorsque l'image confidentielle ne correspond pas à l'image existante, le destinataire saura qu'il y a eu une sorte de manipulation.

Problématique et objectif :

Les méthodes existantes pour sécuriser les données d'images médicales basent principalement sur de lourds algorithmes de traitement du signal qui nécessitent beaucoup de bande passante et nécessitent une conception complexe prend beaucoup de temps pour atteindre leur objectif. Par contre, il n'existe pas un seul algorithme de tatouage suffisamment sécurisé pour fournir un complètement résultat sans faille et sans perte. La plupart des algorithmes symétriques sont plus rapides mais plus facile à percer, alors que les algorithmes asymétriques sont plus sécurisés mais prend plus de temps.

Notre objectif est de créer un système qui protège les images médicales en améliorant la technologie de tatouage pour devenir une technologie de conception simple et facile à utiliser tout en préservant la confidentialité de l'image médicale du patient après l'avoir transférée à une autre personne. Pour cela, on va adopter un algorithme de chiffrement robuste et de fonction de hachage sûre.

Organisation du mémoire:

Ce rapport est divisé en quatre chapitres

Le premier chapitre c'est une introduction aux images numériques. Plus précisément, nous expliquons certains termes et certains concepts dans le domaine des images numériques tels que la numérisation et les caractéristiques et types d'images et les techniques d'imagerie médicales dans le domaine des images médicales tels que radiologie, scanner...etc.

Dans le deuxième chapitre, nous allons commencer par parler sur le tatouage d'images numériques. Après nous allons passer à connaître et parler des filigranes numériques et de toutes les informations qui y sont liées.

Dans le troisième chapitre nous allons parler sur des récents techniques et recherches dans le domaine de tatouage numérique. Quatre algorithmes de tatouage (techniques) ont évalué dans ce chapitre. Les conclusions obtenues serviront pour le prochain chapitre.

Le dernier chapitre sera consacré à la partie de conception et implémente de technique proposée pour chiffrer les informations médicales.

Nous terminons notre travail par une conclusion générale.

CHAPITRE 01 :
IMAGES MEDICALES

1.1. Introduction

En tant que moyen de communication mondial qui nous permet de transférer, de préserver et de comprendre des informations, l'image est l'un des moyens les plus importants que les humains utilisent et c'est la méthode la plus efficace où chacun peut analyser l'image à sa manière pour obtenir une impression et ainsi extraire une certaine quantité d'informations.

Une image est une représentation d'une scène ou d'un objet généralement situé dans un espace 3D.

Dans ce chapitre, nous présentons dans la première partie quelques concepts de base du traitement d'image numérique tels que : définition, types et caractéristiques de l'image. La deuxième partie de ce chapitre est consacrée à l'imagerie médicale. Aujourd'hui, les médecins utilisent couramment cinq techniques : la radiographie et la numérisation, l'échographie, la mammographie et Imagerie par résonance magnétique (IRM).

1.2. Une image

L'image est un signal bidimensionnel, elle peut aussi être décrite comme une fonction (x, y) définie dans un champ spécifique [1].

L'image numérique est une conversion d'une image analogique en valeurs numériques, compatible avec la luminosité mesurée pour chaque pixel.

L'image numérique est produite à travers le moyen de l'échelle du faisceau d'imagerie ou du balayage d'une image analogique (photographique, ...) [2].

1.3. La structure d'image

Il existe 2 sortes d'images numériques, l'image matricielle et l'image vectorielle.

1.3.1. L'image matricielle

Les images matricielles (ou image en mode point, en anglais « bitmap » ou « raster » est un ensemble de points appelés pixels qui composent une image avec une définition précise, il est utilisé pour composer une image numérique.

Lorsqu'on le grandie trop, sa qualité est perdue et le pixel devient plus clair (points carrés) [3].

Les images matricielles appartiennent aux formats de fichiers suivants : JPG, JPEG, PNG et en particulier "GIF" pour gérer les transparents.

Dans le bitmap, la qualité de l'image est élevée, la taille du fichier est grande. "Cette image est réaliste" [4].

1.3.2. L'image vectorielle

Dans une image vectorielle, les données sont représentées mathématiquement par des figures géométriques simples.

Cette image est utilisée pour d'autres formes composées de lignes et de graphiques simples [3].

Il existe des formats gratuits comme "SVG" (SVG-Edit ou Inkscape) et des formats spéciaux comme ".ai" (Adobe Illustrator).

Dans l'image vectorielle, il a la capacité de s'étendre sans bordures et est léger, ce qui est utilisé dans des graphiques simples [4].

Les figures 1.1 et 1.2 illustre les différences entre image vectorielle et matricielle.

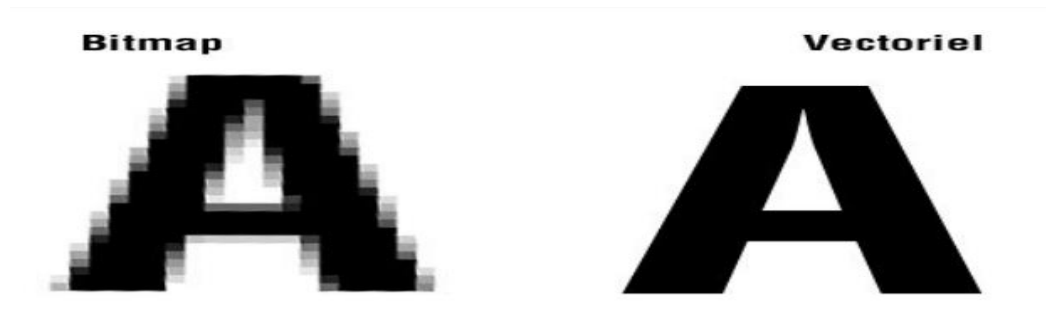


Figure 1.1 : Différences entre image vectorielle et matricielle [3].



Figure 1.2 : Différences entre image vectorielle et matricielle [3].

1.4. Numérisation d'une image

1.4.1. Définition

La numérisation est la conversion d'un signal analogique en un signal numérique (D'une quantité illimitée d'amplitudes à une quantité limitée de valeurs).

La numérisation peut se décomposer en trois opérations principales : l'échantillonnage, la quantification, et le codage [5].

1.4.2. Procédures de numérisation

La numérisation suit les étapes suivantes :

- Echantillonnage

C'est la première étape de la numérisation.

L'échantillonnage consiste à remplacer une fonction continue dans le temps ou dans l'espace par la suite des valeurs qu'elle prend en des instants (échantillonnage temporel) [6].

- Quantification

La quantification est l'opération par laquelle : La mesure de l'amplitude instantanée se fait à chaque top d'échantillonnage, examinée, puis représentée la valeur par un nombre entier. C'est à dire qu'on arrondit les valeurs. La valeur retenue est moyenne [7].

- Codage

C'est la transformation de valeurs quantitatives en un langage codé binaire et cela se fait selon des règles spécifiques.

1.5. Définitions relatives à l'image

1.5.1. Pixel

Le pixel (abréviation venant de l'anglais : Picture élément) est l'élément de base d'une image ou d'un écran, c'est-à-dire un point (le plus petit point de l'image). L'ensemble de ces pixels compose l'image (Voir la figure 1.3).

Dans le cas d'une image monochrome, chaque pixel est codé sur un octet.

Dans une image couleur (R.V.B.), un pixel peut être représenté sur trois octets : un octet pour chacune des couleurs : rouge (R), vert (V) et bleu (B)[8].



Figure 1.3 : Une image constitue d'un ensemble des pixels [8].

1.5.2. La taille d'une image

Pour connaître la taille (en octets) d'une image, il est nécessaire de compter le nombre de pixels, et le multiplier par la taille (ou poids) d'un pixel, Pour chaque pixel on a : 3 couleurs (RVB), Pour chaque couleur on a : 1 octets ou 8bits [9].

1.5.3. La résolution

La résolution d'une image correspond au nombre de pixels par unité de longueur (pouce ou centimètre). On utilise aussi le mot résolution pour désigner le nombre total de pixels ; quand le nombre est élevé la qualité est mieux.

La résolution d'impression d'une imprimante ou de capture d'un scanner s'exprime en « DPI » (« dots per inch ») ou en français « PPP/PPI » (« points par pouce/inch »), un pouce mesure 2,54 cm [10].

1.6. Caractéristiques des images

1.6.1. La luminance

C'est le degré de luminosité des points de l'image, la luminance de la couleur est une valeur calculer en moyennent les trois canaux d'une image en niveaux de gris à partir d'une image couleur [11].

$$a = \frac{r + v + b}{3}$$

La figure 3.9 illustre le passage d'une image couleur à une image de luminance en niveaux de gris.



Figure 1.4 : Le passage d'une image couleur à une image de luminance en niveaux de gris [11].

1.6.2. Le contraste

C'est l'opposition marquée entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de cette image. Le contraste est défini en fonction des luminances de deux zones d'images (le plus exploité dans les mesures de qualité d'image). En effet, un carré, de luminance moyenne, présenté sur un fond foncé apparaît plus clair que ce même carré présenté sur un fond clair (Voir la figure 1.5) [12].

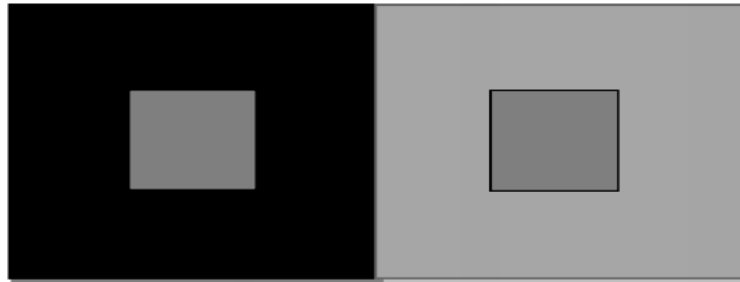


Figure 1.5 : Contraste de la luminosité [12].

D'après E. Durand et E. Blandiux "Un diagnostic est généralement fait en discernant le signal anormal d'une lésion au sein d'un organe normal. C'est donc le contraste entre les deux qui permet le diagnostic." [13].

Le contraste généralement utilisé dans les modèles du SVH dépend de plusieurs paramètres [12].

1.6.3. La notion de bruit

Le bruit dans l'image est une distorsion du signal et correspond à un phénomène aléatoire inclus dans l'image idéale.

Son effet est de rendre l'image illisible, dégradation de la résolution spatiale [13].

1.6.4. L'histogramme

Un histogramme est un graphique statistique permettant de représenter la distribution des intensités des pixels d'une image, c'est-à-dire important pour contrôler l'exposition d'une image.

Il peut être utile dans les cas suivants :

- Pour contrôler et affiner les réglages de prise de vue.
- Pour corriger ou modifier l'exposition de l'image, ainsi que l'échelle des couleurs.
- Pour apparaître les détails et les nuances acquises par le capteur et présentes dans le fichier, mais non visibles à l'œil.

La Figure 1.6 représente le niveau d'intensité en abscisse en allant du plus foncé (à gauche) au plus clair (à droite) [14].

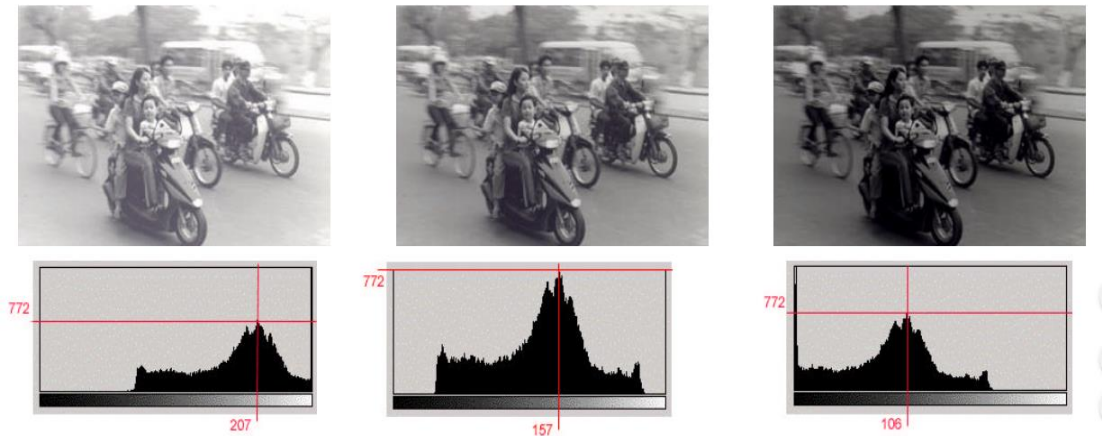


Figure 1.6 : Histogrammes pour une même image "plus ou moins bien exposée" [14].

Ainsi, l'histogramme d'une image en 256 niveaux de gris sera représenté par un graphique possédant 256 (de 0 à 255) valeurs en abscisse, et le nombre de pixels de l'image en ordonnée [14].

1.7. Les types d'image

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

1.7.1. Image binaire

D'après M. Chilowicz " Une image numérique binaire se caractérise par des pixels codés sur un bit définis par deux valeurs : 0 ou 1. L'utilisation d'images binaires peut par

exemple être utilisée pour la représentation de documents scannés en noir et blanc ou alors pour des télécopies." [15].

1.7.2. Images au niveau de gris

D'après D. Müller "Dans une image en niveaux de gris, chaque pixel est noir, blanc, ou à un niveau de gris entre les deux. Cela signifie que les trois composantes ont la même valeur.

L'œil est plus sensible à certaines couleurs qu'à d'autres. Le vert (pur), par exemple, paraît plus clair que le bleu (pur). Pour tenir compte de cette sensibilité dans la transformation d'une image couleur en une image en niveaux de gris, on ne prend généralement pas la moyenne arithmétique des intensités de couleurs fondamentales, mais une moyenne pondérée.

La formule standard donnant le niveau de gris en fonction des trois composantes est :

Gris = int (round (0.299·rouge + 0.587·vert + 0.114·bleu))" [16].

La Figure 1.7 illustre la convertir une image couleur en une image en niveaux de gris.



Figure 1.7 : Convertir une image couleur en une image en niveaux de gris [16].

1.7.3. Image couleur

Pour représenter l'image à l'écran, les applications numériques utilisent la base RVB (Rouge Vert Bleu) en utilisant ses composants (Cet espace de couleur est basé sur le principe de la synthèse additive, c'est à dire le mélange des trois composantes R, V et B à leur valeur maximale donne du blanc, à l'instar de la lumière.).

Chaque couleur est représentée par un triplé de réels dans $[0, 1]$ (le triplet $(1, 1, 1)$ étant la couleur blanche et $(0, 0, 0)$ la couleur noire) [15].

1.8. Formats d'enregistrement d'une image

Choix d'un format pour la pérennité des informations numériques est très important. En fonction de nouveaux besoins et l'apparition de nouveaux formats :

1.8.1. BMP

D'après R. Caloz, C. Collet " le format BMP (Bit Map) de base dans la programmation de Windows pour des images en mode point et les accessoires standards de Windows.

Les images et les icônes de Windows sont stockés dans ce format BMP " [2].

1.8.2. GIF

Le format GIF (Graphics Interchange format) est un format populaire utilisé pour l'affichage de graphiques et d'images dans des pages Internet. Il est limité à 256 couleurs, donc il ne convient pas dans le cas de photographies très colorées.

Ce format d'image est utilisé pour les images contenant peu de nuances de couleurs et avec des transitions brusques, comme les logos ... [17].

1.8.3. JPEG

Le format JPEG (Joint Photographic Experts) est largement utilisé pour l'affichage de photographies dans Internet.

Ce format utilise une compression avec perte d'information, Il ne gère pas l'effet de transparence comme le GIF mais il dépasse la limite des 256 couleurs. Le taux de compression d'une image peut varier entre 1 et 99% [17].

1.8.4. TIFF

Le format TIFF (Tagged Image File Format), Il s'agit d'un format spécial pour les documents numérisés, conçu pour stocker des documents de différents types (texte,

image...). C'est un excellent format d'archivage qui garantit la qualité des documents, le processus de stockage peut être de grandes tailles.

Les algorithmes relisant le format TIFF doivent pouvoir décoder le codage sans perte [18].

1.8.5. PNG

Le format PNG (pour portable networks graphics) a été conçu comme codage de graphiques en mode balayage et compression sans perte. Il a été développé en concurrence du format GIF (graphics interchange format) de CompuServe.

PNG est très utilisé pour les arts graphiques.

Le format PNG supporte :

- complètement les images en couleur.
- également les informations de transparence associées à une image.

PNG ne supporte pas :

- les graphiques animés (au contraire de GIF) [18].

1.9. Les techniques d'imagerie médicale

1.9.1. Radiologie

D'après P.G. Frija, P.B. Mazoyer [19] "La radiographie standard 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 où elle permet d'étudier les traumatismes osseux (fractures, etc.), les déformations du squelette ou les implantations dentaires. La pneumologie y a aussi recours (radio des poumons).

Chez la femme, la radiographie du sein (mammographie) est devenue un examen systématique de prévention du cancer du sein. Il est aussi 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. " [19].

La Figure 1.8 illustre un schéma d'un tube à rayons X.

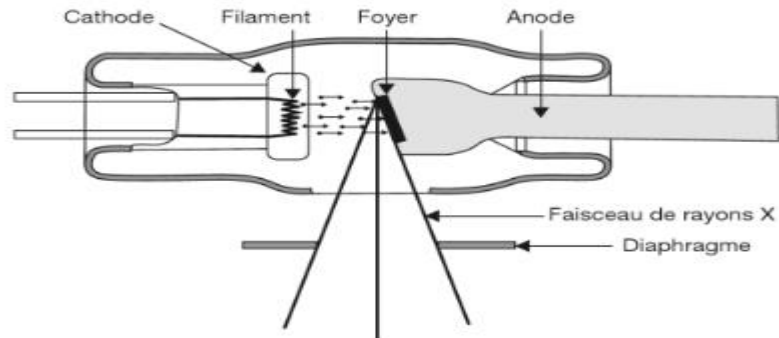


Figure 1.8 : Schéma d'un tube à rayons X [20].

1.9.2. Scanner

Le scanner est en quelque sorte une « endoscopie virtuelle » qui nous permet de créer une image tridimensionnelle des organes ou des tissus qui composent les zones numérisées.

Dans sa première apparition, il est devenu célèbre en neurosciences pour sa capacité à voir le cerveau, maintenant il est remplacé par la résonance magnétique lorsque cela est possible car le scanner est capable de visualiser un changement de taille ou de déformation de la structure, mais ne capable pas de déterminer sa nature (inflammation, cancer ...).

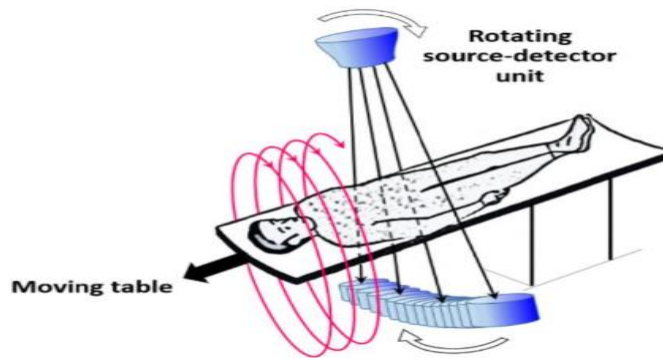


Figure 1.9 : Géométrie d'un scanner [21].

Le scanner est un examen aux rayons X, et utilisé dans de nombreux domaines.

Les résultats sont placés sur CD-ROM pour un stockage facile [19].

La figure 1.9 au-dessus illustre un schéma d'un tube à rayons X

1.9.3. Echotomographie

L'échotomographie utilise l'échographie pour obtenir une image anatomique des diapositives corporelles, c'est une technique utilisée pour le diagnostic médicale pour sa simplicité et son efficacité avec un coût minimal, de sorte que son importance ne peut être niée [22].

Il est largement utilisé pour les femmes enceintes, comme il est indiqué au figure 1.10[23].

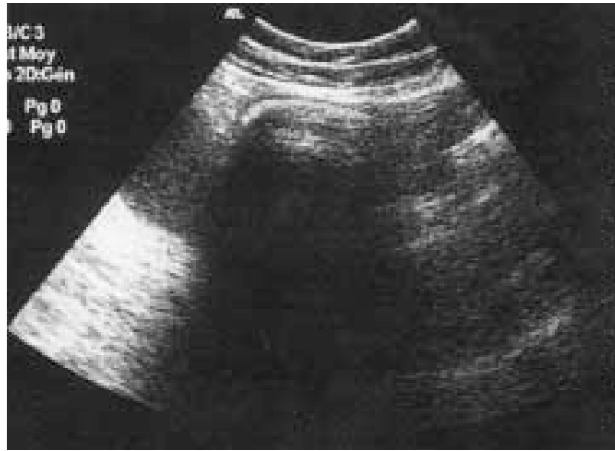


Figure 1.10 : Echotomographie abdominale [24].

1.9.4. La mammographie

La mammographie est une méthode par laquelle les rayons X sont projetés sur le sein avec beaucoup moins d'énergie que celle utilisée pour la radiographie générale.

Les systèmes et détecteurs sont spécifiquement conçus pour produire des images de haute qualité afin de détecter les anomalies mammaires (masses, etc.), ce qui facilite le diagnostic des femmes et la facilité de détection de leur cancer du sein, avec ou sans symptômes mammaires [21].

La Figure 1.11 représente une mammographie d'un sein de femme à cancer (la masse suspecte).



Figure 1.11 : Mammographie d'un sein de femme à cancer (la masse suspecte) [21].

1.9.5. Imagerie par résonance magnétique

L'imagerie par résonance magnétique est le meilleur outil pour l'imagerie médicale, le contraste automatique de haute qualité inhérent à l'IRM permet notamment l'identification des lésions cérébrales et le développement incontrôlé d'une circulation partielle près de la tumeur et bientôt des anomalies de la circulation sanguine.

L'IRM utilise les propriétés magnétiques des protéines d'hydrogène pour leur efficacité contre les tailles souterraines (comme les poumons) [25].

La Figure 1.12 représente un scanner d'IRM.



Figure 1.12 : Scanner d'IRM [26].

Grâce aux détecteurs ultra-sensibles (des SQUID) fonctionnant à très basse température, il est possible de prendre des photos dans des zones très faibles [26].

1.10. La sécurité d'une image médicale

Pour atteindre une confiance totale avec le patient, ce qui est d'une grande importance dans le travail des médecins, ces derniers doivent s'appuyer sur les derniers développements technologiques.

Pour assurer la corrélation correcte entre le patient et la radiographie et pour éviter toute confusion avec la radiographie d'un autre patient (il peut s'agir d'une action illégale ou d'une erreur administrative), les chercheurs dans ce domaine travaillent à créer des systèmes plus sûrs, notamment des tatouages et d'autres systèmes [27].

1.11. Conclusion

Dans ce chapitre, nous avons couvert une idée générale sur l'image avec une explication sur chaque propriété et en particulier l'image numérique.

L'imagerie médicale est un ensemble de techniques utilisées pour diagnostiquer des parties du corps comme diagnostic médical préliminaire, des techniques qui ont conduit à l'émergence d'applications auxiliaires pour le médecin et la médecine.

En fait, par exemple, les rayons et les ultrasons nous fournissent des informations qui révèlent une maladie humaine qui peut être utilisée de manière illégale, et nous abordons ici la question de la confidentialité et du secret et l'émergence de ce que l'on appelle : la vie privée des patients.

Par conséquent, nous avons besoin d'un moyen de préserver la vie privée du patient et de protéger et tatouer les informations, et ce sera le sujet du prochain chapitre.

CHAPITRE 02 :
TATOUAGE NUMERIQUE

2.1. Introduction

Il est très simple de falsifier n'importe quelle image et mettre à la disposition, pour ça les logiciels de manipulation d'image numériques, et le tatouage numérique ici l'une des solutions de ce problème [28].

Le tatouage numérique est un domaine scientifique moderne apparu au début des années 90, est considéré comme l'un des moyens de masquer des informations, comme tatouer un message ou une image secondaire dans une image principale.

Le tatouage numérique est un bon moyen de protéger la propriété contre la copie illégale. Le tatouage numérique Intègre un message connu dans un morceau de données numériques comme moyen d'identifier Propriétaire légal des données. Ces techniques peuvent être utilisées sur de nombreux types de données numériques, comme les images fixes, les films et la musique.

L'idée de base du tatouage numérique consiste à cacher dans un document une information Invisible, dans ce chapitre on présentera un peu historique, quelques définitions de tatouage numérique et ces caractéristiques. Après nous présenterons les différentes applications possibles du tatouage numérique pour les images. Ensuite nous présenterons les classifications des algorithmes de tatouage numérique, à la fin de ce chapitre nous présenterons les attaques existantes.

2.2. Historique

L'histoire de la dissimulation des informations remonte à l'Antiquité afin qu'ils aient utilisé des moyens primitifs pour cacher les informations et assurer leur confidentialité et leur arrivée en toute sécurité, parmi ces méthodes primitives, ils écrivaient le message dans la tête humaine après se raser les cheveux et lorsque les cheveux poussent, le message est envoyé, le destinataire rase à nouveau les cheveux pour lire Le message.

Au Moyen-Âge, l'encre invisible est apparue, car elle était fabriquée à partir de jus d'oignon et de chlorure d'ammoniac, et cette encre se desserre en approchant le papier des flammes des bougies.

2.3. Définition

1. Le tatouage numérique consiste à ajouter une signature dans l'image qui doit être imperceptible et disparaître après la modification de contenu du document [29].
2. Le tatouage numérique est une technique permettant d'insérer une marque dans les composants du document numérique.
3. Cette marque compose d'un ou plusieurs messages secrets et doit être imperceptible et robuste aux attaques [30].
4. Le tatouage numérique consiste à insérer une marque invisible (tatouage) dans une image ou document numériques, pour différents buts comme piratage d'informations et la protection des droits d'auteur.

L'insertion de la marque est effectuée en générale dans le domaine spatial ou fréquentiel.

2.4. Propriétés du tatouage numérique

Pour concevoir un algorithme de tatouage performant prendre en compte les principales contraintes techniques suivant :

- Capacité : représente la quantité d'information que l'on veut insérer dans une image. Cette quantité varie selon l'application [31].
- Robustesse : le système de tatouage devrait être robuste contre plusieurs attaques [31].
- Imperceptibilité : le tatouage numérique va certainement introduire des distorsions. Cette contrainte exige que lesdites distorsions soient les plus faibles possibles afin que visuellement l'image tatouée reste fidèle à l'image originale [31].

La Figure 2.1 représente des propriétés du tatouage numérique.

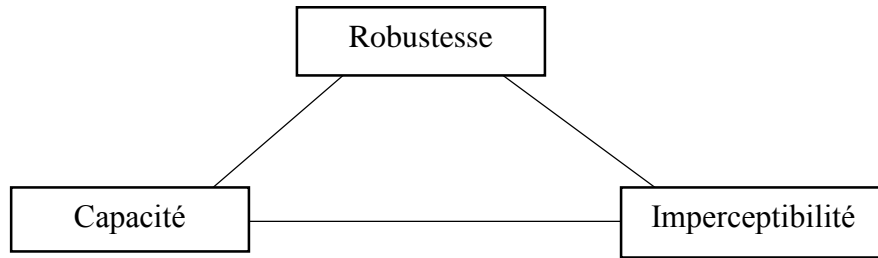


Figure 2.1 : Propriétés du tatouage numérique [28].

2.5. Le tatouage numérique des images

Les images constituent la grande partie de l'ensemble des documents numériques manipulés et échangés dans le monde de l'Internet.

Le tatouage numérique d'image est un concept récent, l'objectif du tatouage est d'insérer une information (le nom ou le logo de l'auteur) dans l'image de manière invisible et indélébile dans le but de la protéger contre les copies [32].

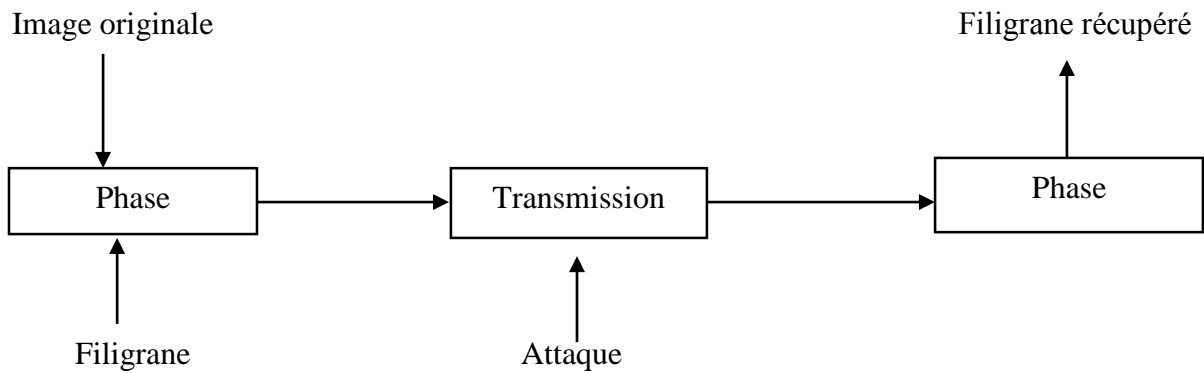


Figure 2.2 : Schéma général d'un système de tatouage numérique des images [33].

Le schéma général d'un système de tatouage numérique des images peut être décrit principalement par deux phases fondamentales : l'insertion et l'extraction de la marque.

La Figure 2.2 au-dessus représente un schéma général d'un système de tatouage numérique des images.

2.5.1. Phase d'insertion

L'insertion de la marque consiste à insérer dans l'image originale I , une marque M et ainsi créer une nouvelle image appelée image tatouée I_w . Un troisième paramètre facultatif peut être ajouté : la clé secrète de marquage C_m qui permet d'assurer un certain niveau de sécurité au processus de tatouage, comme indiqué sur la Figure. 2.3.

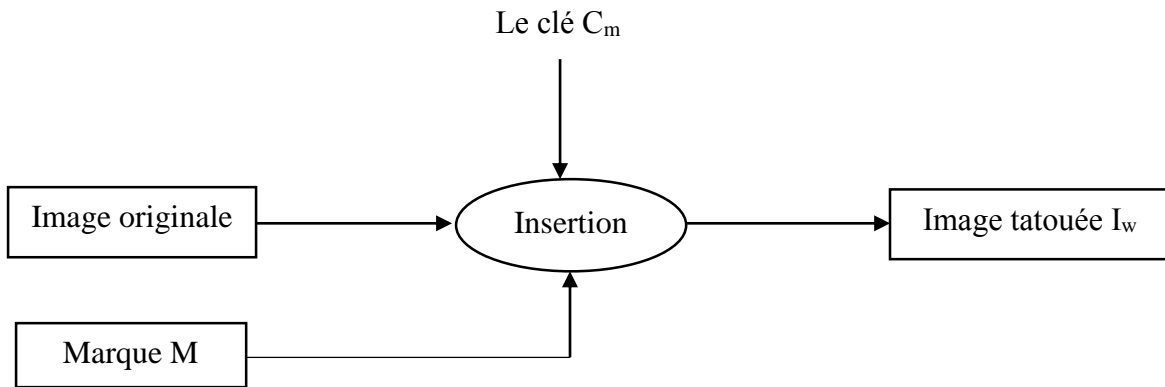


Figure 2.3 : Schéma général de l'insertion d'une marque [37].

2.5.2. Phase d'extraction

Lors de cette phase on peut avoir besoin de l'image originale I . Dans ce cas, on parle d'un tatouage informé ou non aveugle. Dans le cas contraire, le tatouage est dit non informé ou aveugle. Dans certains cas, l'utilisation d'un tatouage informé permet de déterminer si l'image tatouée a été attaquée. Par exemple, si celle-ci a subi une transformation géométrique, la présence de l'image originale fournit des informations supplémentaires qui peuvent servir pour améliorer l'extraction de la marque. L'utilisation de l'image originale à la phase extraction apporte beaucoup de robustesse à l'algorithme de tatouage numérique des images.

La figure 2.4 illustre un schéma général d'extraction non aveugle d'une marque.

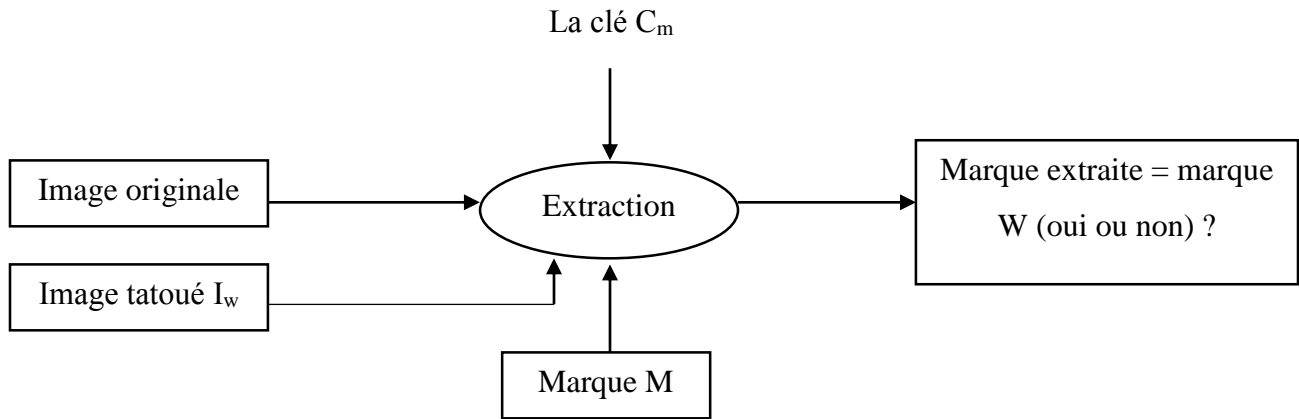


Figure 2.4 : Schéma général d'extraction non aveugle d'une marque [37].

2.6. Les applications du tatouage numérique

La création d'un algorithme universel adaptable à toutes les applications est impossible ce qui fait les applications du tatouage numérique sont nombreuses [34].

2.6.1. Protection des droits d'auteur

L'application la plus évidente du tatouage est le droit d'auteur, le but est d'insérer une signature permettant d'identifier le propriétaire, de façon très robuste.

Les deux principales qualités à respecter sont la robustesse et l'invisibilité de la marque [31].

La marque doit être invisible mais aussi la plus résistante possible, car il est utilisé pour parer le piratage de données [35].

2.6.2. La prévention de la copie illégale ou « fingerprinting »

Fingerprints (Les empreintes digitales) sont les caractéristiques d'un objet qui ont tendance à le distinguer des autres petits objets.

Comme dans les applications de protection du droit d'auteur, le filigrane pour l'empreinte digitale est utilisé pour retracer les utilisateurs autorisés qui violent le contrat de licence et distribuer illégalement le matériel protégé par le droit d'auteur. Ainsi, les informations intégrées dans le contenu concernent généralement le client, telles que son numéro d'identification [36].

2.6.3. L'authentification des données

Permet de savoir si l'image a subi des malversations et si tel est le cas, certaines informations pointant la localisation des dégradations peuvent être extraites.

Comme son nom l'indique, cette méthode de tatouage ne doit pas être robuste, mais bien au contraire la marque insérée doit être la plus fragile possible pour être effacée dès lors qu'une malversation apparaît [35].

2.6.4. Contrôle d'accès

Un paiement différent permet aux utilisateurs d'avoir différents privilèges (contrôle de lecture / copie) sur l'objet, il est souhaitable dans certains systèmes d'avoir un mécanisme de contrôle de copie et d'utilisation pour empêcher la copie illégale du contenu ou limiter le nombre de copies.

Un filigrane robuste peut être utilisé à cette fin [36].

2.7. Classification des algorithmes de tatouage

Cette classification est basée sur le regroupement des techniques de tatouage (Voir la figure 2.5) en fonction de degré de la robustesse contre les attaques (Robuste, fragile et semi fragile), les algorithmes de l'extraction (Aveugle, semi aveugle et non aveugle), les techniques de l'insertion (Additif ou substitutif), en fonction de préservation de l'image originale (réversible ou irréversible) [37].

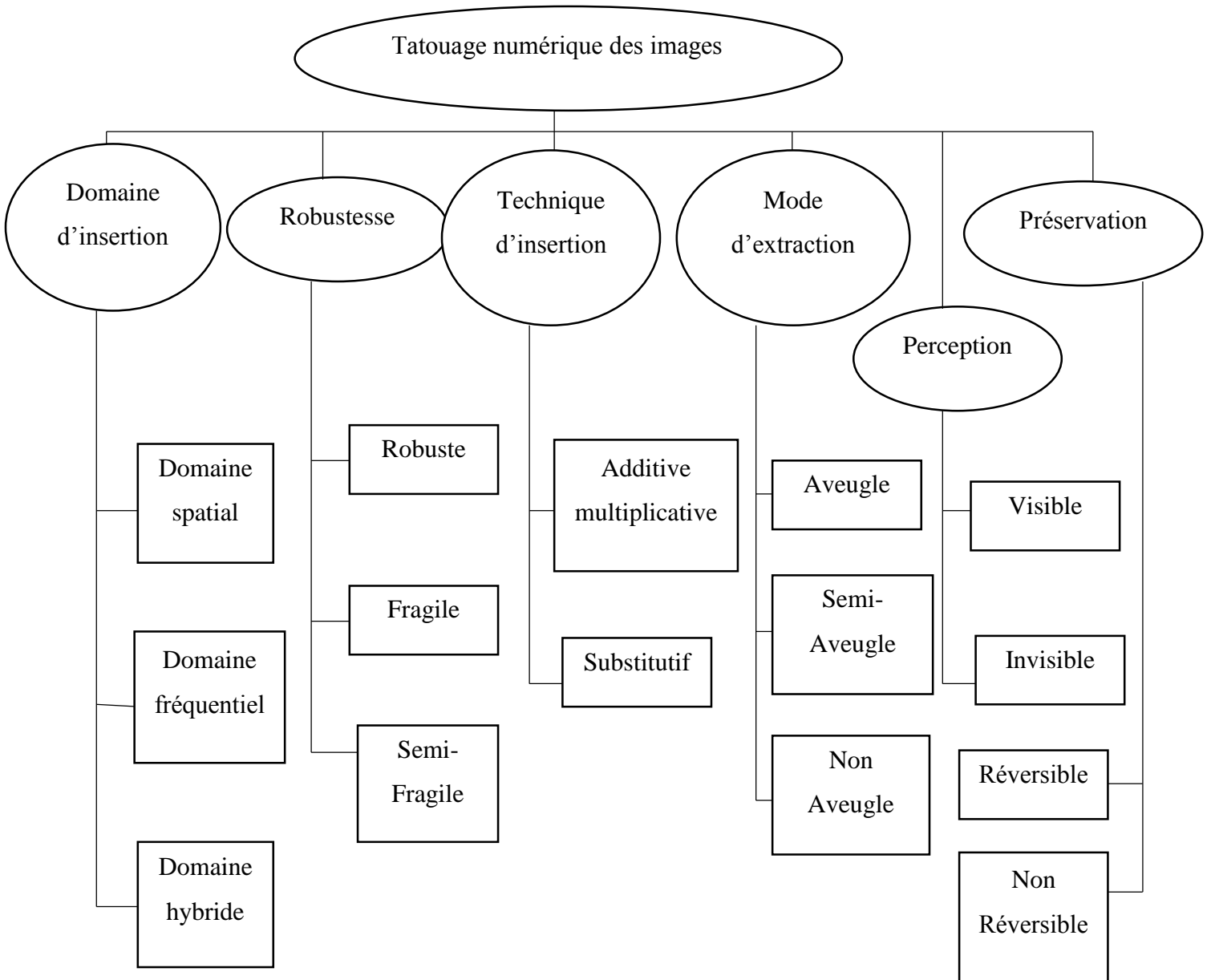


Figure 2.5 : Organigramme de la classification des algorithmes de tatouage numérique [37].

2.7.1. Classification des algorithmes de tatouage numérique selon le domaine d'insertion

Le tatouage peut être classé en deux domaines : le domaine spatial et le domaine fréquentiel.

2.7.1.1. Insertion dans le domaine spatial

L'insertion dans le domaine spatial a été logiquement la première à être envisagée. Si les méthodes utilisées sont assez simples, elles montrent souvent assez vite leurs limites [31].

- Utilisation des bits de poids faible (LSB)

L'utilisation des LSB (Least Significant Bit) est une méthode très simple, aux limites évidentes. Elle consiste à insérer des données uniquement au niveau des bits de poids faible de l'image. Pour une image codée sur 8 bits, une modification du LSB entraîne une variation du niveau de gris de 1 sur une échelle de 256. 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. Un bit de donnée est ainsi inséré par pixel de l'image [31].

- Technique de Patchwork

Consiste à choisir aléatoirement N paires de pixels selon une clé. Ensuite leurs valeurs de luminance sont modifiées, en ajoutant un seuil T pour l'une et diminuant l'autre par le même seuil. On rend ainsi les pixels sombres plus sombres et les pixels lumineux plus lumineux. La limitation de cette technique réside dans la quantité d'information à insérer qui est limitée [31].

2.7.1.2. Insertion dans le domaine fréquentiel

Le domaine fréquentiel permet d'analyser plus finement l'image et d'obtenir une représentation plus adéquate au tatouage numérique [38].

Il existe différentes méthodes qui sont utilisées dans le domaine fréquentiel tel que.

- Transformée en ondelettes discrète (DWT)

La transformée en ondelettes discrète (DWT : discrete wavelet transform) décompose une image en quatre sous-bandes, à savoir une sous-bande d'approximation LL et trois sous-bandes de détails : LH, HH et HL, correspondant, respectivement aux détails verticaux, diagonaux et horizontaux. La lettre H correspond au filtrage passe-haut et la lettre L à celui du passe-bas appliqué de façon séparable sur les lignes et les colonnes. La décomposition de la sous-bande

d'approximation LL permet d'obtenir une représentation sous forme pyramidale. Pour insérer le tatouage nous modifions les coefficients DWT dans la bande de LL :

$$LLw(i, j) = LL(i, j) + \alpha kW(i, j) \quad (1)$$

Où : $i, j = 1, \dots, n$ [39].

- Transformée en cosinus discrète (DCT)

Cette technique (DCT : discrete cosine transform) consiste à diviser l'image en un certain nombre de carrés de 8x8 pixels, puis effectuer la transformée en cosinus de ces blocs, les bits du Filigrane sont alors insérés sur les moyennes fréquences, sachant que la modification des basses fréquences modifierait trop l'image, les régions de DCT est illustrée sur la figure 2.6.

Le DCT transforme un signal ou une image du domaine spatial au domaine fréquentiel.

Le calcul de la transformée discrète en cosinus d'une image x de dimensions $N \times N$ s'effectue grâce à la formule [39] :

$$DCT(m, n) = \frac{1}{\sqrt{2N}} c(m).c(n) \sum_{k=0}^{N-1} \sum_{l=0}^{N-1} x(k, l) \cos\left(\frac{(2k+1)m\pi}{2N}\right) \cos\left(\frac{(2l+1)n\pi}{2N}\right) \quad (2)$$

$$c(m) = \begin{cases} \frac{1}{\sqrt{2}} & \text{si } i = 0 \\ 1 & \text{si } i > 0 \end{cases} \quad (3)$$

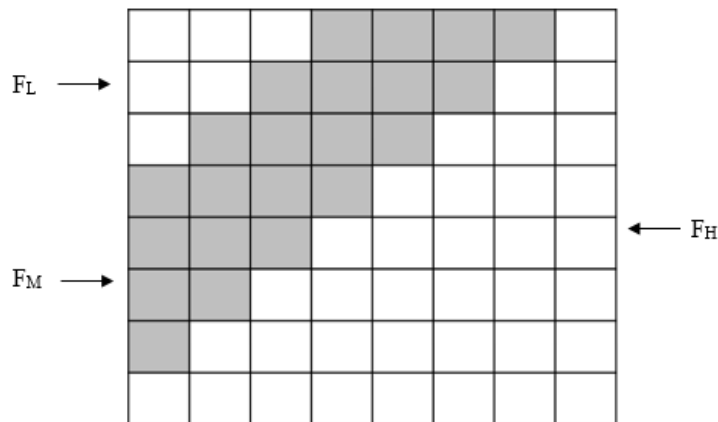


Figure 2.6 : Les régions de DCT [32].

Avec :

- DCT (m, n) : Coefficient DCT.
 - c (m) : les coefficients calculés.
 - x (k, l) : est la valeur du pixel du domaine spatial.
 - FL : band frequency low.
 - FM : band frequency middle.
 - FH : band frequency high.
- Décomposition en valeur singulière (SVD)

Le concept de Décomposition en valeur singulière (SVD : Singular value decomposition) est basé sur un théorème de l'algèbre linéaire qui décompose une matrice rectangulaire A en trois matrices : une matrice orthogonale U, une matrices diagonale S et la transposition d'une matrices orthogonal V.

La représentation mathématique d'une matrice carrée A d'ordre N après transformation SVD est donnée comme suit [32] :

$$A (m*n) = U * S * V^T = \begin{matrix} \begin{bmatrix} u_{11} & \dots & u_{1r} \\ \vdots & \ddots & \vdots \\ u_{m1} & \dots & u_{mr} \end{bmatrix} & \begin{bmatrix} s_{11} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & s_{rr} \end{bmatrix} & \begin{bmatrix} v_{11} & \dots & v_{1n} \\ \vdots & \ddots & \vdots \\ v_{r1} & \dots & v_{rn} \end{bmatrix} \end{matrix} \quad (4)$$

$m*r$ $r*r$ $r*n$

Où :

- U : matrice orthogonale.
- S : matrice diagonale.
- V^T : la transposition d'une matrice orthogonale.
- A : matrice carrée.

2.7.1.3. Algorithmes hybrides

Fridrich a proposé une telle méthode hybride, mais utilise un filigrane avec une robustesse relativement faible. Par conséquent : premièrement, pour joindre un filigrane très robuste avec un filigrane fragile pour une protection combinée des droits d'auteur, une inviolabilité et une authentification ; deuxièmement, une intégration intelligente de la partie fragile qui préserve pleinement le filigrane robuste ; troisièmement, une extension de ce schéma à un filigrane robuste et semi-fragile [40].

2.7.2. Classification des algorithmes de tatouage numérique selon la robustesse

Les algorithmes de tatouage numérique des images peuvent être classifiés selon leur robustesse. On peut distinguer dans cette classification trois catégories de tatouage numérique : robuste, fragile et semi-fragile.

2.7.2.1. Algorithmes de tatouage numérique robustes

La robustesse est une capacité de détecter le Filigrane après des opérations de modifications (traitements), par exemple, plus la qualité d'information dans l'image augmente, plus la signature sera visible ou perceptible et donc la robustesse diminue [41].

Ce type de tatouage sert à garantir la protection des droits d'auteurs [37].

2.7.2.2. Algorithmes de tatouage numérique fragiles

Ce schéma de tatouage est utilisé pour réserver l'authentification et il est robuste à certains types de manipulations ou dégradations comme la compression avec perte, plusieurs méthodes et travaux reposent sur ce schéma ont été réalisés [42].

2.7.2.3. Algorithmes de tatouage numérique semi-fragiles

Le tatouage semi-fragile vise à résister à certains traitements du document, tant que son contenu sémantique n'est pas altéré. On distingue les attaques légitimes (ex : compression JPEG), auxquelles la méthode est robuste, des attaques illégitimes auxquelles elle est fragile [42].

2.7.3. Classification des algorithmes de tatouage numérique selon la technique d'insertion

On distingue les techniques de tatouage selon la façon de l'insertion de la signature dans un document hôte, soit de façon additive connue par les techniques additives, ou de façon substitutive connue par les techniques substitutives.

2.7.3.1. Insertion additive

Les schémas additifs permettent d'ajouter le Filigrane ou la signature à l'image hôte elle-même ou aux coefficients de transformées de celle-ci issue de transformation selon le type d'espace de transformation utilisé, la marque est générée à l'aide d'une clé k de façon pseudo aléatoire comme dans le cas de l'étalement de spectre [37].

2.7.3.2. Insertion par substitution

La marque n'est pas ajoutée mais substituée à des composants de l'image (pixel, coefficient de transformés...) sélectionnés à l'aide une clé secrète. La signature est insérée selon des contraintes appliquées sur les composants de l'image. Dans la phase d'extraction, on calcule le degré de similitude entre le Filigrane retrouvée à partir des composants de l'image tatouée et la marque originale [37].

2.7.4. Classification des algorithmes de tatouage numérique selon le mode d'extraction

On peut aussi classifier les techniques de tatouage selon l'algorithme de l'extraction :

2.7.4.1. Le tatouage Aveugle

C'est-à-dire que pour extraire la marque, n'utilise pas l'image originale [32].

C'est utilisable dans tous les cas de tatouage nécessitant une clef privée.

2.7.4.2. Le tatouage Semi-Aveugle

Pour l'extraction n'a pas besoin forcement de l'utilisation l'image originale mais seulement de quelques caractéristiques de celle-ci.

2.7.4.3. Le tatouage Non Aveugle

C'est-à-dire l'utilisation de l'image originale et la clé sont nécessaires.

2.7.5. Classification des algorithmes de tatouage numérique selon la perception de la marque

Selon la perception de Filigrane on peut classer en deux techniques visible et invisible.

2.7.5.1. Le tatouage invisible

Un exemple de ce scénario est l'enregistrement numérique des images d'événements d'actualité ou historiques. Les images doivent être filigranées lors de la capture afin que les services de nouvelles puissent être sûrs qu'aucune image n'a été modifiée. La distribution illimitée de copies des images est beaucoup moins un problème ici que la vérification de l'origine et du contenu d'une image. Il s'agit d'une question très critique dans la protection des images historiques et des images utilisées par les tribunaux comme preuves [44].

2.7.5.2. Le tatouage visible

Masquage d'un document à l'aide d'une ou plusieurs marques visibles qui sont effaçables correctement que si on possède une clé secrète.

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

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

2.7.6.1. Le tatouage réversible

Le tatouage réversible est utilisé pour assurer l'intégrité de l'image, mais il a l'avantage de retrouver l'image originale. Cette réversibilité est très demandée pour tous les secteurs d'imagerie sensible, surtout pour le secteur médical [45].

2.7.6.2. Le tatouage non réversible

Dans le tatouage non réversible, il n'existe aucun moyen de retrouver l'image originale à partir de l'image tatouée [42].

2.8. Les attaques

Une attaque est tout traitement sur l'image, il existe de nombreux types d'attaques qui peuvent être utilisées. Les attaques basées sur la suppression, la modification du format de compression, l'ajout de bruit ou diverses transformations pouvant être apportées à l'image.

2.8.1. Attaques de traitement d'image

S'inspirent du domaine de traitement d'image qui tente d'évaluer ou d'estimer l'image originale à partir de l'image tatouée en appliquant plusieurs traitements (compression, lissage, conversion analogique numérique, addition de bruit, filtrage...) [37].

2.8.2. Attaques géométriques

Toutes les manipulations qui affectent la géométrie de l'image (déformer ou déplacer l'image tatouée) telles que le retournement, la rotation, le recadrage, etc. doivent être détectables.

Une attaque de recadrage depuis le côté droit et le bas de l'image est un exemple de cette attaque [36].

2.8.3. Attaques cryptographiques

Les attaques cryptographiques traitent de la fissuration de la sécurité. Exemple de ce type d'attaque est l'attaque oracle. Dans l'attaque d'Oracle, un objet non filigrané est créé lorsqu'un dispositif de détection de filigrane public est disponible. Ces attaques sont similaires aux attaques utilisées en cryptographie [36].

2.8.4. Attaques de protocole

Les attaques de protocole ne visent ni à détruire les informations embarquées ni à désactiver la détection des informations embarquées (désactivation du filigrane). Plutôt que cela, ils profitent des déficits sémantiques de la mise en œuvre du filigrane. Par conséquent, un filigrane

robuste ne doit pas être inversible ou être copié. Une attaque de copie, par exemple, viserait à copier un filigrane d'un média dans un autre sans connaître la clé secrète [36].

2.9. Conclusion

Dans ce chapitre nous avons présentés un aperçu de l'état de l'art de tatouage numérique et certains algorithmes de tatouage des images existants. Après avoir présenté la classification des schémas globale de tatouage numérique des images, nous avons présenté la classification selon le domaine d'insertion, la robustesse, selon leurs techniques, la classification selon le mode d'extraction de la marque, la perception de la marque et la préservation de l'image originale. Dans le prochain chapitre, nous allons expliquer les techniques de tatouage des images médicales existantes.

CHAPITRE 03 :

TECHNIQUES DE TATOUAGE BASEES SUR DWT

3.1. Introduction

Selon ce que nous avons mentionné dans le chapitre précédent, il existe de nombreuses techniques utilisées dans le tatouage et elles diffèrent selon leurs classifications.

Dans ce chapitre, nous avons choisi les techniques utilisées en fonction du domaine fréquentiel et nous discuterons des travaux qui existent sur le tatouage, toutes les techniques que nous avons adoptées se basent sur la technique DWT (Discret Wavelet Transform), sont des algorithmes basés sur l'insertion de la signature non pas directement dans l'image mais dans les coefficients de transformés de celle-ci, ce domaine est réalisé après une décomposition par transformés. Et nous testerons ces techniques sur des images médicales.

3.2. Technique DWT

Le DWT (Discret Wavelet Transform) est transformé l'image en quatre parties : une partie est la fréquence inférieure de l'image d'origine, la partie supérieure droite contient les détails horizontaux de l'image, la partie inférieure gauche contient les détails verticaux de l'image originale et la partie inférieure droite contient une fréquence plus élevée de l'image originale. Les coefficients de fréquence inférieure sont plus robustes pour incorporer un tatouage car contient plus d'informations sur l'image originale, la reconstruction de l'image originale à partir d'une image décomposée est réalisée par IDWT (Inverse Discret Wavelet Transform).

La figure 3.9 illustre un modèle de décomposition DWT en 2 niveaux.

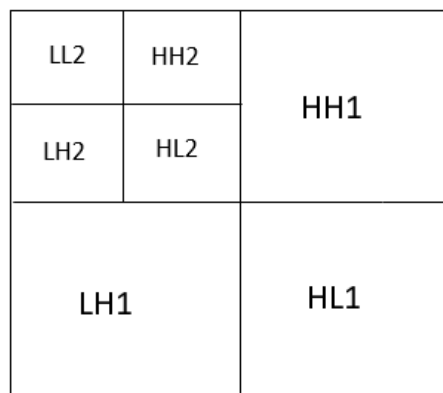


Figure 3.1 : Modèle de décomposition DWT en 2 niveaux [46].

Anuradha et R. Pratap Singh [46] ont proposé une approche de filigrane basée sur des ondelettes est proposée dans laquelle un filigrane visuellement reconnaissable est ajouté aux coefficients d'ondelettes d'une image. Le filigrane extrait est visuellement reconnaissable pour revendiquer la propriété. Le filigrane intégré est difficile à détecter par la perception visuelle humaine. Dans le procédé proposé des pixels de filigrane sont noyés dans des coefficients d'ondelettes correspondant aux points situés dans un voisinage d'entropie maximale.

3.2.1. Algorithmes pour l'intégration de Filigrane

1. Appliquer le DWT Haar transform et décomposer l'image originale et la Filigrane.
2. Après la décomposition en ondelette, la composante basse fréquence est équivalente ou similaire à l'image d'origine donc la bande à ajouter à la robustesse du Filigrane.
3. Sélectionner le coefficient ordonné de 1 à N pour obtenir le coefficient N, la formule d'insertion de la marque est suivante :

$$C_w(i) = Y_0(i) + \alpha_1 W(i) \quad (5)$$

Où :

- α est appelé intensité d'incorporation.
4. Après cela, appliquer la transformée en ondelettes inverse IDWT à l'image pour trouver l'image tatouée.

La figure 3.2 illustre le schéma explicatif pour l'insertion par la technique DWT.

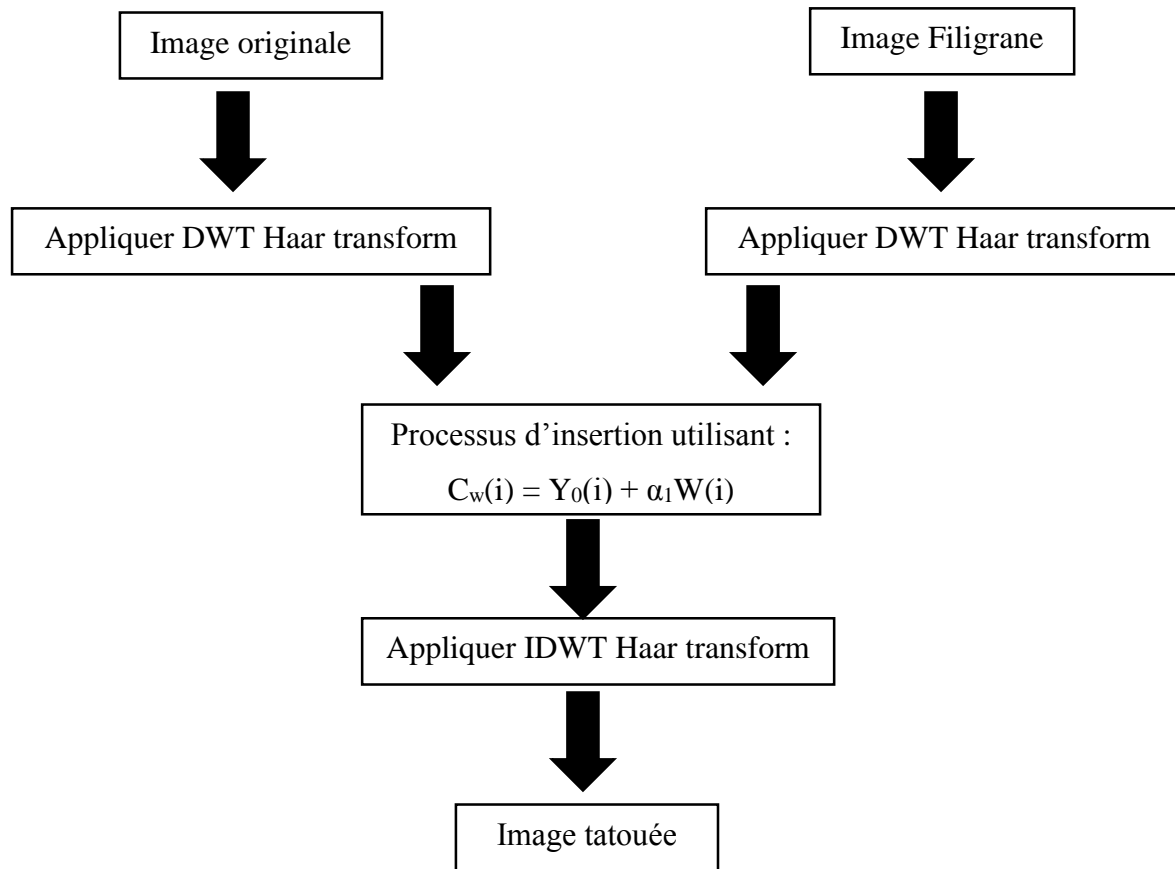


Figure 3.2 : Schéma explicatif pour l'insertion par la technique DWT [46].

3.2.2. Algorithmes pour l'extraction de Filigrane

1. Le processus d'algorithme d'extraction est l'inverse du processus d'insertion. L'opération de séparation des canaux est appliquée sur l'image couleur tatouée pour générer ses sous-images, puis une transformée en ondelettes discrète à 2 niveaux est appliquée sur les sous-images pour générer les coefficients approximatifs et les coefficients de détail.
2. Après cela, l'opération similaire est appliquée à l'image d'origine et génère à la fois les coefficients (approximatifs et de détail). Avec les deux coefficients de l'image tatouée et de l'image originale, nous pourrions extraire les données de la Filigrane via l'algorithme d'extraction de Filigrane, en utilisant la formule suivante :

$$W(i) = (Y_w(i) + Y_0(i)) / \alpha \quad (6)$$

3. Après cette exécution, la transformée en ondelettes discrètes à 2 niveaux inverses est appliquée aux données de la marque pour générer trois images de filigrane extraites.

La figure 3.3 illustre le schéma explicatif pour l'extraction par la technique DWT.

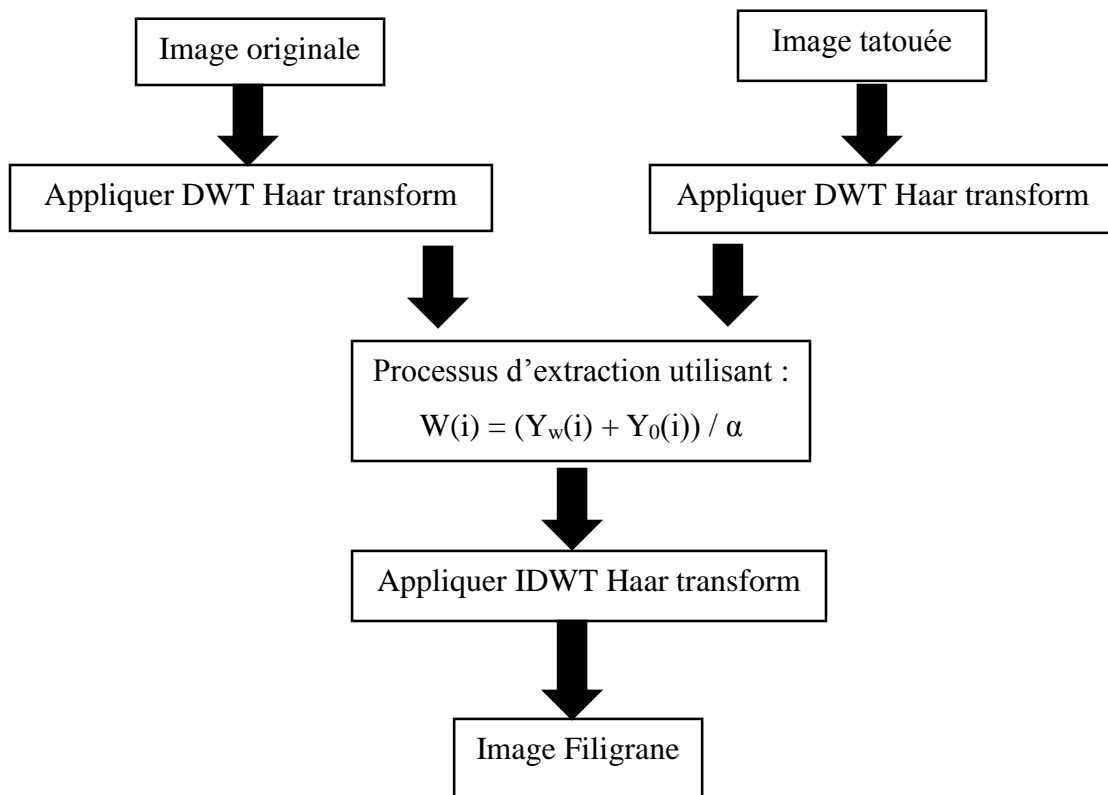


Figure 3.3 : Schéma explicatif pour l'extraction par la technique DWT [46].

3.3. Technique DWT-DCT

Ali Al-Haj [47] a créé une autre technique qui est une combinaison entre la DWT (Discrete wavelet transform) et DCT (Discrete cosine transform). Les conversions DCT et DWT (algorithme combiné DCT-DWT) sont largement utilisées dans les applications de traitement du signal numérique.

Comment sont-ils liés à la mise en œuvre du tatouage numérique ?

3.3.1. Algorithme d'intégration

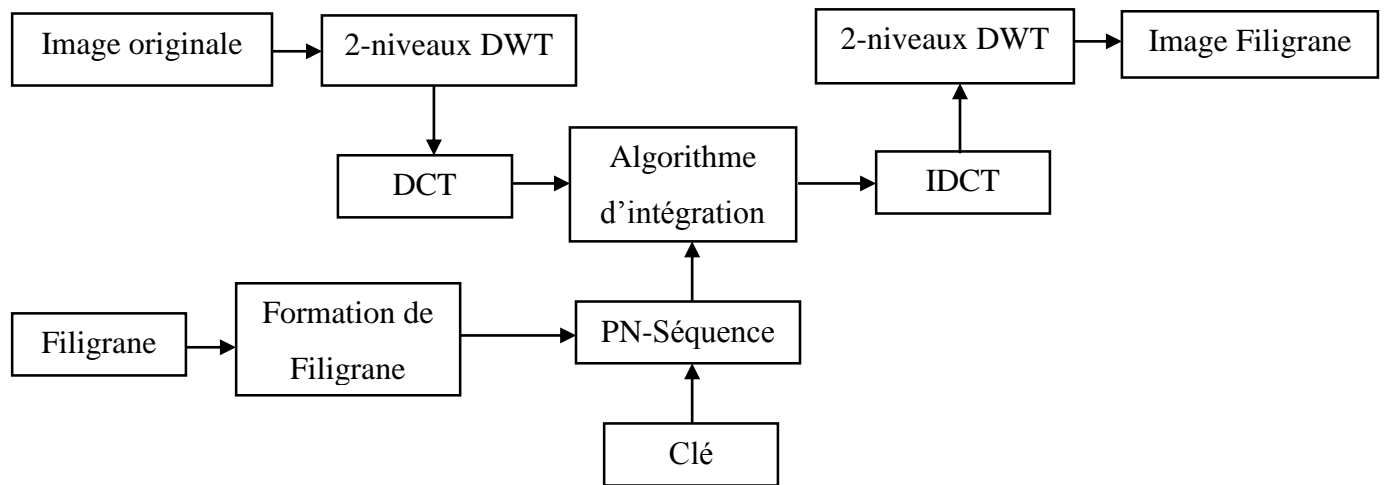


Figure 3.4 : Procédure combinée d'intégration du filigrane DWT-DCT [47].

La procédure d'intégration du filigrane est illustrée sur la figure 3.4, suivie d'une explication détaillée.

1. Appliquer DWT pour décomposer l'image hôte de couverture en quatre sous-bandes multi-résolution non superposées : LL1, HL1, LH1 et HH1.

Où :

- LL : Low Low frequency band.
- HL : High Low frequency band.
- LH : Low High frequency band.
- HH : High High frequency band.

2. Appliquez à nouveau DWT à la sous-bande HL1 pour obtenir quatre sous-bandes plus petites et choisissez la sous-bande HL2 comme indiqué sur la Figure. 3.5. a. Ou, DWT est appliquée à la sous-bande HH1 pour obtenir quatre sous-bandes plus petites et choisissez la sous-bande HH2 comme indiqué sur la Figure. 3.5.b.

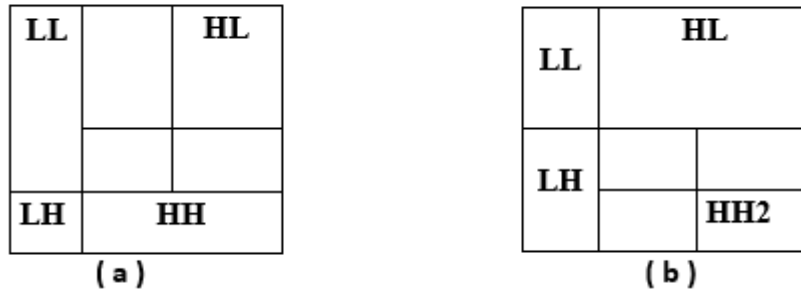


Figure 3.5 : Sous-bandes DWT multi-résolution de l'image originale [47].

3. La sous-bande HL2 (ou HH2) est divisé en blocs de 4 x 4.
4. L'application de DCT à chaque bloc dans la sous-bande choisie (HL2 ou HH2).
5. Reformuler l'image du filigrane à niveaux de gris en un vecteur des zéros et des uns.
6. Génération de deux séquences pseudo-aléatoires non corrélées. Une séquence est utilisée pour incorporer le bit de filigrane 0 (PN_0) et l'autre séquence est poursuivie pour incorporer le bit de filigrane 1 (PN_1).

Le nombre d'éléments dans chacune des deux séquences pseudo-aléatoires doit être égal au nombre d'éléments de bande médiane des sous-bandes DWT transformées en DCT.

7. Incorporer les deux séquences pseudo-aléatoires, PN_0 et PN_1, avec un facteur de gain α , dans les blocs 4x4 transformés DCT des sous-bandes DWT sélectionnées de l'image hôte.

L'incorporation n'est pas appliquée à tous les coefficients du bloc DCT, mais uniquement aux coefficients DCT de bande médiane. Si nous donnons X comme matrice des coefficients de bande médiane du bloc transformé DCT, alors l'incorporation se fait comme suit : Si le bit de filigrane est 0 alors :

$$X' = X + \alpha * PN_0 \quad (7)$$

Sinon, si le bit de filigrane est 1 alors :

$$X' = X + \alpha * PN_1 \quad (8)$$

Où :

- α est le facteur de gain.
 - PN_0 : incorporer le bit de filigrane 0.
 - PN_1 : incorporer le bit de filigrane 1.
 - X : matrice des coefficients de bande médiane du bloc transformé DCT.
8. L'application de DCT inverse (IDCT : Inverse Discret cosine transform) à chaque bloc après que ses coefficients de bande médiane ont été modifiés pour incorporer les bits de filigrane comme décrit à l'étape précédente.
 9. L'application de DWT inverse (IDWT) sur l'image transformée DWT, y compris la sous-bande modifiée, pour produire l'image hôte en filigrane.

3.3.2. Algorithme d'extraction

Algorithme de filigrane, et donc l'image hôte d'origine n'est pas nécessaire pour extraire le filigrane.

1. L'application de DWT pour décomposer l'image filigranée en quatre sous-bandes multi-résolution sans chevauchement : LL1, HL1, LH1 et HH1.
2. L'application de DWT à HL1 pour obtenir quatre sous-bandes plus petites et choisissez la sous-bande HL2, comme indiqué sur la Figure. 3.5. a. Ou, DWT est appliquée à la sous-bande HH1 pour obtenir quatre sous-bandes plus petites et choisissez la sous-bande HH2, comme indiqué sur la Figure. 3.5. b.
3. La sous-interdiction HL2 (ou HH2) est divisé en 4 x 4 blocs.
4. L'application de DCT à chaque bloc dans la sous-bande choisie (HL2 ou HH2) et L'extraction des coefficients de bande médiane de chaque bloc transformé DCT.
5. Régénération des deux séquences pseudo-aléatoires (PN_0 et PN_1) en utilisant la même graine utilisée dans la procédure d'intégration du filigrane.

6. Pour chaque bloc de la sous-bande HL2 (ou HH2), la corrélation est calculée entre les coefficients de bande médiane et les deux séquences pseudo-aléatoires générées (PN_0 et PN_1).

Si la corrélation avec PN_0 était supérieure à la corrélation avec PN_1, alors le bit de filigrane extrait est considéré comme 0, sinon le filigrane extrait est considéré comme 1.

7. Le filigrane est reconstruit à l'aide des bits de filigrane extraits et calculez la similitude entre les filigranes originaux et extraits.

La figure 3.6 illustre la procédure d'extraction de filigrane DWT-DCT combinée.

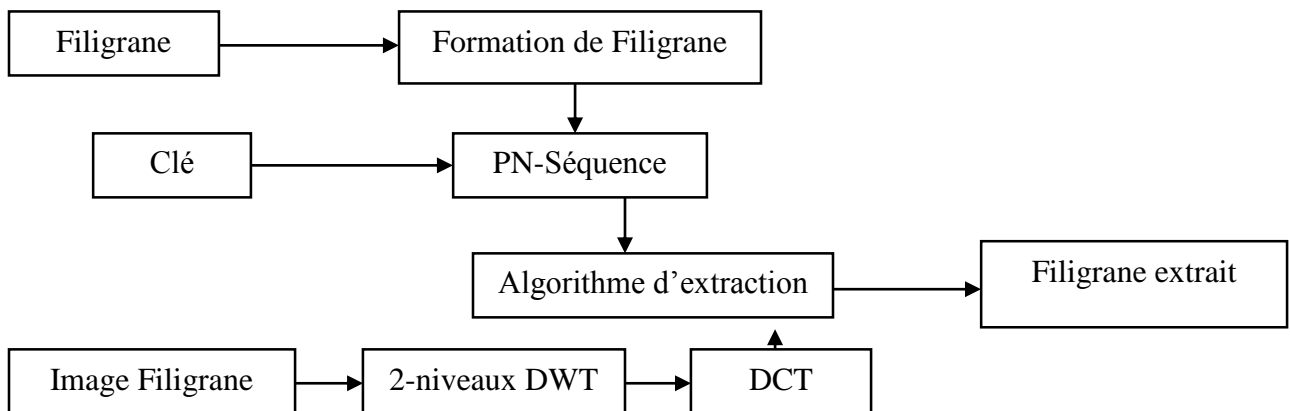


Figure 3.6 : Procédure d'extraction de filigrane DWT-DCT combinée [47].

3.4. Technique DWT-SVD

Anumol Joseph et k. Anusudha [48] proposer un concept appeler DWT-SVD (DWT : Discrete wavelet transform, SVD : Singular value decomposition). Le système proposé est basé sur la technique DWT-SVD. L'image hôte et les images de filigrane sont décomposées par DWT en utilisant l'ondelette Haar. Une décomposition à deux niveaux a été appliquée sur l'image hôte et une décomposition à un niveau sur les images en filigrane. Les images en filigrane sont intégrées aux bandes HL et LH de l'image hôte en modifiant les valeurs singulières de l'image hôte. La figure 3.7 montre la méthode proposée.

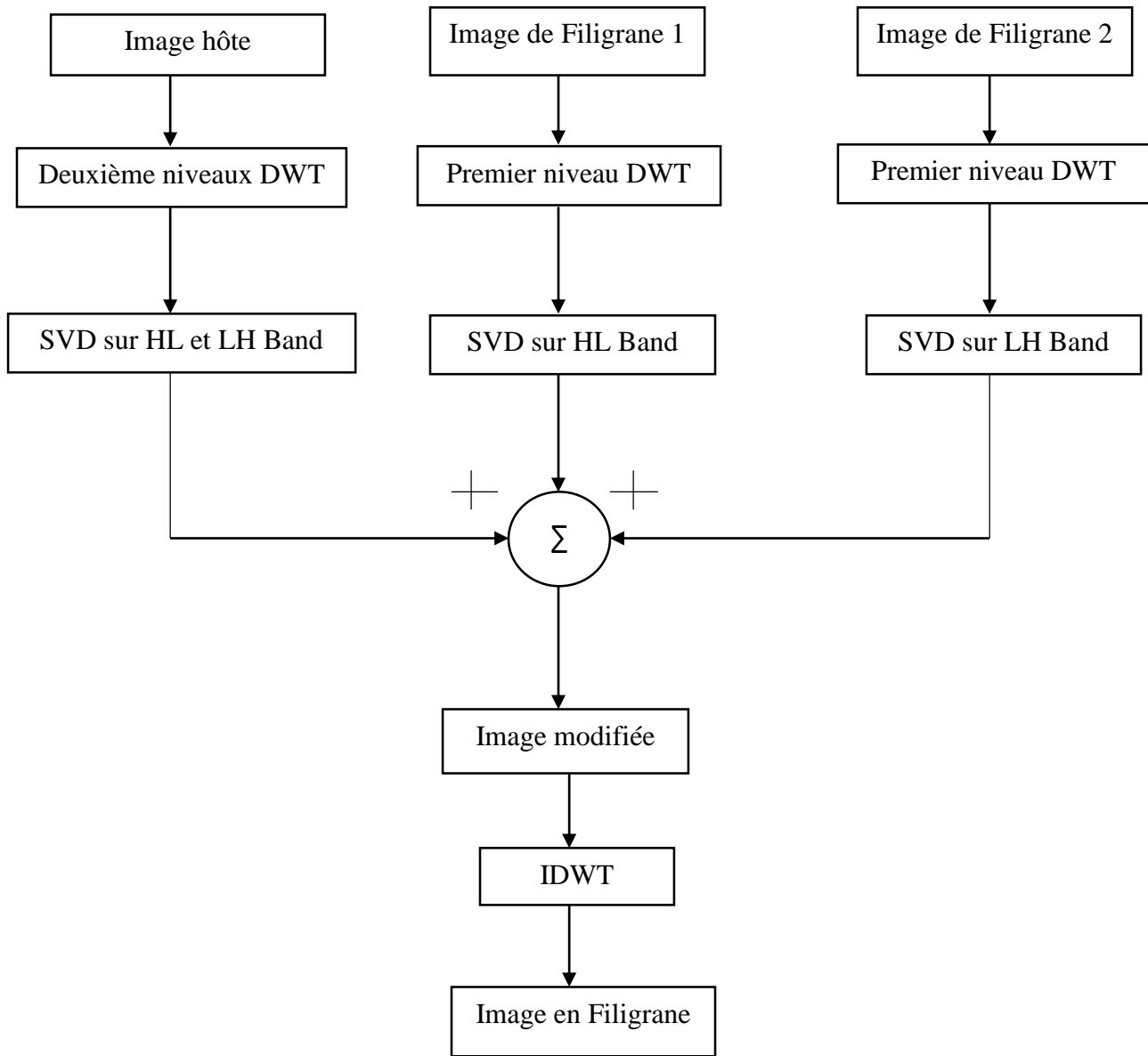


Figure 3.7 : Système proposé [48].

3.4.1. Algorithme-Intégration d'un Filigrane

1. L'application de DWT à 2 niveaux sur l'image hôte.
2. Une décomposition en valeurs singulières est effectuée dans la bande HL et LH de l'image hôte.

$$H_1 = P_{H1} * Q_{H1} * R_{H1}^T \quad (9)$$

$$H_1 = P_{H2} * Q_{H2} * R_{H2}^T \quad (10)$$

Où :

- H : image hôte.
 - P*Q*R : une matrice réelle générale d'ordre m x n et sa SVD est la factorisation.
 - P et R : des matrices orthogonales (unitaires) et T est le Transpose.
 - Q : diag (F₁, F₂... F_r) qu'est F_i Avec i = 1 à r et r = min (m, n).
3. Une transformée en ondelettes de Haar de premier niveau est appliqué sur les images du filigrane.
 4. Une décomposition en valeurs singulières est effectuée sur la bande HL de l'image en filigrane 1.

$$W_1 = P_{W1} * Q_{W1} * R_{W1}^T \quad (11)$$

Où :

- W : watermark.
5. Une décomposition en valeurs singulières est effectuée sur la bande LH de l'image de filigrane 2.

$$W_2 = P_{W2} * Q_{W2} * R_{W2}^T \quad (12)$$

6. La valeur singulière de l'image hôte est modifié avec la valeur singulière des images de filigrane.

$$Q_{WM} = Q_H + \alpha Q_w \quad (13)$$

Où :

- w_M est Watermark.

7. Obtenir l'image modifiée.

$$I = P_H * Q_{WM} * R_H^T \quad (14)$$

Où :

➤ I est Image modifiée.

8. L'application de DWT inverse pour obtenir l'image en filigrane.

3.4.2. Algorithme-extraire le Filigrane

1. Effectuer une transformation en ondelettes à 2 niveaux sur l'image en filigrane.

2. Effectuer SVD sur les bandes HL et LH de l'image filigranée.

$$I_{WM} = P_{WM} * Q_{WM} * R_{WM}^T \quad (15)$$

3. Les valeurs singulières du filigrane secondaire peuvent être extraites comme :

$$Q_W' = (Q_{WM} - Q_H) / \alpha \quad (16)$$

4. L'image en filigrane peut être obtenue :

$$W' = P_W * Q'_W * R_W^T \quad (17)$$

3.5. Technique DWT-DCT-SVD

Nilesh Rathi et G. Holi [49] proposer un schéma de tatouage basé sur les trois techniques DWT, DCT, et SVD. L'image est décomposée en quatre bandes de fréquences (bande LL, HL, LH et HH) par DWT, prenez la bande HH de ces quatre bandes et appliquer DCT à la bande solaire choisie. On considère-le comme une matrice A, le schéma proposé remplace les valeurs singulières e la matrice A par les valeurs singulières du Filigrane.

La Figure 3.8 représente un schéma explicatif pour l'insertion de la Filigrane.

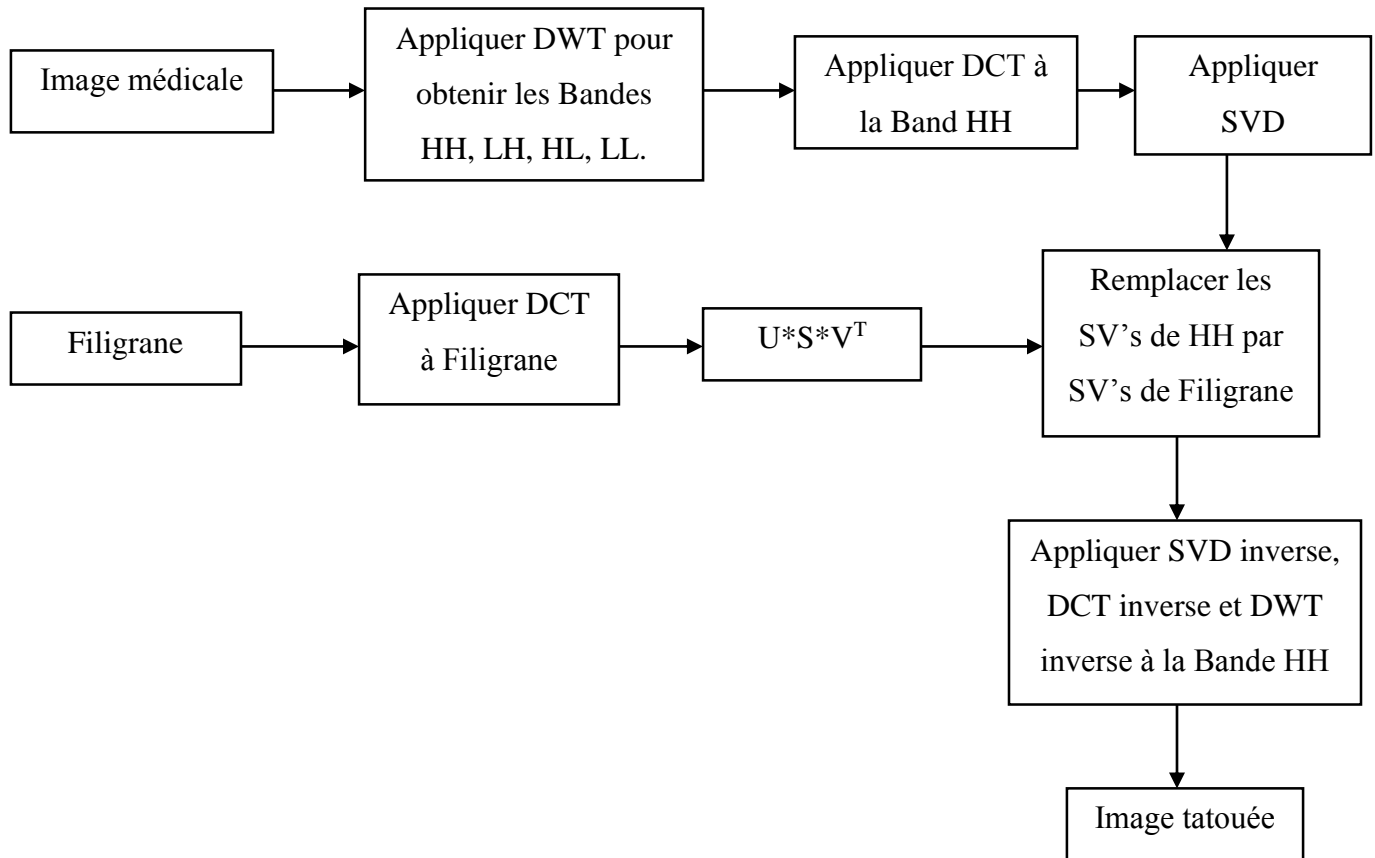


Figure 3.8 : Schéma explicatif pour l’insertion par la technique DWT-DCT-SVD [49].

3.5.1. Procédure d’intégration

1. Le watermark est décomposé en utilisant SVD :

$$W=U_w * S_w * V_w^T \quad (18)$$

Où :

- U et V sont les matrices unitaires telles que $U * U^T = I$.
- $V * V^T = I$, où, I est une matrice d'identité.
- S =diagonal matrice ((1, 1), (2, 2), (3, 3) (n, n)), avec S (1,1) est le plus grand.

2. Appliquer DWT et décomposer l’image médicale en quatre sous-bandes : LL, HL, LH, et HH.

3. Appliquer DCT à la bande HH et le décomposer en utilisant la technique SVD :

$$H=U_H *S_H *V_H^T \quad (19)$$

Où : H est band.

4. Les valeurs singulières de la bande ci-dessus sont remplacé par les valeurs singulière du Filigrane.

5. Appliquer SVD inverse et DCT inverse pour obtenir la bande HH modifiée :

$$H'= U_H *S_W *V_H^T \quad (20)$$

6. Appliquer DWT inverse pour produire l'image médicale tatouée.

7. Passer la bande HH pour extraire l'image médicale originale.

3.5.2. Procédure d'extraction

1. L'image tatouée est décomposée en quatre sous-bandes : LL, HL, LH, HH, à l'aide de DWT.
2. Appliquer DCT à la bande HH et SVD supplémentaire à celui-ci :

$$H=U_H *S_H *V_H \quad (21)$$

3. Extraire les valeurs singulières de bande HH.
4. Le watermark est construit en utilisant des valeurs singulières et des matrices orthogonales U_W et V_W obtenues en utilisant SVD du watermark original.

$$W_E=U_W *S_H *V_W^T \quad (22)$$

5. L'image médicale récupérée est construit par DCT inverse, DWT inverse en utilisant la bande HH et la bande de repos de l'image tatouée.

La figure 3.9 illustre comment obtenir l'image médicale récupérée en appliquant le DWT-DCT-SVD inverse en utilisant bande HH et le reste bandes d'images tatouée.

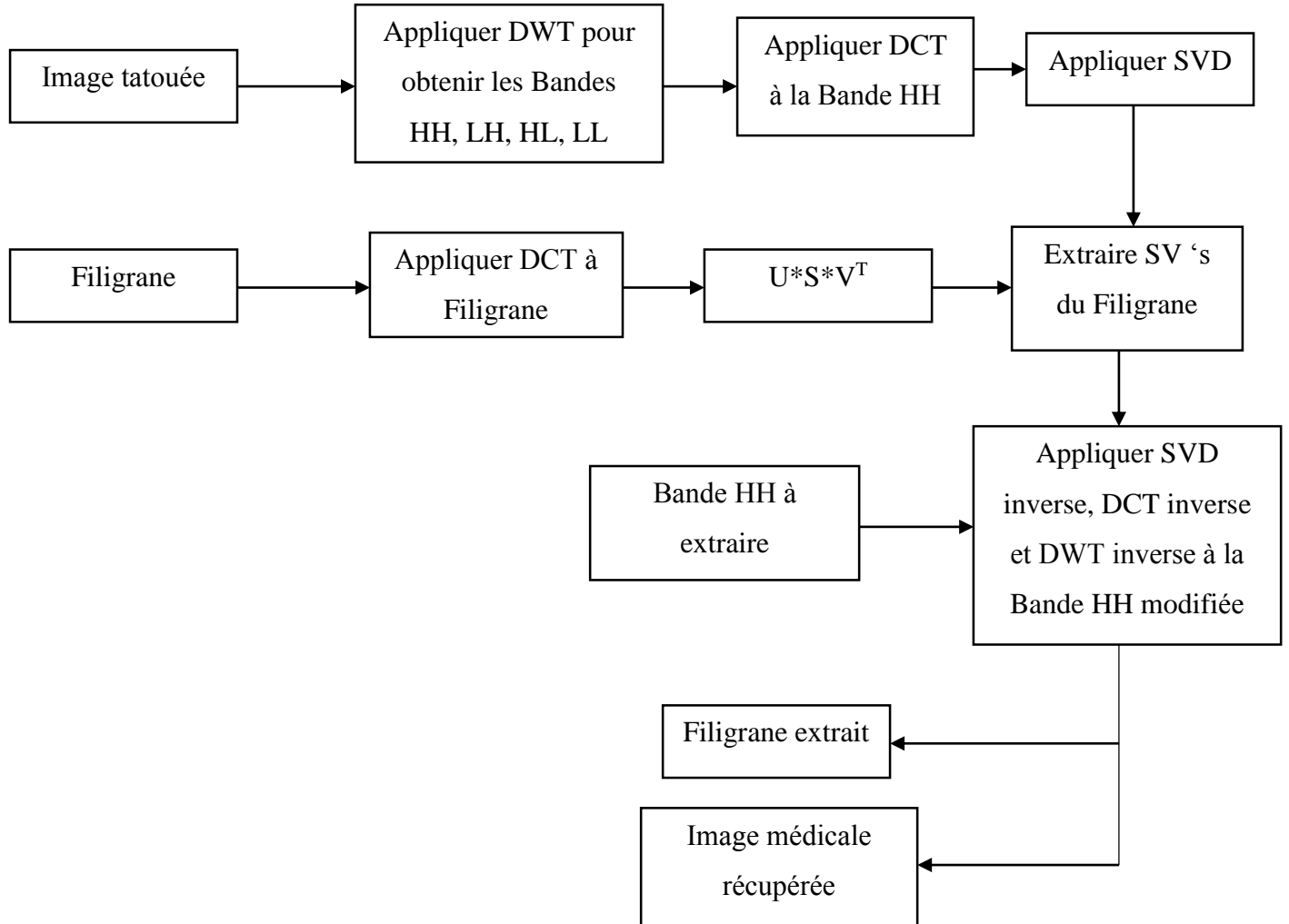


Figure 3.9 : Schéma explicatif pour l'extraction par la technique DWT-DCT-SVD [49].

3.6. Comparaison

Dans cette section, nous ferions une comparaison des œuvres que nous avons examinées dans ce chapitre. Notre comparaison basée sur les caractéristiques communes de ces œuvres.

Une technique de tatouage numérique doit satisfaire aux six propriétés suivantes :

- Imperceptibilité.
- Robustesse.
- Sécurité.

- Complexité.
- Capacité.

Les algorithmes de tatouage sont généralement évalués en fonction de deux mesures : imperceptibilité et robustesse, comme indiqué sur la Table. 3.1.

Techniques	Propriétés
La transformée en ondelettes discrète (DWT)	La technique DWT a deux propriétés haute: fidélité et robustesse, cette supériorité peut grandement contribuer à l'amélioration de l'efficacité du filigrane dans les situations qui nécessitent un traitement en temps réel tel que le filigrane d'image vidéo.
La transformée en ondelettes discrète (DWT) et Transformée en cosinus discrète (DCT)	La combinaison des deux transformations DWT-DCT a considérablement amélioré les performances de filigrane par rapport à l'approche de filigrane DWT uniquement. En conclusion, dans les applications de tatouage numérique basées sur DWT, la combinaison de transformations appropriées avec le DWT peut avoir un impact positif sur les performances du système de tatouage.
La transformée en ondelettes discrète (DWT) et Décomposition en valeur singulière	La technique DWT-SVD est robuste contre divers types d'attaques.
La transformée en ondelettes discrète (DWT) et Transformée en cosinus discrète (DCT) et Décomposition en valeur singulière (SVD)	L'algorithme de filigrane basé sur DWT-DCT-SVD est robuste par rapport à la méthode DWT-SVD. Cette méthode peut être utilisée à des fins d'authentification et de masquage des données. Les travaux futurs peuvent être étendus pour remplacer la méthode DWT par une transformée en cosinus discrète afin d'améliorer la robustesse du filigrane.

Table. 3.1: Comparaison des techniques des tatouages numériques.

3.7. Conclusion

Dans ce chapitre nous avons expliqué les techniques de tatouage d'image existants qui basée sur la technique DWT, Pour intégrer une marque (Filigrane) dans une image (image médicale et couleur). Dans le prochain chapitre, Nous allons présenter notre technique proposée.

CHAPITRE 04 :
APPROCHE PROPOSEE ET IMPLEMENTATION

4.1. Introduction

Le tatouage d'image médicale est une technique très importante pour garantir leur confidentialité lorsqu'ils sont transportés dans des réseaux non sécurisés et pour le stockage. Plusieurs algorithmes ont été proposés pour le tatouage d'image. Cependant, presque tous ces algorithmes sont moins sécurisés.

Dans ce chapitre nous proposerons un nouveau schéma améliorer à un algorithme déjà existe pour garantir la confidentialité et la fiabilité de l'image médicale.

4.2. Notre Approche

Notre approche est basée sur la technique DWT avec le chiffrement. Ce dernier a deux primitives de chiffrement : AES et la fonction de hachage (SHA-256).

Notre approche proposée, basée sur quatre étapes principales (Voir la figure 4.1) :

1. Appliquer l'algorithme AES sur le Filigrane original, qui devenir un Filigrane chiffrée.
2. Appliquer la fonction de hachage sur le Filigrane chiffrée, qui devenir un texte haché.
3. Appliquer le technique DWT sur l'image médicale et le Filigrane Originale, que devenir une image médicale tatouée.
4. Masquer le texte haché dans l'image médicale tatouée, l'image obtenue est l'image médicale tatouée finale.

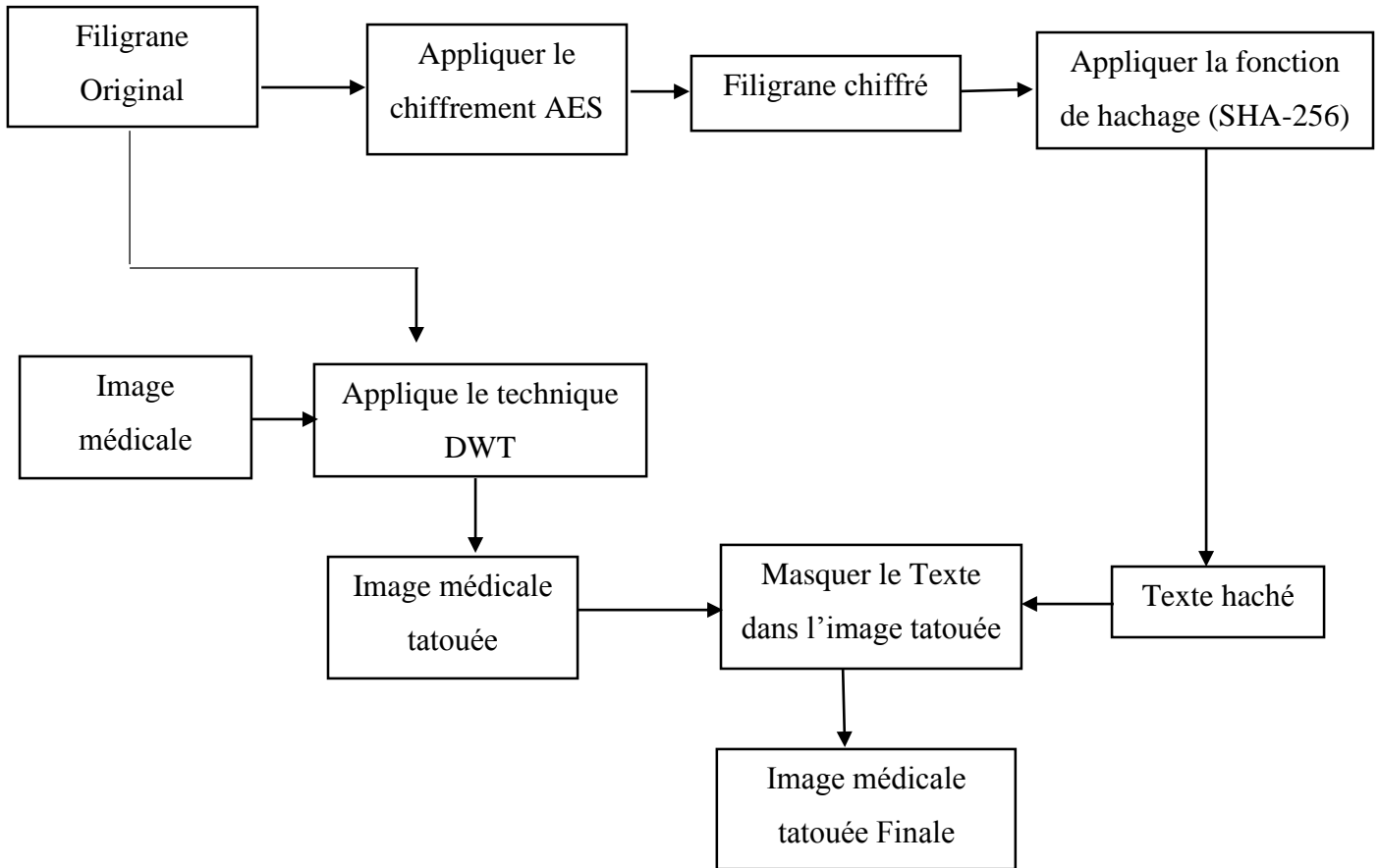


Figure 4.1 : Schéma explicatif pour intégration de Filigrane par DWT amélioré.

L'inverse de cette approche proposée se compose également de cinq étapes (Voir la figure 4.2) :

1. Après la réception nous avons extrait le texte haché de l'image médicale tatouée finale.
2. Appliquer l'inverse de technique DWT (IDWT) sur l'image médicale tatouée.
3. Appliquer la fonction de hachage sur le Filigrane chiffré.
4. Comparer le texte haché obtenu après le hachage et le texte haché qui est extrait de l'image médicale tatouée, le but principal de cette étape est de garantir la confidentialité du filigrane après l'envoi.
5. Si le hash est identique, appliquer le déchiffrement AES sur le Filigrane chiffré pour obtenir le Filigrane Original. Si non, donc les informations ne sont pas correctes.

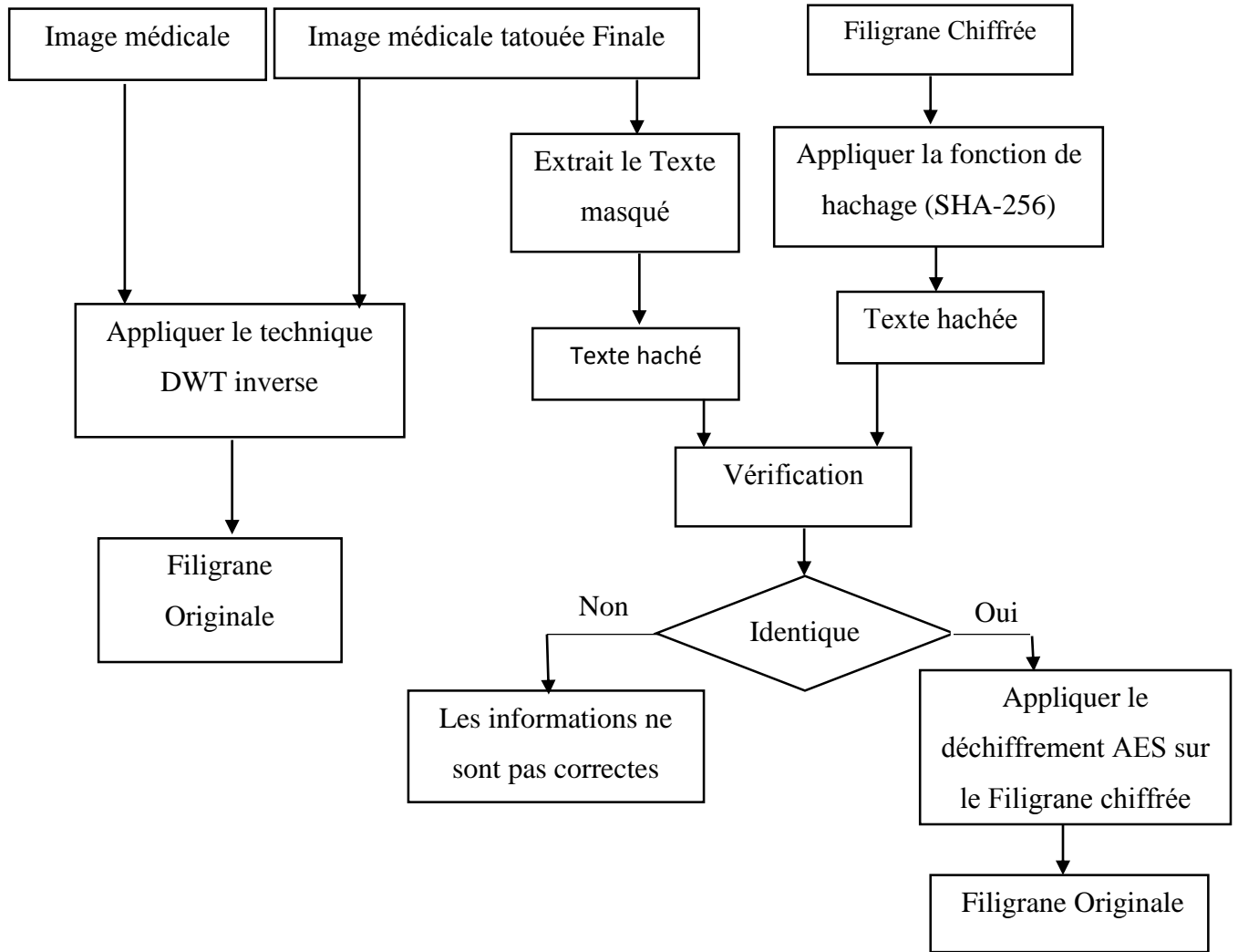


Figure 4.2 : Schéma explicatif pour extrait le Filigrane par DWT amélioré.

4.3. Implémentation

Nous avons utilisé langage Python dans l'éditeur SPYDER pour l'implémentation de notre approche.

- **PYTHON** : est le langage de programmation open source le plus employé par les informaticiens. Ce langage s'est propulsé en tête de la gestion d'infrastructure, d'analyse de données ou dans le domaine du développement de logiciels. 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 langages plus anciens. Ainsi, développer du code avec Python est plus rapide qu'avec d'autres langages [50].

- **SPYDER** : l'environnement de développement scientifique Python, est un environnement de développement intégré (IDE) gratuit qui est inclus avec Anaconda. Il comprend des fonctionnalités d'édition, de test interactif, de débogage et d'introspection [51].

4.4. Bibliothèque

- OpenCv (OpenSource Computer Vision) : Librairies plus avancée de manipulation et de traitement d'images que PIL. Est aussi utilisée dans le cadre de la reconnaissance automatique en IA [52].
- Hashlib : Est un module propre à Python implémentant une interface commune à plusieurs algorithmes de hachage sécurisés et de synthèse de messages [53].
- Numpy : Bibliothèque de bas niveau écrite en C (et FORTRAN) pour les fonctions mathématiques de haut niveau [52].
- Pywt (PyWavelets) : Est un logiciel de transformation en ondelettes open source pour Python. Il combine une interface simple de haut niveau avec des performances C et python de bas niveaux [54].
- PIL (Python Imaging Library) : Une des bibliothèques de base pour la manipulation d'images en Python. Pillow est un fork beaucoup plus récent et actif [52].
- Stegano : est un module de stéganographie pur Python. Différentes méthodes de stéganographie et de sémanalyse sont disponibles [55].

4.5. Environnement matériel

L'application a été créée depuis un PC HP 2000 Notebook PC :

- Mémoire : 4,00 GO RAM.
- Processeur : Intel ® Core™ i3 3110M CPU @ 2.40 GHZ.
- Système d'exploitation : Windows 10 Ultimate 64 bits.
- Carte Graphique : 4000 Family.

4.6. Résultats expérimentaux

Dans cette section, nous présentons les différents résultats expérimentaux de l'approche existante et notre approche.

4.6.1. Filigrane avec DWT

1. Pour l'image IRM

La Figure 4.3 présente l'IRM avant et après le DWT. (a) : image médicale de l'IRM, (b) : image de Filigrane originale, (c) : image tatouée de l'IRM par DWT, (d) : image de Filigrane extraite de l'IRM par DWT inverse.

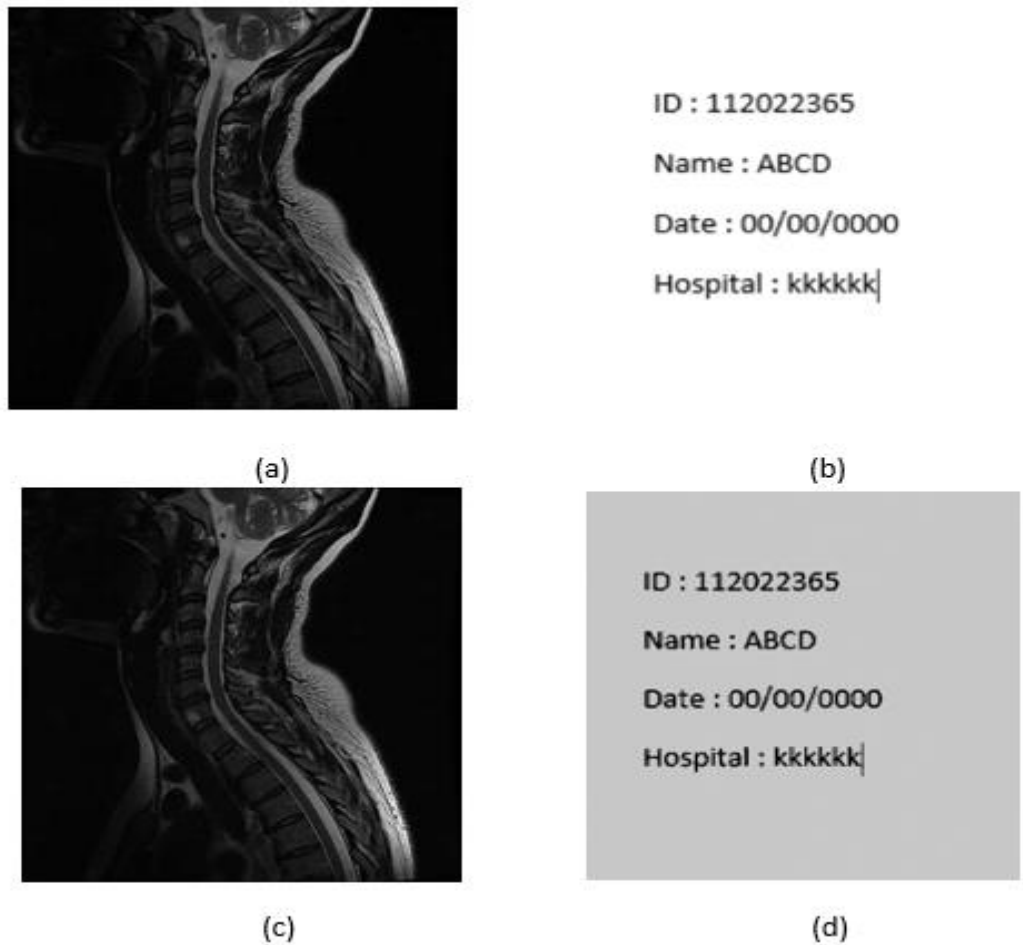


Figure 4.3: IRM avant et après le DWT.

2. Pour l'image Scanner

La Figure 4.4 présente le Scanner avant et après le DWT. (a) image médicale de Scanner, (b) : image de Filigrane originale, (c) : image tatouée de Scanner par DWT, (d) : image de Filigrane extraite de Scanner par DWT inverse.



(a)

ID : 112022365
Name : ABCD
Date : 00/00/0000
Hospital : kkkkkk|

(b)



(c)



(d)

Figure 4.4: Scanner avant et après le DWT.

- Les histogrammes

La Figure 4.5 présente les résultats obtenus de l'IRM par DWT. (a): image médicale IRM, (b) : image IRM tatouée par DWT, (c) : histogramme d'image médicale IRM, (d) : histogramme d'image IRM tatouée par DWT.

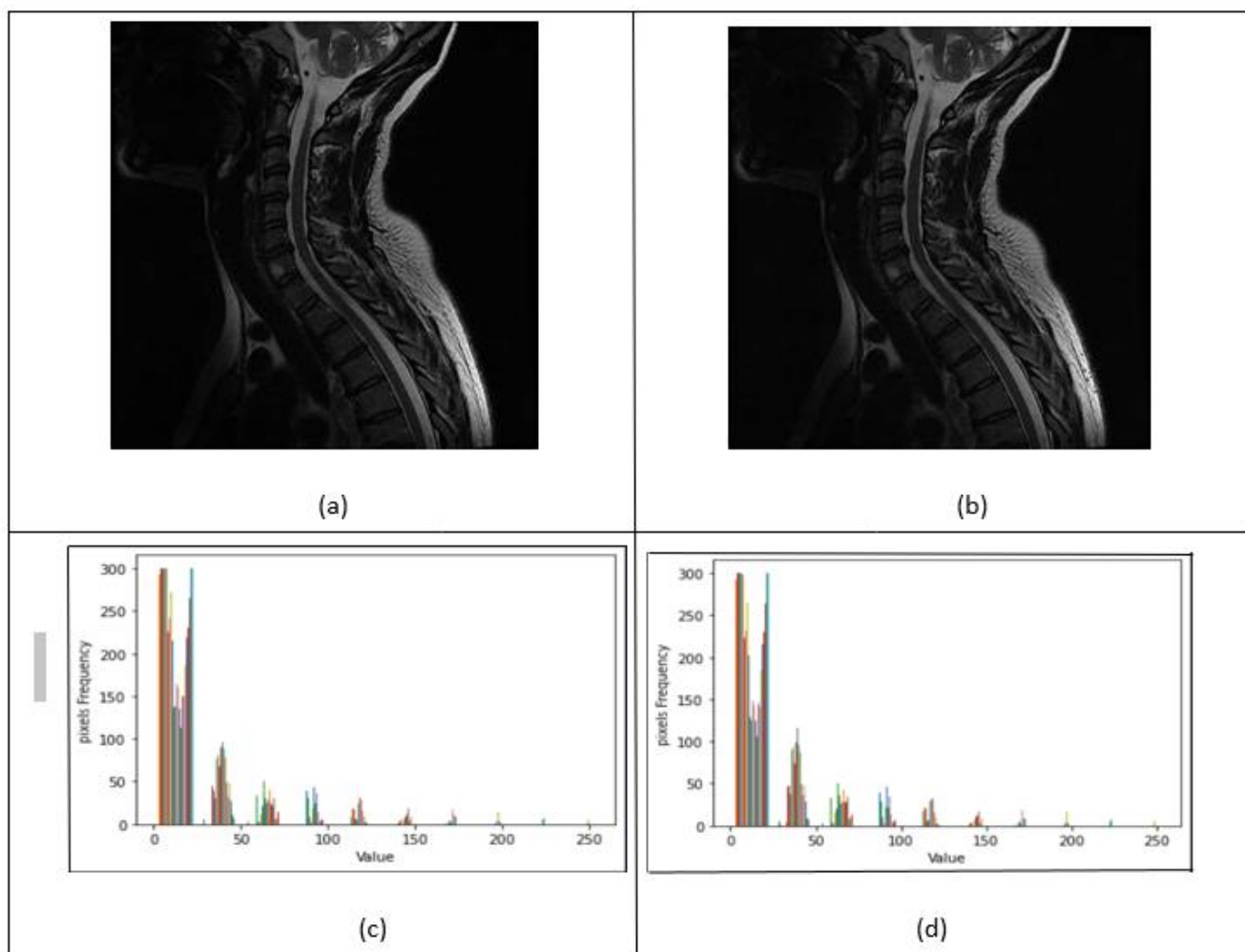


Figure 4.5: Les résultats obtenus de l'IRM par DWT.

La Figure 4.6 présente les résultats obtenus de Scanner par DWT. (a) : image médicale Scanner, (b) : image Scanner tatouée par DWT, (c) : histogramme d'image médicale Scanner, (d) : histogramme d'image Scanner tatouée par DWT.

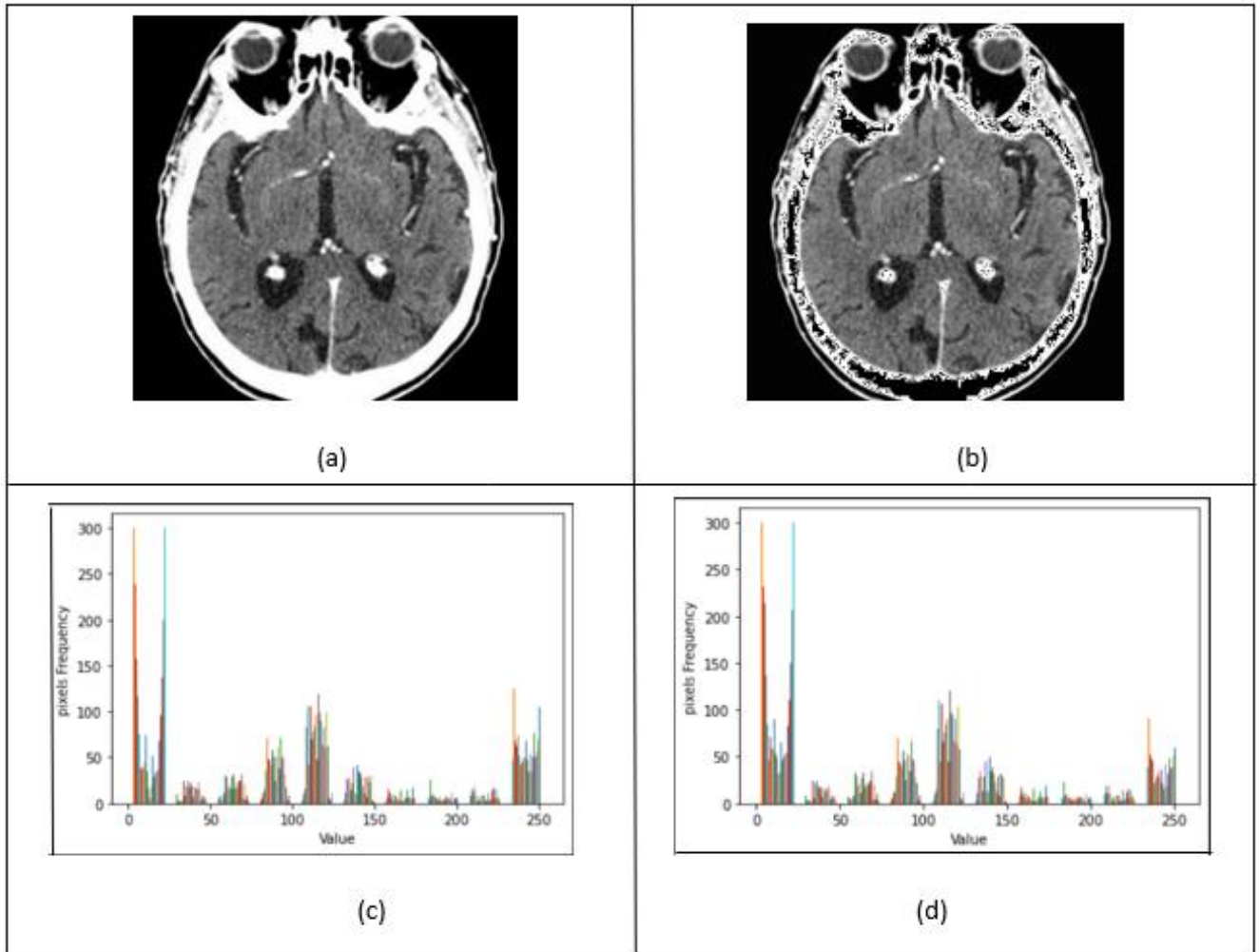


Figure 4.6: Les résultats obtenus de Scanner par DWT.

La Figure 4.7 présente les résultats obtenus de l'IRM par DWT inverse. (a): image IRM tatouée par DWT, (b) : image Filigrane extrait par DWT inverse, (c) : histogramme d'image IRM tatouée par DWT, (d) : histogramme d'image Filigrane extrait par DWT inverse.

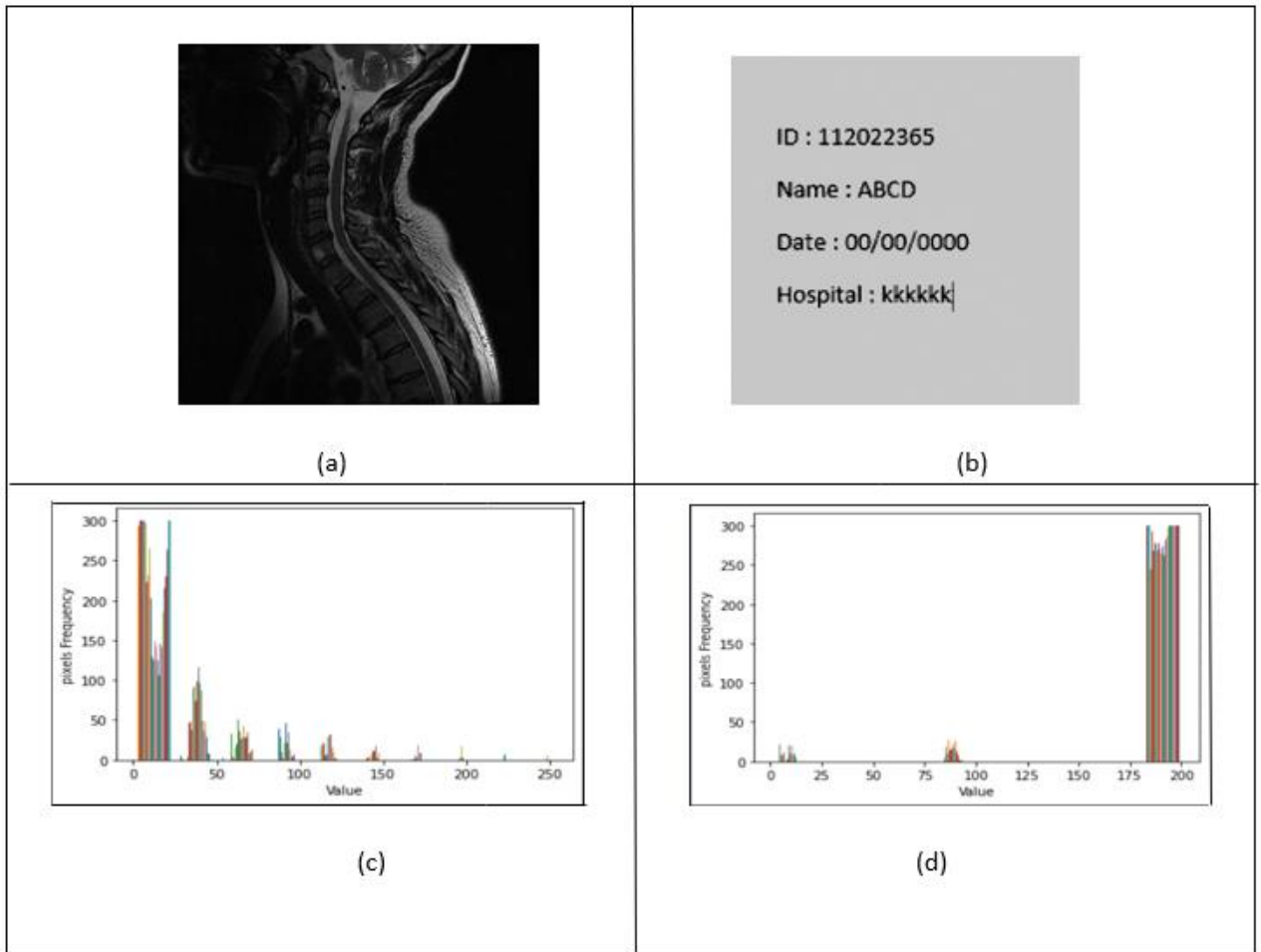


Figure 4.7: Les résultats obtenus de l'IRM par DWT inverse.

La Figure 4.8 présente les résultats obtenus de Scanner par DWT inverse. (a): image Scanner tatouée par DWT, (b) : image Filigrane extrait par DWT inverse, (c) : histogramme d'image Scanner tatouée par DWT, (d) : histogramme d'image Filigrane extrait par DWT inverse.

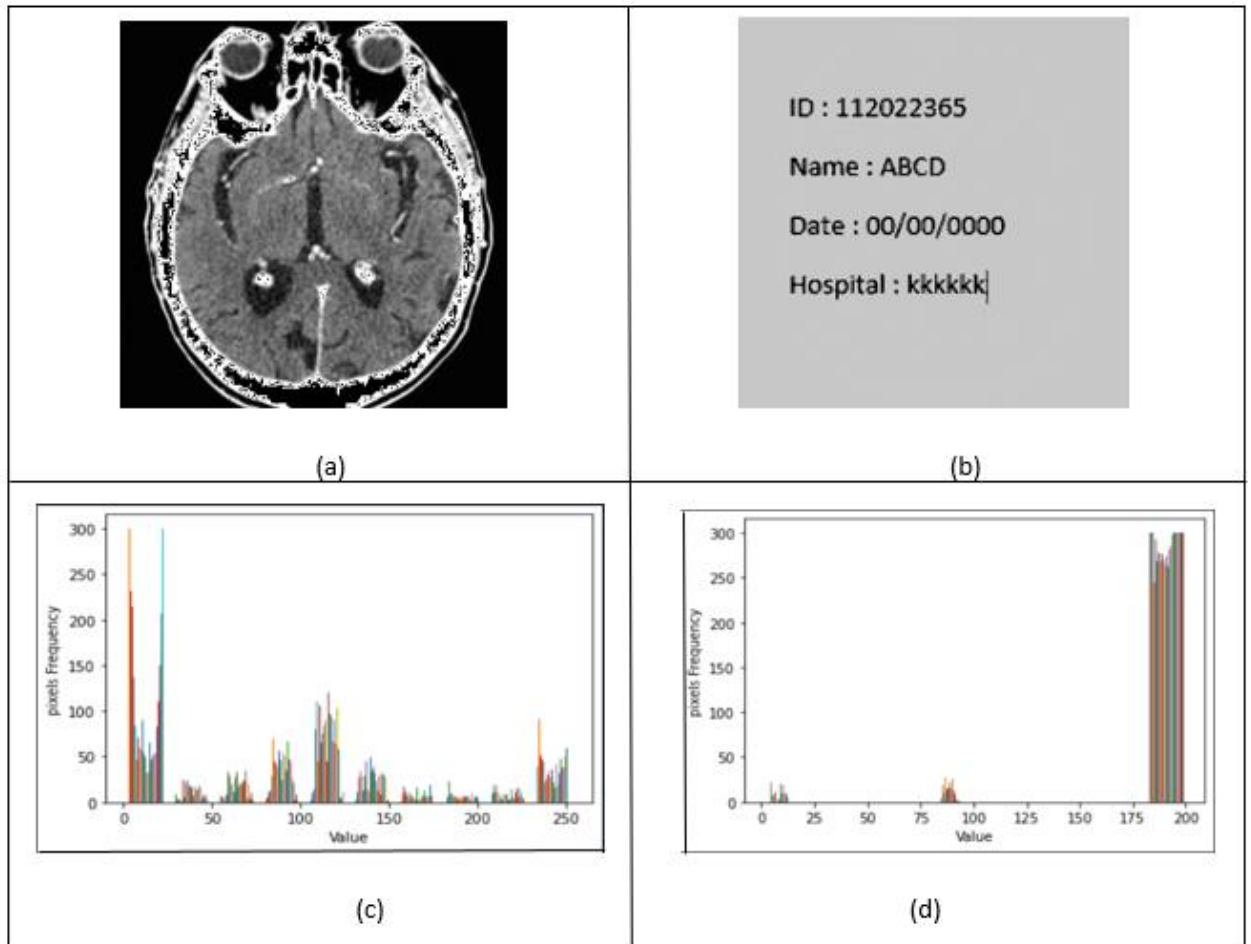


Figure 4.8: Les résultats obtenus de Scanner par DWT inverse.

4.6.2. Filigrane avec DWT amélioré

1. Pour l'image IRM

La Figure 4.9 présente IRM avant et après le DWT amélioré. (a) : image médicale de l'IRM, (b) : image de Filigrane originale, (c) : image tatouée de l'IRM par DWT amélioré, (d) : image de Filigrane extraite de l'IRM par DWT inverse amélioré.

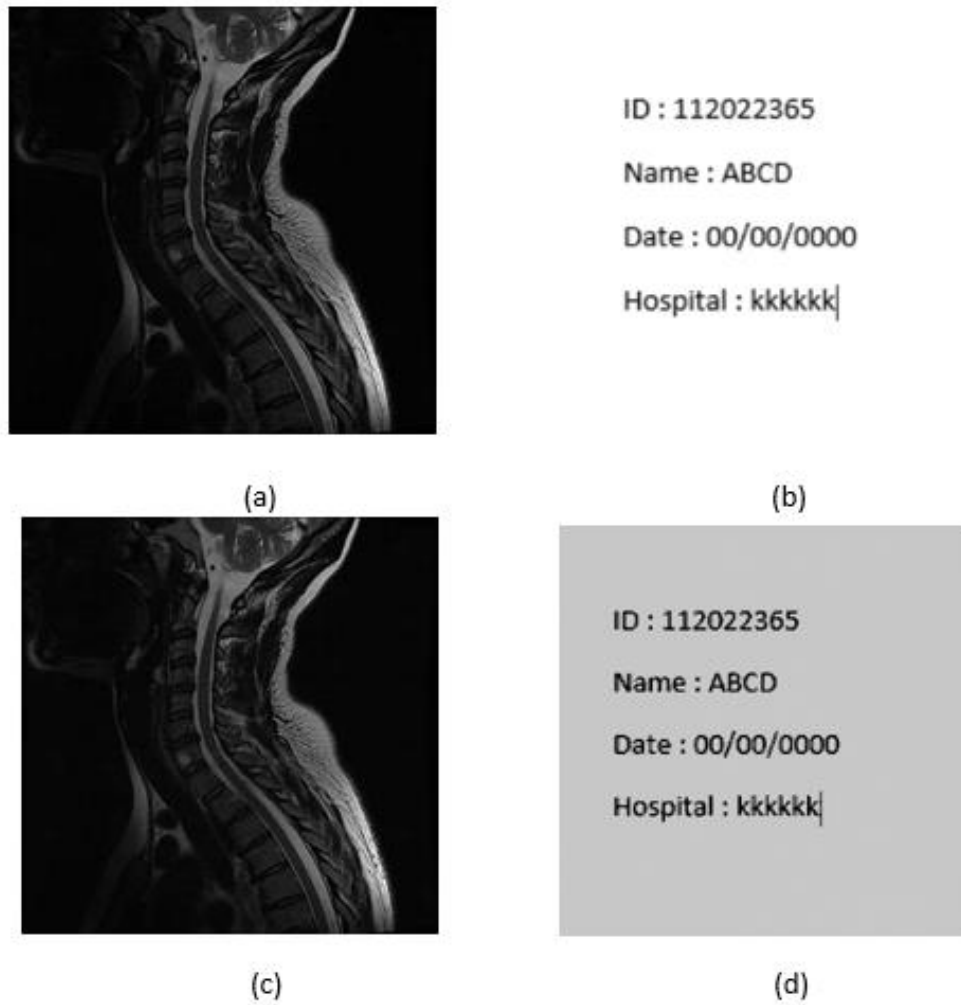


Figure 4.9: IRM avant et après le DWT amélioré.

2. Pour l'image Scanner

La Figure 4.10 présente Scanner avant et après le DWT amélioré. (a): image médicale de Scanner, (b) : image de Filigrane originale, (c) : image tatouée de Scanner par DWT amélioré, (d) : image de Filigrane extraite de Scanner par DWT inverse amélioré.



(a)

ID : 112022365
Name : ABCD
Date : 00/00/0000
Hospital : kkkkkk|

(b)



(c)



(d)

Figure 4.10: Scanner avant et après le DWT amélioré.

- Les histogrammes

La Figure 4.11 présente les résultats obtenus de l'IRM par DWT amélioré. (a) : image médicale IRM, (b) : image IRM tatouée par DWT amélioré, (c) : histogramme d'image médicale IRM, (d) : histogramme d'image IRM tatouée par DWT amélioré.

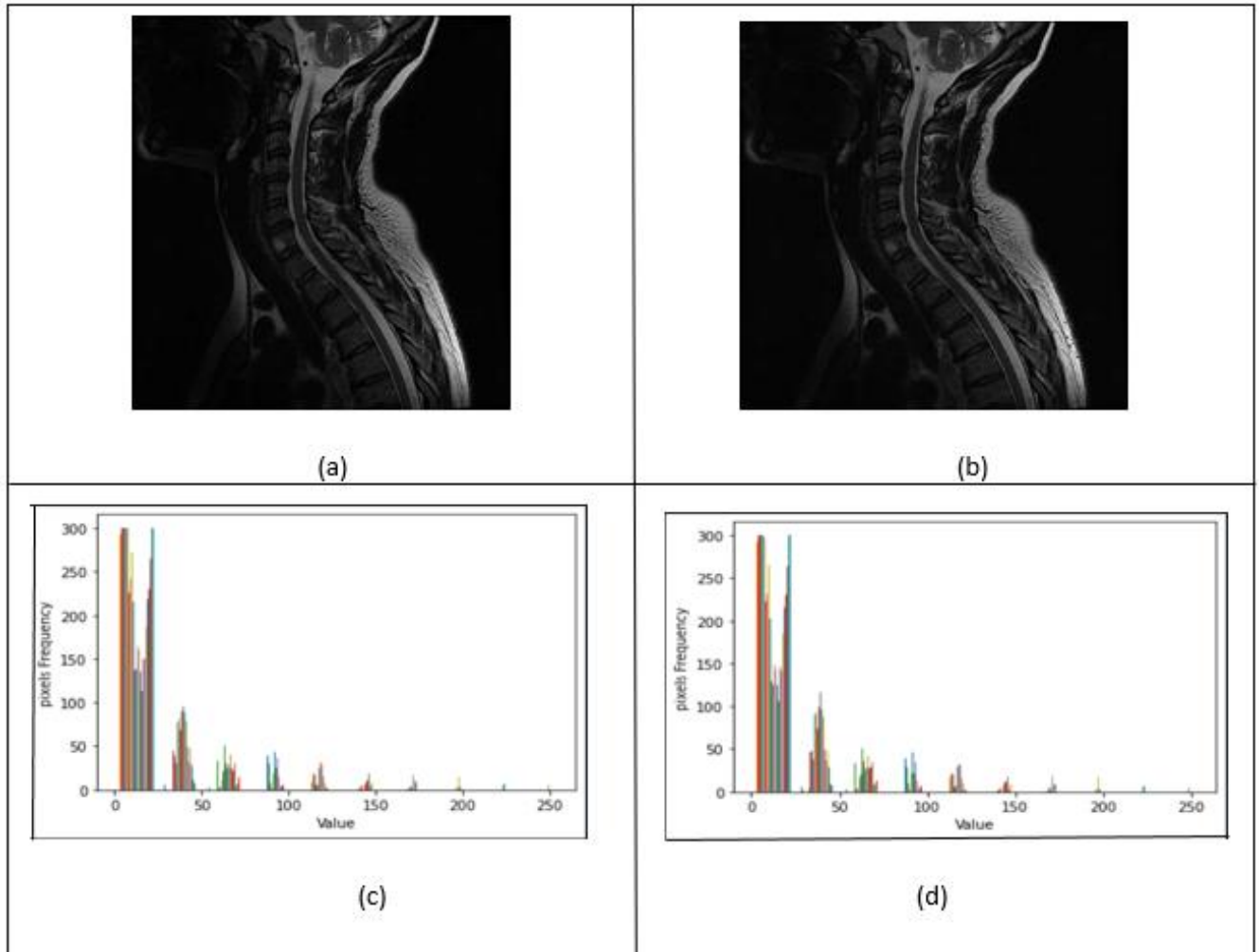


Figure 4.11: Les résultats obtenus de l'IRM par DWT amélioré.

La Figure 4.12 présente les résultats obtenus de Scanner par DWT amélioré. (a): image médicale Scanner, (b) : image Scanner tatouée par DWT amélioré, (c) : histogramme d'image médicale Scanner, (d) : histogramme d'image Scanner tatouée par DWT amélioré.

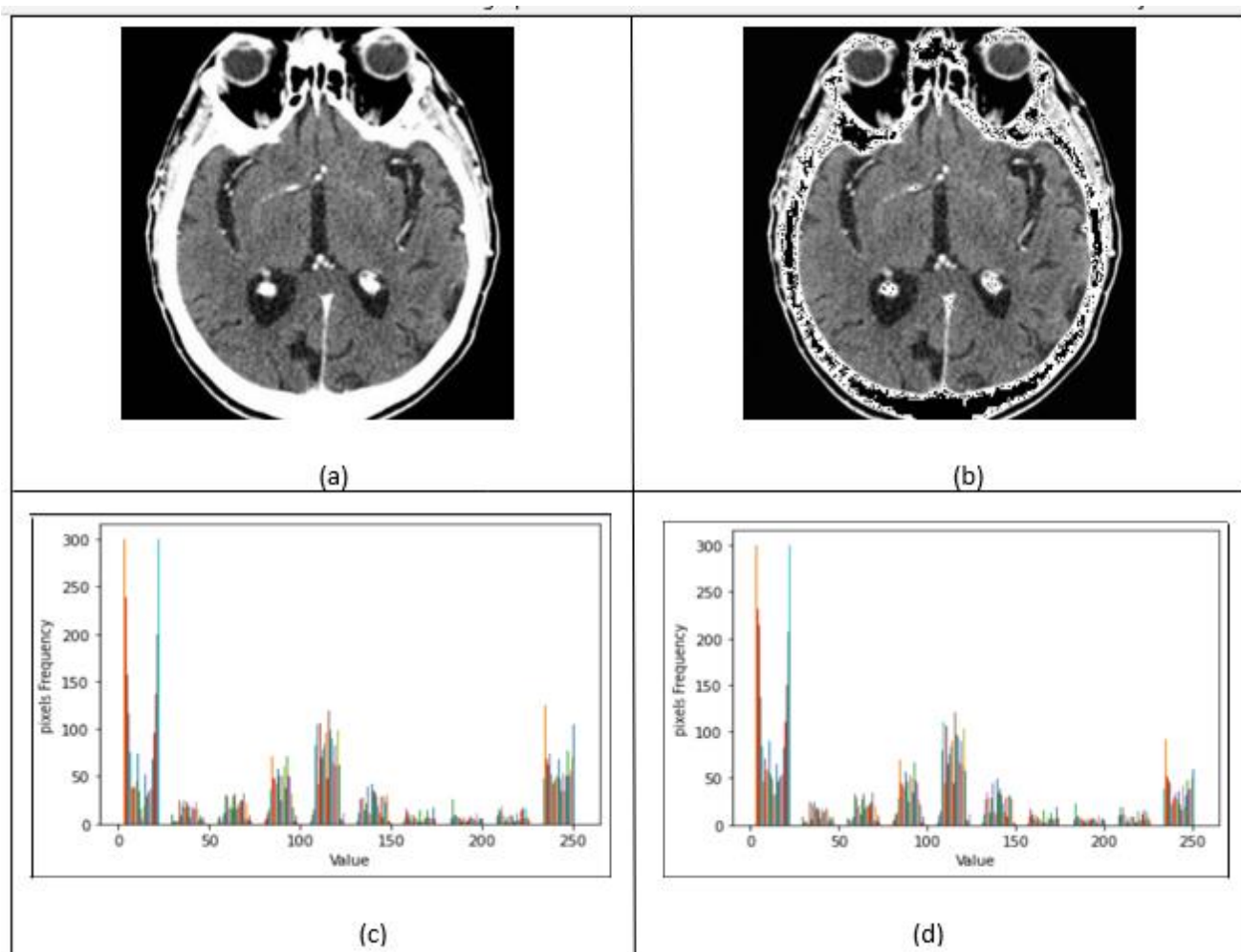
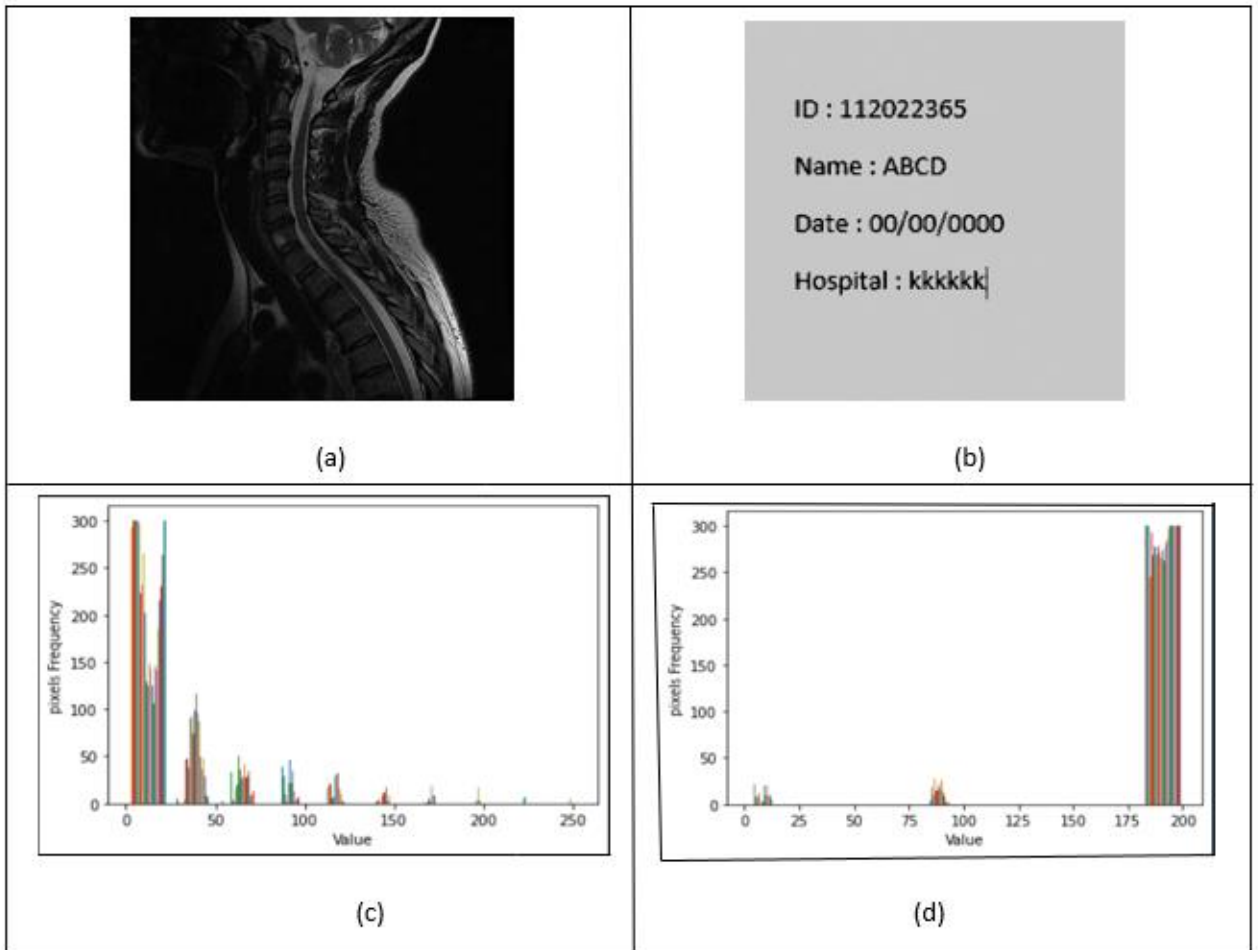


Figure 4.12: Les résultats obtenus de Scanner par DWT amélioré.

La Figure 4.13 présente les résultats obtenus de l'IRM par DWT inverse amélioré. (a) : image IRM tatouée par DWT amélioré, (b) : image Filigrane extrait par DWT inverse amélioré, (c) : histogramme d'image IRM tatouée par DWT amélioré, (d) : histogramme d'image Filigrane extrait par DWT inverse amélioré.



. **Figure 4.13:** Les résultats obtenus de l'IRM par DWT inverse amélioré

La Figure 4.14 présente les résultats obtenus de Scanner par DWT inverse amélioré. (a): image Scanner tatouée par DWT amélioré, (b) : image Filigrane extrait par DWT inverse amélioré, (c) : histogramme d'image Scanner tatouée par DWT amélioré, (d) : histogramme d'image Filigrane extrait par DWT inverse amélioré.

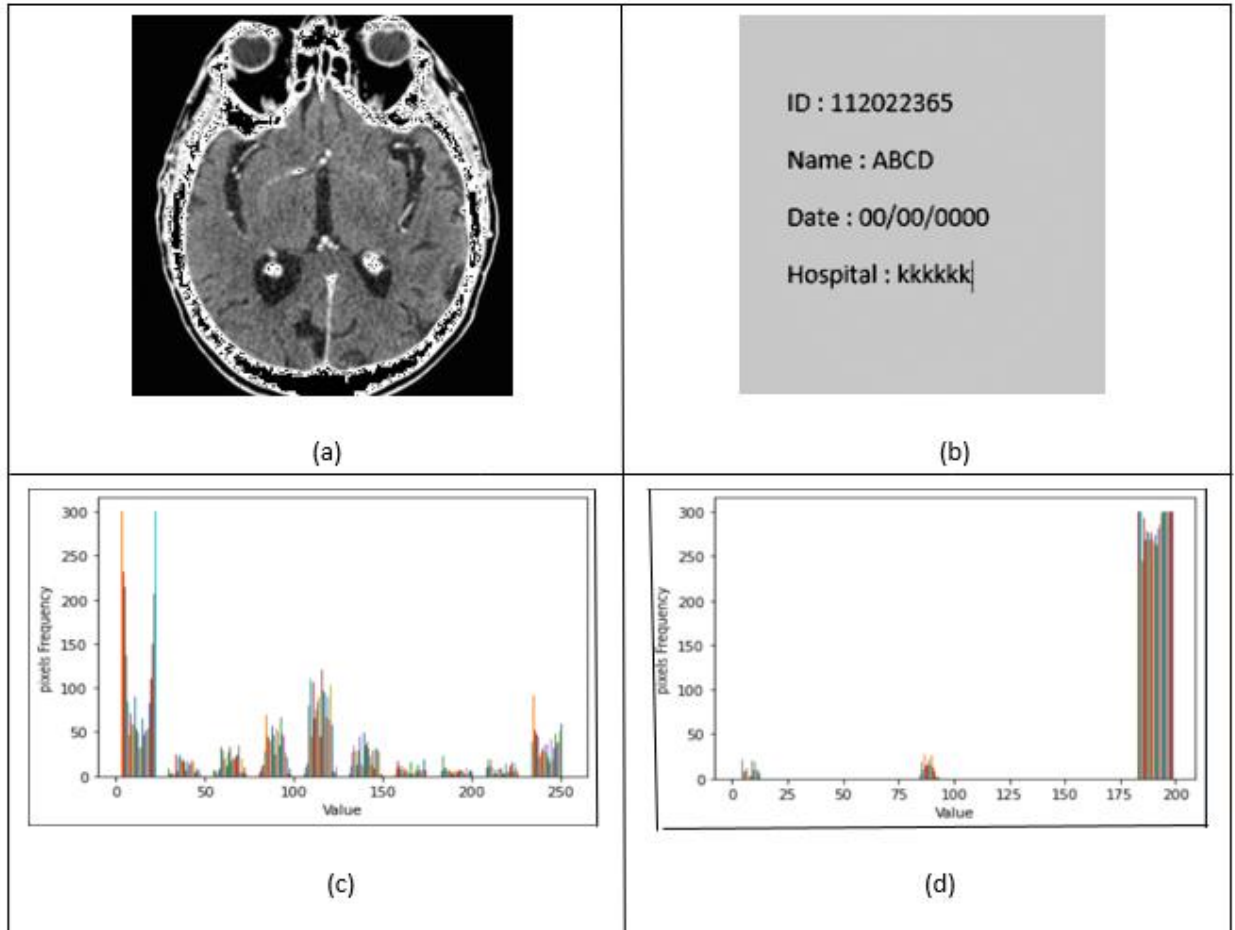


Figure 4.14: Les résultats obtenus de Scanner par DWT inverse amélioré.

4.6.3. PSNR (peak signal-to-noise ratio)

Le terme rapport signal / bruit de crête (PSNR) est une expression du rapport entre la valeur maximale possible (puissance) d'un signal et la puissance du bruit de distorsion qui affecte la qualité de sa représentation.

Il est nécessaire d'établir des mesures quantitatives / empiriques pour comparer les effets des algorithmes d'amélioration d'image sur la qualité d'image [56].

Pour notre approche la valeur PSNR de l'intégration d'une image IRM est 37.447819188491785 par contre dans l'approche existe est 37.438572264731114.

Pour notre approche la valeur PSNR de l'intégration d'une image Scanner est 12.415453678858771 par contre dans l'approche existe est 12.409628179381881.

Pour notre approche la valeur PSNR de l'extraction d'une Filigrane du IRM est 13.315167599009978 par contre dans l'approche existe est 13.128465733201356.

Pour notre approche la valeur PSNR de l'extraction d'une Filigrane du Scanner est 13.378672953919414 par contre dans l'approche existe est 13.222213400358802.

4.6.4. SSIM (Structural Similarity Index)

Est une métrique perceptuelle qui quantifie la dégradation de la qualité de l'image causée par un traitement tel que la compression de données ou par des pertes lors de la transmission de données. Il s'agit d'une métrique de référence complète qui nécessite deux images de la même capture d'image : une image de référence et une image traitée [57].

Pour notre approche la valeur SSIM de l'intégration d'une image IRM est 0.966 par contre dans l'approche existe est 0.966.

Pour notre approche la valeur SSIM de l'intégration d'une image Scanner est 0.7973640115867439 par contre dans l'approche existe est 0.7973639219278222.

Pour notre approche la valeur SSIM de l'extraction d'une Filigrane du IRM est 0.952286691882741 par contre dans l'approche existe est 0.9584628293877243.

Pour notre approche la valeur SSIM de l'extraction d'une Filigrane du Scanner est 0.9515916064035511 par contre dans l'approche existe est 0.9579747114075606.

4.7. Discussion

Voici la fin de notre travail, qui s'est concentré sur le tatouage d'images par la technique de DWT pour sécuriser la transmission d'informations. Au cours de ce travail, nous avons montré comment une image peut être mieux protégée. Nous recherchons des algorithmes de tatouage photo médical pour le tatouage de filigrane d'image médicale (emballage), tous ces algorithmes sont basés sur la technologie DWT.

Cependant, nous proposons une méthode améliorée basée sur une combinaison de technologie de hachage hash-256 et d'algorithme cryptographique. Nous avons sélectionné deux technologies d'imagerie médicale, Scanner et IRM, pour tester et comparer les techniques étudiées.

Pour évaluer les performances de chaque algorithme, nous l'implémentons dans l'environnement python.

Les algorithmes implémentés sont les suivants : algorithme DWT et algorithme DWT améliorée.

La table 4.1, présente les valeurs PSNR de l'approche améliorée et l'approche existante.

Type de l'image	Approche existe DWT		Approche améliorée	
	Image tatouée	Filigrane extraite	Image tatouée	Filigrane extraite
IRM	37.438	13.128	37.447	13.315
Scanner	12.409	13.222	12.415	13.378

Table. 4.1 : les valeurs PSNR de l'approche améliorée et l'approche existante.

On note que plus le PSNR élevé, la qualité de l'image est mieux, en plus des modifications qui ont été apportées au filigrane avant d'effectuer la technique, que ce soit en intégration ou en extraction. Les histogrammes montrent que la précision n'a pas été beaucoup affectée par le retour au PSNR. La même chose est vraie pour le facteur SSIM (Voir la table 4.2).

Type de l'image	Approche existe DWT		Approche améliorée	
	Image tatouée	Filigrane extraite	Image tatouée	Filigrane extraite
IRM	0.966	0.958	0.966	0.952
Scanner	0.797	0.957	0.797	0.951

Table. 4.2 : Les valeurs SSIM de l'approche améliorée et l'approche existante.

Par conséquent, l'histogramme de l'image tatouée n'est pas très différent après la technique, même l'attaquant ne peut pas extraire les informations de l'histogramme de l'image cryptée.

Notre approche utilise des algorithmes de cryptage AES et hash-256, par contre, la méthode d'envoi de l'image cryptée avec l'image tatoué, la comparaison avec les résultats de la technique et la vérification de leur conformité pour ensuite décrypter l'image et obtenir le filigrane d'origine est une méthode très infaillible pour protéger les informations et la fiabilité.

Dans une petite comparaison de notre approche avec une autre approche utilisant des histogrammes et des valeurs PSNR et SSIM, nous avons conclu que notre approche était plus sécurisée avec une assurance complète de la confidentialité des patients et ses informations, avec une meilleure qualité d'image.

4.8. Conclusion

Dans ce chapitre nous avons présenté notre approche, qui dépend sur une amélioration de l'algorithme DWT, pour sécuriser les images médicales.

Nous avons utilisé l'algorithme de cryptage symétrique AES pour crypter le Filigrane et l'algorithme de hash-256 pour hacher le Filigrane chiffrée. Enfin, nous avons discuté des résultats obtenus.

CONCLUSION GÉNÉRALE

De nos jours, de plus en plus les images médicales sont transférées ou stockées sur les réseaux informatiques. Avec le temps, la confidentialité de l'image médicale est devenue indispensable. Au cours de ce mémoire, nous avons proposé un schéma de sécuriser l'image médicales basé sur l'algorithme DWT de tatouage numérique avec l'algorithme de cryptographie symétrique AES, qui utilisé pour chiffrer le Filigrane et l'algorithme de hash (SHA-256) qui haché le Filigrane chiffrée hachée.

Le but principal de ce chiffrement et ce hachage c'est de garantir la confidentialité de l'information de l'image après l'envoi.

Les résultats expérimentaux montrent que notre approche dispose un niveau élevé de sécurité et d'efficacité.

Finalement les comparaisons entre notre approche améliorée et l'approche existante DWT, montre que l'approche proposée offre des performances très favorables.

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

BIBLIGRAPHIE

- [1] E. Tonye, A. Akono, A. Ndi Nyoungui, Le traitement des images de télédétection par l'exemple, Gordon and Breach Science Publishers, L'univers de la télédétection, 01 janvier 2000.
- [2] R. Caloz, C. Collet, Précis de télédétection - : Traitements numérique d'images de télédétection, Volume 3, Le Delta I,2875, boul. Laurier, bur.450 Sainte-Foy (Québec) Canada G1V 2M2, Presses de l'Université du Québec, 2001.
- [3] R. Isdant, Traitement numérique de l'image, 2009.
- [4] O. Poutarédy, Formation méthodes et outils, 2015.
- [5] D. Chareyron, Numérisation d'un signal acoustique : Effect de la quantification (Partie 1), 10 Octobre 2013 .EE
- [6] O. Granier, D. Chareyron, N. Taberlet, La physique Animee – Conversion analogique - numérique : Echantillonnage temporel ,2016.
- [7] J.M. Mermet, Techniques de Numérisation, 2009-2010.
- [8] Gralon, www.gralon.net , 30 Septembre 2008.
- [9] Maxicours, www.maxicours.com , 23 Mars 2020.
- [10] Phototrend, <https://phototrend.fr/phototrend.fr> , 13 Janvier 2016.
- [11] G. Peyré, Le traitement numérique des images, 2011.
- [12] M.C. Daikha, Amélioration et évaluation de la qualité des images, Doctorat, Oran, 2014/2015.
- [13] E. Durand, E. Blandiux, Imagerie médicale : Caractéristique d'une image médicale, 2017.
- [14] Univ-rennes2, www.sites.univ-rennes2.fr/ , 24 Mars 2020.
- [15] M. Chilowicz, Une synthèse sur les formats usuels d'images numériques fixes.

- [16] D. Müller, Informatique (presque) débranchée : Traitement d'images, Juin 2018.
- [17] M. Colinet, Le traitement des images, Mai 2004.
- [18] H. Maitre, Du photon au pixel L'appareil photographique numérique seconde édition, 20 Décembre 2016.
- [19] P.G. Frija, P.B. Mazoyer, L'imagerie médicale, 2002.
- [20] N. Henri, Traité d'imagerie médicale - volume 1 – 2^e éd, Médecine Sciences Publication, Paris, 2014.
- [21] R.B. Kahla, A. Barkaoui, T. Merzouki, Série ingénierie mathématique et mécanique : volume 8, Méthode des éléments finis et techniques d'imagerie médicale en biomécanique osseuse, ISTE Edirions Ltd, Great Britain, Février 2020.
- [22] Y. Michqud, Le Renouveau de l'observation dans les sciences, Odile Jacob, Paris, Octobre 2003.
- [23] B. Blanc, A. Potier, Imagerie médicale en gynécologie, Springer-Verlag France, Paris, 2000.
- [24] Sementicscholar, www.semanticscholar.org/ , 25 Mars 2020.
- [25] A.C. Boccara, L. Garnero, Image : Imagerie, Représentation, Modèles, 2004.
- [26] Doctissimo, <https://www.doctissimo.fr/> , 27 Mars 2020.
- [27] blogrecherche, <https://blogrecherche.wp.imt.fr/> , 26 Mars 2018.
- [28] C. Rey, J. Dugelay, Blind Detection of malicious alterations on still image using robust watermarks.
- [29] A.Manoury , Tatouage d'images numériques par paquets d'ondelettes , Ecole Centrale de Nantes (ECN); Université de Nantes, 2001, Français.
- [30] V. Martin¹, M. Chabert¹, B. Lacaze², Un algorithme de Tatouage d'images numériques reposant sur les changements d'horloge périodiques, Institut National polytechnique de Toulous 3 Rue Camichel, BP 7122, 31071 Toulous Cedex 7, France.

- [31] I. Assini, A. Badri, K. safi, Technique Hybride de Compression pour le Tatouage des images, 2015.
- [32] S. M. Mousavi, A. Naghsh, S.A.R. Abu-Bakar, Watermarking technique used in Medical images: à Survey, Published online, 29 Mai 2014.
- [33] I. Assini, A. Badri, K. safi, Technique avancée pour le Tatouage des images médicales, Faculté des Sciences et Technique Mohammedia, Université Hassan II Casablanca, Maroc.
- [34] A. Manoury, Tatouage d'images numériques par paquets d'ondelettes, 21 Décembre 2001.
- [35] F. Atrousseau, Tatouage d'images fondé sur la modélisation su système visuel humain et sur la transformation mojette, 7 Novembre 2002.
- [36] P. Singh, R.S. Chadha, A survey of digital watermarking technique, Applications and attacks, Issue 9, Mars 2013.
- [37] B. Souad, Etude et implémentation des techniques de tatouage numérique, 30 Avril 2017.
- [38] A. Bassem, If watermarks could talk on Telltale watermarks and their Application for digital content authentification, Mémoire de maîtrise, Université d'Ottawa, Mars 2003.
- [39] I. Assini, A. Badri, K. Safi, A. Sahel, A. Baghdad, Tatouage robuste des images couleurs RGB basé sur une nouvelle technique DWT-DCT-SVD.
- [40] F. Deguillaume, S. Voloshynovskiy, T. Pun, Hybrid robust watermarking resistant against copy attach, 24 Rue du General Dufour.
- [41] C. Rey, J. Dugelay, Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images, Traitement du Signal, 2001.
- [42] V. Martin, Contribution des filtres LPTV et des techniques d'interpolation au tatouage numérique.
- [43] H.B. Razafindrading, P.A. Randriamitantsoa, Tatouage robuste et aveugle dans le domaine des valeurs singulières, 22 Janvier 2010.
- [44] I. Christine, B. Raymond, Perceptual watermarks for digital Image and Video.

- [45] I. F. Kallel, J. C. Lapayre, M. S. Bouhlel, Tatouage Réversible des images médicales couleurs, Tunisie, 22-26 Mars, 2009.
- [46] Anuradha, R. P. Singh, DWT Based Watermarking Algorithm using Haar Wavelet, International Journal of Electronics and Computer Science Engineering (IJECSSE), volume1, Number 1, 01 Jun.
- [47] A. Al-Haj, Combined DWT-DCT Digital Image Watermarking, Journal of Computer Science 3, 2007.
- [48] A. Joseph, K. Anusudha, Robust Watermarking Based on DWT-SVD, International Journal of Signal & Image Processing Issue, Volume 1 October 2013.
- [49] N. Rathi, G. Holi, Securing Medical Images by Watermarking Using DWT-DCT-SVD, International Journal of Computer Trends and Technology (IJCTT) - volume X Issue Y-Month 2014.
- [50] JDN, www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/ , 10 Septembre 2020.
- [51] Annaconda Documentation, <https://docs.anaconda.com/anaconda/user-guide/tasks/integration/spyder/> , 10 Septembre 2020.
- [52] Les créateurs de mondes, <https://www.createursdemondes.fr/veille-techno/librairies-de-programmation-langages/les-meilleures-librairies-multi-langages/les-meilleures-librairies-pour-python/>, 10 Septembre 2020.
- [53] Bibliothèque python ,<https://he-arc.github.io/livre-python/hashlib/index.html> , 10 Septembre 2020.
- [54] pywavelets.readthedocs <https://pywavelets.readthedocs.io/en/latest/> , 10 Septembre 2020.
- [55] security online,<https://securityonline.info/stegano-python-steganography-module/> , 21 Septembre 2020.
- [56] Ni, <https://www.ni.com/en-lb/innovations/white-papers/> , 21 Septembre 2020.
- [57] Imatest , <https://www.imatest.com/docs/ssim/> , 21 Septembre 2020.