République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Kasdi Merbah - Ouargla

FACULTÉ DES NOUVELLES TECHNOLOGIES DE L'INFORMATION ET

DE LA COMMUNICATION

Mémoire

Présenté pour l'obtention du diplôme de :

Master en Informatique

Option :

Administration et Sécurité des Réseaux

Thème

Sécurisation des images médicales échangées en télémédecine par tatouage numérique

Présenté par

Meghnai Khedidja et Bekkouche Selssabil

Devant la commission d'examen composée de :

Superviser	: Dr. Khaldi Amin	Pr	Université de Ouargla
Président	: Dr. Eushi Saleh	Pr	Université de Ouargla
Examinateurs	: Dr. Kahlessenane.Fares	Pr	Université de Ouargla

Année universitaire: 2021/2022

REMERCÎMENT

Louange à Dieu beaucoup, et louange à Ses innombrables bénédictions, et de Lui nous ont permis de terminer ce travail, car c'est grâce à notre grande générosité. Dans notre gratitude, nous exprimons nos sincères remerciements, nos sincères louanges et notre sincère gratitude à chacun de nous pour nous avoir aidés à accomplir ce travail, et en particulier à **M. Khaldi. Amin** pour avoir accepté de superviser cette humble étude avec tous les efforts et le temps, avec soin, conseils et soutien.

N'oubliez pas non plus les professeurs du Département d'informatique pour leurs conseils et leurs orientations. En conclusion, nous sommes heureux d'exprimer nos sincères remerciements et notre gratitude à tous ceux qui nous ont un peu ou beaucoup aidés. Nous leur souhaitons récompense et récompense de la part de Dieu, et louanges à Dieu, Seigneur des Mondes.

DEDICATION

Du fond du cœur, avec amour et sincérité, je voudrais dédier cette thèse à tous ceux qui m'ont accompagné dans les moments difficiles avant les moments heureux, dans ma faiblesse avant ma force, et à chaque étape de ma vie.

A la première femme de ma vie… à celle qui m'a accueilli avec son sourire et m'a dit adieu avec ses prières… à celle qui m'a enseigné et m'a donné amour et affection… à celle dont la supplication a été le secret de ma réussite… à celui qui m'a appris à aimer le bien des autres, la bonté de cœur et l'optimisme en tout. Ma mère, mon amour et mes cieux, que Dieu les protège.

Pour celui qui m'a appris à donner sans attendre… pour celui qui porte son nom avec beaucoup de fierté… pour celui qui m'a appris la pudeur, les valeurs et la morale… pour celui qui m'a appris à compter sur Dieu, mon père et le sommet de ma tête, que Dieu le protège.

A mon cher époux, je dédie cette humble recherche, en guise d'expression de mes remerciements envers lui; Pour être à mes côtés pour réaliser mon ambition scientifique.

Mes sœurs et frères… Les mots s'emballent et rivalisent pour organiser la décennie de remerciements et de louanges que vous méritez tous… Je vous souhaite le meilleur et la prospérité dans vos vies… Et aussi à tous ceux que j'aime, à tous les membres de ma famille élargie, mes professeurs et tous mes amis… je vous aime tous, merci beaucoup.

Enfin, mon rêve de diplôme s'est réalisé, Dieu merci.

Bekkouche selssabil

A ceux qui m'ont soutenu et qui ont sacrifié leur vie au cours de mes études. Ils m'ont tout donné depuis la plus belle suite de mes études et m'ont encouragé à continuer jusqu'à ce que j'en sois là. Merci beaucoup à vous deux Je vous dédie mon diplôme et ce succès. Je dédie mon diplôme à mon cher père, que Dieu le préserve, qui m'a accompagné sur tous les chemins et tous les chemins pour l'emmener sur le chemin du succès.

Et à celle qui a fait le ciel sous ses pieds, à celle qui m'a plongé dans le flot de sa tendresse, à celle qui a brûlé pour éclairer mon chemin, à celle qui a eu faim d'être rassasiée et crié de rire, et qui a arrosé moi de la source de sa tendresse et de sa sincérité, à celle qui m'a élevé jeune et m'a conseillé grand, le réconfort de mes yeux et de mon cœur, ma chère mère, que Dieu prolonge sa vie et fasse d'elle une tente au-dessus de nos têtes.

A ceux qui ont partagé mes joies et mes peines avec mes frères A ceux avec qui la chaire du savoir et de l'amitié m'a réuni Mes collègues et confrères pour qui j'ai les plus hautes expressions d'amour A tous mes professeurs qui m'ont accompagné tout au long de mon parcours académique. Merci.

Meghnai khedidja

Résumé :

Afin de contribuer au partage et à la transmission des images médicales, nous présentons dans ce travail la méthode du filigrane multicouche. Ce dernier est la dissimulation d'informations dans le document, qui peut être du texte, de l'audio et de la vidéo. Pour une image, il modifie les niveaux de gris de ses pixels pour encoder le message. Par exemple, masquer les données du patient dans une image médicale. Il doit garantir l'intégrité et la confidentialité des données lorsqu'elles sont partagées, pour que ça ne soit pas vulnérable aux différents types d'attaques (compression JPEG, copier-coller, transformations géométriques, etc.)

Mots-clés : tatouage numérique, image médicale, télémédecine, domaine fréquentiel.

Abstract:

In order to contribute to the sharing and transmission of medical images, we present in this work the method of multilayer watermarking. The latter is the hiding of information in the document, which can be text, audio and video. For an image, it changes the grey levels of its pixels to encode the message. For example, hiding patient data in a medical image. It must guarantee the integrity and confidentiality of the data when it is shared, so that it is not vulnerable to various types of attack (JPEG compression, copy and paste, geometric transformations, etc.)

.**Keywords:** digital watermarking, medical image, telemedicine, frequency domain.

ملخص

من أجل المساهمة في مشاركة الصور الطبية ونقلها، نقدم في هذا العمل طريقة العلامة المائية متعددة الطبقات. هذا الأخير هو إخفاء المعلومات في المستند، والتي يمكن أن تكون نصية وصوتية وفيديو. بالنسبة للصورة ، فإنه يعدل المستويات الرمادية لوحدات البكسل الخاصة بها لتشفير الرسالة. على سبيل المثال ، إخفاء بيانات المريض في صورة طبية. يجب أن ، ولصق النسخ تضمن سلامة البيانات وسريتها عند مشاركتها ، بحيث لا تكون عرضة لأنواع مختلفة من الهجمات (ضغط ، والتحويلات الهندسية ، وما إلى ذلك).

الكلمات المفتاحية: الوشم ، الصورة الطبية ، التطبيب عن بعد ،مجال التردد .

TABLE DES MATIÉRES

REMERCÎMENT 1
DEDICATION II
Résumé : IV
Abstract: IV
ملخص IV
TABLE DES MATIÉRES V
Liste des figures : IX
Table d'abréviations : X
Liste des tableaux : XI
INTRODUCTION GÉNÉRALE 1
Chapitre 01 : 1
L'IMAGE NUMERIQUE 1
1.1 Introduction : 1
1.2 Définition de L'image numérique : 1
1.3 Types d'images numériques : 1
1.3.1 Les images matricielles: 1
1.3.2Les images vectorielles : 1
1.4 Les formats des images numériques : 2
1.4.1Formats d'image matricielle : 2
1.4.1.1 JPEG (Joint Photographic Expert Group) : 2
1.4.1.2 GIF (Graphics Interchange Format) : 2
1.4.1.3 PNG (Portable Network Graphic): 2
1.4.1.4 TIFF (Tagged Image File Format): 2
1.4.1.5 BMP (BitMaP): 3
1.4.1.6 PSD (Photoshop document) : 3
1.4.2 Formats d'image vectorielle : 3
1.4.2.1 PICT(Picture) : 3
1.4.2.2 PS (PostScript) : 3
1.4.2.3 DXF : 3
1.4.2.4 WPG : 3
1.5 Les caractéristiques d'une image numérique : 3
1.5.1 Pixel : 4
1.5.2 Résolution : 4

1.5.3 Son poids : 4
1.5.4 Son codage de la couleur : 5
1.6 Taille d'une image - compression d'images : 5
1.7 Propriétés des images numériques : 6
1.7.1 Histogramme : 6
1.7.2 Luminance : 7
1.8 Traitement d'images : 7
1.9 Les techniques d'imagerie médicale : 8
1.9.1 Radiologie : 8
1.9.2 Scanner : 9
1.9.3 Echotomographie : 9
1.9.4 La mammographie : 10
1.9.5 Imagerie par résonnance magnétique : 10
1.10 La sécurité d'une image médicale : 11
1.11 Conclusion : 11
Chapitre 02 : 12
TATOUAGE NUMÉRIQUE 12
2.1 Introduction : 13
2.2 Historique : 13
2.3 Définition 13
2.4 Techniques numériques pour la protection des données : 13
2.4.1 La cryptographie : 14
2.4.2 La stéganographie : 14
2.4.3 Le tatouage d'images : 15
2.5 Propriétés du tatouage numérique : 15
2.5.1 Le tatouage numérique des images : 15
2.5.1.1 Phase d'insertion : 16
2.5.1.2 Phase d'extraction : 16
2.6 Les applications du tatouage numérique 17
2.6.1 Protection des droits d'auteur : 17
2.6.2 La prévention de la copie illégale ou « fingerprinting » : 17
2.6.3L'authentification des données : 17
2.6.4 Contrôle d'accès : 17
2.7 Les attaque : 17

2.7.1 Attaques de traitement d'image :.....17
2.7.2 Attaques géométriques :.....17
2.7.3 Attaques cryptographiques :.....17
2.7.4 Attaques de protocole :.....18
2.8 Classification des algorithmes du tatouage numérique :.....18
2.8.1 Classification selon le type du support hôte :.....18
2.8.2 Classification selon la perceptibilité de watermark :.....18
2.8.2.1Tatouage visible :.....18
2.8.2.2 Tatouage invisible :.....18
2.8.3 Classification selon le domaine d'insertion :.....18
2.8.3.1 Domaine spatial :.....18
2.8.3.2 Domaine fréquentiel :.....19
2.8.4 Classification selon la robustesse :.....19
2.8.4.1Tatouage robuste :.....19
2.8.4.2 Tatouage fragile :.....19
2.8.4.3 Tatouage semi-fragile :.....19
2.8.5 Classification selon la méthode de cryptage :.....20
2.8.5.1 Méthodes symétriques ou méthodes à clé privée :.....20
2.8.5.2 Méthodes asymétriques ou méthodes à clé publique :.....20
2.8.6 Classification selon le processus d'insertion :.....20
2.8.6.1 Schémas d'insertion aveugle :.....20
2.8.6.2 Schémas d'insertion informée :.....20
2.8.7 Classification selon la qualité d'image tatouée :.....20
2.8.7.1 Schémas de tatouage irréversible :.....20
2.8.7.2 Schémas du tatouage réversible :.....20
2.8.8 Classification selon le processus d'extraction :.....21
2.8.8.1 Schémas du tatouage non aveugle :.....21
2.8.8.2 Schémas du tatouage semi-aveugle :.....21
2.8.8.3 Schémas du tatouage aveugle :.....21
2.9 Conclusion :.....21
Chapitre 03:.....22
Conception et implémentation d'un tatouage fragile par LSB replacement 22
3.1 Introduction:.....23
3.2 Environnement de travail:.....23

3.2.1 Matériel:.....23
3.2.2 Logiciel : 23
3.2.2.1 Langage de programmation MATLAB : 23
3.3 PSNR : 24
3.4 SSIM : 24
3.5L'organigramme de l'algorithme :.....25
3.6 Least Significant Bit Hiding Technique (LSB):.....25
3.7 Algorithme d'isertion : 26
3.7.1 Entrées : 26
3.7.2 Etapes :.....26
3.7.3 Sortie : 27
3.8 Déroulement de L'application :.....27
3.9 Résultat : 27
3.10 Phase d'insertion :.....27
3.11 Evaluation de l'algorithme :.....28
3.12 Analyse de l'imperceptibilité : 29
3.13 Discussion :.....31
3.14 Conclusion :.....31
Conclusion Générale 33
Bibliographie 36

Liste des figures :

Figure 1.1: Exemple d'Image matricielles. 1
Figure 1.2: Exemple d'Image vectorielle. 2
Figure 1.3: L'image conserve la même qualité. 2
Figure 1.4: image qui a une définition de 400 pixels de largeur sur 300 pixels de hauteur.. 4
Figure 1.5: image montrant La résolution 4
Figure 1.6: Image la représentation la taille (en octet). 6
Figure 1.7:Exemple de spectre UV-Visible 6
Figure 1.8:Exemple d'histogramme d'une Image. 7
Figure 1.9:Exemple de luminance. 7
Figure 1.10: Illustre un schéma d'un tube à rayons X [10]. 9
Figure 1.11:Géométrie d'un scanner [12]. 9
Figure 1.12:Echotomographie abdominale [15]. 10
Figure 1.13:Mammographie d'un sein de femme à cancer (la masse suspecte)[12]. 10
Figure 1.14:Scanner d'IRM [17]. 11
Figure 2.15: Exemple de la cryptographie. 14
Figure 2.16: Exemple de la stéganographie. 14
Figure 2.17:Propriétés du tatouage numérique [19]. 15
Figure 2.18:Schéma général d'un système de tatouage numérique des images [25]. 16
Figure 2.19:Schéma général de l'insertion d'une marque [27]. 16
Figure 2.20: Schéma général d'extraction non aveugle d'une marque [27]. 16
Figure 3.21:Fenêtre PSNR et SSIM. 24
Figure 3.22: Fonctionnement générale de l'algorithme 25
Figure 3.23:Méthode LSB 26
Figure 3.24:Chargement de l'image original et la marque. 27
Figure 3.25:Image tatouée 28
Figure 3.26:Images original. 29
Figure 3.27:Images tatouée. 30

Table d'abréviations :

JPEG	Joint Photographic Expert Group)
GIF	Graphics Interchange Format
PNG	Portable Network Graphic
TIFF	Tagged Image File Format
BMP	Bit Map
PSD	Photoshop document
PICT	Picture
PS	Pos Script
WPG	Word Perfect Graphic
LSB	Least Significant Bit
PSNR	Peak Signal to Noise Rational
SSIM	Structural Similarity Index Method
SVD	Singular Value Decomposition
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
VQ	Vector Quantization

Liste des tableaux :

Tableau 1:présente en plusieurs niveaux de couleurs.....5
Tableau 2:présente les valeurs de PSNR. Et SSIM.....31

INTRODUCTION GÉNÉRALE

INTRODUCTION GÉNÉRALE

Le développement des réseaux de communication et le développement de la technologie qui s'est produit à l'heure actuelle ont conduit à différents domaines afin de compléter le service et de faciliter les tâches. Ce qui nous intéresse particulièrement dans ce travail, notre travail cible le domaine médical, d'où la télémédecine à l'origine. Notre approche s'inscrit dans ce cadre et consiste à concevoir un système et une surveillance visant à protéger les données médicales diffusées entre les hôpitaux.

Les réseaux numériques et le développement rapide de la technologie informatique. Il permet la transmission de pratiquement toutes sortes d'informations textuelles, audio et d'images. Les images constituent l'essentiel de tous les documents numériques qui ont des problèmes et des attaques. Nous constatons que le numérique est une des solutions efficaces à ce problème.

L'idée était alors de penser à un filigrane numérique. Le filigrane numérique consiste à insérer une marque invisible dans l'image, tandis que la restauration du filigrane dans les données sert à prouver l'intégrité des données avec toutes les méthodes de cryptage Il reste un texte des données lorsqu'il est objecté par l'ennemi doutant qu'il est un message crypté et tente de le déchiffrer avec toutes les méthodes de cryptage ici Pour cacher du texte dans une image particulière et de préférence placer du texte LSB in Gray scal dans la thèse Le but de la thèse est d'appliquer la marque numérique en masquant le texte dans une image.

Le premier chapitre présente les concepts de base des images numériques, leurs caractéristiques, types et formes. Nous introduisons également quelques concepts importants dans le domaine du traitement d'images numériques ainsi que de la technologie d'imagerie médicale.

Le deuxième chapitre est lié au tatouage numérique, qui contient le principe général du tatouage ainsi que ses limitations, techniques et attaques existantes, ainsi que divers domaines d'application, puis nous terminons le chapitre avec des métriques d'évaluation de la qualité des images numériques.

Dans le dernier chapitre, nous avons utilisé le langage de programmation MATLAB et l'algorithme LSB pour implémenter le filigrane dans le masquage de texte dans l'image, Analyse de l’imperceptibilité et présenter les résultats expérimentaux obtenus à partir de cette application.

Chapitre 01 :
L'IMAGE NUMERIQUE

1.1 Introduction :

Le traitement d'images est un domaine très vaste qui a connu, et qui connaît encore, un Développement important depuis quelques dizaines d'années. On désigne par traitement d'images numériques l'ensemble des techniques permettant de modifier une image numérique afin d'améliorer ou d'en extraire des informations. De ce fait, le traitement d'images est l'ensemble des méthodes et techniques opérant sur celles-ci, dans le but de rendre cette opération possible, plus simple, plus efficace et plus Agréable, d'améliorer l'aspect visuel de l'image et d'en extraire des informations jugées Pertinentes. Dans ce chapitre, nous abordons les notions de base nécessaires à la compréhension des Techniques de traitement d'images. Ensuite, nous allons donner un aperçu sur les différentes techniques connues dans ce domaine.

1.2 Définition de L'image numérique :

Le terme d'image numérique désigne, dans son sens le plus général, toute image qui a été acquise, traitée et sauvegardée sous une forme codée représentable par des nombres (valeurs numériques).
La numérisation est le processus qui permet de passer de l'état d'image physique (image optique par exemple) qui est caractérisé par l'aspect continu du signal qu'elle représente (une infinité de valeur dans l'intensité lumineuse par exemple), à l'état d'image numérique qui est caractérisé par l'aspect discret (l'intensité lumineuse ne peut prendre que des valeurs quantifiées en un nombre fini de points distincts).
C'est cette forme numérique qui permet une exploitation ultérieure par des outils logiciels sur ordinateur [1].

1.3 Types d'images numériques :

1.3.1 Les images matricielles:

Il s'agit d'images pixellisées, c'est-à-dire un ensemble de points (pixels) contenus dans un tableau, chacun de ces points possédant une ou plusieurs valeurs décrivant sa couleur [2].

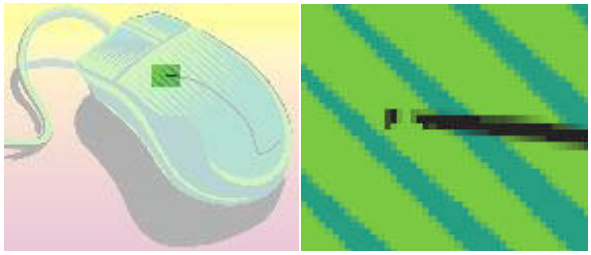


Figure 1.1: Exemple d'Image matricielles.

1.3.2Les images vectorielles :

Les images vectorielles sont des représentations d'entités géométriques telles qu'un cercle, un rectangle ou un segment. Ceux-ci sont représentés par des formules mathématiques (un rectangle est défini par deux points, un cercle par un centre et un rayon, une courbe par plusieurs points et une équation). C'est le processeur qui sera chargé de "traduire" ces formes en informations interprétables par la carte graphique [2].

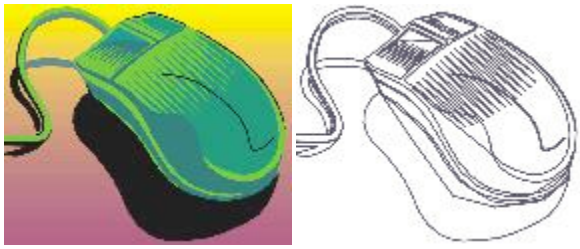


Figure 1.2: Exemple d'Image vectorielle.

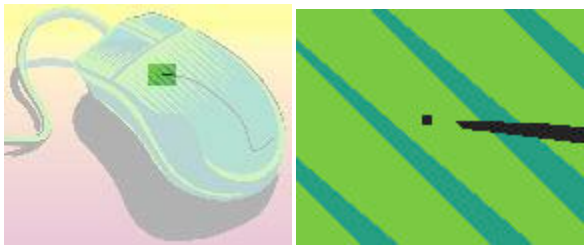


Figure 1.3: L'image conserve la même qualité.

Le défaut de ces images est d'être un peu trop "rigides" au niveau des formes, ce qui fait qu'elles se prêtent surtout à l'illustration, à la lettre, au graphisme, et à la CAO. Pour des effets subtils de texture, peinture etc. ou pour la photographie, on utilisera plutôt les images bitmap.

1.4 Les formats des images numériques :

1.4.1Formats d'image matricielle :

1.4.1.1 JPEG (Joint Photographic Expert Group) :

Ce format offre des taux de compression inégalés, même si la qualité de l'image s'en ressent au fur et à mesure que vous augmentez la compression. Avec des taux de compression élevés donnant lieu à des fichiers images de petite taille, ce format est devenu le standard des formats d'image sur internet. En effet, des fichiers de petites tailles seront chargés rapidement, même par une connexion bas débit[3].

1.4.1.2 GIF (Graphics Interchange Format) :

Ce format est l'autre standard d'internet. Les fichiers gif sont de petites tailles, ce qui est dû au fait que ces images ne peuvent enregistrer que 256 couleurs : le plus gros avantage du format est lié à son plus gros inconvénient. Le format gif permet également la création d'animations et de détourage [3].

1.4.1.3 PNG (Portable Network Graphic):

C'est le format appelé à devenir le futur standard internet. Comme le gif il permet le détourage des images, mais là où le format gif enregistre 256 couleurs, le png en retient 16.7 MILLIONS ce qui offre une image parfaite, avec un excellent rendu des nuances et des dégradés. La taille des fichiers reste raisonnable, et, technologie dont ce format est le seul à disposer, il permet la compression sans perte de donnée ! C'est donc le format en devenir[3].

1.4.1.4 TIFF (Tagged Image File Format):

Ce format est orienté vers les professionnels (imprimeurs, publicitaires...) car il a l'avantage d'être reconnu sur tous types de système d'exploitation : Windows, Mac, Linux, Unix ... Il permet d'obtenir

une image de très bonne qualité, mais sa taille reste volumineuse, même si elle est inférieure à celle des fichier BMP[3].

1.4.1.5 BMP (BitMaP):

Le format BMP est le format par défaut du logiciel Windows. C'est un format matriciel. Les images ne sont pas compressées [3].

1.4.1.6 PSD (Photoshop document) :

Le format Photoshop (PSD) est le format de fichier par défaut ; il est, avec le format de document volumineux (PSB), le seul format à prendre en charge toutes les fonctionnalités de Photoshop. Grâce à l'intégration étroite entre les produits Adobe, certaines autres applications Adobe comme Illustrator, InDesign, première, After Effects et GoLive peuvent directement importer des fichiers PSD en préservant de nombreuses fonctionnalités Photoshop. Pour plus de détails, consultez l'aide de ces applications Adobe [5].

1.4.2 Formats d'image vectorielle :

1.4.2.1 PICT(Picture) :

Le format PICT est un format vectoriel interne au fonctionnement du Macintosh. C'est le format utilisé par le Presse-papiers du Macintosh. Il peut contenir des éléments graphiques ou des images numérisées. Ce format a quelques problèmes au niveau de la gestion de la séparation des couleurs, étape nécessaire à l'impression couleur [3].

1.4.2.2 PS (PostScript) :

Avec la majorité des applications d'aujourd'hui, autant les logiciels de mise en pages, de traitement de textes et autres, il est possible d'exporter un document en format PS (PostScript) lequel pourra être acheminé vers un périphérique d'impression. Ce format est également une façon sûre de rendre disponible un document seulement pour impression sans droit de modification. Il s'agit toutefois d'un format très lourd à éviter lorsqu'il doit être transféré par Internet sur des liens à basse vitesse [3].

1.4.2.3 DXF :

Le format DXF est un format vectoriel créé par la compagnie AutoDesk pour son logiciel de CAO AUTOCAD. Bien qu'étant un format très répandu dans le monde de la conception et du dessin assisté par ordinateur, le format DXF est très peu répandu en d'autres domaines [3].

1.4.2.4 WPG :

Le format WPG est un format utilisé par les logiciels de la gamme de WordPerfect (WordPerfect, DrawPerfect, WP Présentations et autres) sous DOS, Windows ou Macintosh. C'est un format vectoriel qui donne un résultat acceptable lors de l'impression, mais qui doit surtout être utilisé en tant que format de travail. D'autant plus que ce n'est pas un format qui est reconnu par tous les logiciels [3].

1.5 Les caractéristiques d'une image numérique :

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants :

1.5.1 Pixel :

On appelle "définition" le nombre de pixels constituant l'image, c'est-à-dire sa « dimension informatique » (le nombre de colonnes de l'image que multiplie son nombre de lignes). Une image possédant 640 pixels en largeur et 480 en hauteur aura une définition de 640 pixels par480, notée 640 x 480

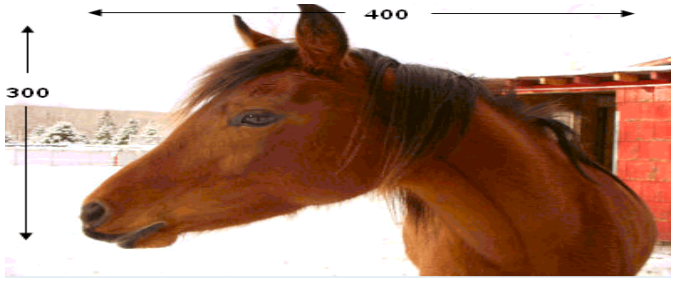


Figure 1.4: image qui a une définition de 400 pixels de largeur sur 300 pixels de hauteur..

Une image numérique est composée d'une grille de pixels. Ces pixels sont autant de petits carrés porteurs d'une information de couleur élémentaire. Notre image en comprend donc 400 x 300, soit 120 000 pixels [6].

1.5.2 Résolution :

La résolution, terme souvent confondu avec la "définition", détermine par contre le nombre de points ou pixels par unité de surface, exprimé en *points par pouce* (PPP, en anglais DPI pour *Dots Per Inch*); un pouce représentant 2.54 cm [6].

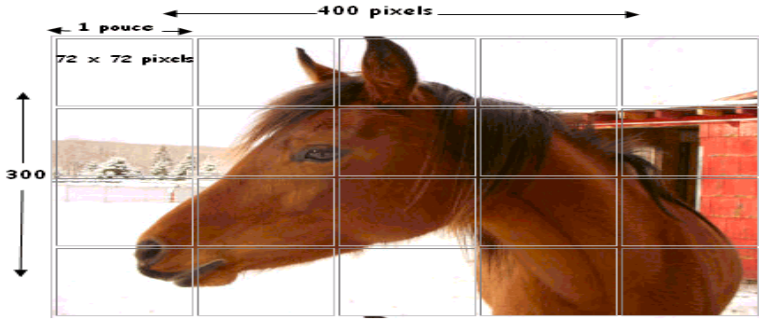


Figure 1.5: image montrant La résolution

La résolution permet ainsi d'établir le rapport entre le nombre de pixels d'une image et la taille réelle de sa représentation sur un support physique (impression d'une photo). Une résolution de 300 dpi signifie donc 300 colonnes et 300 rangées de pixels sur un pouce carré ce qui donne donc 90 000 pixels sur un pouce carré [6].

1.5.3 Son poids :

Pour connaître le poids (en octets) d'une image, il est nécessaire de compter le nombre de pixels que contient l'image, cela revient à calculer le nombre de cases du tableau, soit la hauteur de celui-ci que multiplie sa largeur. Le poids de l'image est alors égal à son nombre de pixels que multiplie le poids de chacu de ces éléments.
Le poids de l'image est alors égal à son nombre de pixels que multiplie le poids de chacun de ces éléments.

Voici le calcul pour une image 640x480 en *True color* :

Nombre de pixels: 640 x 480 = 307 200 pixels

Poids de chaque pixel: 24 bits / 8 = 3 octets (1 octet = 8 bits)

Le poids de l'image est ainsi égal à : 307 200 x 3 = 921 600 octets / 1024 = 900 Ko

(Pour connaître la taille en Ko il suffit de diviser par 1024) [6].

1.5.4 Son codage de la couleur :

Une image est donc représentée par un tableau à deux dimensions dont chaque case est un pixel. Pour représenter informatiquement une image, il suffit donc de créer un tableau de pixels dont chaque case contient une valeur. La valeur stockée dans une case est codée sur un certain nombre de bits déterminant la couleur ou l'intensité du pixel, on l'appelle profondeur de codage (parfois *profondeur de couleur*) [6].

Les images informatisées se présentent en plusieurs niveaux de couleurs :

Tableau 1:présente en plusieurs niveaux de couleurs

Niveau	Couleurs
1 bit	2 (noir et blanc)
4 bits	16 couleurs (16 dégradés de gris allant du noir au blanc ou bien 16 couleurs différentes)
8 bits	256 couleurs ou nuances de gris (256 dégradés de gris allant du noir au blanc ou bien 256 couleurs différentes)
16 bits	65 536 couleurs (16 dégradés de gris allant du noir au blanc ou bien 16 couleurs différentes)
24 bits ou vraies couleurs	16 777 216 couleurs (cette représentation permet de représenter une image en définissant chacune des composantes (RGB, pour rouge, vert et bleu). Chaque pixel est représenté par un entier comportant les trois composantes, chacune codée sur un octet, c'est-à-dire au total 24 bits)
30 bits	1 073 741 824 couleurs

Certains numériseurs numérisent les images en couleurs à 24 bits par défaut. Il peut être alors utile de diminuer le niveau de couleurs.

À moins de faire de la retouche photographique, vous n'aurez pas souvent besoin des niveaux 24 ou même 16 bits. Faites des essais à 8 bits : vous pourriez avoir de bonnes surprises [6].

1.6 Taille d'une image - compression d'images :

La description que nous avons faite concerne certains formats d'images, dont le bitmap (Bmp). Ce sont des images numériques non compressées. La taille en octets d'une telle image RVB 24 bits s'obtient en multipliant le nombre total de pixels de l'image par 3 (car 3 octets par pixels). Par exemple, une image, la couleur, 24 bits non compressés de pixels a pour taille 1 440 000 octets (+ en-tête du fichier), soit 1,37 Mio environ. Pour rappel, Mio est un mébioctet et on a.

De manière générale, la taille (en octet) d'une image non compressée correspond au produit de sa définition par le nombre d'octets par pixel.

Lors de la transmission d'images (mail, pages Internet, …), on peut préférer des images compressées. À l'aide d'algorithmes mathématiques, les données sont compactées afin que le fichier soit moins gros. Pour une image compressée, l'enjeu est de trouver un compromis entre sa qualité (aspect visuel) et sa taille [7].

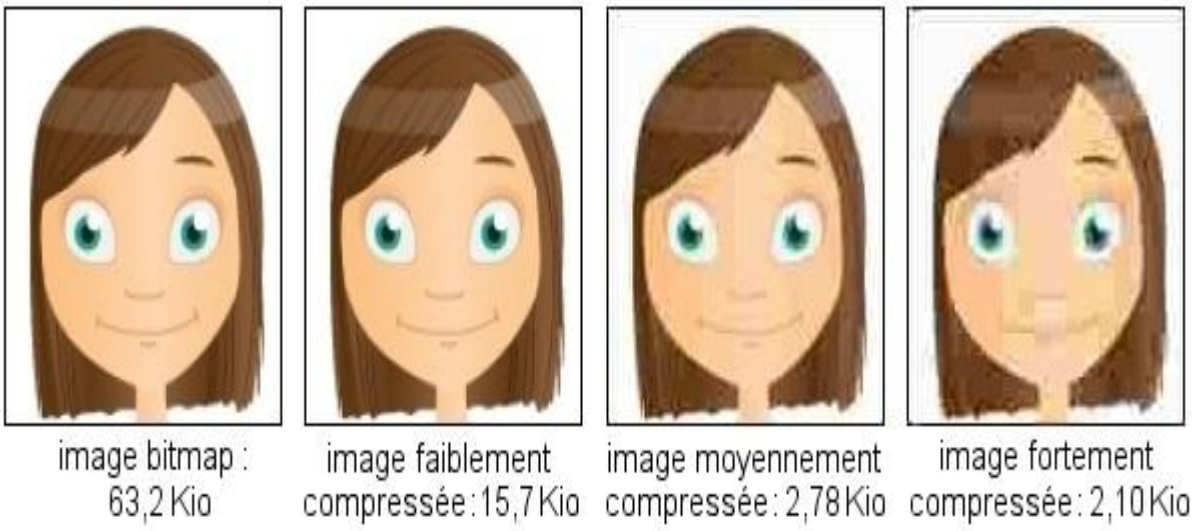


Figure 1.6: Image la représentation la taille (en octet).

Remarque : Kio signifie kibioctet et $1\,\text{Kio} = 2^{10}\,\text{octets}$.

1.7 Propriétés des images numériques :

• Les images numériques ne vieillissement pas (elles sont la pure information), contrairement à des images imprimées. En effet, du moment que le fichier n'est pas altéré, il conserve l'information sans modification dans le temps.

• L'échange de fichiers image est facile par les moyens courants de communication : mail, etc.

• La plupart des formats image mis à disposition du public sont aisément lisibles par les ordinateurs et assimilés (portables, …).

• Une image numérique peut être modifiée par des logiciels dédiés. Certains sont accessibles pour un utilisateur non-spécialiste.

• En sciences, la numérisation de l'image donnée par un capteur optique peut être exploitée pour en tirer des informations : acquisition de spectres (spectre UV-Visible) [7].

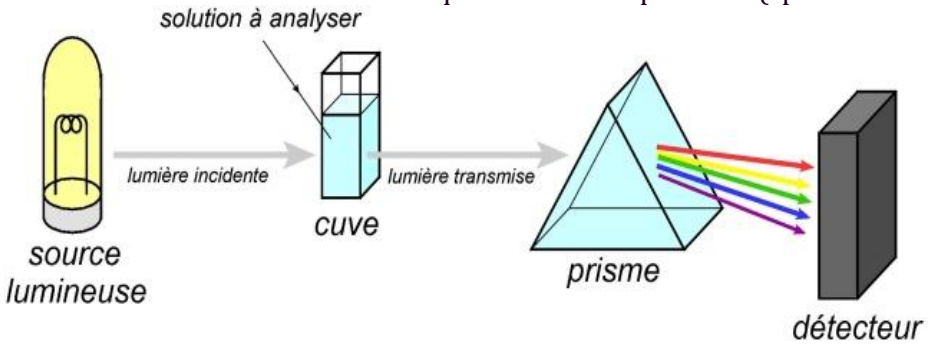


Figure 1.7:Exemple de spectre UV-Visible

• Le plus gros défaut visuel d'une image numérique matricielle est sa pixellisation, en particulier pour des images comportant peu de pixels (petits fichiers) [7].

1.7.1 Histogramme :

L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image. Il permet de donner un grand nombre d'information sur la distribution de ces niveaux et de voir entre quelles bornes sont reparties dans le cas d'une image trop claire ou d'une image trop foncée.

Il peut être utilisé pour améliorer la qualité d'une image (rehaussement d'image) en introduisant quelques modifications, pour pouvoir extraire les informations utiles de celle-ci[8].

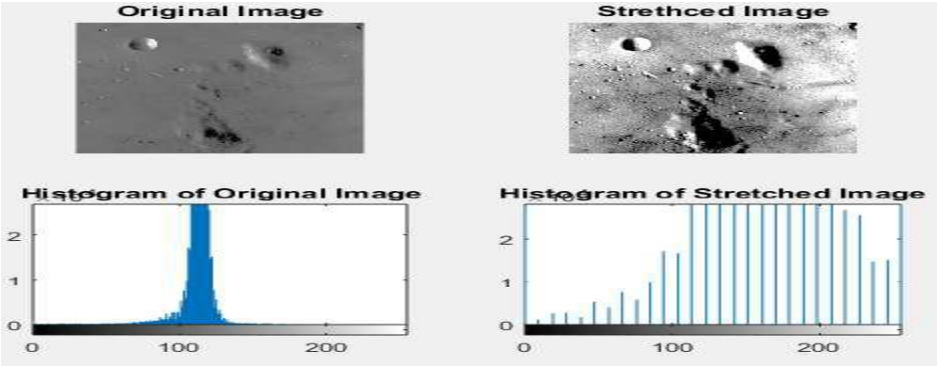


Figure 1.8:Exemple d'histogramme d'une Image.

1.7.2 Luminance :

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, pour un observateur lointain, le mot luminance est substitué au mot brillance.

Figure 1.9:Exemple de luminance.

1.8 Traitement d'images :

Le traitement d'images est une discipline de l'informatique et des mathématiques appliquées qui étudie les images numériques et leurs transformations, dans le but d'améliorer leur qualité ou d'en extraire de l'information.

Il s'agit d'un sous-ensemble du traitement du signal dédié aux images et aux données dérivées comme la vidéo (Par opposition aux parties du traitement du signal consacrées à d'autres types de données : son et autres signaux monodimensionnelle notamment), tout en opérant dans le domaine numérique (par opposition aux techniques analogiques de traitement du signal, comme la photographie ou la télévision traditionnelles).

Dans le contexte de la vision artificielle, le traitement d'images se place après les étapes d'acquisition et de numérisation, assurant les transformations d'images et la partie de calcul permettant d'aller vers une interprétation des images traitées. Cette phase d'interprétation est

d'ailleurs de plus en plus intégrée dans le traitement d'images, en faisant appel notamment à l'intelligence artificielle pour manipuler des connaissances, principalement sur les informations dont on dispose à propos de ce que représentent les images traitées (connaissance du « domaine »).

La compréhension du traitement d'images commence par la compréhension de ce qu'est une image. Le mode et les conditions d'acquisition et de numérisation des images traitées conditionnent largement les opérations qu'il faudra réaliser pour extraire de l'information. En effet, de nombreux paramètres entrent en compte, les principaux étants :

• la résolution d'acquisition et le mode de codage utilisé lors de la numérisation, qui déterminent le degré de précision des éventuelles mesures de dimensions ;

• les réglages optiques utilisés (dont la mise au point) qui déterminent par exemple la netteté de l'image ;

• les conditions d'éclairage, qui déterminent une partie de la variabilité des images traitées ;

• le bruit de la chaîne de transmission d'image.

Quelques exemples types d'informations qu'il est possible d'obtenir d'une image numérique :

• la luminance moyenne ;

• le contraste moyen ;

• la couleur prédominante ;

• le taux d'acuité moyen (précis ou flou) ;

• le taux d'uniformité des couleurs ;

• la présence ou l'absence de certains objets

• D'après P.G. Frija, P.B. Mazoyer ''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 [9].

1.9 Les techniques d'imagerie médicale :

1.9.1 Radiologie :

D'après P.G. Frija, P.B. Mazoyer [10].''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. '' [10].

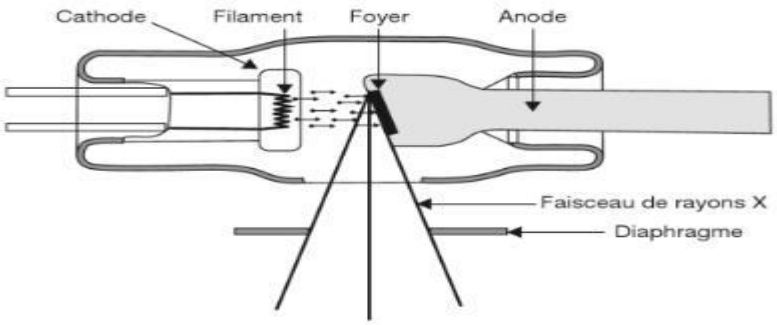


Figure 1.10: Illustre un schéma d'un tube à rayons X [10].

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 ...).

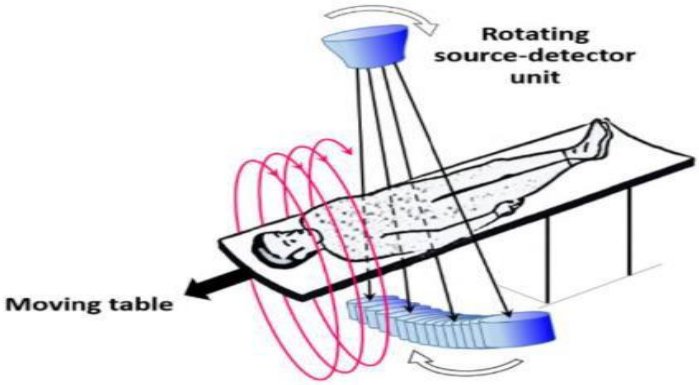


Figure 1.11:Géométrie d'un scanner [12].

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 [10].

Figure 1.11 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 [13].

Il est largement utilisé pour les femmes enceintes, comme il est indiqué au Figure 1.12 [14].

Figure 1.12:Echotomographie abdominale [15].

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 [12].

La Figure 1.13 représente une mammographie d'un sein de femme à cancer (la masse suspecte).

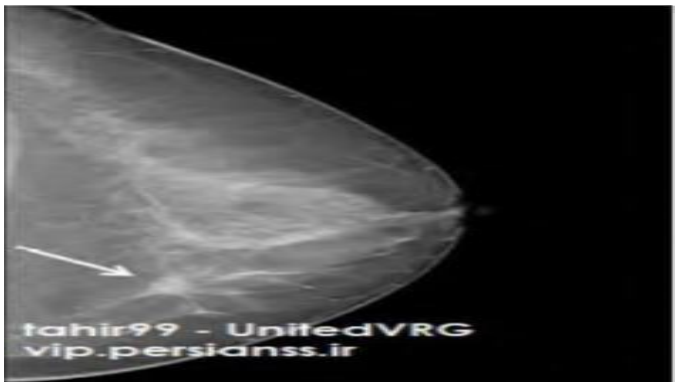


Figure 1.13:Mammographie d'un sein de femme à cancer (la masse suspecte)[12].

1.9.5 Imagerie par résonnance 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) [16].

La Figure 1.14 représente un scanner d'IRM.

Figure 1.14:Scanner d'IRM [17].

Grâce aux détecteurs ultra-sensibles (des SQUID) fonctionnant à très basse température, il est possible de prendre des photos dans des zones très faibles [17].

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 [18].

1.11 Conclusion :

Dans ce chapitre, nous avons pressentes les images numériques d'une maniére générale. Nous nous sommes intéressé aux terminologies et aux notions pertinentes dans le domaine des images numériques telles que la numérisation, le codage, le stockage. Nous avons engagement pressentes quelques aspects du traitement d'image, tels que le filtrage, la compression et le tatouage, et c'est ce dernier qui est pressentes le long de ce me moire.

Chapitre 02 :
TATOUAGE NUMÉRIQUE

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'images numériques, et le tatouage numérique ici l'une des solutions de ce problème [19].

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. Ensuit-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 et imperceptible disparaître après la modification de contenu du document [20].

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 [21].

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 général dans le domaine spatial ou fréquentiel.

2.4 Techniques numériques pour la protection des données :

Trois techniques interviennent dans la transmission des informations de manière secrète : la cryptographie, la stéganographie et le tatouage. Dans les trois cas, il s'agit de transmettre une information afin qu'elle soit inintelligible par une personne non autorisée ; la cryptographie et la stéganographie ont été utilisées avant le commencement de notre ère à des fins militaires. Elles font partie des sciences du secret. Le tatouage de document est un domaine beaucoup plus récent qui s'apparent à la stéganographie.

Cette section a pour but de détailler ces différents domaines en précisant les similitudes et les complémentarités.

2.4.1 La cryptographie :

La cryptographie est une méthode de protection des informations et des communications par l'utilisation de codes, de sorte que seuls les destinataires des informations puissent les lire et les traiter. Le préfixe « crypt » signifie « caché » ou « coffre-fort » et le suffixe « -graphie » signifie « écriture ».

En informatique, la cryptographie désigne des techniques d'information et de communication sécurisées dérivées de concepts mathématiques et d'un ensemble de calculs basés sur des règles, appelés algorithmes, pour transformer les messages de manière difficile de déchiffrer. Ces algorithmes déterministes sont utilisés pour la génération de clés cryptographiques, la signature numérique, la vérification pour protéger la confidentialité des données, la navigation sur Internet et les communications confidentielles telles que les transactions par carte de crédit.et le courrier.

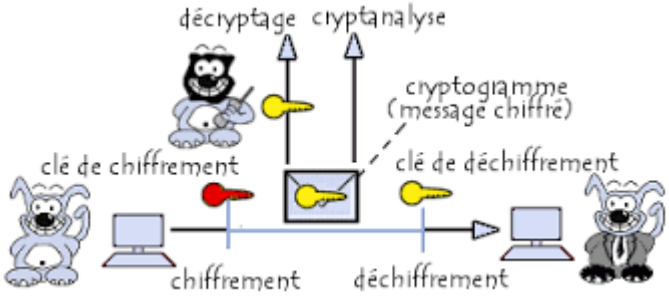


Figure 2.15: Exemple de la cryptographie.

2.4.2 La stéganographie :

La stéganographie est un domaine où l'on cherche à dissimuler discrètement de l'information dans un média de couverture (typiquement un signal de type texte, son, image, vidéo, etc...). Elle se distingue de la cryptographie qui cherche à rendre un contenu inintelligible à autre que qui-de-droit Lorsqu'un acteur extérieur regarde un contenu cryptographie, il peut deviner la nature sensible de l'information qui lui est cachée. L'intérêt de la stéganographie réside précisément dans la possibilité de communiquer en échangeant des contenus d'apparences anodines de telle sorte à ne pas éveiller de soupçons.

Pour prendre une métaphore, la stéganographie consisterait à enterrer son argent dans son jardin là où la cryptographie consisterait à l'enfermer dans un coffre-fort — cela dit, rien n'empêche de combiner les deux techniques, de même que l'on peut enterrer un coffre dans son jardin [23].

Figure 2.16: Exemple de la stéganographie.

2.4.3 Le tatouage d'images :

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 général dans le domaine spatial ou fréquentiel.

2.5 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 [25].

Le robuste : le système de tatouage devrait être robuste contre plusieurs attaques [25].

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 [25].

Figure1.17 représente des propriétés du tatouage numérique [25].

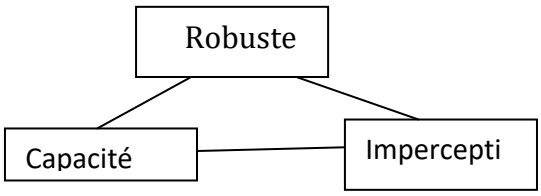


Figure 2.17:Propriétés du tatouage numérique [19].

2.5.1 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 [26].

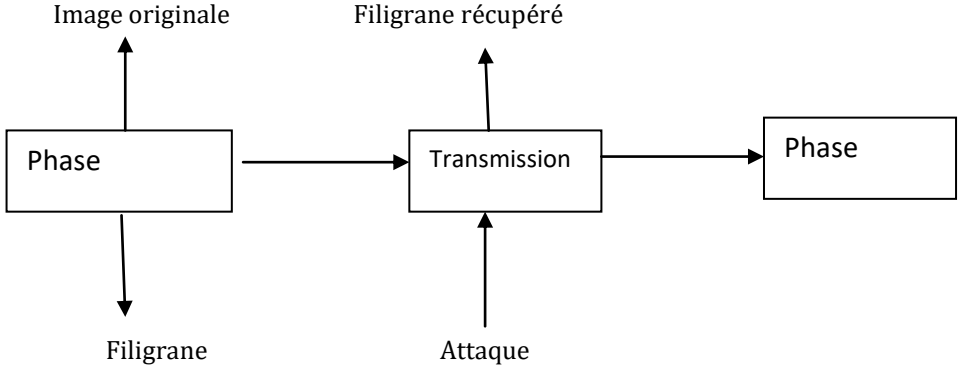


Figure 2.18:Schéma général d'un système de tatouage numérique des images [25].

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.

Figure1.18 au-dessus, représente un schéma général d'un système de tatouage numérique des images.

2.5.1.1 Phase d'insertion :

De la marque, consiste à insérer dans l'image originale I, une marque M et ainsi créer une nouvelle image appelée image tatouée Iw Un troisième paramètre facultatif peut être ajouté la clé secrète de marquage Cm qui permet d'assurer un certain niveau de sécurité au processus de tatouage, comme indiqué sur la Figure 1.19.

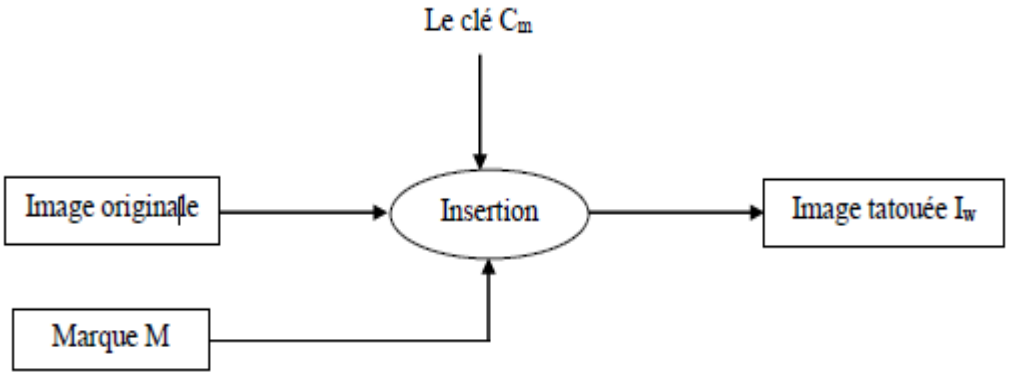


Figure 2.19:Schéma général de l'insertion d'une marque [27].

2.5.1.2 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.

Figure 1.20 illustre un schéma général d'extraction non-aveugle d'une marque.

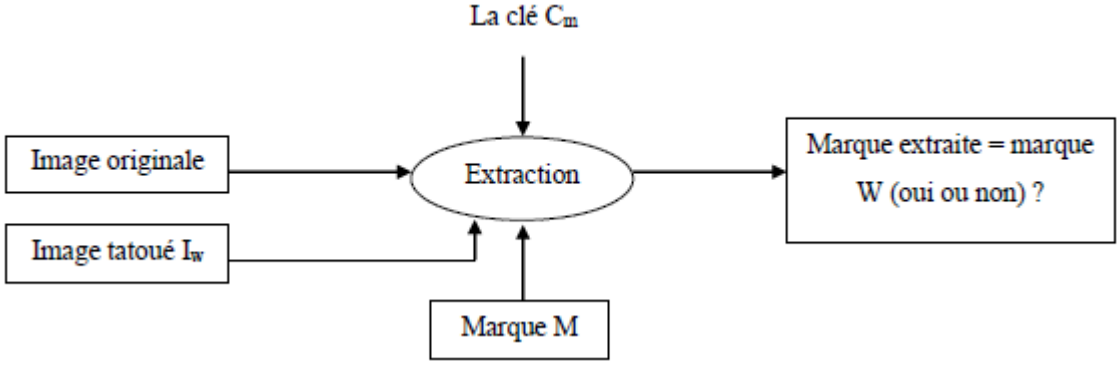


Figure 2.20: Schéma général d'extraction non aveugle d'une marque [27].

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 est nombreux [27].

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 [20].

La marque doit être invisible, mais aussi la plus résistant possible, car il est utilisé pour parer le piratage de données [28].

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, tel que son numéro d'identification [29].

2.6.3L'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 [28].

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 [29].

2.7 Les attaque :

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.

2.7.1 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...) [38].

2.7.2 Attaques géométriques :

Toutes les manipulations qui affectent la géométrie de l'image (déformer ou déplacer l'image tatouée) telle 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 [29].

2.7.3 Attaques cryptographiques :

Les attaques cryptographiques traitent de la fissuration de la sécurité. L'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 [29].

2.7.4 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 oeuvre 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 [29].

2.8 Classification des algorithmes du tatouage numérique :

Les méthodes du tatouage numérique peuvent être classées en différentes catégories : selon le type de données (texte, image, audio, vidéo), la perceptibilité du watermark, le domaine d'insertion, la robustesse, la méthode de cryptage utilisé, le processus d'insertion et le processus d'extraction [30].

Dans les sous-sections suivantes, les catégories de base des méthodes de tatouage sont discutées :

2.8.1 Classification selon le type du support hôte :

La méthode du tatouage peut être classée selon le support hôte dans lequel le watermark est inséré : tatouage du texte, d'image, d'audio ou de vidéo. Dans le tatouage audio, image et vidéo, le watermark peut être inséré dans les coefficients de basse ou de haute fréquence du domaine fréquentiel ou peut être inséré dans les bits les moins significatifs de données spatiales LSB [31,32].

Dans le tatouage du texte, les espaces entre les lignes, les espaces entre les caractères, les espaces après la ponctuation, et les espaces à la fin des phrases sont utilisés pour insérer le watermark [31].

2.8.2 Classification selon la perceptibilité de watermark :

En se basant sur la perception humaine, les méthodes du tatouage numérique sont classées en deux catégories : un tatouage visible et invisible [31].

2.8.2.1Tatouage visible :

Dans les méthodes du tatouage visible, le watermark est inséré dans les données originales d'une manière d' être perceptible à l'oeil humain. Le tatouage visible est utilisé principalement pour insérer un logo ou une marque commerciale, pour indiquer la propriété des données et pour confirmer l'authentification. Cette méthode de tatouage est fragile aux attaques [31].

Hu et Jeon [33], Yip [34] et Tsai [35] ont proposé des méthodes de tatouage numérique visible.

2.8.2.2 Tatouage invisible :

Dans le tatouage invisible, le watermark est inséré dans les données originales de manière à être imperceptible à l'oeil humain. Il est utilisé pour plusieurs raisons telles que l'identification de la propriété, l'authentification et vérification de l'intégrité [31].

Vongpradhip et Rungraungsilp [36], Karthigaikumar et al. [48] et Sathik et Sujatha [38] ont proposé des méthodes de tatouage numérique invisible.

2.8.3 Classification selon le domaine d'insertion :

Selon le domaine d'insertion du watermark, les méthodes du tatouage numérique peuvent être classées en deux catégories : méthodes conçues dans le domaine spatial et méthodes conçues dans le domaine fréquentiel [30].

2.8.3.1 Domaine spatial :

Dans le domaine spatial, le watermark est chargé directement dans les valeurs des pixels des données originales. Les algorithmes conçus dans ce domaine offrent une large capacité

d'insertion, et par conséquent, ils permettent d'insérer plusieurs copies du watermark pour fournir une robustesse supplémentaire contre les différentes attaques, afin que la possibilité de supprimer tous les copies du watermark devienne faible. Les techniques d'insertion du watermark dans le domaine spatial sont les techniques des bits les moins significatifs LSB et les techniques à modulation de spectre étalé SS (Spread Spectrum) [39,30].

Wu et al. [40], Su et al. [41] et Su et Chen [42] ont proposé des méthodes de tatouage numérique conçues dans le domaine spatial.

2.8.3.2 Domaine fréquentiel :

Dans le domaine fréquentiel ou domaine de transformation, le watermark peut être inséré dans les coefficients des fréquences. Les transformations les plus utilisées sont la décomposition en valeurs singulières SVD (Singular Value Decomposition), la transformée en cosinus discrète DCT (Discrete Cosine Transform), la transformée en ondelettes discret DWT (Discrete Wavelet Transform) [41]. Vongpradhip et Rungraungsilp [36], Karthigaikumar et al. [37] et Sathik et Sujatha [38] ont proposé des méthodes de tatouage numérique conçues dans le domaine fréquentiel.

2.8.4 Classification selon la robustesse :

Les méthodes de tatouage peuvent être classées selon leur résistance aux modifications issues d'opérations de traitement de signal du support hôte, ou aux différentes attaques qui sont des modifications qui visent à détruire le watermark ou d'affecter la fiabilité d'un système de tatouage. Cette résistance est appelée robustesse [43].

Selon le niveau de robustesse, on peut distinguer les trois catégories du tatouage suivantes :

2.8.4.1Tatouage robuste :

Dans un tatouage robuste, le watermark est conçu de manière à résister aux attaques et aux manipulations du support hôte tels que la compression avec perte, le filtrage et les distorsions géométriques (rotation, mise à l'échelle, etc). Mais, en pratique, aucun schéma de tatouage ne peut résister à tous les types des attaques [43].

Les méthodes du tatouage robuste sont utilisées dans les applications de preuve de propriété, la surveillance de la diffusion, le suivi des transactions et le contrôle de la copie [43].

Liu et al. [44], Wu et al. [40] et Su et Chen [42] ont proposé des méthodes de tatouage numérique robuste.

2.8.4.2 Tatouage fragile :

Dans un tatouage fragile, le watermark peut être facilement détruit par toute modification malveillante ou non malveillante. Pour cela, le watermark est conçu de manière à être fragile à toute sorte d'attaque malveillante telle que le copier-coller et la quantification vectorielle VQ (Vector Quantization) et les attaques non malveillantes telles que la compression avec perte, la mise à l'échelle et la transformation fréquentielle d'images. La destruction ou la perte du watermak implique une altération [30].

Généralement, les méthodes du tatouage fragile sont utilisées pour les applications d'authentification et de vérification de l'intégrité du contenu.

Elles ne sont demandées que dans les applications sensibles telles que les applications militaires, lesapplications d'images médicales et les applications d'image satellite [30].

Chen et Wang [45], Rawat et Raman [46] et Singh et Singh [47] ont proposé des méthodes de tatouage numérique fragile.

2.8.4.3 Tatouage semi-fragile :

Les méthodes du tatouage semi-fragiles combinent les caractéristiques de tatouage fragile et robuste, elles sont des méthodes robustes à un certain ensemble de manipulations ou attaques

qui sont considérées comme légitimes et autorisées telle que la compression avec pertes, et au même temps fragiles contre d'autres attaques. Ces méthodes du tatouage peuvent être utilisées dans des cas d'authentification au lieu des méthodes fragiles [43].

Ho et Li [48] et Qi, et Xin [49] [50] ont proposé des méthodes de tatouage numérique semi-fragile.

2.8.5 Classification selon la méthode de cryptage :

L'insertion et l'extraction du watermark sont généralement contrôlées par une clé privée ou publique afin d'augmenter le niveau de sécurité [43]. Les méthodes de tatouage peuvent être classées en deux groupes selon la clé utilisée pendant les processus d'insertion et l'extraction du watermark.

2.8.5.1 Méthodes symétriques ou méthodes à clé privée :

Dans ces méthodes, la même clé est utilisée pour insérer et détecter le watermark [43].

2.8.5.2 Méthodes asymétriques ou méthodes à clé publique :

Contrairement aux méthodes symétriques, dans le processus de détection, ces schémas utilisent une clé différente de celle utilisée lors du processus d'insertion. Une clé privée est utilisée pour l'insertion, et une autre clé publique pour la détection. Des nombreuses clés publiques peuvent être produites pour chaque clé privée. Ces schémas asymétriques sont difficiles à concevoir [43].

2.8.6 Classification selon le processus d'insertion :

Les méthodes de tatouage peuvent être classées en deux catégories selon les informations prises en compte lors du processus d'insertion du watermark :

2.8.6.1 Schémas d'insertion aveugle :

Dans un schéma aveugle, les données du signal hôte sont considérées comme un bruit ou une interférence [43].

Donc, le tatouage est considéré comme un problème de communication classique de la transmission du signal sur un canal bruité. Mais, dans le cas du tatouage, les restrictions sur des distorsions imposées au support hôte par le watermark doivent être prises en considération [43].

2.8.6.2 Schémas d'insertion informée :

Lors de l'insertion dans les schémas d'insertion informée, les données de signal hôte sont connues. La connaissance des données de l'hôte peut être utilisée pour améliorer les performances d'extraction du watermark. Elles considèrent le tatouage, au niveau de l'émetteur, comme un problème de communication avec des informations secondaires, ces méthodes sont aussi appelées méthodes d'état de l'hôte connu [43].

2.8.7 Classification selon la qualité d'image tatouée :

Selon la qualité d'image tatouée, le tatouage peut être classé en deux groupes : tatouage réversible et irréversible [30].

2.8.7.1 Schémas de tatouage irréversible :

Dans les schémas de tatouage irréversible ou non-inversible, les modifications de l'image originale lors de processus d'insertion du watermark reste d'une façon permanente, malgré que ces modifications soient souvent insignifiantes [30].

Notez que certaines applications sensibles et de grande importance ne peuvent pas utiliser ces schémas de tatouage, tels que les applications d'images militaires, juridiques et médicales, où toute petite distorsion est difficile à accepter [30].

2.8.7.2 Schémas du tatouage réversible :

Au contraire des schémas irréversible, après l'extraction du watermark, le tatouage réversible (inversible) permet de récupérer le signal original, tous en supprimant le watermark

et en restaurant les données originales qui sont écrasées lors du processus d'insertion du watermark [30]. Les méthodes de tatouage réversibles sont appropriées aux applications d'authentification et les applications militaires et médicales [30].

2.8.8 Classification selon le processus d'extraction :

Selon les ressources requises au processus d'extraction pour extraire le watermark , les méthodes de tatouage peuvent être classées en trois catégories :

2.8.8.1 Schémas du tatouage non aveugle :

Ces méthodes nécessitent la disponibilité du signal original ou certaines informations liées à ce signal original pendant la phase d'extraction du watermark.

Ces schémas sont considérés comme les méthodes du tatouage les plus robustes, mais leurs applications sont limitées, car la disponibilité des données originales n'est pas toujours garantie [30, 51].

2.8.8.2 Schémas du tatouage semi-aveugle :

Dans les méthodes du tatouage semi-aveugle, la phase d'extraction nécessite le watermark original et la clé pour extraire le watermark [30].

2.8.8.3 Schémas du tatouage aveugle :

Les éthodes du tatouage aveugle ne nécessitent que l'image tatouée et la clé secrète pour la détection du watermark, elles ne requièrent pas la dis [30].

2.9 Conclusion :

Dans ce chapitre, nous avons présenté 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:
Conception et implémentation d'un tatouage fragile par LSB replacement

3.1 Introduction:

Dans ce chapitre, nous introduisons un algorithme pour Tatouage les images en niveaux de gris et concluons qu'il fonctionne bien. La technique de Tatouage fragile t'est efficace pour les types de bruit à haute énergie et à basse pression (JPEG). En revanche, dans le cas des filtres et des distorsions géométriques, on ne voit pas l'efficacité de la technologie utilisée (l'effet de la technologie est nul).

3.2 Environnement de travail:

3.2.1 Matériel:

Afin de mener à bien ce projet, nous avons utilisé un ensemble de matériaux dont les principales caractéristiques qui sont les suivants :

Fabricant : acer
Évaluation : 5.1 Indice de performance Windows
Processeur : Intel (R) Core (TM) i3-4005U @ 1,70 GHz.
RAM : 4,00 Go
Type de système : système d'exploitation 64 bits.

3.2.2 Logiciel :

3.2.2.1 Langage de programmation MATLAB :

MATLAB (forme abrégée de "Matrix Laboratory") est un programme informatique ou de programmation langage qui offre à l'utilisateur un environnement pratique pour effectuer de nombreux types de calculs et calculs techniques. Il intègre la visualisation, le calcul et la programmation dans un environnement facile à utiliser [52].

Il est utilisé pour résoudre de nombreux problèmes techniques nécessitant des formulations matricielles et vectorielles, en outre, il est généralement utilisé pour résoudre des équations différentielles et c'est un moyen efficace et peut être considéré comme facile et rapide. Les utilisations typiques de MATLAB sont les suivantes :

• Calcul et mathématiques.

• Analyse, visualisation et exploration des données.

• Modélisation et simulation d'algorithmes.

• Calculs scientifiques.

• Applications de traitement d'images.

• Développement d'applications.

• Fenêtre MATLAB

Lorsque MATLAB est exécuté, la fenêtre ci-dessous apparaît. L'environnement MATLAB est divisé en 4 fenêtres :

Fenêtre de commande : il s'agit de la fenêtre principale. Il contient une invite de commande (>>). Le lieu où l'utilisateur tape toute la commande.

Espace de travail : il répertorie toutes les variables que le programme ou l'utilisateur a générées dans la session en cours, dans en plus du type et de la taille de la variable.

Historique des commandes : affiche la liste des commandes précédemment saisies.

Répertoire actuel : affiche les fichiers et les dossiers du répertoire actuel [53].

3.3 PSNR :

Le bloc PSNR calcule le rapport signal/bruit de crête, en décibels, entre deux images. Ce rapport est utilisé comme mesure de qualité entre l'original et une image compressée. Plus le PSNR est élevé, meilleure est la qualité de l'image compressée ou reconstruite.

Pour calculer le PSNR, le bloc calcule d'abord l'erreur quadratique moyenne à l'aide de l'équation suivante :
EQM =∑M, N [I1 (m, n) −I2 (m, n)] 2M∗N
Dans l'équation précédente, M et N sont le nombre de lignes et de colonnes dans les images d'entrée. Ensuite, le bloc calcule le PSNR à l'aide de l'équation suivante :
PSNR=10log10 (R2/MSE) [55]. R=255.

3.4 SSIM :

La méthode de l'indice de similarité structurelle est un modèle basé sur la perception. Dans cette méthode, la dégradation de l'image est considérée comme le changement de perception des informations structurel. Il collabore également avec d'autres faits importants basés sur la perception tels que le masquage de luminance, le masquage de contraste, etc. Le terme informations structurel met l'accent sur les pixels fortement interdépendants ou les pixels spatialement fermés. Ces pixels fortement interdépendants renvoient à des informations plus importantes sur les objets visuels dans le domaine de l'image. le masquage de contraste est un terme où les distorsions sont également moins visibles dans la texture d'une image. SSIM estime la qualité perçue des images et des vidéos.

SSIM=

$$SSIM(x,y) = l(x,y).c(x,y).s(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_x\sigma_y + c_2)(cov_{xy} + c_3)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)(\sigma_x\sigma_y + c_3)}$$

Figure 3.21:Fenêtre PSNR et SSIM.

3.5L'organigramme de l'algorithme :

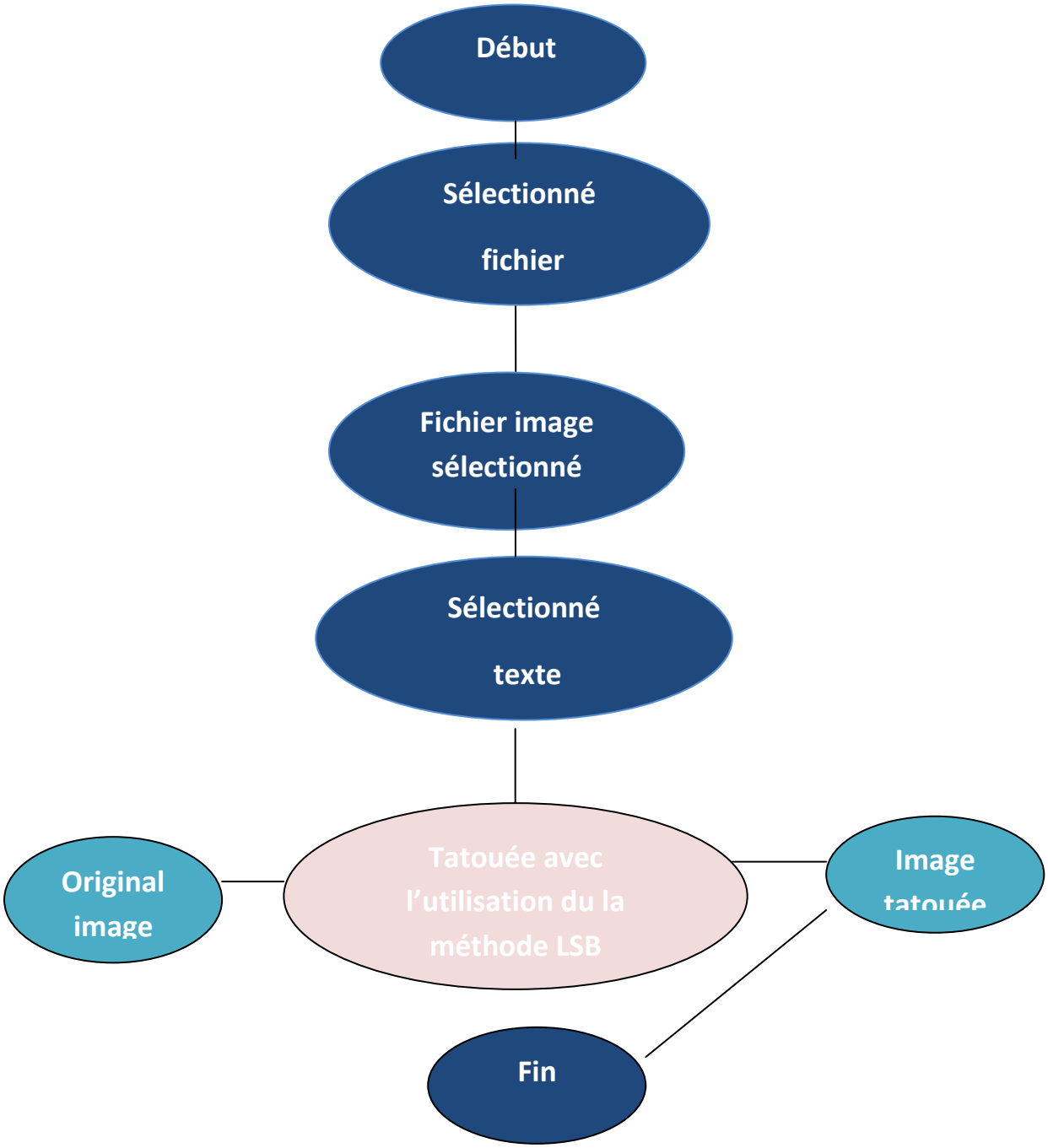


Figure 3.22: Fonctionnement générale de l'algorithme

3.6 Least Signifiant Bit Hiding Technique (LSB):

LSB signifie bit le moins significatif. L'idée derrière l'intégration LSB est que si nous modifions la dernière valeur de bit d'un pixel, il n'y aura pas beaucoup de changement visible dans la couleur. Par exemple, 0 est noir. Changer la valeur à 1 ne fera pas beaucoup de différence, car il est toujours noir, juste une nuance plus claire. L'encodage se fait en suivant les étapes suivantes :

1. Convertir l'image en niveaux de gris

2. Redimensionner l'image si nécessaire

3. Convertir le message dans son format binaire

4. Initialiser l'image de sortie comme l'image d'entrée

5. Parcourez chaque pixel de l'image et procédez comme suit :

• Convertir la valeur du pixel en binaire

• Obtenez le prochain bit du message à intégrer.

• Si le bit de message et le LSB du pixel sont identiques, définissez temps = 0.

• Si le bit de message et le LSB du pixel sont différents, définissez temps = 1.

• Ce réglage de temps peut être fait en prenant le XOR du bit de message et le LSB du pixel

• Mettre à jour le pixel de l'image de sortie pour entrer la valeur du pixel de l'image + temps

6. Continuez à mettre à jour l'image de sortie jusqu'à ce que tous les bits du message soient intégrés.

7. Enfin, écrivez l'image d'entrée ainsi que l'image de sortie sur le système local [56].

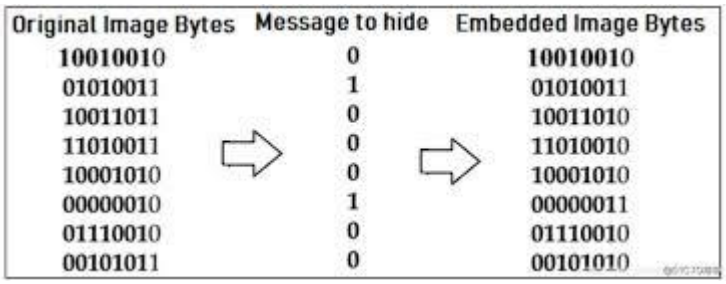


Figure 3.23:Méthode LSB

3.7 Algorithme d'insertion :

3.7.1 Entrées :

X= image de taille m × m.

3.7.2 Etapes :

1. Nous lisons l'image en niveaux de gris, puis on trouve les dimensions de la matrice.
2. Nous convertissons l'image au système binaire (Binary) afin de pouvoir changer le bon huitième bit.
3. Nous entrons le texte et le convertissons en code AScii puis en système binaire, puis nous transférons les bits de chaque caractère dans le bit LSB de l'image, et chaque caractère sera stocké dans le huitième bit de droit.
4. Maintenant, nous stockons chacun des sept bits de chaque caractère dans une ligne de l'image dans la huitième colonne qui représente LSB

5. Nous passons au bit opposer dans le deuxième mot et continuons jusqu'à la dernière lettre, puis revenons au deuxième bit avec le premier mot, puis au deuxième bit avec le deuxième mot et continuons.
6. Maintenant, nous cachons le texte à l'intérieur de l'image, puis nous convertissons l'image de binaire en décimale et ramenons les dimensions de la matrice à ses dimensions initiales.
7. Nous dessinons l'image avant et après y avoir stocké le texte.

3.7.3 Sortie :

Image tatouée de taille m × m.

3.8 Déroulement de L'application :

• En cas d'insertion, l'utilisateur choisit l'image qu'il souhaite tatouer en cliquant sur Cliquez sur le bouton "Télécharger votre photo".
• Sélectionne le texte à masquer en cliquant sur le bouton "Charger le texte".
• Ajoutez ensuite le tag (texte ou image) en entrant le texte dans la zone de texte ou de téléchargement.
• Image en cliquant sur le bouton "Télécharger votre marque".
• Ensuite, pour appliquer la méthode LSB, l'utilisateur clique sur le bouton "Tatoue" après avoir enregistré l'image tatouée.

3.9 Résultat :

Pour évaluer notre application, nous présentons l'exécution de cet exemple :

3.10 Phase d'insertion :

L'algorithme d'insertion génère l'mage tatoué en utilisent l'image hôte x et le water mark w. Il est la modalité par la fonction d'insertion E suivante :

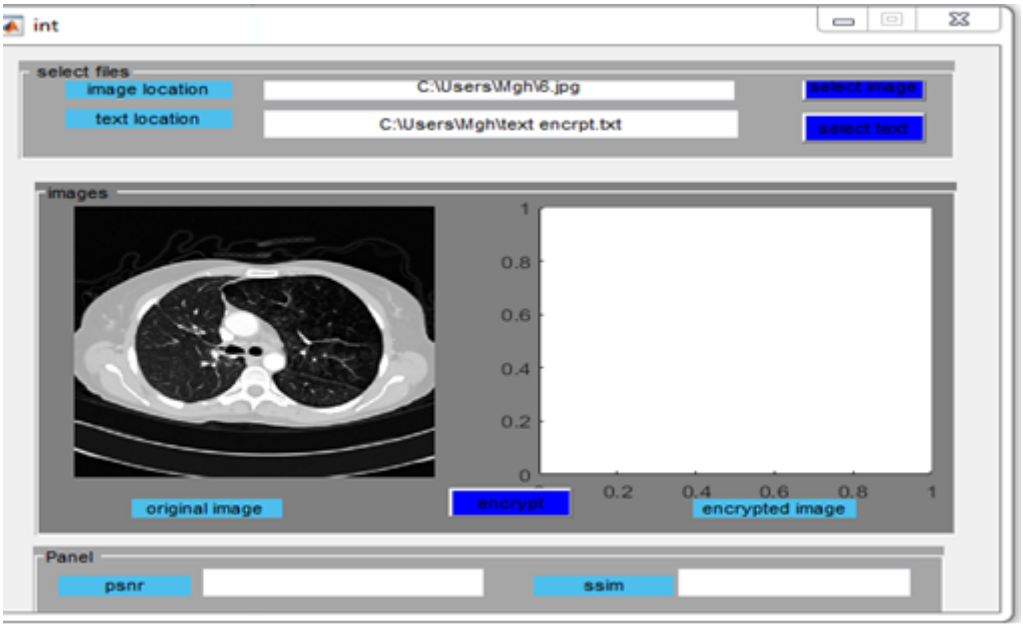


Figure 3.24:Chargement de l'image original et la marque.

Pour saisir du texte dans l'image, cliquez sur le bouton "Tatouage". Le résultat J'ai eu ceci est la photo tatouée.

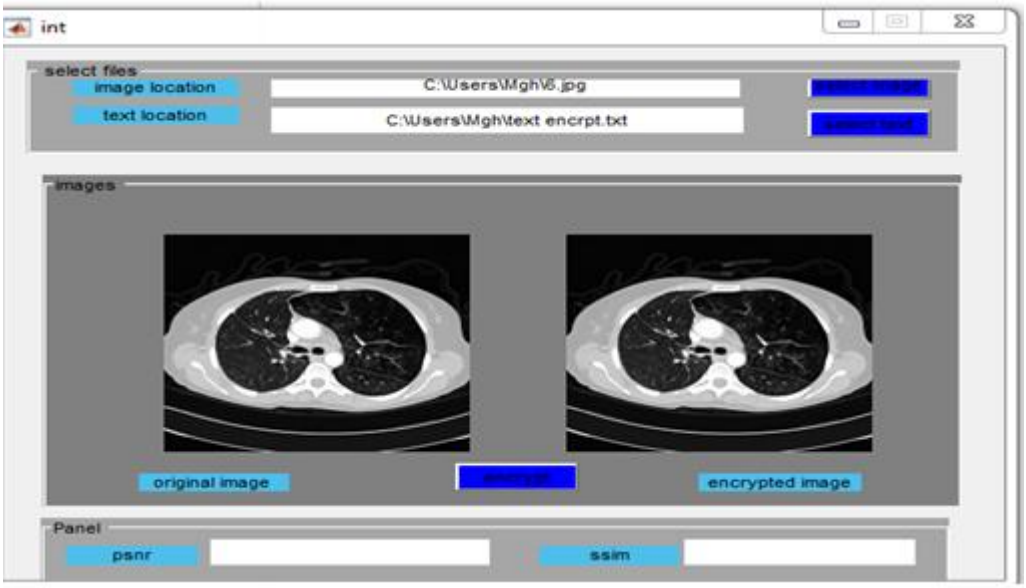


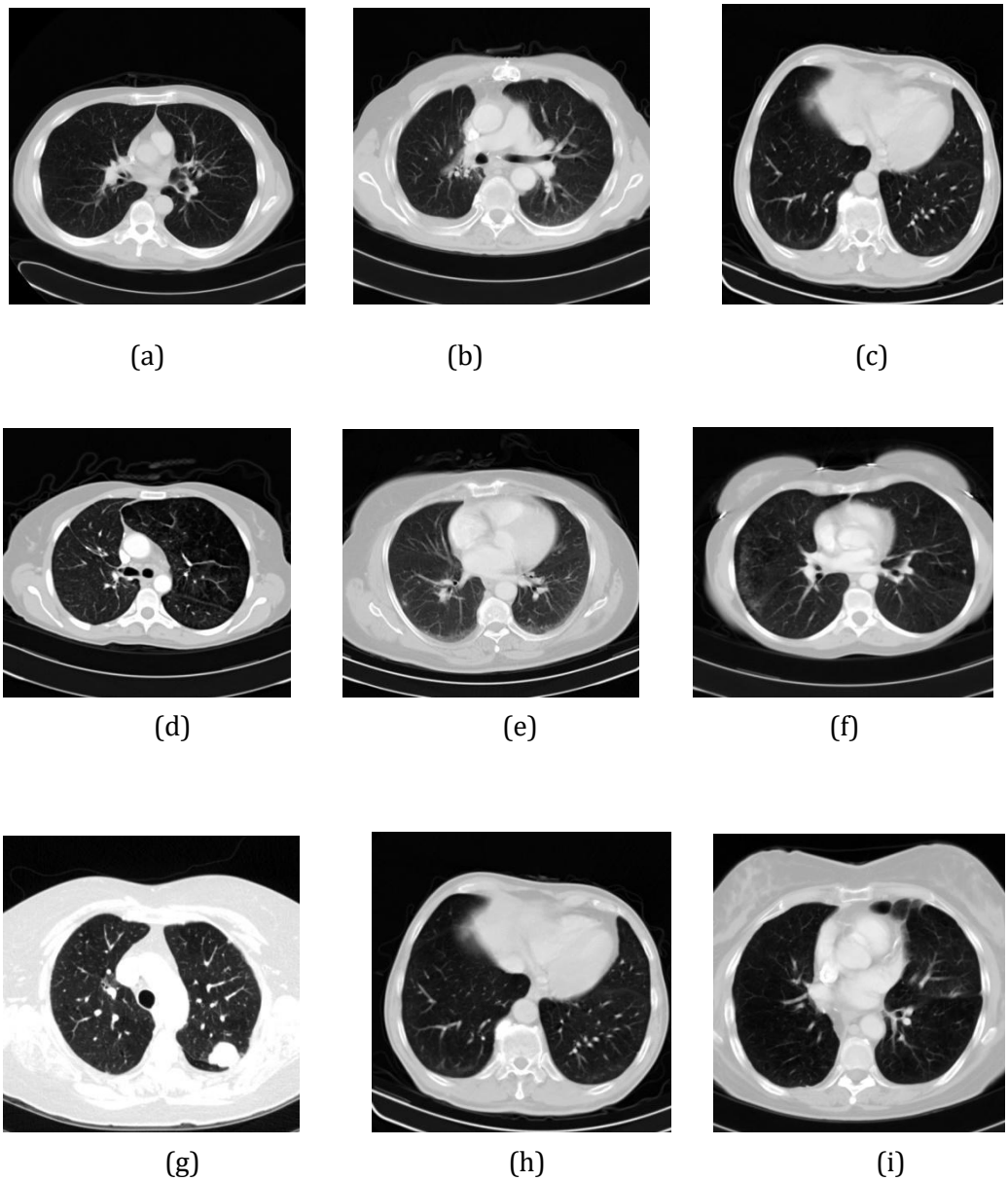
Figure 3.25:Image tatouée

3.11 Evaluation de l'algorithme :

Dans cette partie, nous avons évalué l'efficacité de notre algorithme à la sensibilité de la modification. Pour ceci, nous avons analysé la propriété d'imperceptibilité.

3.12 Analyse de l'imperceptibilité :

Nous avons appliqué notre méthode à des images de type (JPEG), pour confirmer les résultats obtenus. Les images hôtes sont utilisées pour tester la non-perception, À partir de notre algorithme (Figure 3.26), les images filigranées sont présentées dans (Figure 3.27).

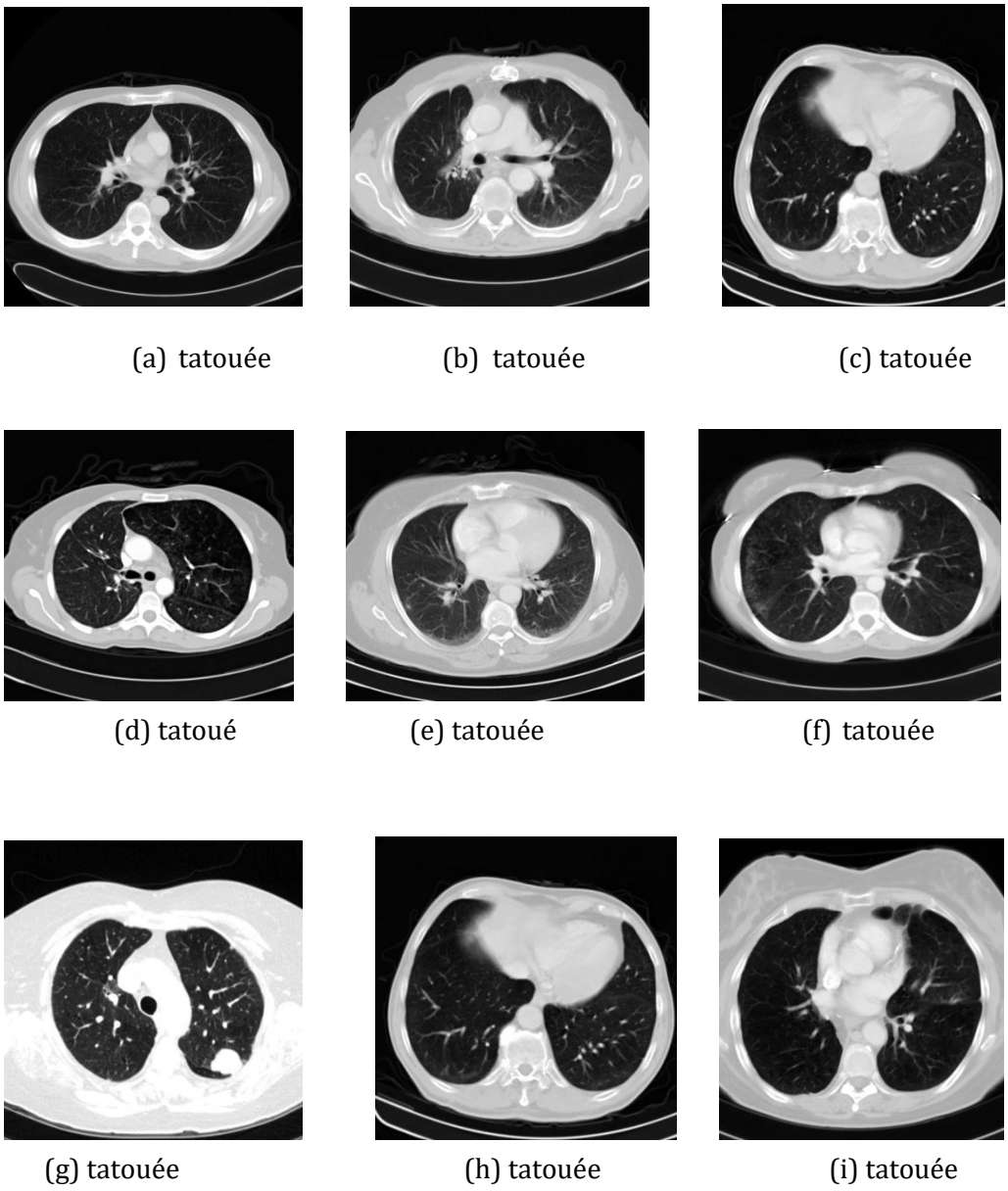


(a) (b) (c)

(d) (e) (f)

(g) (h) (i)

Figure 3.26:Images original.



(a) tatouée (b) tatouée (c) tatouée

(d) tatoué (e) tatouée (f) tatouée

(g) tatouée (h) tatouée (i) tatouée

Figure 3.27:Images tatouée.

À partir de neuf figures tatouées (neuf images JPEG) on peut voir que la dégradation des images tatouées est imperceptible par l'observateur. Le Tableau 2 présente les valeurs de PSNR et SSIM.

Tableau 2: présente les valeurs de PSNR et SSIM

Image JPEG	**PSNR**	**SSIM**
Image (a) tatouée	98.63	0.9999
Image (b) tatouée	98.63	1.0000
Image (c) tatouée	97.54	1.0000
Image (d) tatouée	98.05	0.9999
Image (e) tatouée	98.63	0.9999
Image (f) tatouée	99.30	1.0000
Image (g) tatouée	98.05	0.9999
Image (h) tatouée	100.09	1.0000
Image (e) tatouée	99.30	1.0000

En plus le tableau 2 PSNR et SSIM aussi clarifier que les valeurs très bonnes, ce qui signifie que notre méthode de tatouage fragile garantir une haute qualité d'images tatouées.

3.13 Discussion :

Dans l'imagerie médicale, plusieurs manipulations malveillantes peuvent causer la disparition de certains signes visibles d'une pathologie, faussant alors le diagnostic du médecin.
Dans cette situation, le tatouage numérique joue un rôle primordial non seulement pour la sécurité des images, mais le plus sensible, c'est pour la protection du patient contre les diagnostics erronés.

3.14 Conclusion :

Dans ce chapitre, nous introduisons un algorithme pour Tatouage les images en niveaux de gris et concluons qu'il fonctionne bien. La technique de Tatouage fragile est efficace pour les types de bruit à haute énergie et à basse pression (JPEG). En revanche, dans le cas des filtres et des distorsions géométriques, on ne voit pas l'efficacité de la technologie utilisée (l'effet de la technologie est nul).

Conclusion GÉNÉRALE

Conclusion Générale

Le tatouage d'image en tant que technique trouve sa place dans le domaine de la télémédecine. Dans ce contexte, notre travail de recherche vise à comparer différentes techniques de tatouage à des images médicales ; de ce fait, et en tant que technique, notre étude s'appuie sur l'utilisation d'algorithmes de tatouage.

Dans un premier temps, nous avons introduit les concepts de base liés au domaine de l'image numérique et à son traitement en donnant quelques définitions importantes à ce sujet. Nous avons également introduit les filigranes numériques, leurs limites et leurs fonctionnalités.

Dans cette thèse, nous avons implémenté des algorithmes de tatouage fragile pour des images en niveaux de gris basés sur l'utilisation de la méthode LSB, dans le but de vérifier l'authentification et l'intégrité des images numériques.

En appliquant la puissante technologie aux images en niveaux de gris, les résultats montrent une amélioration du PSNR et du SSIM notamment en termes de bruit. En revanche et sur d'autres attaques également : distorsions géométriques, filtres et compression avec perte de données, les résultats d'une technologie robuste ne montrent pas une telle amélioration.

Par conséquent, dans notre cas, la protection par cette technique est insuffisante.

Les résultats expérimentaux montrent la faisabilité de notre algorithme proposé, et que cette méthode (LSB) permet d'obtenir des images tatouées de haute qualité et en même temps très sensible contre plusieurs types d'attaques conventionnelles.

Pour cela, d'autres solutions ont été explorées, comme révéler une atteinte comme c'est le cas des tatouages fragiles.

Les résultats expérimentaux montrent la faisabilité de notre algorithme proposé, et que cette

La méthode (LSB) permet d'obtenir une haute qualité d'images tatouées et en même temps, elle est très sensible contre plusieurs types d'attaques conventionnelles.

Dans une perspective, et pour une bonne détection et protection dans le réseau télémédecine, il est essentiel d'aider les cliniciens à diagnostiquer les images médicales.

À partir du travail réalisé dans le cadre de ce mémoire, quelques perspectives peuvent être dégagées :

• Notre contribution se place dans le cadre de proposer des nouveaux schémas de tatouage d'images en niveaux de gris. Nous avons voulu améliorer notre travailler sur différents critères : robuste/fragile, domaine spatial/domaine transforme.

• Etendre notre algorithme de tatouage d'images proposé pour l'utilisation à la vidéo.

• S'orienter vers d'autres applications, en dehors du contexte sécuritaire du watermarking, telles que l'augmentation ou l'enrichissement des contenus (indexation multimédia, canal caché), la création de méta-documents,….etc.

• Nous pouvons envisager à la correction des erreurs en utilisant des codes correcteurs d'erreurs tels que les turbo-codes.

•Nous nous sommes bases dans l'étude expérimentale sur l'utilisation des métriquesbaséespixels. Dans la future, nous essayerons d'utiliser des métriques psychos

visuelles. Telles que JNCD Nous essayerons aussi d´élaborer un mécanisme pour assurer la Contrainte de sécurité.

Bibliographie

Bibliographie

[1]" Définition de l'image numérique," http://www.map.toulouse.archi.fr/works/panoformation/imagenum/imagenum.htm,

Mars 12, 2022, 20:30.

[2] " Images bitmap et vectorielles", https://www.commentcamarche.net/contents/1217-images-bitmap-et-vectorielles, Mars 12, 2022, 20:35.

[3]" Les formats de fichiers d'images,« https://tecfa.unige.ch/tecfa/teaching/staf13/fiches-mm/formatfichier.htm, Mai 31, 2022,14 :02.

[4] " Portable Network Graphics« , https://fr.wikipedia.org/wiki/Portable_Network_Graphics April 22, 2022, 22:11.

[5] https://helpx.adobe.com/fr/photoshop/using/file-formats.html April 22, 2022, 22:55.

[6] " Les caractéristiques d'une image numérique" , https://fpt113-vg.espaceweb.usherbrooke.ca/dochtml/caracteristique-image.htm#:~:text=On%20appelle%20%22d%C3%A9finition%22%20le%20nombre,pixels%20par%20480%2C%20not%C3%A9e%20640x480, Mai 31, 2022,23 :18.

[7] https://www.maxicours.com/se/cours/caracteristiques-d-une-image-numerique/ , Mai 22, 2022,13 :09.

[8] www. master-ivi.univ-lille1.fr/fichiers/Cours/seance8_wmk.pdf, Mai 22, 2022,10 :23.

[9]" Traitement d'images " ,https://fr.wikipedia.org/wiki/Traitement_d%27images April 11, 2022, 09:14.

[10] P.G. Frija, P.B. Mazoyer, L'imagerie médicale, 2002.

[11] N. Henri, Traité d'imagerie médicale - volume 1 – 2e éd, Médecine Sciences Publication, Paris, 2014

[12].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..

[13].Y. Michqud, Le Renouvellement de l'observation dans les sciences, Odile Jacob, Paris, Octobre 2003.

[14] B. Blanc, A. Potier, Imagerie médicale en gynécologie, Springer-Verlag France, Paris, 2000.

[15] Sementicscholar, www.semanticscholar.org/ , Mai 30, 2022,23 :25.

[16] A.C. Boccara, L. Garnero, Image : Imagerie, Représentation, Modèles, 2004.

[17] Doctissimo, https://www.doctissimo.fr/ , Mai 30, 2022,23 :50.

[18] blogrecherche, https://blogrecherche.wp.imt.fr/ , Mai 31, 2022,00 :15.

[19]. C. Rey, J. Dugelay, Blind Detection of malicious alterations on still image using robust watermarks.

[20]A.Manoury, Tatouage d'images numériques par paquets d'ondelettes, Ecole Centrale de Nantes (ECN); Université de Nantes, 2001, Français

[21]. 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.

[22]. https://actualiteinformatique.fr/cryptomonnaie/definition-cryptographie , Mai 23, 2022,16 :52.

[23] https://fr.wikipedia.org/wiki/St%C3%A9ganographie, Mai 30, 2022,17 :00.

[24] tatouage image

[25] 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.

[26].S. M. Mousavi, A. Naghsh, S.A.R. Abu-Bakar, Watermarking technique used in Medical images: à Survey, Published online, 29 Mai 2014.

[27].B. Souad, Etude et implémentation des techniques de tatouage numérique, 30 Avril 2017.

[28] F. Autrusseau, Tatouage d'images fondé sur la modélisation su système visuel humain et sur la transformation mojette, 7 Novembre 2002.

[29] P. Singh, R.S. Chadha, A survey of digital watermarking technique, Applications and attacks, Issue 9, Mars 2013.

[30] Belferdi, W. (2019).A Robust Watermarking Approach for Images Authentication and Traceability.PhD thesis, Université de Batna 2.

[31] Al-Ghadi, M. Q. (2018). Watermarking approaches for image authentication in applications with time constraints. PhD thesis, Université de Bretagne occidentale - Brest.

[32] Singh, N., Jain, M., and Sharma, S. (2013).A survey of digital watermarking techniques. International Journal of Modern Communication Technologies and Research, 1(6):265852.

[33] Hu, Y. and Jeon, B. (2006).Reversible visible watermarking and lossless recovery of original images. IEEE Transactions on Circuits and Systems for Video Technology, 16(11):1423–1429.

[34] Yip, S.-K., Au, O. C., Ho, C.-W., and Wong, H.-M.(2006).Lossless visible watermarking. In 2006 IEEE International Conference on Multimedia and Expo, pages 853–856.

[35] Tsai, M.-J.(2009).A visible watermarking algorithm based on the content and contrast aware (cocoa) technique. Journal of Visual Communication and Image Representation, 20(5):323–338.

[36] Vongpradhip, S. and Rungraungsilp, S. (2012). Qr code using invisible watermarking in frequency domain. In 2011 Ninth International Conference on ICT and Knowledge Engineering, Pages 47–52.

[37] Karthigaikumar, P., Baskaran, K., and Anumol (2012). Fpga implementation of high speed low area dwt based invisible image watermarking algorithm. Procedia Engineering, 30:266–273.

[38] Sathik, M. M. and Sujatha, S. (2012). A novel dwt based invisible watermarking technique for digital images. Int. Arab. J. e Technol., 2(3) :167–173.

[39] Boreiry, M. and Keyvanpour, M.-R. (2017).Classification of watermarking methods based on watermarking approaches.

In 2017 Artificial Intelligence and Robotics (IRANOPEN), pages 73–76. IEEE.

[40] Wu, X., Guan, Z.-H., and Wu, Z. (2007). A chaos based robust spatial domain watermarking algorithm. In International Symposium on Neural Networks, pages 113–119.Springer.

[41] Su, Q., Niu, Y., Wang, Q., and Sheng, G. (2013). A blind color image watermarking based on dc component in the spatial domain. Optik, 124(23):6255–6260.

[42] Su, Q. and Chen, B. (2018).Robust color image watermarking technique in the spatial domain. Soft Computing, 22(1):91–106

[43] Tefas, A., Nikolaidis, N., and Pitas, I. (2009). Chapter 22 - image watermarking: Techniques and applications. In The Essential Guide to Image Processing, pages 597 – 648.Academic press.

[44] Liu, J.-L., Lou, D.-C., Chang, M.-C., and Tso, H.-K.(2006).A robust watermarking scheme using self-reference image. Computer Standards & Interfaces, 28(3):356–367.

[45] Chen, W.-C. And Wang, M.-S.(2009).A fuzzy cmeans clustering-based fragile watermarking scheme for image authentication. Expert Systems with Applications, 36(2):1300–1307.

[46] Rawat, S. and Raman, B. (2011). A chaotic system based fragile watermarking scheme for image tamper detection. AEUInternational Journal of Electronics and Communications, 65(10):840–847.

[47] Singh, D. and Singh, S. K. (2017). Dct based efficient fragile watermarking scheme for image authentication and restoration. Multimedia Tools and Applications, 76(1):953–977.

[48] Ho, C. K. and Li, C.-T.(2004).Semi-fragile watermarking scheme for authentication of jpeg images. In International Conference on Information Technology: Coding and computing, 2004 Proceedings.ITCC 2004.volume 1, pages 7–11. IEEE.

[49] Qi, X. and Xin, X. (2011).A quantization-based semifragile watermarking scheme for image content authentication. Journal of visual communication and image representation, 22(2):187–200.

[50] Qi, X. and Xin, X. (2015).A singular-value-based semifragile watermarking scheme for image content authentication with tamper localization. Journal of Visual Communication and Image Representation, 30:312–327.

[51] Golea, N. E.-H. (2010). Tatouage numérique des images couleurs RGB. PhD thesis, Université de Batna 2.

[52] Waleed K Ahmed, "Advantages and Disadvantages of Using MATLAB/ode45 for Solving Differential Equations in Engineering Applications", Article February 2013.

[53] https://fr.mathworks.com/discovery/machine-learning.html , Mars 26, 2022, 13:00.

[55] https://www.mathworks.com/help/vision/ref/psnr.html , May 23, 2022, 10:20.

[56]https://www.scirp.org/journal/paperinformation.aspx?paperid=90911&fbclid=IwAR3q629c_fFXZCYs9ud6VjO9nv_3XcVFSHvltFG6G0SVCvzlD_nmL_Pcq_Q ,May 23, 2022, 10:35.

[57] https://fr.acervolima.com/steganographie-d-image-basee-sur-lsb-utilisant-matlab/, May 23, 2022, 11:00.

[58] A.Manoury, Tatouage d'images numériques par paquets d'ondelettes, Ecole Centrale de Nantes (ECN); Université de Nantes, 2001, Français.

[59] 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.