Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Ghardaia

Faculté des Sciences et de la Technologie

Département des Mathématiques et d'Informatique

Mémoire en vue de l'obtention du **Diplôme de Master** en Informatique

Spécialité : Systèmes Intelligents pour l'Extraction de Connaissances

Thème

Authentification des images médicales couleurs en utilisant le tatouage numérique

Présenté par:

HAMAMA Siham

Membres du jury :

M. OULADNAOUI Slimane	MCB	Univ. Ghardaia	Président
M. BELLAOUAR Slimane	MCB	Univ. Ghardaia	Examinateur
M. ADJILA Abderrahmane	MAA	Univ. Ghardaia	Examinateur
Melle. BELFERDI Wassila	MAB	Univ. Ghardaia	Encadrant

Année Universitaire : 2019/2020

Résumé

La révolution numérique et l'avancement rapide des systèmes de communication en réseau entraînent une croissance considérable d'échange des images dans divers domaines tels que le commerce électronique, la sécurité nationale et la télémédecine. D'autre part, la disponibilité des outils puissants du traitement d'images pose des problèmes concernant l'authentification et l'intégrité des images. Dans ces circonstances, la protection des images devient un besoin urgent, notamment, dans les applications sensibles telles que les applications de la télémédecine où toute modification peut provoquer des erreurs de diagnostic et de décisions.

Le tatouage numérique a attiré beaucoup l'attention des chercheurs comme une technique de protection, en raison de son efficacité de la résolution des problèmes concernant l'authentification et l'intégrité des images.

Dans ce contexte, diverses méthodes d'authentification ont été proposées, néanmoins, la plupart de ces méthodes proposées se focalisent sur les images en niveau de gris, en plus, si elles détectent les modifications, elles n'offrent pas la restauration des zones modifiées ou elles les récupèrent que dans le cas des petits taux de modification.

Dans ce mémoire, nous avons étudié le tatouage numérique des images en général, ses propriétés, ses applications et ses classifications. Puis, le tatouage numérique pour l'authentification du contenu des images médicales en particulier. Nous avons implémenté une méthode de tatouage fragile basé sur l'auto-insertion pour l'authentification, la détection et la restauration de modification d'image couleur RVB. Après, nous avons fait des expérimentations sur des images couleurs générales et des images médicales couleurs attaquées par les opérations de collage, de coupure et des attaques hybrides.

Les résultats expérimentaux ont montré l'invisibilité du watermark, la précision de la détection et la haute qualité de l'image couleur récupérée avec la plupart des images couleur en exception de quelques images médicales.

Mots clés : Tatouage numérique, Images médicales, Authentification, Intégrité, Tatouage fragile, Image couleur RVB.

Abstract

The digital evolution and the fast advancement of networked communication systems provide a huge growth in image exchange in various fields such as e-commerce, national security and telemedicine. On the other hand, the availability of powerful image processing tools poses challenges for authentication and image integrity. In these circumstances, the protection of images becomes an urgent need, especially, in sensitive applications such as telemedicine applications where any modification may lead to false diagnosis or bad decisions.

The digital watermarking has attracted the attention of researchers as a protective technique, because of its efficiency in solving authentication and image integrity issues.

In this context, various authentication methods have been proposed. However, most of these proposed methods have focused on grayscale images, in addition, if they detect the modifications, they do not offer the restoration of the modified zones or they only get them in the case of small change rates.

In this thesis, we have studied the digital watermarking of images in general, its properties, its applications and its classifications. Then, digital watermarking for the authentication of the content of medical images in particular. We implemented an auto-insertion-based fragile watermark method for the authentication, detection and restoration of RGB color image modification. Afterwards, we carried out experiments on general color images and medical color images attacked by the operations of gluing, cutting and hybrid attacks.

Experimental results have shown the invisibility of the watermark, the accuracy of detection and the high quality of the recovered color image with most color images except a few medicals images.

Key words : Digital watermarking, Medical images, Authentication, Integrity, fragile watermarking, RGB color image.

ملخص

تشهد الثورة الرقمية والتقدم السريع لأنظمة الاتصالات الشبكية نموًا هائلاً في تبادل الصور في مختلف المجالات مثل التجارة الإلكترونية والأمن القومي والطب عن بُعد. كما أن توفر أدوات المعالجة المتطورة للصور يطرح مشكلات تتعلق بمصادقة الصورة، ما يجعل حماية الصورة حاجة ملحة، خاصة في التطبيقات الحساسة مثل تطبيقات التطبيب عن بُعد حيث قد يؤدي أي تعديل غير مرخص في هذه الصور إلى أخطاء في التشخيص و اتخاذ القرارات.

يعد الوشم الرقمي حلا لهذا المشكل، حيث أنه يجذب الكثير من الاهتمام من قبل الباحثين كتقنية حماية بسبب كفاءته في حل المشاكل المتعلقة بمصادقة الصورة.

نتناول في هذا السياق مصادقة الصور الطبية عن طريق الوشم الرقمي. إذ أُقترحت العديد من طرق المصادقة، ومع ذلك فقد ركزت معظم هذه الأساليب المقترحة على الصور الرمادية، بالإضافة إلى ذلك، إذا إكتشفت التعديلات، فإنها لا تقدم استعادة المناطق المعدلة أو تقدمها فقط في حالة معدلات التغيير الصغيرة.

في هذه المذكرة، درسنا الوشم الرقمي للصور بشكل عام، تطرقنا إلى متطلباته، ثم تطرقنا إلي تطبيقاته وتصنيفاته، ثم الوشم الرقمي والمصادقة على محتوى الصور الطبية بشكل خاص. قمنا بتطبيق طريقة للوشم الهش ذاتية الإدراج للمصادقة والكشف عن التعديل واستعادة الصورة الملونة RVB، وبعد ذلك أجرينا تعديلات غير مصرحة على الصور الملونة بشكل عام و الصور الملونة الطبية بشكل خاص بعمليات القص، اللصق و القص واللصق في أن واحد. أظهرت النتائج التجريبية شفافية العلامة المائية ودقة الكشف والجودة العالية للصورة الملونة التي تم استردادها مع معظم الصور الملونة باستثناء عدد قليل من الصور الطبية.

الكلمات المفتاحية: الوشم الرقمي، الصور الطبية، المصادقة، النزاهة، العلامة المائية، الوشم الهش، صورة ملونة RVB.

Remerciments

Tout d'abord un merci plein de solennité à « ALLAH ALKARIME » de m'avoir donné la santé, la force et la volonté pour accomplir et pour présenter ce modeste travail.

Un grand merci plein d'amour et de respect à mes parents pour leurs soutiens constants et leurs aides précieuses.

Je tiens à remercier mon encadreur BELFERDI Wassila pour ses conseils précieux, ses encouragements et son aide tout au long de la réalisation de ce travail.

Je remercie sincèrement les membres de jury pour avoir accepté de juger ce modeste travail.

Je tiens à remercier particulièrement mon enseignant KERRACHE Chaker Abdelaziz pour ses conseils et ses encouragements.

Je remercie tous mes enseignants de master.

Merci également à mes collègues de master.

HAMAMA Siham.

Je dédie ce modeste travail
À mon cher père et ma chère mère qua Dieu les protège.
À mes chères sœurs et mes chers frères.
À tous ceux qui m'aiment . . .

HAMAMA Siham.

Table des matières

Table des figures

Liste des tableaux

Liste des Abréviations

REP	**R**apport **E**lectronique de **P**atient
RVB	**R**ouge **V**ert **B**leu
CFA	**C**olor **F**ilter **A**rray
DCT	**D**iscrete **C**osine **T**ransform
DICOM	**D**igital **I**maging and **CO**mmunication in **M**edicine
DS	**D**igital **S**ignature
DWT	**D**iscrete **W**avelet **T**ransform
JPEG	**J**oint **P**hotographic **E**xperts **G**roup
LSB	**L**east **S**ignificant **B**it
MAC	**M**essage **A**uthentication **C**ode
MSB	**M**ost **S**ignificant **B**it
NC	**N**ormalized **C**orrelation
PACS	**P**icture **A**rchiving and **C**ommunication **S**ystems
PN	**P**seudo-random **N**oise
PSNR	**P**eak **S**ignal to **N**oise **R**atio
R_{FA}	**F**alse **A**larm **R**ate
RLE	**R**un **L**enght **E**ncoding
ROI	**R**egion **O**f **I**nterest
RONI	**R**egion **O**f **N**o **I**nterest
R_T	**T**ampering **R**atio
R_{TD}	**T**ampering **D**etection **R**ate
SHA	**S**ecure **H**ash **A**lgorithm
SS	**S**pread **S**pectrum
SSIM	**S**tructural **SIM**ilarity
SVD	**S**ingular **V**alue **D**ecomposition
UID	**U**nique **ID**entifier
URL	**U**niform **R**esource **L**ocator
VQ	**V**ector **Q**uantization

Introduction Générale

La révolution numérique et l'avancement rapide des systèmes de communication en réseau entraînent une croissance considérable d'échange de documents multimédias (texte, images, audio, vidéo) dans divers domaines tels que le commerce électronique, la sécurité nationale et la télémédecine. D'autre part, la disponibilité des outils puissants du traitement du signal et d'image rend le contenu numérique susceptible de falsification ou de manipulations malveillantes. Dans ces circonstances, la protection du contenu devient un besoin urgent, notamment, dans les applications sensibles telles que les applications militaires et les applications de la télémédecine où toute modification peut conduire à des erreurs de diagnostic ou de décision.

La cryptographie a été considérée le principal outil de protection du contenu de document lors de son transmission de l'expéditeur au destinataire, mais après la réception et le décryptage, ce contenu devient clair et n'est plus protégé, et il peut être modifié ou distribué. Donc, la cryptographie reste à besoin d'un complément ou d'une alternative qui renforce la sécurité par la protection du contenu même après son décryptage.

Le tatouage numérique est une alternative efficace de protection, il peut-être défini comme l'intégration des informations appelées un watermark en permanence dans un document numérique afin d'assurer un service de sécurité (protection des droits d'auteur, authentification, etc.) ou à but d'information.

Le tatouage numérique a beaucoup d'intérêt que les autres techniques de protection en raison de son efficacité de la résolution des problèmes concernant l'authentification du contenu et la protection des droits d'auteur. Il peut répondre efficacement aux exigences principales de la protection des données médicales et il est considéré comme une approche prometteuse pour garantir l'authentification du contenu ou l'intégrité des images médicales, notamment, avec l'évolution des systèmes de santé et les besoins de partage des images médicales entre médecins et hôpitaux par internet ou par les réseaux locaux en raison du télédiagnostic, de téléconférences entre les médecins et la consultation médicale [Al-Ghadi, 2018].

Dans ce contexte, plusieurs schémas du tatouage numérique pour l'authentification du contenu ont été conçus pour décider si une image médicale reçue est authentique ou non. Il existe d'autres schémas d'authentification du contenu dit complets qui sont capables même de détecter les zones altérées et les récupérer. Les schémas les plus populaires traitent les images en niveau de gris, alors que la minorité traite celles en couleur.

Nous avons implémenté un schéma du tatouage numérique fragile pour l'authentification du contenu, la détection et la restauration de modification d'image couleur basée sur une technique d'auto-insertion et utilise un filtre chromatique pour réduire l'image hôte couleur en un watermark en niveau de gris afin de diminuer la quantité d'informations insérées et par conséquent, de préserver la qualité d'image, et pour améliorer la sécurité, il utilise la permutation de Torus automorphisme pour brouiller le watermark. Après, nous l'avons appliqué sur une variété des images générales couleurs et sur des images médicales couleurs afin d'évaluer ses performances.

Ce mémoire est composé de trois chapitres :

Chapitre 1 présente une définition des techniques de protection des données numériques (la cryptographie, la stéganographie et le tatouage) et la différence entre eux, l'avantage du tatouage numérique, l'historique du tatouage, les exigences et le modèle général d'un système de tatouage numérique d'images, plus, les applications et la classification de ces systèmes, les attaques possibles contre elles, et enfin, les métriques principales de performance de ces systèmes.

Chapitre 2 présente les grands types d'imagerie médicale, les exigences du tatouage numérique des images médicales, les applications de ce tatouage, les classifications existantes des méthodes de ce tatouage avec quelques exemples. Il présente aussi, l'utilité d'une méthode ou d'un système d'authentification d'image, le modèle général, les exigences et la classification de ces systèmes, et enfin, la description de fonctionnement, des étapes et des techniques de quelques méthodes d'authentification.

Chapitre 3 comprend le coté pratique de ce mémoire, il présente les différents processus du schéma d'authentification d'image implémenté, les techniques utilisées, les résultats expérimentaux et l'évaluation de performances de cette méthode.

Enfin, la conclusion résume tout ce que nous avons vu dans ce mémoire.

Chapitre 1

Généralités sur le tatouage numérique

1.1 Introduction

Le multimédia numérique est devenu une partie importante de la vie moderne avec la disponibilité d'internet, des appareils électroniques et l'avancement rapide des systèmes de communication en réseau. Le contenu multimédia numérique (image, audio, vidéos) est largement utilisé dans divers domaines tels que le commerce électronique, la sécurité nationale, la télémédecine et les communications réseau.

Le contenu multimédia numérique est devenu susceptible de manipulations et d'altérations malveillantes grâce à la puissance des outils du traitement du signal et d'image disponibles (Photoshop, GIMP,...). Ceci rend la protection de ces données numériques une nécessité très urgente.

Dans la littérature, trois techniques sont utilisées pour protéger les données numériques : la cryptographie, la stéganographie et le tatouage. Le tatouage numérique attire beaucoup l'attention des chercheurs que les autres techniques de protection en raison de son efficacité pour résoudre les problèmes concernant l'authenticité, l'intégrité et la protection des droits d'auteur [Al-Ghadi, 2018].

Dans ce chapitre, nous présentons une discussion sur les techniques de protection des données numériques (la cryptographie, la stéganographie et le tatouage) et une comparaison entre eux. Ensuite, nous introduisons l'historique du tatouage, puis, les propriétés d'un système de tatouage numérique sont présentées, après, un modèle général de tatouage numérique est décrit. Nous présentons aussi les applications du tatouage numérique, la classification des algorithmes du tatouage selon plusieurs techniques et les attaques contre le système du tatouage numérique. Enfin, les métriques de performance du système de tatouage numérique d'images sont présentées.

1.2 Techniques de protection des données numériques

Dans cette section, nous présentons les différentes techniques de protections des données numériques (Figure 1.1) :

1.2.1 La cryptographie

Jusqu'à récemment, la cryptographie a été considérée le principal outil pour protéger le contenu numérique lors de sa transmission de l'expéditeur au destinataire en le transformant en un format illisible (cryptogramme) à l'aide d'une clé K_C selon l'équation suivante :

$$C = E_{K_C}(M) \tag{1.1}$$

Pour le déchiffrement du cryptogramme en contenu numérique clair on applique la transformation inverse avec une clé K_D :

$$M = D_{K_D}(C) = D_{K_D}\left(E_{K_C}(M)\right) \tag{1.2}$$

Où
C : Cryptogramme (message chiffré).
M : Message clair.
E : Fonction de chiffrement.
D : Fonction de déchiffrement.

Mais, le problème qu'après la réception et le déchiffrement, le contenu numérique devient clair et n'est plus protégé, et il peut être modifié ou distribué [Cox et al., 1999]. C'est ce qu'ont amené les chercheurs à penser à trouver un complément à la cryptographie ou une alternative qui renforce la sécurité et la protection du contenu même après son décryptage [Cox et al., 2007].

De ce fait, la dissimulation d'information (en anglais data hiding) est devenue la solution idéale de ce problème. Elle consiste à insérer une certaine quantité d'informations secrètes de manière imperceptible dans un document numérique [Lu, 2004, Chikhi, 2008].

La stéganographie et le tatouage (en anglais watermarking) sont deux disciplines de dissimulation d'information.

1.2.2 La stéganographie

La stéganographie est l'acte de communication secrète, où seul l'émetteur et le le récepteur sont au courant de cette communication secrète. En d'autres termes, la stéganographie est la pratique de modifier indétectablement un objet de couverture **qui n'a pas de valeur** pour cacher un message secret n'a aucun lien avec cet objet de couverture qui le porte [Cox et al., 2007].

Soit K l'ensemble des clés possibles, M l'ensemble des messages possibles insérables, et C l'ensemble des objets de couverture.

Formellement, un schéma stéganographique est caractérisé par deux fonctions :

— Une fonction d'insertion I utilisée par l'émetteur et qui prend en entrée un objet de couverture $c \in C$, une clé privée $k \in K$ et un message à dissimuler $m \in M$, et qui retourne en sortie un nouveau élément de C contenant le message secret, appelé le stégo-médium.

$$I : C \times M \times K \rightarrow C \tag{1.3}$$

— Une fonction d'extraction E utilisée par le récepteur et qui prend en paramètre le stégo-médium reçu et une clé stéganographique, et qui retourne le message secret en sortie.

$$E : C \times K \rightarrow M \tag{1.4}$$

Un schéma stéganographique se traduit par :

$$E\left(I\left(c, m, k\right), k\right) = m, \forall \left(c, m, k\right) \in C \times M \times K \tag{1.5}$$

1.2.3 Le tatouage numérique

Le tatouage numérique est défini comme la pratique de modifier imperceptiblement ou perceptiblement un document pour insérer un message (watermark) **à propos de ce document** [Cox et al., 2007, Cox et al., 1999].

Chun-Shien Lu défini le tatouage numérique comme le fait d'incorporer un signal (un watermark) en permanence dans des données numériques (audio, images, vidéo et texte) afin de l'extraire plus tard pour faire des affirmations sur les données. Le watermark est caché dans les données de l'hôte de telle sorte qu'elle est inséparable des données et qu'il résiste à de nombreuses opérations non dégradantes de la qualité du document hôte. Au tatouage, le document est toujours accessible mais il reste tatoué en permanence [Lu, 2004].

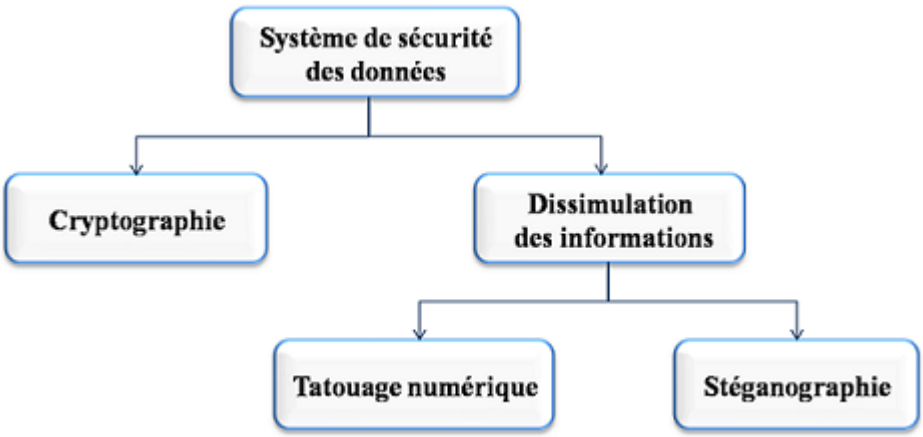


FIGURE 1.1 – Techniques de protection des données numériques.

Le tatouage numérique peut-être aussi défini comme l'insertion d'une information subliminale dans un document numérique afin d'assurer un service de sécurité (copyright, intégrité, traçabilité, etc.) ou à but d'information [Rey and Dugelay, 2001].

1.2.4 Cryptographie vs stéganographie

La cryptographie et la stéganographie sont deux techniques différentes de protections des données numériques :

— La cryptographie permet d'échanger des messages illisibles afin que seules les personnes autorisées puissent les lire. Dans ce cas, la sécurité repose sur l'incompréhensibilité de message transmis, par contre, la sécurité de la stéganographie dépend de la question de l'existence du message secret [Chikhi, 2008].

— La cryptographie protège un document numérique durant sa transmission. Après la réception et le décryptage, ce document devient clair et non protégé. Donc il peut être facilement copié et distribué. À la stéganographie le message secret resté protégé même après la réception [Chikhi, 2008].

— Une autre différence au niveau des attaques, en cryptographie, le pirate va essayer de décrypter le message, tandis qu'en stéganographie l'attaquant va essayer de détecter l'objet de couverture [Chikhi, 2008].

1.2.5 Stéganographie vs tatouage numérique

La stéganographie et le tatouage sont deux approches de la dissimulation d'information mais n'ont pas les mêmes objectifs, ni les mêmes contraintes :

— Dans le cas de la stéganographie, la quantité des données cachées peut aller jusqu'à la dissimulation d'une image entière dans une autre image ou un document dans un autre. Dans le cas du tatouage numérique, on cherche à dissimuler une quantité limitée d'information afin de vérifier l'intégrité du document par exemple ou de protéger les droits d'auteur [Chikhi, 2008].

— Dans la stéganographie, l'existence d'un message caché doit rester secrète, tandis que pour le tatouage numérique, l'existence du message peut être connue mais il doit rester caché [Chikhi, 2008].

— En stéganographie, l'attaquant va tenter de lire le message caché dans le document, alors que dans le cas du tatouage numérique, l'attaquant va essayer par exemple d'usurper l'identité de l'auteur en remplaçant la marque [Chikhi, 2008].

— La stéganographie est utilisée pour la communication secrète, tandis que le tatouage est utilisé pour la protection du contenu, la protection des droits d'auteur, l'authentification du contenu et la détection de modification [Potdar et al., 2005].

— À la stéganographie, il doit être impossible de distinguer si l'objet de couverture contient un message utile ou non. La contrainte la plus importante est alors l'imperceptibilité. Au tatouage numérique, le message intégré est lié au document de couverture, alors il doit rester présent et possible de récupérer à tout moment, même si le document était altéré par une ou plusieurs attaques non destructives. Dans ce cas, la contrainte principale est la robustesse [Chikhi, 2008, Rey and Dugelay, 2002].

— En tatouage numérique, les données externes sont les informations importantes (par exemple : les images, les voix, etc.) et les données internes (watermark) sont des données supplémentaires pour protéger les données externes et pour prouver l'intégrité ou la propriété. Cependant, en stéganographie, les données internes sont les plus importantes et les données externes (objet de couverture) sont juste un transporteur de ces informations importantes [Lu, 2004].

Les avantages de tatouage numérique par rapport à la cryptographie et à la stéganographie ont attiré l'attention des chercheurs, le tatouage a beaucoup d'intérêt que les autres approches de protection en raison de la préoccupation croissante concernant l'authenticité, l'intégrité, la protection des droits d'auteur et le contrôle de la copie.

1.3 Historique de tatouage numérique

Quoique la fabrication du papier ait été inventée en Chine plus de mille ans, le tatouage du papier n'est apparu qu'en 1282 en Italie. Il a été utilisé intensivement au 18 ème siècle en Amérique et en Europe comme marque et méthode contre la falsification des livres et d'argent [Cox et al., 2007, Seitz, 2005].

Le terme tatouage numérique (en anglais digital watermarking) a été introduit pour la première fois en 1993 par Tirkel et al. [Tirkel et al., 1993] qui ont présenté deux techniques pour masquer des données dans des images numériques. Ces méthodes étaient basées sur des modifications du bit le moins significatif LSB (Least Significant Bit) des valeurs des pixels [Lu, 2004].

Le tatouage numérique est le fait d'insérer des données dites watermark dans un support numérique (texte, audio, vidéo ou images) en utilisant un algorithme informatique afin de les extraits ultérieurement pour faire une affirmation sur ce support [Seitz, 2005].

Depuis 1995, la préoccupation du tatouage numérique a augmenté. Le premier atelier sur la dissimulation d'information IHW (Information Hiding Workshop) à été crée en 1996, la société des ingénieurs en instrumentation photographique SPIE (Society of Photographic Instrumentation Engineers) a commencé à consacrer une conférence sur le tatouage numérique et la sécurité multimédia en 1999, des organisations telles que groupe de travail technique sur la protection contre la copie CPTWG (The Copy Protection Technical Working Group) ont été fondées [Cox et al., 2007, Zehda, 2014].

Récemment, plusieurs journaux dédiés aux problématiques de sécurité de l'information ont été créé tels que IEEE Transactions on Information Forensics and Security et IEE Proceedings Information Security en 2005 [Cox et al., 2007, Zehda, 2014].

Depuis 1995 jusqu'aujourd'hui, le tatouage numérique a occupé une place importante dans les recherches scientifiques et a évolué très rapidement où nombreuses entreprises et industriels sont intéressés à ce domaine tels que Digimarc qui rassemble des brevets de base sur le tatouage, Verance qui fournit les outils de contrôle de flux audiovisuel et Liquid Audio qui fournit également un système de tatouage audio. En plus, le nombre de publications à ce sujet est accru et plusieurs méthodes de tatouage numérique ont été développées dont certaines sont présentées dans le chapitre 2.

1.4 Propriétés d'un système de tatouage numérique

Chaque système de tatouage numérique est caractérisé par un certain nombre de propriétés spécifiques. L'importance et même l'interprétation de chaque propriété peuvent varier selon les objectifs de l'application [Cox et al., 2007]. Alors, le choix d'un ensemble de propriétés satisfaites par tous les systèmes du tatouage n'est pas possible. Les propriétés les plus importantes sont : la sécurité, la robustesse, la fidélité, le coût de calcul, la résistance à la falsification et les taux de faux positifs. Néanmoins, la conception d'un système de tatouage qui répond à toutes ces propriétés est pratiquement impossible. Par conséquent, Il est nécessaire de faire des compromis entre eux [Belferdi, 2019].

Dans ce qui suit on décrit les exigences essentielles pour la conception d'un système du tatouage comme suit :

1.4.1 Sécurité

Un système du tatouage sécurisé est un système capable de résister aux attaques intentionnelles (section 1.8) : les attaques de suppression de watermark non autorisées, d'insertion et d'extraction non autorisées [Al-Ghadi, 2018].

Un utilisateur non autorisé ne peut pas extraire ou supprimer le watermark inséré sans avoir des informations complètes sur l'algorithme utilisé pour insérer le watermark. L'approche du tatouage devrait garantir que seul l'utilisateur autorisé peut accéder au watermark inséré [Al-Ghadi, 2018].

1.4.2 Robustesse

La robustesse est la capacité d'un watermark à survivre à un traitement. En d'autres termes, c'est la capacité de détecter le watermark inséré après les opérations de traitement d'images telles que le filtrage, la compression avec perte et les distorsions géométriques (rotation, mise à l'échelle, etc.) [Cox et al., 2007].

Il existe des applications ne nécessitent pas la robustesse, dans certains cas, le tatouage doit être fragile tel que les applications d'authentification qui indique si une image a été modifiée ou non [Belferdi, 2019].

La corrélation normalisée NC (Normalized Correlation) est une métrique utilisée pour exprimer les performances d'un système du tatouage d'image en termes de robustesse, le NC est une mesure de la similitude entre le watermark original et le watermark extrait. Le NC est compris entre 0 et 1, si la valeur de NC est plus proche de 1, cela signifie que les deux images sont plus similaires [Belferdi, 2019].

Le NC est calculé selon l'équation (1.6).

$$NC(I, I') = \frac{\sum_{i=1}^{3}\sum_{x=1}^{N}\sum_{y=1}^{M}\left[I_i(x,y) \times I'_i(x,y)\right]}{\sqrt{\sum_{i=1}^{3}\sum_{x=1}^{N}\sum_{y=1}^{M}\left[I_i(x,y)\right]^2} \times \sqrt{\sum_{i=1}^{3}\sum_{x=1}^{N}\sum_{y=1}^{M}\left[I'_i(x,y)\right]^2}} \tag{1.6}$$

1.4.3 Imperceptibilité

Le watermark doit être inséré de manière invisible [1] à l'œil humain avec une dégradation minimale de la qualité du contenu. L'image tatouée doit être similaire à celle d'origine sous observation normale. En d'autres termes, la similitude perceptuelle entre l'image originale et l'image tatouée est calculée afin d'exprimer le taux d'imperceptibilité. S'il est élevé, cela signifie une faible distorsion dans la qualité de perception d'image originale [Belferdi, 2019, Al-Ghadi, 2018, Khurana, 2011].

L'imperceptibilité est l'une des exigences les plus recherchées dans les approches de tatouage. La garantie de l'imperceptibilité du watermark permet d'éviter les tentatives de la substitution, la déformation ou la suppression du watermark [Belferdi, 2019, Al-Ghadi, 2018, Khurana, 2011].

Pour exprimer les performances d'une approche du tatouage d'image en termes d'imperceptibilité deux métriques sont utilisés le PSNR et le SSIM :

1. **Rapport signal/bruit PSNR (Peak Signal to Noise Ratio)**
   Le PSNR est une mesure d'imperceptibilité exprime la qualité de perception visuelle de l'image tatouée par rapport à l'image d'origine. Une valeur de PSNR plus élevée prouve que le watermark inséré est hautement imperceptible et provoque moins de dégradation de la qualité de l'image originale. Donc, elle indique aussi une grande similitude entre l'image originale et l'image tatouée [Al-Ghadi, 2018].

1. Parfois le watermark est inséré de manière visible et cela dans le cas de tatouage visible.

En général, la qualité visuelle est considérée acceptable, si les valeurs PSNR sont supérieures à 30 (dB) [Belferdi, 2019].
Le PSNR est calculé selon l'équation (1.7).

$$PSNR(I, I') = 10 \log \frac{3 \times N \times M \times 255^2}{\sum_{i=1}^{3} \sum_{x=1}^{N} \sum_{y=1}^{M} \left[I_i(x,y) - I'_i(x,y) \right]^2} \tag{1.7}$$

Où I est l'image originale, I' est l'image tatouée ou récupérée, et N, M désignent l'hauteur et la largeur de l'image respectivement.

2. **Indice de similarité structurelle SSIM (Structural SIMilarity)**
SSIM est une mesure de similarité entre deux images, la valeur 1 indique la similarité totale des deux images [Mousavi et al., 2014].
Le SSIM est calculé selon l'équation (1.8).

$$SSIM(I, I') = \frac{(2\mu_I \times \mu_{I'} + c_1) \times (2 \times \mathrm{cov}_{I'} + c_2)}{(2\mu_I^2 \times \mu_{I'}^2 + c_1) \times (\sigma_I^2 \times \sigma_{I'}^2 + c_2)} \tag{1.8}$$

où I est l'image original, I' est l'image tatouée ou récupérée, et N, M désignent respectivement l'hauteur et la largeur de l'image. μ_I et $\mu_{I'}$ sont les moyennes de I et I', respectivement ; σ_I^2 et $\sigma_{I'}^2$ sont les variances de I et I' respectivement ; $\mathrm{cov}_{I'}$ est la covariance de I' ; pour stabiliser la division avec un dénominateur faible les deux variables $c_1 = (k_1 L)^2$, $c_2 = (k_2 L)^2$ sont utilisées où L est la plage dynamique des valeurs des pixels.

1.4.4 Capacité

La capacité est la quantité d'informations qui peut être insérée dans l'image sans affecter sa qualité tout en assurant l'imperceptibilité et la robustesse [Belferdi, 2019, Tao et al., 2014].

Les propriétés de capacité, robustesse et imperceptibilité sont en conflit et limitées les unes par les autres. L'augmentation de la robustesse du tatouage diminue l'imperceptibilité du watermark. En d'autre coté, le watermark devrait être inséré invisiblement avec la séparation maximale possible afin d'éviter les erreurs d'extraction du watermark en cas de corruption d'image tatouée, on peut augmenter la charge utile des données en diminuant le nombre d'échantillons alloués à chaque bit caché mais cela conduit à une perte de robustesse. Donc, c'est impossible de satisfaire ces trois exigences à la fois. Alors un compromis approprié peut être trouvé (Figure 1.2) [Belferdi, 2019, Tao et al., 2014].

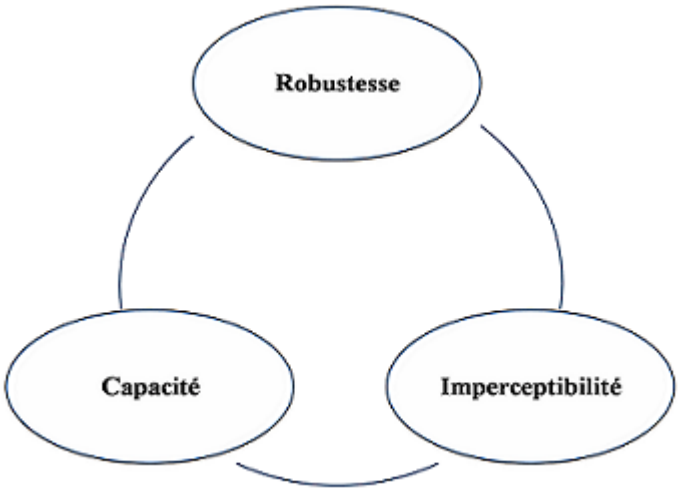


FIGURE 1.2 – Compromis entre les trois exigences essentielles du système de tatouage : robustesse, imperceptibilité et capacité.

1.4.5 Complexité de calcul

La complexité est la durée nécessaire à un algorithme de tatouage pour insérer et extraire un watermark . Elle se réfère au nombre d'étapes et à la quantité de calcul requise pour les processus d'insertion et d'extraction. L'application en temps réel (par exemple l'application de contrôle de diffusion) nécessite des algorithmes de faible complexité (rapides) et efficaces [Al-Ghadi, 2018].

1.5 Modèle général d'un système du tatouage numérique

Généralement, un système du tatouage numérique est constitué de trois processus fondamentaux : la génération du watermark, l'insertion du watermark et l'extraction du watermark. Un modèle général d'un système du tatouage numérique est illustré dans la Figure 1.3.

Le tatouage numérique peut être utilisé pour protéger les documents multimédia tels que les images, les textes, les audio et les vidéos.

1.5.1 Génération du watermark

Le watermark est généré selon les objectifs de l'application du tatouage, de telle sorte que son contenu soit complexe et unique, afin de rendre son extraction et sa distorsion difficile par les attaquants. Un watermark peut être un bruit, un message ou une image [Belferdi, 2019, Ling and Ur-Rehman, 2015].

Généralement, un certain prétraitement est effectué pour générer le watermark, il peut être des permutations pseudo-aléatoires [Ur-Rehman and Zivic, 2018].

Dans le cas d'auto-insertion, le watermark est l'image hôte compressée [Ur-Rehman and Zivic, 2018, Belferdi, 2019].

Ce processus peut être modélisé par la fonction suivante :

$$G\left(D_O\right) = W \tag{1.9}$$

Où
G : Fonction de génération de watermark.
D_O : Données originales.
W : watermark.

1.5.2 Insertion du watermark

Le watermark doit être inséré dans l'image hôte sans détruire cette dernière ou ses caractéristiques, et d'une manière qui rend difficile à l'attaquant d'extraire, localiser ou détruire le watermark inséré. Pour ce faire, une permutation ou une clé secrète peut être utilisée pour l'insertion [Ur-Rehman and Zivic, 2018].

La fonction d'insertion du watermark doit satisfaire les différentes exigences du tatouage en considérant où et comment insérer le watermark [Belferdi, 2019].

La fonction d'insertion *Ins* prend en entrée l'image originale I_O, des clés secrètes K et le watermark W, et retourne en sortie une image tatouée I_W :

$$Ins\left(I_O, W, K\right) = I_W \tag{1.10}$$

Cette image tatouée peut rencontrer des distorsions ou des attaques lors de sa transmission. Certaines distorsions peuvent être intentionnelles comme les attaques de suppression, d'insertion et de remplacement de watermark. D'autres distorsions sont involontaires, comme le bruit ou la compression d'image [Ling and Ur-Rehman, 2015].

1.5.3 Extraction du watermark

L'extraction du watermark est le processus inverse de l'insertion. Le watermark ne peut être localisé ou extrait que par les destinataires concernés de l'image tatouée qui utilisent les mêmes clés secrètes utilisées au processus d'insertion [Ur-Rehman and Zivic, 2018].

La fonction d'extraction *Ext* prend en entrée l'image tatouée I_W et les clés secrètes K, et retourne en sortie un watermark extrait W_E :

$$Ext\left(I_W, K\right) = W_E \tag{1.11}$$

Le watermark extrait W_E de l'image tatouée sera analysé et comparé pour décider par exemple si l'image est authentique ou non (modifiée). Donc la

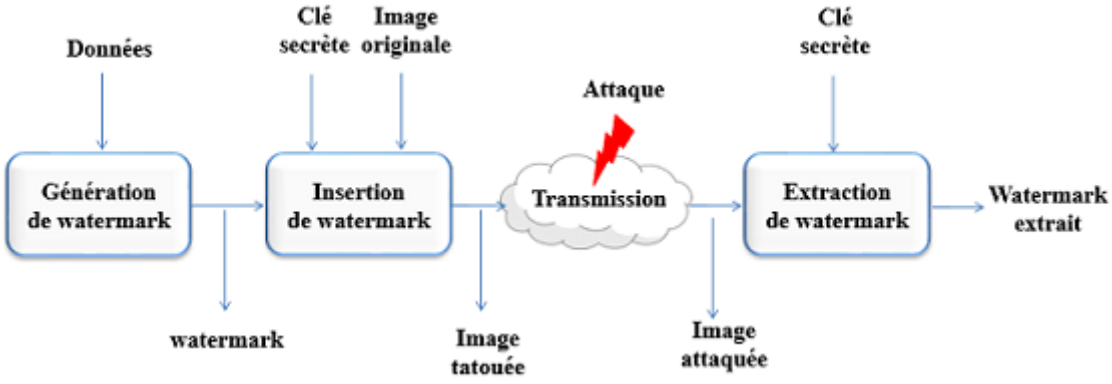


FIGURE 1.3 – Modèle général d'un système du tatouage numérique d'image.

fonction d'extraction aide à prendre une décision selon l'objectif de l'application du tatouage [Ur-Rehman and Zivic, 2018, Belferdi, 2019].

1.6 Applications du tatouage numérique

Une application du tatouage numérique peut avoir différents objectifs qui peuvent être des objectifs de sécurité ou de non sécurité. Objectifs de sécurité pour atteindre certaines propriétés de sécurité telles que l'intégrité de l'image et objectifs non liés à la sécurité pour annoter une base de données d'images afin d'améliorer la gestion [Nyeem et al., 2014] (Figure 1.4).

La plupart des applications du tatouage numérique ont des objectifs de sécurité.

Dans cette section, nous présentons des principaux domaines d'application du tatouage numérique.

1.6.1 Protection des droits d'auteur

La protection des droits d'auteur a été la première préoccupation dans la littérature du tatouage numérique. Les données insérées dans cette application, sont des informations sur le propriétaire légal ou le distributeur. Elles sont utilisées pour notifier un utilisateur que l'article est protégé par des droits d'auteur, pour prouver la propriété de l'article, ou pour suivre des copies illégales de l'article [Tefas et al., 2009].

1.6.2 Contrôle de diffusion

Le tatouage est considéré comme une solution pour fournir des services de surveillance de diffusion. Pour cette application, les informations insérées sont utilisées pour plusieurs buts liés à la diffusion de médias numériques (audio, vidéo). Les données insérées peuvent être utilisées pour vérifier si la diffusion réelle de contenu (par exemple des publicités) est conforme aux

conditions convenues, c'est-à-dire, si le contenu a été diffusé au bon moment et pendant la bonne durée [Tefas et al., 2009].

En plus, les informations insérées peuvent être utilisés pour calculer le taux de regarde/ écoute d'une certaine émission (mesure d'audience), ou pour la conception d'un système automatisé de collecte de redevances pour les données protégées par le droit d'auteur (chansons, films) qui est diffusé par les opérateurs de diffusion [Tefas et al., 2009].

Il faut noter que la surveillance de la diffusion est effectuée généralement par des stations de surveillance automatisées [Tefas et al., 2009].

1.6.3 Suivi des transactions

Dans les applications de contrôle de diffusion et d'identification des propriétaires, le même watermark est inséré à toutes les copies du même contenu. Cependant, dans l'application de suivi des transactions, un watermark unique est inséré dans chaque copie individuelle, ces watermarks utilisés dans ce cas sont souvent appelés empreintes digitales (en anglais fingerprints), ils permettent au propriétaire ou au distributeur de contenu d'identifier la source d'une copie illégale [Cox et al., 2000].

Dans ce cas, le watermark est inséré non seulement pour porter des informations sur le propriétaire ou le distributeur légal de l'article numérique, mais également pour marquer la copie de la transaction. Donc, les informations insérées peuvent être utilisées pour l'identification des responsables sur la distribution illégale de l'objet numérique ou qui n'a pas prend des dispositions efficaces pour empêcher la copie ou la distribution de l'objet et pour décourager de telles actions [Tefas et al., 2009].

1.6.4 Contrôle de copie

Les tatouages pour la surveillance de diffusion, suivi des transactions, identification du propriétaire et preuve de propriété n'empêchent pas la copie illégale. Ils sont utilisés plutôt comme un outil de dissuasion de violation des droits intellectuels ou un outil d'enquête. Cependant, dans les applications de contrôle de copie, les informations insérées peuvent être utilisées avec des appareils appropriés qui réagissent avec ces informations pour interdire l'enregistrement non autorisé d'un élément numérique (contrôle de copie) ou la lecture de copies non autorisées (contrôle de lecture). Donc, le tatouage dans ce cas, permet de contrôler les conditions d'utilisation du contenu numérique [Tefas et al., 2009, Cox et al., 2000].

L'un des exemples de cette application c'est le contrôle de copie et de lecture du DVD à l'aide du tatouage.

1.6.5 Amélioration des anciens systèmes

Dans cette application, le tatouage permet de développer la fonctionnalité des anciens systèmes. Les informations insérées peuvent être utilisées pour

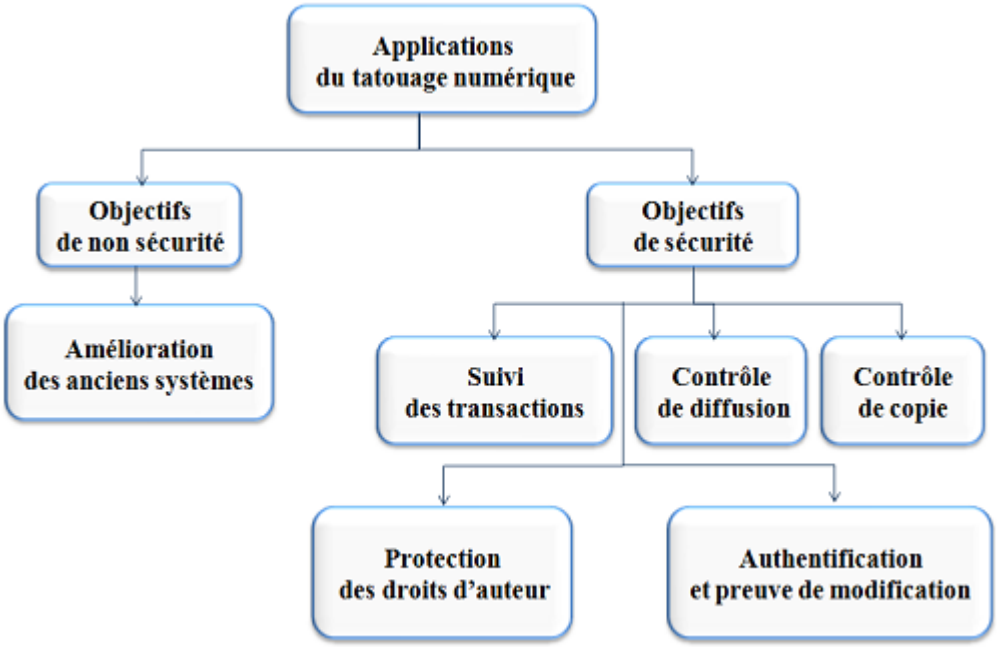


FIGURE 1.4 – Classification des applications du tatouage numérique [Belferdi, 2019].

améliorer les fonctions ou les informations fournies par les systèmes existants tout en maintenant la compatibilité. Par exemple, on peut insérer dans une image numérique une adresse web URL (Uniform Resource Locator) liée à l'objet représenté. Ensuite, cette URL inséré peut être utilisé pour la connecter automatiquement à la page web correspondante. Ainsi, les dossiers des patients peuvent être stockés dans les images médicales radiographiques [Tefas et al., 2009, Belferdi, 2019].

1.6.6 Authentification et preuve de falsification (modification)

L'authentification et la détection de modification des documents numériques sont devenues une grande préoccupation à cause de falsifications faciles fournies par les outils du traitement. Le tatouage numérique est considéré comme un moyen puissant pour l'authentification et la vérification d'intégrité. Dans ce cas, un tatouage fragile doit être utilisé, où toutes les modifications apportées à l'image seront également apportées au watermark. En d'autres termes, toute modification de l'image détruit le watermark. Par conséquent, le contenu devient non fiable (non authentique) [Belferdi, 2019].

Il faut noter que certaines méthodes du tatouage d'authentification peuvent être capables de localiser et récupérer les zones altérées.

1.7 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 (Figure 1.5) [Belferdi, 2019].

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

1.7.1 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 [Al-Ghadi, 2018, Singh et al., 2013].

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 [Al-Ghadi, 2018].

1.7.2 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 [Al-Ghadi, 2018].

Tatouage visible

Dans les méthodes du tatouage visible, le watermark est inséré dans les données originales d'une manière à être perceptible à l'œil 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 [Al-Ghadi, 2018].

Hu et Jeon [Hu and Jeon, 2006], Yip et al. [Yip et al., 2006] et Tsai [Tsai, 2009] ont proposé des méthodes de tatouage numérique visible.

Tatouage invisible

Dans le tatouage invisible, le watermark est inséré dans les données originales de manière à être imperceptible à l'œil humain. Il est utilisé pour plusieurs raisons telles que l'identification de la propriété, l'authentification et vérification de l'intégrité [Al-Ghadi, 2018].

Vongpradhip et Rungraungsilp [Vongpradhip and Rungraungsilp, 2012], Karthigaikumar et al. [Karthigaikumar et al., 2012] et Sathik et Sujatha [Sathik and Sujatha, 2012] ont proposé des méthodes de tatouage numérique invisible.

1.7.3 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 [Belferdi, 2019].

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 permetent 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 [2] (Spread Spectrum) [Boreiry and Keyvanpour, 2017, Belferdi, 2019].

Wu et al. [Wu et al., 2007], Su et al. [Su et al., 2013] et Su et Chen [Su and Chen, 2018] ont proposé des méthodes de tatouage numérique conçues dans le domaine spatial.

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 [3] (Singular Value Decomposition), la transformée en cosinus discrète DCT [4] (Discrete Cosine Transform), la transformée en ondelettes discrète DWT [5] (Discrete

2. SS : La modulation à spectre étalé fait référence à la transmission d'un signal à bande étroite sur une largeur de bande beaucoup plus grande [Al-Ghadi, 2018].

3. SVD est une méthode d'algèbre linéaire qui est utilisée pour diagonaliser une image symétrique afin d'obtenir trois nouvelles matrices U, S et V : matrice singulière (gauche), matrice singulière (droite) et matrice singulière, respectivement [Shehab et al., 2018].

4. DCT : La transformée en cosinus discrète transforme les données du domaine spatial en domaine fréquentiel. Ayant la propriété du compactage énergétique, elle divise l'image en trois parties : basses fréquences, fréquences moyennes et hautes fréquences, la plupart de l'énergie est concentrée dans les basses fréquences [Al-Ghadi, 2018].

5. DWT est la transformation la plus populaire opérant dans le domaine fréquentiel. La décomposition en ondelette est généralement utilisée pour la fusion des images. Elle divise les informations d'une image en approximation (basses fréquences) et des sous-signaux de détail (hautes fréquences). Le sous-signal d'approximation (LL) montre la tendance générale des valeurs des pixels et les trois autres sous-signaux de détail montrent les détails verticaux (LH), horizontaux (HL) et diagonaux (HH) [Boujemaa et al., 2016].

Wavelet Transform) [Belferdi, 2019].

Vongpradhip et Rungraungsilp [Vongpradhip and Rungraungsilp, 2012] , Karthigaikumar et al. [Karthigaikumar et al., 2012] et Sathik et Sujatha [Sathik and Sujatha, 2012] ont proposé des méthodes de tatouage numérique conçues dans le domaine fréquentiel.

1.7.4 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 appelé robustesse [Tefas et al., 2009].

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

Tatouage 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 [Tefas et al., 2009].

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 [Tefas et al., 2009].

Liu et al. [Liu et al., 2006], Wu et al. [Wu et al., 2007] et Su et Chen [Su and Chen, 2018] ont proposé des méthodes de tatouage numérique robuste.

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 telles que le copier-coller et la quantification vectorielle VQ [6](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 [Belferdi, 2019].

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, les applications d'images médicales et les applications d'image satellite [Belferdi, 2019].

6. VQ : La quantification vectorielle est l'approximation d'un signal d'amplitude continue par un signal d'amplitude discrète, elle est utilisée souvent dans la compression avec pertes de données.

Chen et Wang [Chen and Wang, 2009], Rawat et Raman [Rawat and Raman, 2011] et Singh et Singh [Singh and Singh, 2017] ont proposé des méthodes de tatouage numérique fragile.

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 [Tefas et al., 2009].

Ho et Li [Ho and Li, 2004] et Qi et Xin [Qi and Xin, 2011] [Qi and Xin, 2015] ont proposé des méthodes de tatouage numérique semi-fragile.

1.7.5 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 [Tefas et al., 2009].

Les méthodes de tatouage peuvent être classées en deux groupes selon la clé utilisée pendant les processus d'insertion et l'extraction du watermark.

Méthodes symétriques ou méthodes à clé privée

Dans ces méthodes, la même clé est utilisée pour insérer et détecter le watermark [Tefas et al., 2009].

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 [Tefas et al., 2009].

1.7.6 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 :

Schémas d'insertion aveugle

Dans un schéma aveugle, les données du signal hôte sont considérées comme un bruit ou une interférence [Tefas et al., 2009]. 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 [Tefas et al., 2009].

Schémas d'insertion informé

Lors de l'insertion dans les schémas d'insertion informé, 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 connue [Tefas et al., 2009].

1.7.7 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 [Belferdi, 2019].

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 [Belferdi, 2019].

Notez que certaines applications sensibles et de grande importance ne peuvent pas utiliser ces schémas de tatouage, telles que les applications d'images militaires, juridiques et médicales, où toute petite distorsion est difficile à accepter [Belferdi, 2019].

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 [Belferdi, 2019].

Les méthodes de tatouage réversibles sont appropriées aux applications d'authentification et les applications militaires et médicales [Belferdi, 2019].

1.7.8 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 :

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 [Belferdi, 2019, Golea, 2010].

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 [Belferdi, 2019].

Schémas du tatouage aveugle

Les méthodes du tatouage aveugle ne nécessitent que l'image tatouée et la clé secrète pour la détection du watermark, elles ne requièrent pas la disponibilité ni du signal ni du watermark originaux [Belferdi, 2019].

1.8 Attaques contre le système de tatouage numérique d'image

En raison de large disponibilité des logiciels du traitement d'image, les systèmes de tatouage numérique sont devenus sensibles à divers types d'attaques.

Ces attaques peuvent être classées en deux catégories : passives ou non intentionnelles (involontaires) et actives ou intentionnelles (malveillantes) [Nyeem et al., 2014] telle qu'elle est illustrée dans la Figure 1.6.

Dans le contexte du tatouage, une attaque peut être définie comme toute tentative malveillante d'insertion, de suppression ou de détection non autorisée d'un watermark, ou tout traitement qui altère ou rendre le watermark indétectable afin d'empêcher le watermark d'atteindre son objectif [Nyeem et al., 2014].

1.8.1 Attaques passives (involontaires)

Dans ce cas, l'attaquant ne tente pas de supprimer le watermark, mais il essaie juste de déterminer sa présence, en d'autres termes, il tente de détecter

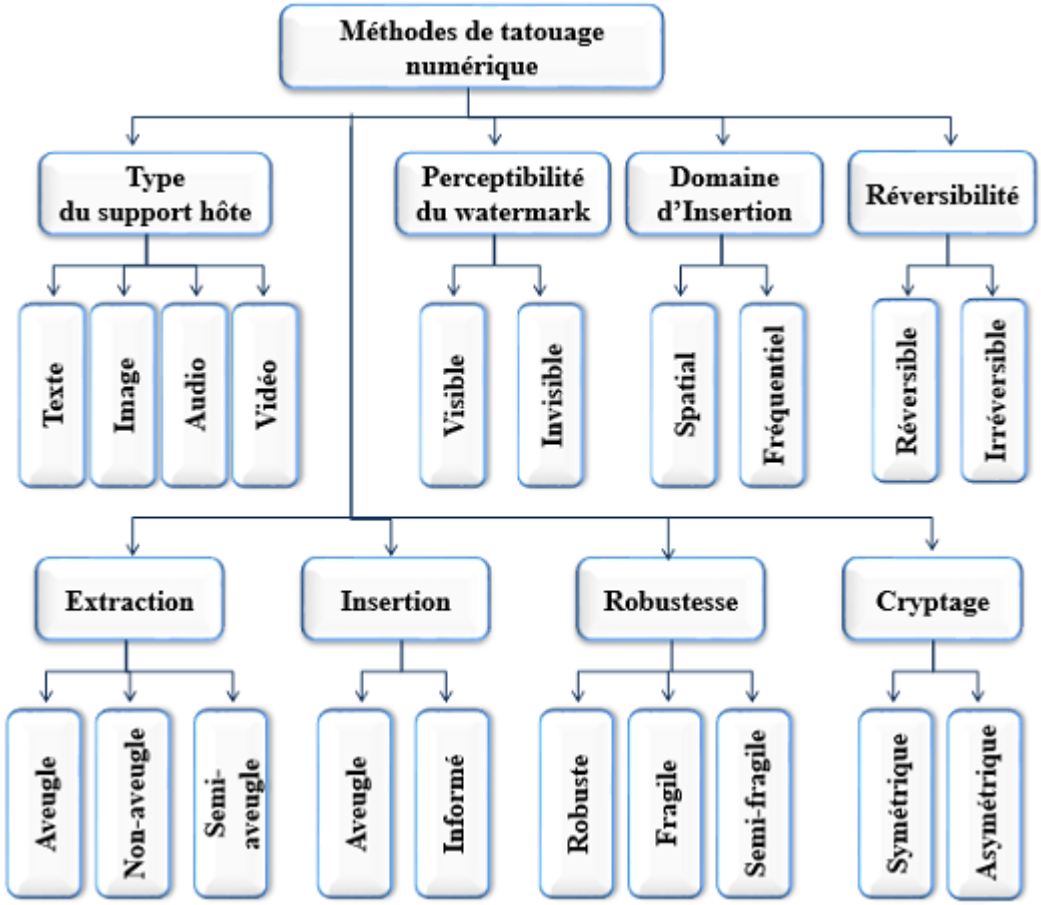


FIGURE 1.5 – Classification des algorithmes du tatouage numérique [Belferdi, 2019].

une communication secrète. La plupart des applications du tatouage ne s'intéressent pas à ce type d'attaque, car la présence du watermark est annoncée pour dissuader les tentatives d'attaque [Cox et al., 2000].

1.8.2 Attaques actives (intentionnelles)

Dans ce cas, un attaquant essaie de supprimer le watermark ou le rendre indétectable afin que l'objectif du watermark soit vaincu [Cox et al., 2000]. Ce type d'attaque est un problème critique pour de nombreuses applications, telles que l'identification du propriétaire, la preuve de propriété, le contrôle de copie et suivi des transactions (les empreintes digitales). Ces attaques actives peuvent être classées en quatre types différents : les attaques de suppression et d'interférence, les attaques géométriques, les attaques cryptographiques et les attaques de protocole [Tao et al., 2014, Saini and Shrivastava, 2014, Jimson and Hemachandran, 2018].

Attaques de suppression et d'interférence

Les attaques de suppression visent à supprimer le watermark. Cependant, les attaques par interférence visent à ajouter un bruit supplémentaire à l'image tatouée. Parmi ces attaques, on a le débruitage, la quantification (par exemple la compression), l'amélioration du contraste, la remodulation, les attaques de collusion et le bruit [Belferdi, 2019, Jimson and Hemachandran, 2018].

1. **Attaques de collusion**
   Cette attaque peut être définie comme une attaque de suppression non autorisée. Dans ce cas, l'attaquant utilise plusieurs copies de l'image tatouée, chacune avec un watermark différent, pour supprimer le watermark et construire une copie de l'image sans tatouage en calculant la moyenne de toutes les copies ou d'une petite partie de chacune des copies [Belferdi, 2019, Al-Ghadi, 2018].
2. **Attaques de débruitage et de compression avec perte**
   Cette catégorie d'attaques comprend des opérateurs de traitement d'image courants tels que la compression avec perte, le débruitage d'image et la quantification. La compression est un schéma populaire pour attaquer des images tatouées. Les attaquants peuvent compresser les images tatouées pour supprimer les watermarks. La compression avec perte et le débruitage peuvent diminuer la capacité du système du tatouage numérique [Belferdi, 2019, Tao et al., 2014].
3. **Attaques de remodulation**
   Dans cette attaque, une soustraction de l'image tatouée à sa version filtrée par un filtre médian est faite pour estimer le watermark, puis, ce watermark estimé est tronqué et filtré par un filtre de passe-haut. Ensuite, ce watermark estimé sera retiré de l'image tatouée [Belferdi, 2019].

Attaques géométriques

Ces types d'attaques sont également appelés attaques de synchronisation ou attaques de transformations. Par contre aux attaques de suppression, les attaques géométriques ne suppriment pas le watermark mais le déforment. En d'autres termes, elles manipulent l'image tatouée de manière rendre le watermark indétectable [Belferdi, 2019].

Les attaques géométriques impliquent généralement des distorsions géométriques issues du traitement d'image comme la rotation, la mise à l'échelle, le recadrage (rognage) et la suppression de colonnes ou de lignes [Belferdi, 2019, Tefas et al., 2009].

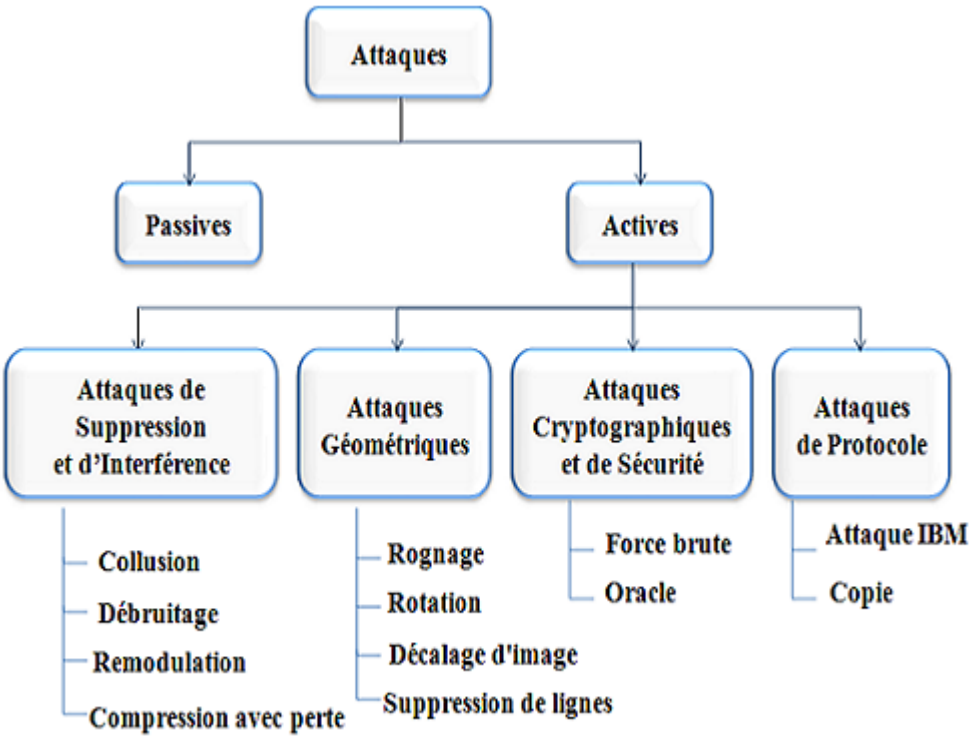


FIGURE 1.6 – Classification des attaques contre un système de tatouage numérique d'image [Belferdi, 2019].

Attaques cryptographiques et de sécurité

Les attaques cryptographiques sont équivalentes aux attaques appliquées en cryptographie. Elles visent à casser les méthodes de sécurité utilisées dans le système de tatouage et à trouver un moyen de supprimer le watermark inséré ou insérer un autre [Belferdi, 2019].

Un exemple de cette catégorie d'attaque est l'attaque de force brute qui vise à découvrir les informations ou les clés secrètes en utilisant les recherches exhaustives, donc, pour lutter contre ces attaques, il est nécessaire d'utiliser des clés avec une longueur sûre [Belferdi, 2019, Voloshynovskiy et al., 2001].

Attaques de protocole (ambiguïté)

L'objectif de cette attaque n'est pas de détruire le watermark inséré ou désactiver son extraction [Belferdi, 2019]. Les attaques de protocole visent à attaquer le concept entier de l'application de tatouage. L'attaque IBM est une attaque de protocole qui consiste à insérer un ou plusieurs watermarks supplémentaires afin que le watermark original soit ambigu [Kaur et al., 2012].

Une autre attaque de protocole est l'attaque de copie qui vise à estimer le watermark inséré et de le copier dans d'autres données, appelées données cibles [Voloshynovskiy et al., 2001].

1.9 Métriques d'évaluation de performance des systèmes du tatouage numérique d'images

Les performances d'un système du tatouage d'image sont évaluées et comparées avec les différents systèmes pour savoir le système du tatouage le plus efficace en termes d'imperceptibilité, de robustesse et de précision de détection [Al-Ghadi, 2018]. Ces performances sont exprimées à l'aide de mesures bien connues telles que le rapport signal/bruit PSNR (Peak Signal to Noise Ratio), indice de similarité structurelle SSIM (Structural SIMilarity) et coefficients de corrélation normalisés NC (Normalized Correlation) (voir la section 1.4).

Précision de détection de modification et restauration de contenu

Pour évaluer les performances d'une approche du tatouage d'image en termes de précision de détection de modification et restauration de contenu trois métriques sont utilisées, le taux de détection de modification R_{TD} (Tamper Detection Rate), le taux de fausse alarme R_{FA} (False Alarm Rate) et le taux de modification R_T (Tampering Ratio) qui sont calculés par les équations (1.12), (1.13) et (1.14) respectivement.

$$R_{TD} = \frac{num_d}{num_m} \times 100\% \tag{1.12}$$

$$R_{FA} = \frac{num_{fd}}{(N \times M \times 3) - (num_m \times n \times m)} \times 100\% \tag{1.13}$$

$$R_T = \frac{num_m \times n \times m}{(N \times M \times 3)} \times 100\% \tag{1.14}$$

Où num_m est le nombre de blocs réellement modifiés, num_d est le nombre de blocs modifiés qui sont détectés, num_{fd} est le nombre de faux pixels détectés, n×m est la taille du bloc et N, M désignent l'hauteur et la largeur de l'image respectivement.

Plus les valeurs de R_{FA} sont faibles, cela signifie que la précision de la détection de modification est meilleure [Belferdi, 2019].

1.10 Conclusion

Dans ce chapitre, nous avons introduit les techniques de protection des données numériques y compris la cryptographie, la stéganographie, le tatouage numérique et la différence entre eux. Nous avons introduit l'historique du tatouage, les propriétés d'un système de tatouage et le modèle général du tatouage numérique, puis, nous avons présenté les différentes applications du tatouage numérique, la classification des algorithmes du tatouage et les attaques possibles contre ces systèmes. Enfin, nous avons introduit les métriques principales d'évaluation de performance du système du tatouage numérique d'image.

Chapitre 2

Tatouage numérique pour l'authentifications des images médicales

2.1 Introduction

Avec l'évolution des systèmes de santé et les besoins de partage des images médicales entre médecins et hôpitaux par internet ou réseaux locaux, la protection de ces images est devenue très nécessaire contre toute modification malicieuse notamment avec l'accès et l'utilisation faciles des outils de la manipulation d'image, ou une modification involontaire issue des erreurs lors de la transmission. Ces modifications peuvent conduire à des erreurs de diagnostic des médecins ou des erreurs d'évaluation d'une pathologie.

Afin de résoudre ce problème, un système qui garantit l'intégrité et l'authenticité des images médicales est nécessaire. Ces systèmes sont basés sur plusieurs méthodes de protection. L'une de ces méthodes c'est le tatouage numérique.

Dans ce chapitre, nous présentons les grands types d'imagerie médicale et les exigences de tatouage numérique des images médicales. Ensuite, nous introduisons les applications et la classification des méthodes de tatouage numérique des images médicales. Après, nous représentons le modèle général d'un système d'authentification d'image, les exigences et la classification de ces systèmes, à la fin de ce chapitre, nous choisissons quelques méthodes d'authentification afin de décrire leurs fonctionnements, leurs étapes et les techniques utilisées.

2.2 Les types d'imagerie médicale

L'image médicale à pris son importance non seulement pour sa nécessité d'établir un meilleur diagnostic, mais aussi pour évaluer les étapes d'une pathologie et assurer l'efficacité d'un traitement.

Selon Benazzouz et Chikhi [Benazzouz, 2014,Chikhi, 2008], il existe quatre types d'imagerie médicale qui sont basés sur l'utilisation des rayons X, des ultrasons, du champ magnétique ou de la radioactivité naturelle ou artificielle (Figure 2.1).

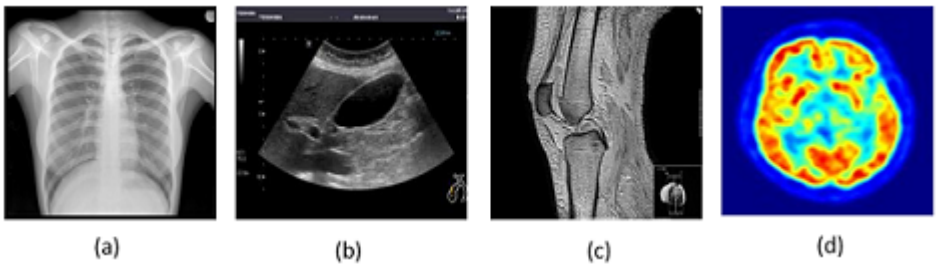


FIGURE 2.1 – Images médicales : (a) image radiographique thoracique, (b) image échographique, (c) IRM de genou, (d) image de médecine nucléaire (cerveau au PET-scan).

2.2.1 Radiographie

Le principe de la radiographie est basé sur l'utilisation des rayons X, dans l'image radiographique les os apparaîtront blancs, les tissus seront en gris et l'air sera noir. La radiographie est utilisée en rhumatologie, en orthopédie, et en orthodontie. En plus, elle est utilisée pour l'observation des anomalies sur certains organes [Benazzouz, 2014, Chikhi, 2008].

2.2.2 Échographie

L'échographie est dérivée du principe du sonar. Les images résultantes de la réflexion des ultrasons sur les organes pleins de l'abdomen, le cœur et tous les organes non masqués par le squelette. Elle est utile à l'observation du fonctionnement des organes [Benazzouz, 2014, Chikhi, 2008].

2.2.3 Imagerie par résonance magnétique

L'imagerie par résonance magnétique (IRM) permet l'acquisition d'images en coupes, dans tous les plans de l'espace, et les représentations tridimensionnelles en visualisant différentes structures, spécialement en les tissus mous et neuro-imagerie [Benazzouz, 2014, Chikhi, 2008].

2.2.4 Image de médecine nucléaire

La médecine nucléaire ou isotopique, c'est un résultat parmi celles de la découverte de la radioactivité où plusieurs types d'images existent y compris :

La scintigraphie

Une scintigraphie est un examen de médecine nucléaire, en utilisant l'injection d'un produit légèrement radioactif, elle permet de prendre des images du corps humain. Ce produit sera fixé suivant l'organe à visualiser, les signaux émis par le produit seront capturés par l'appareil gamma-caméra. La scintigraphie permet le prédiagnostic des anomalies de fonctionnement d'un

organe et de mesurer la dissémination d'un cancer dans l'organisme [Benazzouz, 2014, Chikhi, 2008].

La tomographie par émission de positons (T.E.P.)

La tomographie par émission de positons consiste à observer la répartition et l'utilisation d'une molécule (telle que le glucose) marquée par un isotope radioactif dans les tissus. Cette molécule permet d'obtenir une image des organes et d'observer ses fonctionnements. Cette technique d'imagerie est utilisée pour le diagnostic et le bilan d'extension de plusieurs types de cancers [Benazzouz, 2014].

Le PET-Scan

Le PET-Scan (ou CT-Scan en anglais) est une technique d'imagerie hybride, utilise la tomographie par émission de positons et un scanner à rayons X, en fusionnant les images. La TEP offre l'information isotopique spécifique, le scanner offre une information anatomique précise. Elle est de très haute valeur informative, elle est utilisée pour le diagnostic, le bilan d'extension et la surveillance sous traitement de nombreux types de cancers [Benazzouz, 2014, Chikhi, 2008].

En plus de ces types d'imagerie médicale, il existe **les images médicales microscopiques**.

Dans notre recherche on s'intéresse aux images couleur à cause de leur large utilisation car ces derniers contiennent plus d'informations par rapport aux images en mode gris.

2.3 Exigences de tatouage numérique des images médicales

Le rôle important de l'image médicale impose trois exigences principales : la confidentialité, la fiabilité et la disponibilité [Zain and Fauzi, 2006, Das and Kundu, 2013].

• La confidentialité signifie que seules les personnes autorisées ayant l'accès aux images.

• La fiabilité qui a deux aspects, l'intégrité et l'authenticité. L'intégrité vérifie que les informations n'ont pas été modifiées. L'authenticité garantit que les données concernant le bon patient et vérifie la source d'information.

• La disponibilité : c'est la capacité des utilisateurs autorisés à utiliser les images dans les conditions normales d'accès et de pratique.

Une autre exigence c'est la conservation de la qualité d'image médicale car une dégradation d'image peut affecter le diagnostic.

La technique de tatouage numérique des images médicales permet d'assurer ces exigences.

2.4 Avantages de tatouage numérique des images médicales

En général, le tatouage numérique a apporté plusieurs avantages à la protection des images, comme nous l'avons détaillé dans le chapitre 1. En plus de ces avantages, d'autres apports peuvent être ajoutés dans le domaine médical. Parmi ces apports on peut citer les suivants :

2.4.1 Économie d'espace mémoire

Généralement, les images médicales et les informations médicales relatives au patient sont stockées séparément. En utilisant le tatouage, les informations médicales sont intégrées dans les images correspondantes en une seule entité, ce qui permet d'économiser beaucoup d'espace mémoire [Das and Kundu, 2013, Navas and Sasikumar, 2007].

2.4.2 Évitez le détachement

Comme les images médicales et les dossiers médicaux associés étant stockés séparément, ces dossiers peuvent être détachés des images correspondantes. En outre, une fausse liaison des données à son image médicale correspondante peut entraîner des problèmes majeurs. L'utilisation de tatouage évite cette erreur, en insérant les données dans l'image médicale correspondante [Das and Kundu, 2013, Navas and Sasikumar, 2007].

2.4.3 Économie de bande passante

L'intégration des données de rapport électronique du patient (REP) dans l'image médicale par le tatouage, permet de réduire la bande passante de transmission dans les applications de télémédecine [Das and Kundu, 2013, Navas and Sasikumar, 2007].

2.4.4 Confidentialité et sécurité

L'imperceptibilité et la dépendance des clés dans les techniques de tatouage numérique des images médicales et les techniques de cryptage avancées fournissent des solutions aux problèmes de confidentialité et de sécurité des dossiers des patients, qui sont de haute importance dans la gestion et la distribution des données médicales [Das and Kundu, 2013].

2.4.5 Contrôle d'accès

Le tatouage numérique des images médicales est devenu un mécanisme de contrôle d'accès alternatif, où les métadonnées (rapport électronique du patient (REP)) sont insérées dans l'image de façon à assurer la protection, c'est-à-dire leur accès n'est possible que par l'utilisation d'une clé appropriée [Das and Kundu, 2013, Coatrieux et al., 2000].

2.4.6 Indexage

Les systèmes d'archivage et de communication d'images PACS (Picture Archiving and Communication Systems) récupèrent les images par indexation. Les données démographiques des patients, les codes de diagnostic et les caractéristiques d'acquisition d'images peuvent être utilisés comme des indices ou des mots-clés, le watermark peut également jouer le rôle de mots-clés ou d'indices, en fonction du mécanisme efficace d'archivage et de récupération des requêtes [Das and Kundu, 2013, Giakoumaki et al., 2006].

2.4.7 Sous-titrage

Pour fournir des informations précieuses supplémentaires sur le rapport du patient. Des tatouages de légende ou d'annotation peuvent être utilisés [Das and Kundu, 2013, Giakoumaki et al., 2006].

2.4.8 Authentification

Le tatouage numérique des images médicales combiné avec les techniques cryptographiques fournit un moyen d'authentification d'identité, en insérant le code d'identification du médecin ou la signature numérique cryptée dans l'image médicale. Les données originales ne peuvent être obtenues qu'avec la connaissance de la technique de cryptage et les clés de tatouage [Das and Kundu, 2013, Chao et al., 2002].

2.4.9 Contrôle d'intégrité

L'intégrité des données médicales (images, enregistrements) étant d'une grande importance. Un tatouage numérique fragile des images médicales est utilisé pour la vérification d'intégrité, la localisation des régions modifiées. Il nous aide à déterminer si les données sont fiables ou non [Das and Kundu, 2013, Zain and Fauzi, 2006].

Il existe d'autres applications de tatouage numérique des images médicales telles que la protection de la propriété, la protection des droits d'auteur.

Le tatouage numérique des images médicales est utilisé principalement pour garantir l'authenticité et l'intégrité des images médicales, pour le masquage de rapport électronique du patient (REP) et pour la localisation de modification et la restauration de régions altérées. Il est considéré comme une approche prometteuse pour garantir l'authenticité et l'intégrité des images médicales.

2.5 Classification des méthodes de tatouage numérique des images médicales

Les méthodes de tatouage numérique des images médicales peuvent être classées selon deux critères : l'objectif de l'application et la région d'insertion.

2.5.1 Selon l'objectif

Selon Al-Qershi et Khoo [Al-Qershi and Khoo, 2011], les méthodes de tatouage numérique des images médicales sont classées selon l'objectif de l'application en trois classes : *(i)* masquage de rapport électronique du patient (REP), *(ii)* authentification de contenu (y compris la vérification d'intégrité, la localisation et la restauration des modifications) et *(iii)* méthodes mixtes qui fusionnent le masquage de REP, l'authentification de l'auteur (pour vérifier la source d'information) et l'authentification du contenu.

Méthodes de masquage des données REP

Deux méthodes différentes de tatouage numérique aveugle de masquage des données REP ont été introduites par Parah et al. [Parah et al., 2017]. Les deux méthodes sont basées sur la transformation en cosinus discrète DCT pour insérer le watermark. Les images médicales ont été divisées en région d'intérêt ROI (Region Of Interest) qui contiennent les informations nécessaires pour le diagnostic et de région non d'intérêt RONI (Region Of No Interest) qui est le fond noir de l'image médicale. Dans la première méthode, le watermark et les données REP ont été insérés dans les deux régions ROI et RONI. Dans la deuxième, ils ont été insérés dans le RONI [Qasim et al., 2018].

Méthodes d'authentification du contenu ou contrôle d'intégrité

Pour vérifier le contrôle d'intégrité, plusieurs méthodes masquent un code d'authentification de message MAC (Message Authentication Code) de l'image ou une signature numérique DS (Digital Signature). Au processus d'extraction, une comparaison sera faite entre le MAC ou la DS extrait et recalculé afin de vérifier l'intégrité de l'image.

Parmi les approches proposées pour garantir l'authenticité des images médicales, une méthode consiste à insérer l'identifiant unique de l'en-tête des images DICOM [1] avec les données brutes d'image [Qasim et al., 2018].

Memon et Gilani [Memon and Gilani, 2011] ont proposé une méthode de tatouage numérique aveugle fragile pour assurer l'authentification du contenu des images médicales. Le logo de l'hôpital, les données du patient et le code d'authentification sont insérés dans RONI pour confirmer le contrôle d'intégrité et protéger les données de ROI [Qasim et al., 2018].

Autre méthode de tatouage numérique fragile réversible aveugle a été introduite par Das et Kundu [Das and Kundu, 2013] pour prouver l'intégrité de l'image médicale qui utilise la fonction de hachage sécurisé SHA-256 [2] (secure hash algorithm) pour calculer le hachage de la partie ROI, la compression et le chiffrement sans perte pour insérer les métadonnées DICOM et les informations de localisation de modification dans l'image médicale [Qasim et al., 2018].

Eswaraiah et Reddy [Eswaraiah and Reddy, 2014] ont développé une méthode de tatouage numérique fragile pour valider l'intégrité du ROI, où l'image médicale est divisée en trois parties : les pixels de bordures, ROI et RONI, les informations d'authentification et de récupération du ROI sont insérées dans RONI et le code de hachage de ROI calculé à l'aide de la fonction de hachage sécurisé (SHA-256) est inséré dans les pixels de bordure [Qasim et al., 2018].

D'autres méthodes d'authentification du contenu sont détaillées dans la section 2.6.4.

Méthodes mixtes de tatouage numérique d'authentification et de masquage des données REP

Tareef et al. [Tareef et al., 2014] ont présenté une méthode de tatouage numérique d'authentification et de masquage des données REP afin d'assurer l'intégrité, l'authenticité des images médicales et la récupération des régions altérés. Dans la RONI, la ROI remodelée est insérée pour vérifier l'authentification et récupérer l'image, et le codage clairsemé [3] (Sparse Coding) des données REP est inséré pour enregistrer les informations du patient avec l'image [Qasim et al., 2018].

Pour vérifier l'authentification de la ROI, la détection de modification et la récupération de la région altérée, Al-Qershi et Khoo [Al-Qershi and Khoo,

1. DICOM : Digital Imaging and Communication in Medicine signifie la norme des fichiers numériques issus d'examens d'imagerie médicale de format dcm. Les fichiers DICOM portent des informations textuelles concernant le patient (état civil, âge, poids, etc.), l'examen réalisé (région explorée, technique d'imagerie utilisée, etc.), la date d'acquisition et le praticien https://sti-biotechnologies-pedagogie.web.ac-grenoble.fr/content/fichiers-dicom-format-dcm-en-imagerie-medicale.

2. SHA-256 : la fonction de hachage SHA 256 est une fonction cryptographique qui prend en entrée des données de taille quelconque et calcule un hash de 256 bits https://blog.ippon.fr/2017/02/28/sha-1-hachage-et-securite.

3. Codage clairsemé (Sparse Coding) : Le but du codage clairsemé est de représenter les vecteurs d'entrée comme une combinaison linéaire pondérée d'un petit nombre de vecteurs de base. Ces vecteurs de base capturent ainsi des modèles de haut niveau dans les données d'entrée [Lee et al., 2007].

2011] ont présenté une méthode de tatouage numérique mixte d'authentification et de masquage des données REP. Les informations de patient et le message de hachage de ROI sont insérés dans la partie ROI de l'image médicale DICOM, et en utilisant la transformation en ondelettes discrète DWT (Discret Wavelet Transform), les données de détection et de récupération sont insérées dans la RONI [Qasim et al., 2018].

La Table 2.2 illustre les principales propriétés de quelques méthodes de tatouage des images médicales.

Auteurs	Objectifs	Watermark	Région d'insertion	Technique d'insertion	Réversibilité	Robustesse
Al-Qershi et al.(2011)	-Authentification -Masquage des données	-Données EPR -Message de hachage de ROI -Données de détection et de récupération	ROI RONI	DE DWT	✓	Fragile
Memon et al.(2011)	-Authentification	-Données du patient -Code d'identification -Logo de l'hôpital	RONI	LSB	✓	Fragile
Das et al.(2013)	-Authentification	-Code de hachage ROI -Métadonnées DICOM -Mot-clé d'indexation -Code du médecin -Informations de localisation de modification	Image entière	LSB	✓	Fragile

Auteurs	Objectifs	Watermark	Région d'insertion	Technique d'insertion	Réversibilité	Robustesse
Eswaraiah et al.(2014)	-Intégrité -Détection de modification	-Données d'authentification -Données de récupération du ROI -Code de hachage ROI	-LSB de RONI -LSB de pixels de bordure	LSB	✗	Fragile
Tareef et al.(2014)	-Intégrité Authenticité -Masquage des données	-Code clairsemé d'REP -ROI remodelé	RONI	-Codage clairsemé -SVD	✓	Robuste
Parah et al.(2017)	-Protection des droits d'auteur -Intégrité	-Bits de watermark -Données REP	ROI RONI	DCT	✗	Robuste

TABLE 2.2 – Propriétés de quelques méthodes de tatouage des images médicales [Qasim et al., 2018].

2.5.2 Selon la région d'insertion

Selon Coatrieux et al. [Coatrieux et al., 2006], il existe trois types d'approches de tatouage numérique des images médicales : *(i)* méthodes classiques, *(ii)* méthodes de tatouage de région d'intérêt (ROI) et de région non d'intérêt (RONI) et *(iii)* méthodes de tatouage réversible.

Méthodes de tatouage numérique classiques

Dans les méthodes classiques, le watermark est inséré dans certains détails de l'image comme les LSB ou dans les détails perdus après la compression avec perte d'image tout en minimisant la distorsion [Coatrieux et al., 2006].

Méthodes de tatouage numérique de région d'intérêt (ROI) et de région non d'intérêt (RONI)

Ces méthodes insèrent le watermark dans la région non d'intérêt RONI afin de protéger les données de ROI et donc d'assurer la capacité et la précision de diagnostic, d'autres méthodes insèrent le watermark dans la région d'intérêt (ROI) [Qasim et al., 2018].

Méthodes de tatouage numérique réversible

Les méthodes de tatouage numérique réversibles sont introduites pour récupérer à la fois les informations de tatouage inséré et l'image originale pour éviter toutes erreurs de diagnostic [Qasim et al., 2018].

Ces méthodes réversibles sont classées en quatre sous-groupes selon la technique utilisée : 1) méthodes basées sur la compression pour minimiser la taille des informations de la marque et les informations de récupération de l'image originale, 2) méthodes basées sur la modification de l'histogramme, 3) méthodes basées sur la quantification et 4) méthodes basées sur l'expansion [Qasim et al., 2018].

En plus de ces trois classes (de ROI et de RONI, réversibles, classiques) d'autres méthodes hybrides de tatouage numérique ont été proposées.

Une comparaison entre ces méthodes est représentée dans la Table 2.3.

Classe	Technique d'insertion	Robustesse	Invisibilité	Capacité	Objectifs
Méthodes Classiques	Domaine spatial	Fragile	Haute	Haute	-Intégrité, Authentification
	Domaine fréquentiel	Robuste	Faible	Faible	-Protection de la propriété
Méthodes ROI & RONI	Domaine spatial	Fragile	Haute	Dépendante	-Intégrité, Authentification
	Domaine fréquentiel	Robuste	Faible	Dépendante	-Protection de la propriété
Méthodes Réversibles	Basée sur la compression	Fragile	Haute	Haute	-Intégrité, Authentification
	-Basée sur la modification de l'histogramme	Robuste, Semi-fragile	Faible	Faible	-Protection de la propriété
	-Basée sur la quantification	Fragile	Haute	Haute	-Intégrité, Authentification
	-Basée sur l'expansion	Fragile	Haute	Haute	-Intégrité, Authentification

TABLE 2.3 – Comparaisons entre les trois approches de tatouage numérique des images médicales [Qasim et al., 2018].

2.6 Authentification des images médicales

L'image médicale est importante à l'aide au diagnostic et la prise des décisions, mais avec les problèmes de sécurité de transmission des images, sur l'internet, ou les réseaux locaux, cette dernière doit être protégée contre toute modification ou falsification pour un diagnostic précis et correct. À cette raison, l'authentification des images médicales est devenue l'une des priorités principales de tatouage numérique et plusieurs approches d'authentification ont été proposées.

2.6.1 Modèle général d'un système d'authentification d'image

Généralement, un système d'authentification comme tous les systèmes de tatouage est constitué de trois processus (plus de détails dans la section 1.5) :

1. La génération de watermark à inséré de façon uniques et complexes afin de le rendre difficile à modifier.
2. L'insertion de watermark dans l'image hôte en préservant l'imperceptibilité et les caractéristiques de l'image.
3. L'extraction de watermark pour la décision d'authentification.

Un système d'authentification complet contient deux étapes supplémentaires consistant à localiser et restaurer les zones modifiées (Figure 2.2.)

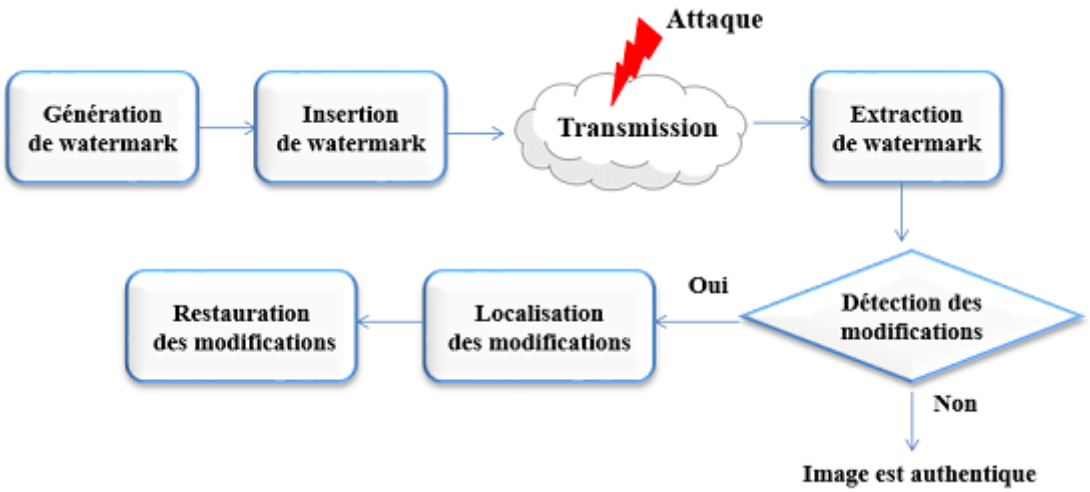


FIGURE 2.2 – Modèle général d'un système d'authentification d'image.

Localisation des modifications

La localisation se réfère à la capacité d'une méthode d'authentification de détecter en précision les régions qui ont été modifiées et les autres régions inchangées [Cox et al., 2007].

Deux approches d'authentification liées à la localisation :

1. **L'authentification par bloc :** consiste à diviser une image en blocs non superposés et insère les données d'authentification dans chaque bloc indépendamment. Si une partie d'image est modifiée, seules les régions affectées ne parviennent pas à s'authentifier. Les méthodes de cette approche sont les plus adaptées [Cox et al., 2007].
2. **L'authentification par échantillon :** est un cas extrême d'authentification par bloc où chaque bloc est réduit à la taille d'un échantillon pour atteindre une localisation plus précise [Cox et al., 2007].

Restauration des zones altérées

La restauration des zones altérées se réfère à la capacité d'une méthode d'authentification de récupérer une partie ou toutes les régions modifiées d'image [Cox et al., 2007].

Il existe deux stratégies de restauration principales : la restauration exacte et le concept le plus récent qui est la restauration approximative [Cox et al., 2007].

1. **La restauration exacte** vise à restaurer l'image à son état original parfait avec la refuse de toute erreur [Cox et al., 2007].
2. **La restauration approximative** vise à restaurer l'image tout en acceptant les différences non significatives entre l'image originale et celle restaurée [Cox et al., 2007].

Cette restauration approximative est divisée en deux approches :

1. Dans la première approche, des informations supplémentaires sont insérées dans l'image afin de l'utiliser dans la restauration [Cox et al., 2007].
2. **La restauration aveugle :** Dans ce cas, un tatouage révélateur [4] peut être utilisé pour déterminer comment l'image a été modifiée. Le watermark est d'abord analysé, puis cette information est utilisée pour inverser la distorsion. Ce processus n'est approprié que si la distorsion est inversible. Ainsi, la restauration aveugle n'est pas utile contre, par exemple, la coupure [Cox et al., 2007].

2.6.2 Exigences d'un système d'authentification d'image

Un système d'authentification efficace, doit satisfaire les exigences suivantes :

4. Le tatouage révélateur : est un tatouage basé sur un watermark révélateur qui permet d'avoir des informations sur la façon dont le watermark inséré a été modifié, plutôt que s'il a été modifié ou non [Cox et al., 2007].

Sensibilité

Un système d'authentification doit être sensible ou capable de détecter toute modification dans l'image tatouée [Haouzia and Noumeir, 2008].

Robustesse

Un système d'authentification doit être tolérant avec les manipulations préservant le contenu et les algorithmes de compression avec pertes telles que JPEG. Cette propriété concerne les algorithmes d'authentification sélective [Haouzia and Noumeir, 2008, Golea, 2010].

Localisation

Un système d'authentification doit avoir la capacité de bien localiser les régions modifiées d'image [Haouzia and Noumeir, 2008].

Récupération

Un système d'authentification doit permettre une restauration totale ou partielle des régions de l'image qui ont été manipulées ou détruites [Rey and Dugelay, 2001].

Portabilité

Un système d'authentification doit porter les informations de tatouage avec l'image protégée lors toute opération de traitement, de transmission ou de stockage [Haouzia and Noumeir, 2008].

Complexité

Un système d'authentification doit utiliser des algorithmes moins complexes qui sont capables de s'effectuer en temps réel [Haouzia and Noumeir, 2008].

Sécurité

Un système d'authentification doit être capable de protéger les données d'authentification contre les modifications [Haouzia and Noumeir, 2008].

2.6.3 Classification des systèmes d'authentification du contenu d'image

Les systèmes d'authentification du contenu (ou une intégrité) d'image (y compris l'image médicale) peuvent être classés en *(i)* authentification stricte ou *(ii)* une authentification sélective [Rey and Dugelay, 2002], tel qu'elle est

démontrée dans la Figure 2.3.

Authentification stricte

Une authentification stricte est utilisée pour les applications qui n'autorisent aucune modification des images protégées telles que les applications médicales et militaires, où une modification d'un ou deux pixels rendre l'image non authentique et peut changer les décisions [Haouzia and Noumeir, 2008].

Les systèmes d'authentification stricte sont divisés en deux groupes selon les techniques utilisées : des méthodes basées sur la cryptographie conventionnelle et des méthodes de tatouage fragile [Haouzia and Noumeir, 2008] (Figure 2.3).

Authentification sélective

Une authentification sélective est utilisée pour les applications où certaines opérations de traitement d'images sont tolérées telles que la compression, le filtrage et les transformations géométriques [Haouzia and Noumeir, 2008].

Les systèmes d'authentification sélective sont divisés en des méthodes basés sur la signature numérique, des méthodes de tatouage semi-fragile et des méthodes de tatouage révélateur [Cox et al., 2007] (Figure 2.3).

La plupart des applications d'image existantes nécessitent l'authentification sélective d'image qui tolère l'utilisation des opérations de traitement d'images afin d'économiser l'espace mémoire et la bande passante ou d'améliorer la qualité de l'image tous en préserve le contenu tel que : la compression, le filtrage, les transformations géométriques et les techniques d'amélioration de l'image [Haouzia and Noumeir, 2008].

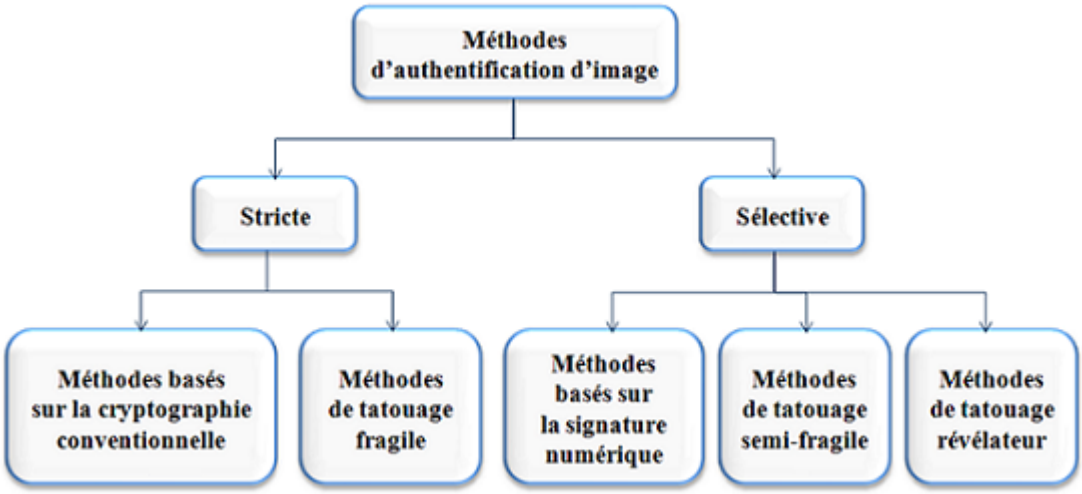


FIGURE 2.3 – Classification des méthodes d'authentification d'image [Belferdi, 2019].

2.6.4 Méthodes d'authentification du contenu (contrôle d'intégrité) des images

Parmi les nombreuses approches d'authentification d'image qui ont été proposées pour maintenir l'authenticité et l'intégrité des images, nous avons choisi quelques méthodes :

Une méthode de tatouage numérique fragile pour l'authentification et la sécurité de contenu des images médicales au niveaux de gris basée sur la transformée en ondelette discrète DWT à été présenté par Boujemaa et al. [Boujemaa et al., 2016]. Dans cette méthode, le watermark est un logo au niveau de gris qui est inséré dans les coefficients des détails des sous-bandes. Avant son insertion, ce logo est converti en une image binaire, puis, cette image binaire est convertie en vecteur, à partir de ce dernier, un autre vecteur est génèré à l'aide d'une clé secrète. Pour insérer ce vecteur, quatre niveaux de la transformée en ondelette discrète DWT sont appliqués sur l'image hôte, puis, le vecteur binaire est inséré dans l'image transformée et la DWT inverse est appliquée pour obtenir l'image tatouée.

A la phase d'extraction, la transformation DWT est effectuée sur l'image reçue, et le watermark est extrait en inversant le processus d'insertion. Le vecteur extrait est décrypté en utilisant la même clé secrète utilisée pour l'insertion, après, il est comparé avec le watermark inséré. Si les deux sont identiques, l'image reçue est authentique, sinon elle est non authentique.

Cette méthode empêche quelques attaques comme l'ajout de bruit (bruit gaussien, sel et poivre), le filtrage (filtrage médian, filtre gaussien et filtrage adaptatif), la rotation et la compression JPEG. Mais, elle est une méthode destinée uniquement à l'authentification du contenu, elle n'est pas capable de restauré les zones endommagés. En plus, elle ne traite que les images médicales en mode gris.

Shehab et al. [Shehab et al., 2018] ont proposé une méthode de tatouage numérique fragile basé sur la décomposition en valeurs singulières SVD (Singular Value Decomposition) pour l'authentification du contenu, pour assurer la localisation de modification et l'auto-récupération des images médicales en niveaux de gris.

Pour fournir une localisation de modification et pour récupérer les régions modifiées, les bits de watermark insérés sont constitués de deux types différents : *(i)* les bits d'authentification de bloc, pour authentifier chaque bloc séparément, où le SVD est calculé pour chaque bloc de 4×4 de l'image hôte. Ensuite, les traces de matrices singulières sont utilisées comme bits d'authentification de bloc, *(ii)* et les bits d'auto-récupération qui sont calculés pour chaque bloc de 2×2, en prenant les 5 premiers bits de poids fort MSB (Most Significant Bit) des valeurs moyennes de chaque bloc. Avant de calculer ces valeurs moyennes, un brouillage Arnold [5] par blocs est effectué et les blocs de

5. La transformation d'Arnold est une méthode de randomisation des blocs d'une image de telle manière qu'ils ne peuvent être inversés que par une clé unique afin de garantir la

4x4 sont à nouveau décomposés en blocs de 2x2, afin que le bloc de voisinage soit récupéré [Shehab et al., 2018].

Pour chaque bloc d'image, les deux types de bits (authentification et auto-récupération) sont insérés dans les deux derniers bits de poids faible LSB (Least Significant Bit) des pixels du bloc de 4x4. Les positions utilisées pour l'insertion de ce watermark sont déterminées à l'aide de la transformation d'Arnold, qui est généré à l'aide d'une clé secrète [Shehab et al., 2018].

À la phase d'extraction, le watermark est extrait de LSB de bloc de 4x4 d'image tatouée, puis mettre à zéros tous les LSB et recalculer les bits d'authentification de bloc. Après le brouillage effectué sur le bloc d'image tatouée avec la même clé que celle utilisée pendant le processus d'insertion. Les bits d'auto-récupération sont calculés de la même manière utilisée au processus d'insertion. Ensuite, les bits d'authentification extraits et les bits d'authentification calculés sont comparés et ainsi les informations d'auto-récupération. Les blocs ayant les mêmes bits d'authentification sont marqués comme non modifiée et le reste est marqué comme modifié. À l'aide des informations d'auto-récupération extraites des LSB de l'image tatouée, les bits des blocs modifiés sont récupérés [Shehab et al., 2018].

Cette méthode empêche quelques attaques comme la suppression de contenu, les attaques de copier-coller, les attaques d'ajout de texte et les attaques de quantification vectorielle VQ (Vector Quantization). Elle est caractérisée par sa capacité de l'authentification du contenu, de la localisation de modification et la récupération de zones altérées des images médicales, mais elle ne traite que les images en mode gris.

Agung et al. [Agung et al., 2012] ont introduit une méthode de tatouage fragile réversible basé sur la compression RLE (Run Lenght Encoding) et la modification des LSB pour l'authentification de contenu, la détection des modifications et la récupération des images médicales aux niveaux de gris.

Dans cette méthode, l'image est divisée en ROI (Region Of Interest) où le watermark sera inséré, et RONI (Region Of Non Interest). La ROI est divisée en blocs de 6x6 pixels et chaque bloc est ensuite divisé en 4 sous-blocs de 3x3 pixels, la RONI est divisée en blocs de 6x1 pixels, une séquence de mappage de blocs est utilisé pour choisir où les informations de récupération d'un bloc seront insérées. Les LSB d'origine sont compressés à l'aide de l'algorithme de compression RLE (Run Lenght Encoding) et seront insérés dans les LSB du bloc des RONI, les LSB d'origine de chaque pixel de l'image sont mis à zéro. Le watermark à insérer est calculé de chaque sous-bloc, il contient 9 bits : 2 bits d'authentification et 7 bits de récupération. Les bits d'authentification sont utilisés pour vérifier si le bloc est altéré ou non, et les bits de récupération qui sont les informations de récupération du sous-bloc correspondant d'un autre bloc (bloc cible) qui sont insérées dans ce bloc pour récupérer les zones altérées, ces informations de récupération sont constituées de 7 bits de poids fort MSB (Most Significant Bit) d'intensité moyenne du sous-bloc. Pour chaque bloc, l'intensité moyenne du bloc et de son sous-bloc sont calculés,

sécurité des blocs d'image hôte et fournir une capacité d'auto-récupération [Shehab et al., 2018].

puis, un bit d'authentification et un bit de parité sont générés pour chaque sous-bloc. Ensuite, les 9 bits sont insérés dans les LSB du sous-bloc.

À la phase de détection des modifications et de récupération, l'image est divisée en ROI et RONI comme dans le processus d'insertion. La ROI est divisée en blocs de 6x6 pixels, ensuite chaque bloc est divisé en quatre sous-blocs de 3x3 pixels. Le bit d'authentification et le bit de parité seront extraits. Les LSB du bloc sont mets à zéro et l'intensité moyenne du bloc et de sous-bloc sont calculées afin de générer le bit d'authentification et le bit de parité, puis les comparez avec le bit d'authentification et le bit de parité extraits pour savoir si le bloc est modifié ou non. Les blocs altérés seront récupérés en localisant ses blocs de récupération en utilisant la séquence de mappage utilisée dans le processus d'insertion. Pour chaque sous-bloc du bloc modifié, la valeur de tous les pixels sera remplacée avec les informations de récupération obtenue à partir de son sous-bloc correspondant.

Afin de restaurer les LSB d'origine d'image, la RONI est divisée en blocs de 6x1 pixels, chaque séquence RLE inséré dans un bloc dans RONI sera obtenue, décodée et insérée aux pixels appropriés.

Cette méthode empêche certaines attaques comme les attaques de modification des blocs, l'attaque globale de la netteté, de la luminosité et l'attaque de réglage du contraste. Elle est considérée comme une méthode d'authentification complète qui assure l'authentification du contenu, la localisation de modification et la récupération de zones altérées des images médicales, c'est une méthode de tatouage réversible ce qui permet de restaurer les valeurs originales des pixels, et par conséquent, d'obtenir une image récupérée très corrélée avec celle d'origine. Tandis que, cette méthode est comme la plupart des méthodes proposées, ne traite que les images en mode gris.

Belferdi et al. [Belferdi et al., 2018] ont proposé une méthode d'auto- insertion de tatouage fragile pour l'authentification, la détection et la restauration de modification d'images couleurs.

Cette méthode est basée sur la technique d'auto-insertion, ce qui signifie que le watermark à insérer est généré de l'image hôte lui-même, où une copie de l'image hôte couleur réduite est insérée. Afin de minimiser la quantité des données d'authentification et de récupération. L'image hôte est divisée en trois composantes couleurs rouge R, verte V et bleue B, chaque composante est divisée en blocs de taille nxm et la moyenne de chaque bloc est calculé pour construire une image couleur réduite, après, cette image réduite sera convertie à une image en mode gris à l'aide de filtre chromatique de Bayer CFA (Color Filter Array) (section 3.3.1). Puis, elle est divisée en quatre parties, chaque partie de ce watermark sera permutée trois fois à l'aide des trois clés différentes en utilisant la permutation de Torus Automorphism (section 3.3.2), ces vecteurs binaires de watermark seront insérées dans l'image hôte.

Pour insérer le watermark, l'image hôte couleur est divisée en trois composantes couleurs rouge R, vert V et bleu B, et chaque composante est divisée en blocs de taille nxm, après, les vecteurs binaires de watermark sont insérés dans les bits LSB des blocs dans des endroits différents des composantes

rouge R, vert V et bleu B de l'image hôte couleur afin d'augmenter la sécurité et la robustesse.

À la phase d'extraction, les valeurs des trois copies de chaque partie de watermark sont extraites puis comparées, si les trois copies de chaque partie de watermark sont égaux, l'image considérée comme authentique, sinon elle est non authentique.

En cas de modification, les auteurs proposent d'utiliser la technique de vote majoritaire pour préciser quelle valeur est modifiée et les quelles restes inchangées. Ces valeurs inchangées sont utilisées pour inverser le processus de réduction et reconstruire une image fortement corrélée avec l'image originale, cette dernière est utilisée à la récupération des régions altérées où chaque pixel modifié dans l'image attaquée est remplacé par le pixel correspondant dans l'image reconstruite.

Cette méthode empêche les attaques de coupure ou suppression de contenu, de collage et des attaques hybrides (coupure et collage). C'est une méthode d'authentification qui assure l'authentification du contenu et capable même de localiser les modifications et récupérer les zones altérées. Elle exploite les caractéristiques des images couleurs pour générer un watermark réduit. En plus, les informations à insérer dans l'image hôte sont des informations de contrôle et de restauration au même temps grâce à la technique d'auto-insertion. Donc, elle traite les images couleurs, tandis que, la plupart des méthodes proposées se sont focalisées sur les images en mode gris. Pour cela nous l'avons choisi pour l'implémenter et tester ces performances sur les images médicales.

La Table 2.5 représente les propriétés de ces quatre méthodes d'authentification du contenu d'image.

Auteurs	Objectifs	Watermark	Région d'insertion	Techniques utilisées	Technique d'insertion	Réversibilité	Robustesse	Image couleur/en gris	Attaques
[Agung et al., 2012]	Authentification	Bits d'authentification	ROI	Compression RLE	LSB	✓	Fragile	en mode gris	Modification des blocs, Attaque globale de la netteté, la luminosité, et le réglage du contraste
	Localisation de modification Restauration	Bits de récupération	RONI						
[Boujemaa et al., 2016]	Authentification	Image logo de docteur	Les coefficients des détails des sous-bandes	DWT	DWT	✗	Fragile	en mode gris	Ajout de bruit, Filtrage, Rotation, Compression jpeg
[Shehab et al., 2018]	Authentification	Bits d'authentification	LSB de l'image entière	SVD	LSB	✗	Fragile	en mode gris	Attaque de copier-coller, Ajout de texte, Coupure, Attaque VQ
	Localisation de modification Restauration	Bits de récupération		Transformation d'Arnold					

Auteurs	Objectifs	Watermark	Région d'insertion	Techniques utilisées	Technique d'insertion	Réversibilité	Robustesse	Image couleur/en gris	Attaques
[Belferdi et al., 2018]	Authentification Localisation de modification Restauration	Image	LSB de l'image entière	CFA Permutation de torus	LSB	✗	Fragile	couleur	Coupure Collage Hybride

TABLE 2.5 – Propriétés des méthodes d'authentification d'image.

2.7 Conclusion

Dans ce chapitre, nous avons présenté les différents types d'imagerie médicale, les applications de tatouage numérique des images médicales et les classifications existantes de ces méthodes de tatouage avec quelques méthodes de chaque classe, après, nous avons présenté le modèle général d'un système d'authentification d'image, les exigences et la classification de ces systèmes, puis, nous avons décrit quelques méthodes d'authentification, leurs fonctionnements, leurs étapes et les techniques utilisées.

D'après les méthodes d'authentification du contenu que nous avons vu dans ce chapitre, nous avons constaté que la diversité des attaques possibles contre un système d'authentification et la différence de type d'image en terme de couleur (image couleur, image en mode gris), rendre l'élaboration d'un système d'authentification idéale qui empêche tous les attaques possibles et traite tous les types d'images (couleur, gris) impossible ou difficile à mise en œuvre, et cela a conduit à la diversité des méthodes d'authentification du contenu proposées et ses caractéristiques.

Nous avons choisi la méthode d'authentification proposée par Belferdi et al. [Belferdi et al., 2018] pour décrire en détail ses processus, l'implémenter et tester ses performances sur les images normales et particulièrement sur les images médicales couleur, et c'est ce que nous discutons dans le chapitre 3.

Chapitre 3

Expérimentation

3.1 Introduction

Dans ce chapitre, nous présentons l'algorithme de tatouage fragile basé sur le modèle de Bayer pour l'authentification, la détection et la restauration des images en couleur que nous avons implémenté. Nous décrivons les différents processus et les résultats expérimentaux, puis nous évaluons ses performances.

Nous commençons par la présentation de l'algorithme, puis les techniques et les processus, ensuite, nous présentons une étude expérimentale sur des images générales couleur et des images médicales couleurs afin d'évaluer les performances de cet algorithme d'authentification.

3.2 Motivation

Pour l'implémentation, nous avons choisi la méthode d'authentification d'image proposée par Belferdi et al. [Belferdi et al., 2018] afin de l'appliquer et tester ses performances sur les images générales couleur et particulièrement sur les images médicales couleurs. Comme les auteurs de cet algorithme ont proposé dans leur future perspective, et en raison de ses caractéristiques : elle est une méthode d'authentification d'image complète qui assure l'authentification du contenu et capable aussi de faire la détection des modifications et la restauration des zones endommagées, elle traite les images couleurs, tandis que, la plupart des méthodes proposées sont focalisées sur les images en niveau de gris.

C'est une méthode de tatouage numérique fragile pour l'authentification du contenu, la détection et la restauration de modification d'image couleur RVB basée sur la technique d'auto-insertion, elle utilise un filtre chromatique CFA pour réduire l'image hôte couleur en un watermark en niveau de gris afin de diminuer la quantité d'informations à insérer et par conséquent, de préserver la qualité d'image tatouée, et pour améliorer la sécurité, elle utilise la permutation de Torus automorphisme pour brouiller le watermark [Belferdi et al., 2018].

3.3 Préliminaires

Belferdi et al. [Belferdi et al., 2018] ont utilisé deux techniques principaux pour construire leur algorithme : une permutation de Torus Automorphism et un filtre chromatique CFA (Bayer Color Filter Array). Le premier est utilisé pour permuter les données insérées afin d'améliorer la sécurité, tandis que, le dernier est utilisé pour réduire l'image hôte en couleur et récupérer les zones endommagées.

3.3.1 Modèle de filtre chromatique de Bayer

Généralement, les composantes rouges (R), vertes (V) et bleues (B) sont les plus utilisés dans une image couleur qui nécessite au moins trois composantes couleurs pour chaque pixel. Cependant, cela serait difficile et coûteux à mettre en œuvre, d'où vienne l'idée d'utiliser des filtres pour minimiser le nombre de composants pour chaque pixel [RajaRao et al., 2015].

L'algorithme d'authentification d'image de Belferdi et al. [Belferdi et al., 2018] utilise le filtre chromatique de Bayer CFA (Color Filter Array) pour convertir une image couleur à une image en niveaux de gris afin de l'utiliser comme un watermark. Ce filtre est l'un des filtres les plus connus et les plus utilisés dans la littérature.

Le filtre chromatique de Bayer (CFA) consiste à capturer pour chaque pixel une seule composante de couleur soit verte, rouge ou bleue tout en préservant la corrélation entre les intensités de pixels voisins [Pei and Tam, 2003].

Le principe de ce filtre se base sur le fait que la composante verte est considérée comme l'information de luminance, ce qui signifie que la modification de cette composante influe sur la qualité visuelle de l'image. En outre, les composantes rouge et bleue sont considérées comme l'information chromatique, alors, la densité des composantes vertes est deux fois supérieure à celle des composantes de couleur rouge et bleue (Figure 3.1), afin d'assurer la meilleure qualité visuelle de l'image [Pei and Tam, 2003].

Pour inverser l'application de ce filtre (Figure 3.1) et obtenir l'image originale couleur, le processus de dématriçage est appliqué. Ce dernier consiste à une interpolation ou une estimation des pixels manquants dans une image CFA où deux couleurs manquantes doivent être interpolées à partir des pixels voisins à chaque emplacement [Pei and Tam, 2003, RajaRao et al., 2015].

L'algorithme d'authentification d'image de Belferdi et al. [Belferdi et al., 2018] utilise aussi ce filtre au processus de détection et de restauration pour interpoler le watermark en niveau de gris, afin d'obtenir une image couleur fortement corrélée avec l'originale.

3.3.2 Permutation de Torus

La permutation de Torus est une fonction pseudo-aléatoire à deux dimensions qui assigne l'index de ligne et de colonne d'un bloc à celui d'un autre [Voyatzis and Pitas, 1996].

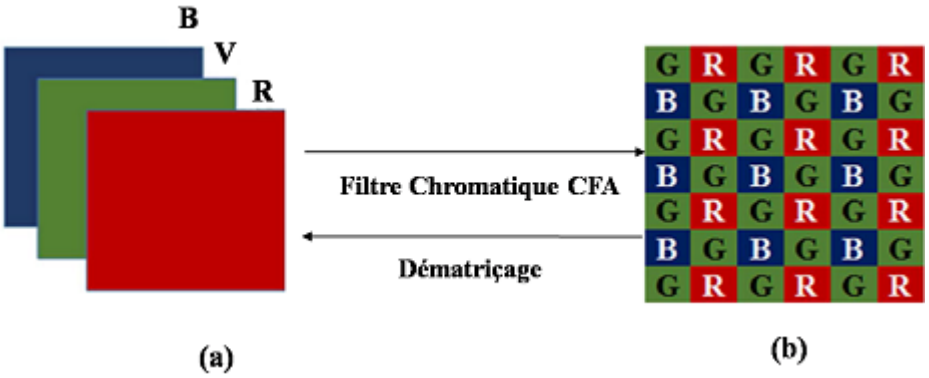


FIGURE 3.1 – Le filtre chromatique de Bayer CFA (Color Filter Array) : (a) : composantes R, V et B des images en couleur, (b) : image CFA [Belferdi et al., 2018].

L'expression d'automorphisme de Torus est définie comme suit [Voyatzis and Pitas, 1996] :

$$\begin{pmatrix} i' \\ j' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ k & k+1 \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \bmod S \tag{3.1}$$

Chaque pixel de watermark à la position (i, j) sera déplacé vers une nouvelle position (i', j'), où S est égale à la taille H × W du watermark, tandis que les valeurs des clés secrètes k sont des nombres premiers aléatoires choisis par l'utilisateur pour brouiller ou désembrouiller le watermark afin d'améliorer la securité.

3.4 Algorithme de tatouage fragile basé sur le modèle de Bayer

L'algorithme d'authentification d'image de Belferdi et al. [Belferdi et al., 2018] est composé de quatre processus comme la Figure 3.2 montre : le processus de prétraitement de watermark, le processus d'insertion de watermark, le processus d'extraction de watermark et le processus de détection et de restauration.

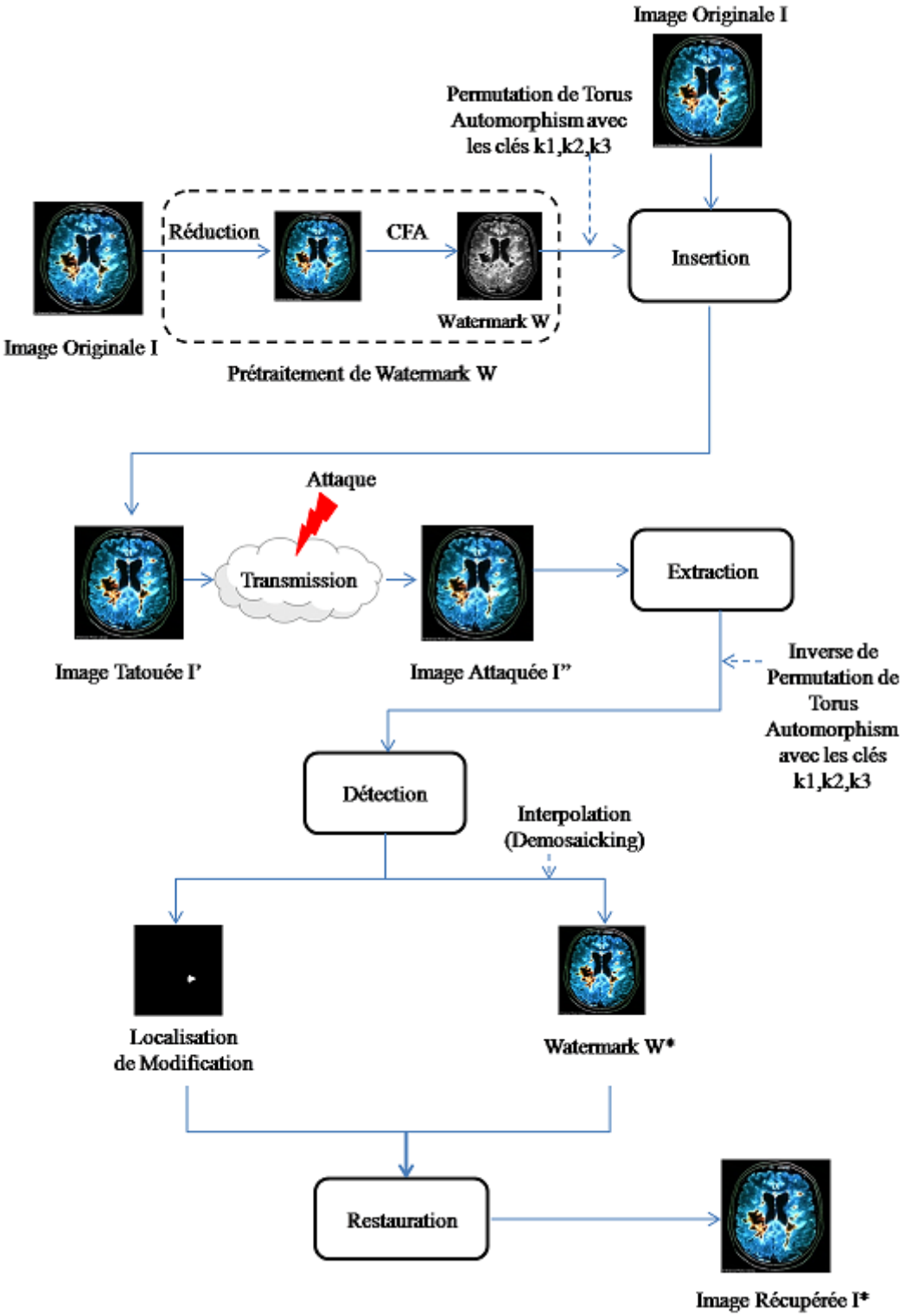


FIGURE 3.2 – Les différentes étapes de la méthode d'authentification d'image de [Belferdi et al., 2018].

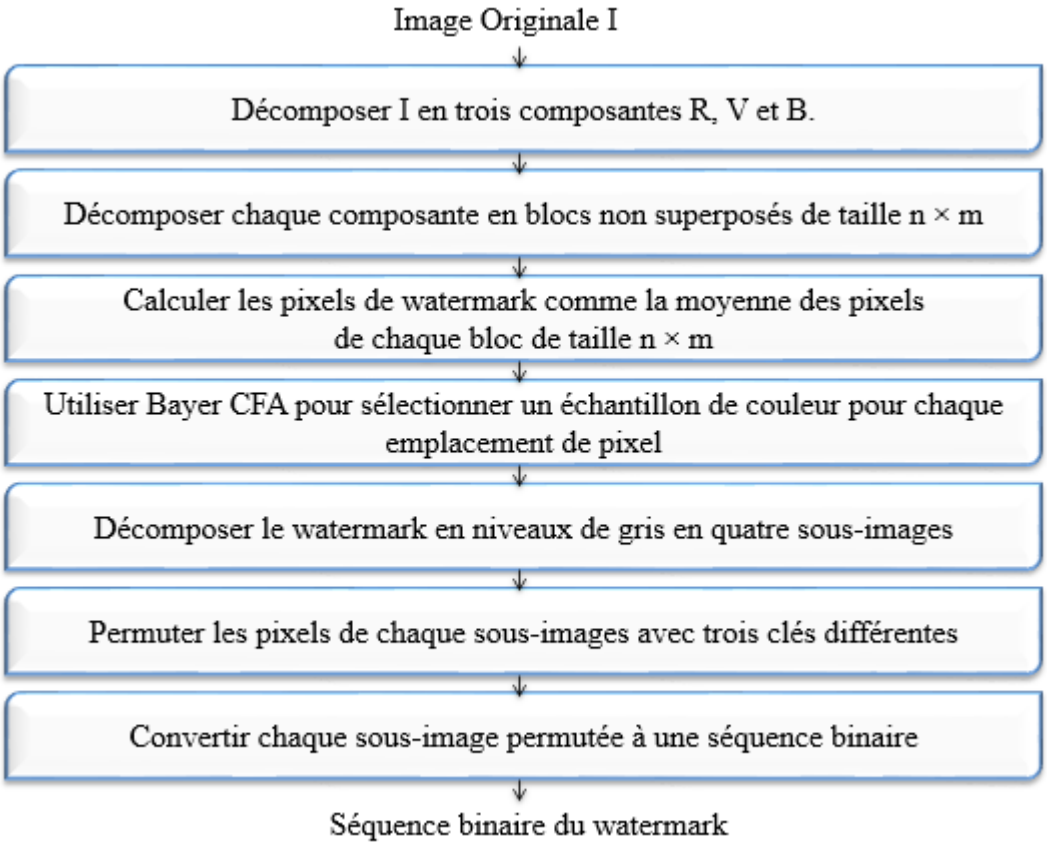


FIGURE 3.3 – Organigramme du processus de prétraitement de watermark [Belferdi et al., 2018].

3.4.1 Processus de prétraitement de watermark

Dans l'algorithme de Belferdi et al. [Belferdi et al., 2018], les auteurs proposent d'utiliser une technique d'auto-insertion pour insérer le watermark, cette technique consiste à utiliser l'image hôte elle-même comme un watermark au lieux d'utiliser une autre image, afin de profiter de watermark extrait pour vérifier l'authentification de l'image d'une part et de récupérer les zones modifiées d'une autre part. Ce qui permet d'éviter l'insertion de deux types d'informations dans l'image (des informations de contrôle et des informations de restauration).

Le problème que l'insertion de l'image hôte tel qu'elle est dans lui-même n'est pas possible, ce qui implique le passage par un certain traitement tel que la réduction, où l'image hôte en couleur est réduite en une image en niveau de gris et utiliser comme un watermark, tel qu'elle est montrée dans la Figure 3.3 et les étapes suivantes :

1. Tout d'abord, l'image couleur I de taille N×M est décomposée en trois composantes R, V et B.
2. Ensuite, chaque composante est décomposée en n×m blocs non superposés, où le bloc de taille n×m est sélectionné selon un compromis entre l'invisibilité du watermark et la qualité d'image (section 1.4).

3. Les pixels du watermark sont calculés comme étant la moyenne des pixels de chaque bloc (n×m) non superposé dans l'image hôte, le watermark obtenu est une image réduite de l'image originale avec une taille de $3 \times \frac{N \times M}{n \times m}$.
4. Pour mieux réduire le watermark et avoir une image en niveaux de gris, le filtre chromatique de Bayer CFA est appliqué. Donc, le watermark obtenu est de taille de $\frac{N \times M}{n \times m}$.
5. Pour améliorer la sécurité et la robustesse de cet algorithme, le watermark en mode gris est décomposé en quatre sous-images $W_{1,2,3,4}(i,j)$ où $i \in \left[1, \frac{M}{2 \times m}\right]$ et $j \in \left[1, \frac{N}{2 \times n}\right]$.
6. Chaque sous-image de watermark $W_{1,2,3,4}(i,j)$ est permutée trois fois avec trois clés différentes k_1, k_2 et k_3 en utilisant la permutation de Torus.
7. Enfin, chaque sous-image permutée est convertie en une séquence binaire.

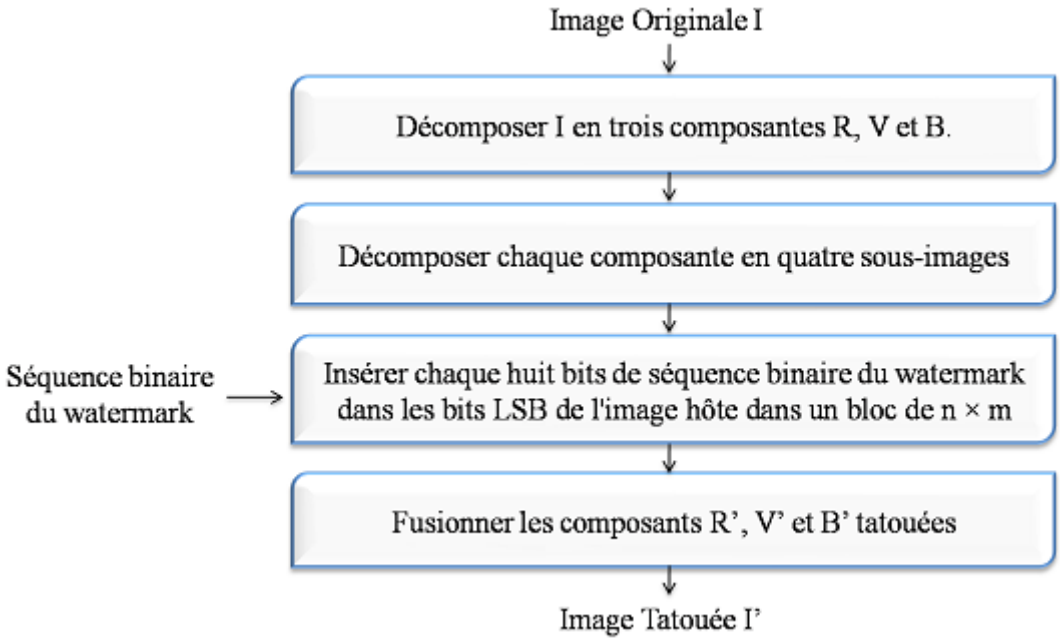


FIGURE 3.4 – Organigramme du processus d'insertion de watermark [Belferdi et al., 2018].

3.4.2 Processus d'insertion de watermark

Après la phase de prétraitement, le watermark est inséré dans l'image hôte couleur en suivant ces étapes (Figure 3.4) :

1. Premièrement, l'image hôte couleur est décomposée en trois composantes R, V et B, et chaque composante est décomposé en quatre sous-images $R_q(i,j)$, $V_q(i,j)$, $B_q(i,j)$ où $q \in \{1,2,3,4\}$ et $i \in \left[1, \frac{N}{2}\right]$ et $j \in \left[1, \frac{M}{2}\right]$.

2. Afin d'améliorer la sécurité et d'augmenter la robustesse, chaque sous-image de watermark [1] est insérée dans une sous image de l'image hôte selon une permutation telle qu'elle est démontrée dans la figure 3.5.
3. Chaque huit bits de l'image watermark sont insérés dans les bits LSB de l'image hôte dans un bloc de n×m.
4. Finalement, les composantes R, V et B tatouées sont fusionnées pour obtenir l'image tatouée.

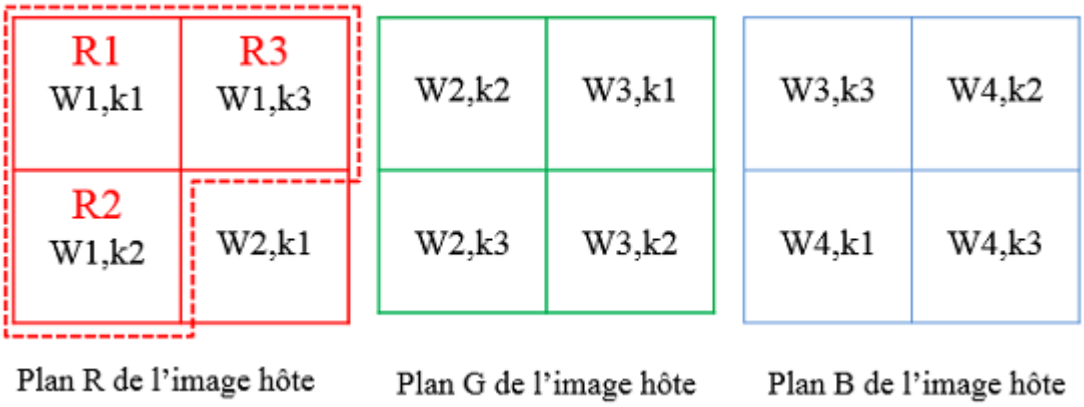


FIGURE 3.5 – Schéma illustrant les positions des sous-images de watermark W_1, W_2, W_3 et W_4 permutées et insérées dans les sous-image de l'image hôte couleur ; (par exemple : la sous-image W_1 du watermark est permutée avec les clés k_1, k_2 et k_3 et insérée dans les sous-images R_1, R_2 et R_3 d'image hôte respectivement [Belferdi et al., 2018].

3.4.3 Processus d'extraction de watermark

Le processus d'extraction est le processus inverse d'insertion [Belferdi et al., 2018], il est appliqué après la réception d'une image tatouée (Figure 3.6) :

1. Premièrement, l'image couleur tatouée probablement modifiée est décomposée en trois composantes R, V et B.
2. Ensuite, chaque composante est décomposée en quatre sous-images $R_q(i,j)$ où $q \in \{1,2,3,4\}$ et $i \in \left[1, \frac{N}{2}\right]$ et $j \in \left[1, \frac{M}{2}\right]$.
3. Chaque sous-image est décomposée en n×m blocs non superposés.
4. Les bits LSB sont extraits et chaque 8 bits extraits de bloc non superposé de n×m sont convertis en valeur entière pour obtenir la valeur en décimale du pixel de watermark.
5. Enfin, la permutation de Torus est inversée en utilisant les mêmes clés k_1, k_2 et k_3 de processus de prétraitement.

1. Chaque sous image de watermark est sous forme d'une séquence binaire.

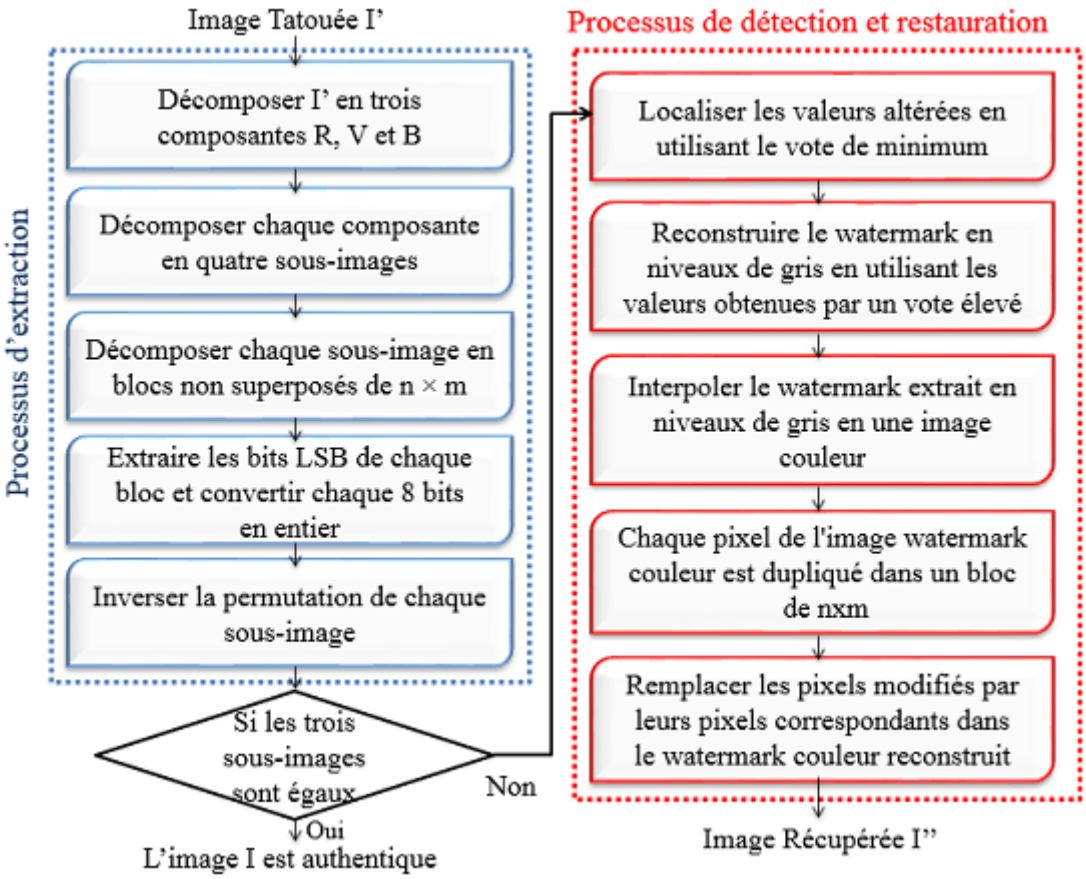


FIGURE 3.6 – Organigramme des processus d'extraction et processus de détection et restauration [Belferdi et al., 2018].

3.4.4 Processus de détection et de restauration

Pour décider si l'image reçue est modifiée ou non. On compare les trois vecteurs de watermark extraits, si chaque trois valeurs extraites de même emplacement sont égaux, l'image est considérée comme authentique. Sinon, un vote majoritaire est appliqué pour préciser les valeurs inchangées afin de les utilisées pour reconstruire le watermark, tandis que, les valeurs modifiées sont marquées par le vote de minimum (Figure 3.6) [Belferdi et al., 2018] :

1. Les valeurs obtenues par un vote élevé sont utilisées pour reconstruire l'image watermark en niveaux de gris avec une taille $\frac{N \times M}{n \times m}$.
2. L'image de watermark extraite en niveaux de gris est interpolée pour avoir une image couleur de taille de $3 \times \frac{N \times M}{n \times m}$.
3. Chaque pixel de watermark reconstruit est dupliqué dans un bloc de n×m, pour obtenir une image de même taille que celle falsifiée, afin de l'utiliser pour récupérer les régions altérées.
4. Enfin, les pixels marqués comme falsifiés sont remplacés par leurs pixels correspondants dans le watermark reconstruit.

3.5 Implémentation et résultats expérimentaux

3.5.1 Environnement

Pour implémenter l'algorithme de [Belferdi et al., 2018], nous avons utilisé un PC avec un processeur Intel Core i5 à 2,60 GHz avec 4 Go de RAM.

Pour le langage de programmation, nous avons utilisé C++ sous l'environnement Microsoft Visual Studio 2015 avec l'intégration de la bibliothèque graphique Open CV 3.3.1.

3.5.2 Implémentation

Selon Belferdi et al. [Belferdi et al., 2018] le choix de la taille de bloc nxm et le choix de nombre de bits LSB se fait selon un compromis entre l'invisibilité de watermark et la qualité de l'image récupérée. Celle ci augmente en diminuant la taille de bloc n×m de l'image hôte et en diminuant le nombre de bits LSB utilisés pour insérer le watermark. Dans leurs recherche, les auteurs ont choisi la taille de bloc égale à 2x2 et le nombre de bits LSB égale à 2 pour implémenter cet algorithme.

Pour concevoir le programme principal, nous avons implémenté plusieurs fonctions, les fonctions principales sont : la fonction de réduction d'image hôte, la fonction de filtre chromatique CFA, la fonction de permutation de Torus automorphism, la fonction de permutation inverse, la fonction d'insertion de watermark, la fonction d'extraction de watermark, la fonction de détection de modification et la fonction de restauration de contenu. En outre, nous avons implémenté d'autres fonctions telles que : les fonctions d'évaluation de performance (PSNR, SSIM, NC, R_{TD}, R_{FA} et R_T).

- Fonction de filtre chromatique CFA

Cette fonction permet de convertir l'image hôte couleur réduite à une image en mode gris.

Entrée : trois composantes d'image couleur RVB.

Sortie : image en mode gris.

```
CvMat*CFA(CvMat*R, CvMat*G, CvMat*B)
{
CvMat*S = cvCreateMat(R->height, R->width, CV_32FC1);

int val_g, val_b, val_r;

for (int i = 0; i < (R->height); i++)
{
for (int j = 0; j < (R->width); j++)
{

bool g = ((((i % 2 == 0) && (j % 2 == 0)))||
(((i % 2 != 0) && (j % 2 != 0)))); //i,j pair ou i,j impair
bool r = ((i % 2 == 0) && (j % 2 != 0));
bool b = ((i % 2 != 0) && (j % 2 == 0));
if (g)
```

```
{
val_g = cvmGet(G, i, j);
cvmSet(S, i, j, val_g);

}
else
{
if (b)
{
val_b = cvmGet(B, i, j);
cvmSet(S, i, j, val_b);

}
else
{
if (r)
{
val_r = cvmGet(R, i, j);
cvmSet(S, i, j, val_r);

} } } } }

return S;

}
```

- Fonction d'insertion de watermark

Cette fonction permet d'insérer un vecteur de watermark dans une sous-image.

Entrée : vecteur de watermark W, composante d'image E et la sous-image P où le watermark W sera inséré.

Sortie : composante d'image tatoué E.

On présente une partie de cette fonction qui fait l'insertion de vecteur de watermark W dans la sous-image 1 (P=1).

```
CvMat* Insertion(int*w, CvMat*E, int p)
{

int C = E->height / 2;
int D = E->width / 2;
int x, y, x1, y1, x2, y2, x3, y3, k;

/************Insertion W en P1**************/
switch (p)
{
case 1:
{
int k = 0;

for (int i = 0; i <C; i += 2)
{
for (int j = 0; j <D; j += 16)
{
x = w[k];
y = w[k + 1];
```

```
cvmSet(E, i, j + 6, x);
cvmSet(E, i, j + 7, y);

x1 = w[k + 2];
y1 = w[k + 3];
cvmSet(E, i, j + 14, x1);
cvmSet(E, i, j + 15, y1);

x2 = w[k + 4];
y2 = w[k + 5];
cvmSet(E, i + 1, j + 6, x2);
cvmSet(E, i + 1, j + 7, y2);

x3 = w[k + 6];
y3 = w[k + 7];
cvmSet(E, i + 1, j + 14, x3);
cvmSet(E, i + 1, j + 15, y3);

k += 8;

}
}
break;
}
...
return E;
}
```

- Fonction d'extraction de watermark

Cette fonction permet d'extraire un vecteur de watermark de sous-image.

Entrée : composante d'image tatoué E et le sous-image P.

Sortie : vecteur de watermark W.

On présente une partie de cette fonction qui fait l'extraction de vecteur de watermark W de la sous-image 1 (P=1).

```
int* Extraction(CvMat*E, int p)
{
int C = E->height / 2;
int D = E->width / 2;

int x, y, x1, y1, x2, y2, x3, y3, k;
int*wext;

int Lw;
Lw = C*D;

wext = new int[Lw];

switch (p)
{
/******* Extraction de wextP1: W1 de E*******/

case 1:
{

k = 0;
```

```
for (int i = 0; i < C; i += 2)
{
for (int j = 0; j < D; j += 16)
{
x = cvmGet(E, i, j + 6);
y = cvmGet(E, i, j + 7);
wext[k] = x;
wext[k + 1] = y;

x1 = cvmGet(E, i, j + 14);
y1 = cvmGet(E, i, j + 15);
wext[k + 2] = x1;
wext[k + 3] = y1;

x2 = cvmGet(E, i + 1, j + 6);
y2 = cvmGet(E, i + 1, j + 7);
wext[k + 4] = x2;
wext[k + 5] = y2;

x3 = cvmGet(E, i + 1, j + 14);
y3 = cvmGet(E, i + 1, j + 15);
wext[k + 6] = x3;
wext[k + 7] = y3;

k += 8;

}
}
break;
}
...
return wext;
}
```

- Fonction de détéction de modifications

Cette fonction permet de décider si l'image est authentique ou non. Elle compare chaque trois vecteurs de watermark extraits afin de préciser les valeurs inchangées pour les utilisées à la construction de l'image de watermark, et celles modifiées pour la construction de l'image de localisation de modification.

Entrée : trois vecteurs de watermark (wkey1, wkey2 et wkey3).

Sortie : vecteur de watermark ws et trois vecteurs de localisation de modification (wdetkey1, wdetkey2 et wdetkey3).

```
void Detection(int*wdetkey1, int*wdetkey2,
int*wdetkey3, int*ws, int*wkey1, int*wkey2,
int*wkey3, int L)
{
int w1, w2, w3;

for (int i = 0; i < L; i++)
{
w1 = wkey1[i];
w2 = wkey2[i];
w3 = wkey3[i];
```

```
if (w1 != w2)
{
if (w1 != w3)
{
if (w2 != w3)   //w1!=w2!=w3
{
wdetkey1[i] = 255;
wdetkey2[i] = 255;
wdetkey3[i] = 255;
ws[i] = w2;
}
else //w2=w3
{
wdetkey1[i] = 255;
ws[i] = w3;
}
}
else //w1=w3
{
wdetkey2[i] = 255;
ws[i] = w1;
}
}
else //w1=w2
{
if (w2 != w3)
{
wdetkey3[i] = 255;
ws[i] = w2;
}
else //w1=w2=w3
{
ws[i] = w3;
}
}
}

}
```

- Fonction de restauration de contenu

Cette fonction permet de restaurer les valeurs des régions endommagées.

Entrée : l'image de localisation de modifications, l'image de watermark reconstruit et l'image attaquée.

Sortie : l'image récupérée.

```
void Restoration(CvMat*det, CvMat*imgw, CvMat*wtrmk)
{
int x, y;

x = 0;
y = 0;

for (int i = 0; i < (imgw->height); i++)
{
for (int j = 0; j < (imgw->width); j++)
```

```
        {
        x = cvmGet(det, i, j);
        if (x == 255)
        {
        y = cvmGet(wtrmk, i, j);
        cvmSet(imgw, i, j, y);
        }
        }
        }
        }
```

La Figure 3.7 montre l'exécution de l'application avec les clés 2, 3, 5 et l'image « Airplaine » de taille 512x512.

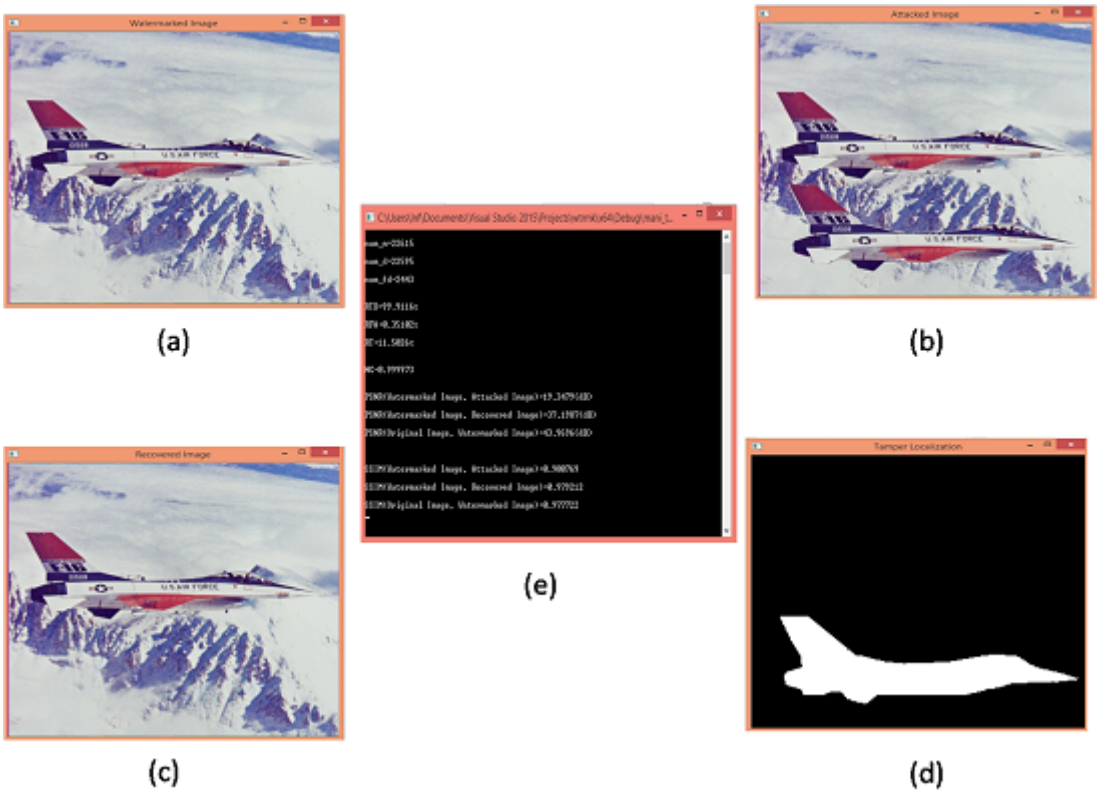


FIGURE 3.7 – Exécution d'application avec les clés 2, 3, 5 et l'image « Airplaine » de taille 512x512 : (a) Image tatouée, (b) Image attaquée, (c) Image récupérée, (d) Localisation de modification, (e) Les valeurs de PSNR, SSIM, NC, R_{TD}, R_{FA} et R_T

3.5.3 Résultats expérimentaux et discussion

Après l'implémentation de l'algorithme, premièrement, nous avons testé ses performances avec la même base de donnée utilisée par les auteurs de cet algorithme où ils sont utilisés une variété d'images couleur de la base de données CVG-UGR [CVG, 2014] telle que «House», «Lena», «Airplane», «Peppers» et «Woman» avec une taille de 512 × 512 et 256 × 256 pixels. On outre, les auteurs de cet algorithme ont proposé comme future perspective

d'appliquer cet algorithme sur les images médicales.

Qualité de l'image tatouée

Pour évaluer les performances de la méthode de Belferdi et al. [Belferdi et al., 2018] en termes d'imperceptibilité et de qualité visuelle d'image tatouée, des images couleurs RVB de taille 512 × 512 sont tatouées, puis on a calculé le PSNR (Peak Signal to Noise Ratio) et la SSIM (Structural SIMilarity) pour mesurer la similitude entre les images hôtes et les images tatouées (section 1.9). Les valeurs PSNR et SSIM correspondants sont présentées dans la Table 3.1.

Images hôtes				
				
Images tatouées				
				
PSNR et SSIM				
PSNR=43.97(dB) SSIM=0.97	PSNR=44.31 (dB) SSIM=0.98	PSNR=45.01 (dB) SSIM=0.96	PSNR=44.52 (dB) SSIM=0.98	PSNR=44.05(dB) SSIM=0.99

TABLE 3.1 – Les images Airplane ,Woman, Blueeye, House, Tahoe, Sedona et leurs images tatouées avec les valeurs PSNR et SSIM correspondantes.

D'après la Table 3.1, la valeur moyenne de PSNR entre l'image originale et l'image tatouée est 44.37 dB et SSIM est 0.97, ce qui démontre que cette méthode assure l'imperceptibilité du watermark et une qualité visuelle élevée des images tatouées.

Robustesse du watermark extrait

À partir de la Table 3.2, on remarque que la valeur moyenne de la corrélation normalisée NC est 1, donc le watermark inséré et le watermark extrait sont fortement corrélés.

Watermark Inséré			
Watermark Extrait			
NC	0.99	1	1

TABLE 3.2 – Qualité des watermarks insérés et extraits et la corrélation normalisée entre eux.

Détection de modification et restauration du contenu

Nous avons effectué des différentes attaques sur les images tatouées telles que les attaques de coupure, collage et des attaques hybrides avec différents pourcentages de modification, puis nous avons détecté et restauré les régions altérées, afin d'évaluer la précision de la détection de modification et la qualité de l'image récupérée.

Images attaquées					
					
PSNR=18.20 (dB) SSIM=0.96	PSNR=15.54 (dB) SSIM=0.94	PSNR=19.35 (dB) SSIM=0.90	PSNR=24.37 (dB) SSIM=0.92	PSNR=22.77 (dB) SSIM=0.94	PSNR=22.17 (dB) SSIM=0.96
Localisation de modification					
					
RTD=99.82% RFA=0.99%	RTD=99.88% RFA=0.15	RTD=99.91% RFA=0.35%	RTD=99.80% RFA=0.30%	RTD=99.63% RFA=0.26	RTD=99.72% RFA=0.13%
Images récupérées					
					
PSNR=43.57 (dB) SSIM=0.99	PSNR=38.23 (dB) SSIM=0.97	PSNR=37.20 (dB) SSIM=0.98	PSNR=39.95 (dB) SSIM=0.98	PSNR=36.28 (dB) SSIM=0.98	PSNR=44.20 (dB) SSIM=0.99

TABLE 3.3 – Les performances de l'algorithme d'authentification d'image avec des attaques de coupure, collage et d'attaques hybrides.

TABLE 3.4 – Les performances d'algorithme d'authentification d'image avec des attaques de coupure, collage et d'attaques hybrides effectuées avec différents pourcentages de modification.

Images Attaquées	Dimension	[a] num_{D}	[b] num_{M}	[c] R_{TD} (%)	[d] R_{FA} (%)	[e] R_{T} (%)	PSNR de l'image attaquée (dB)	SSIM de l'image attaquée	PSNR de l'image récupérée (dB)	SSIM de l'image récupérée
Blueeye	512x512	138	138	100	0.01	0.07	32.39	0.99	69.07	1
Peppers	512x512	1704	1710	99.65	0.03	0.87	27.57	0.99	43.58	1
Sedona	512x512	3480	3499	99.45	0.09	1.77	27.17	0.98	51.75	1
House	256x256	1158	1164	99.48	0.21	2.36	25.81	0.98	43.73	0.99
Woman	256x256	1584	1602	98.88	0.23	3.25	23.78	0.96	46.58	0.99
Toucan	512x512	12585	12722	98.92	0.20	6.47	16.55	0.94	43.69	0.99
Tahoe	512x512	15347	15378	99.79	0.30	7.82	24.36	0.92	39.94	0.98
Peppers	512x512	17607	17628	99.88	0.14	8.96	15.54	0.93	38.23	0.97
Airplane	512x512	22595	22615	99.91	0.35	11.50	19.34	0.90	37.19	0.97
	Moyenne			99.55	0.17	-	23.61	0.95	45.97	0.98

[a] num_{D}–Nombre de blocs détectés modifiés [b] num_{M}–Nombre de blocs réellement modifiés
[c] R_{TD}–Taux de détection de modification [d] R_{FA}–Taux de fausse alarme [e] R_{T}–Taux de modification

Selon les Tables 3.3 et 3.4, les valeurs de PSNR et SSIM des images récupérées peuvent atteindre jusqu'à 69.07 et 1 respectivement, les valeurs de la détection de modification R_{TD} (Tamper Detection Rate) (section 1.9) jusqu'à 100% et 0.35 pour le taux de fausse alarme R_{FA} (False Alarm Rate) avec différents taux de falsification R_{RT} (Tampering Ratio) entre [0.1, 20%], ces résultats démontrent la capacité de l'algorithme d'authentification d'image de localiser et de récupérer les régions altérées.

3.5.4 Contribution proposée : application sur les images médicales

Après l'application de l'algorithme sur les images couleur de la base de données CVG-URG [CVG, 2014] et les bons résultats obtenus, nous l'avons appliqué sur des images médicales [ICIAR, 2018]. Les résultats obtenus sont montrés dans les Tables 3.6 et 3.5.

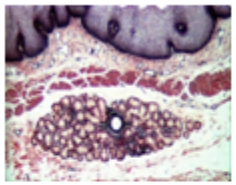
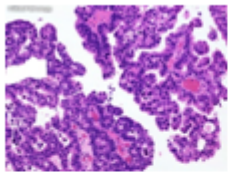
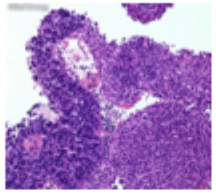
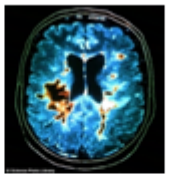
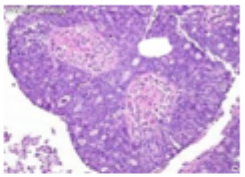
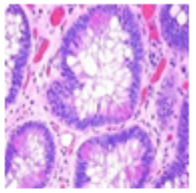
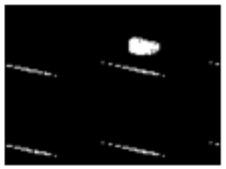
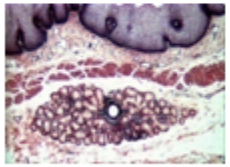
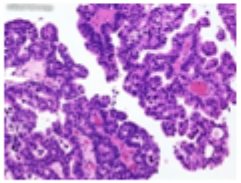
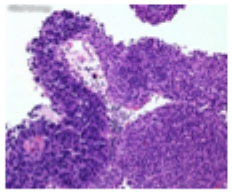
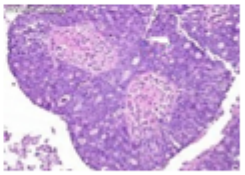
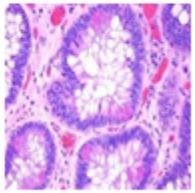
Images Attaquées					
					
Dimension=816x540	Dimension=648x488	Dimension=488x488	Dimension=468x488	Dimension=256x192	Dimension=180x180
PSNR=35.83 (dB) SSIM=0.99	PSNR=27.75 (dB) SSIM=0.98	PSNR=31.22 (dB) SSIM=0.99	PSNR=26.34 (dB) SSIM=0.99	PSNR=28.01 (dB) SSIM=0.98	PSNR=26.20 (dB) SSIM=0.97
Localisation de modification					
					
RTD=97.70% RFA=0.02%	RTD=137.88% RFA=0.08	RTD=99.84% RFA=0.03%	RTD=98.36% RFA=0.03%	RTD=142.50% RFA=0.15%	RTD=100% RFA=0.26%
Images récupérées					
					
PSNR=41.37 (dB) SSIM=0.99	PSNR=32.29 (dB) SSIM=0.99	PSNR=39.28 (dB) SSIM=0.99	PSNR=43.55 (dB) SSIM=0.99	PSNR=32.13 (dB) SSIM=0.98	PSNR=40.24 (dB) SSIM=0.99

TABLE 3.5 – Les performances d'algorithme d'authentification d'image avec des attaques de coupure, collage et d'attaques hybrides effectuées sur des images médicales.

TABLE 3.6 – Les performances d'algorithme d'authentification d'image avec des attaques de coupure, collage et d'attaques hybrides effectuées sur des images médicales avec différents dimensions et différents pourcentages de modification.

Images Attaquées	Dimension	[a] num_{D}	[b] num_{M}	[c] R_{TD} (%)	[d] R_{FA} (%)	[e] R_{T} (%)	PSNR de l'image attaquée (dB)	SSIM de l'image attaquée	PSNR de l'image récupérée (dB)	SSIM de l'image récupérée
Image1	424x600	1167	762	153.15	0.01	0.39	32.00	0.99	42.95	0.99
Image2	236x236	681	693	98.26	0.17	1.65	26.13	0.98	39.08	0.99
Image3	256x192	2280	2427	93.94	0.32	6.58	23.87	0.94	28.50	0.99
Image4	256x192	808	567	142.48	0.15	1.53	28.01	0.98	32.13	0.98
Image5	648x488	6751	4896	137.88	0.08	2.06	27.75	0.98	32.29	0.98
Image6	236x216	486	429	113.28	0.13	1.12	30.65	0.99	39.04	0.99
Image7	236x236	222	221	100.45	0.07	0.52	32.03	0.99	56.62	0.99
Image8	180x180	485	485	100	0.26	1.99	26.20	0.97	40.24	0.99
Image9	192x192	3315	3369	98.39	0.90	12.18	21.86	0.88	26.18	0 .93
	Moyenne			104.15	0.23	-	27.61	0.96	37.44	0.98

[a] num_{D}–Nombre de blocs détectés modifiés [b] num_{M}–Nombre de blocs réellement modifiés
[c] R_{TD}–Taux de détection de modification [d] R_{FA}–Taux de fausse alarme [e] R_{T}–Taux de modification

D'après les Tables 3.5 et 3.6, nous avons remarqué que les valeurs de taux de détection de modification R_{TD} des images peuvent être dépassées 100% tel que : 153.15%, 142.48%, 137.88% qui signifie que le nombre de blocs détectés modifiés est supérieur au nombre de blocs réellement modifiés, ce qui permet de dire qu'il y a une mauvaise détection de modification. En d'autres parts, il ya des bons résultats avec quelques images et des mauvais résultats avec d'autres selon le taux de modification et les détails de l'image elle-même. Donc, l'application de cet algorithme sur les images médicales ne mène pas aux bons résultats dans toutes les images.

3.6 Conclusion

Dans ce chapitre, nous avons présenté l'algorithme d'authentification proposé par Belferdi et al. [Belferdi et al., 2018], ses processus, ses étapes et les techniques principaux pour le construire. Nous avons décrit ses résultats expérimentaux sur les images couleurs en général et sur les images médicales en particulier, et à travers ses résultats, nous avons constaté que la méthode a des bonnes performances sur les images couleurs normales, elle offre des images tatouées et récupérées à haute qualité avec une valeur PSNR supérieur à 44 (dB) pour une image tatouée et 34 (dB) pour une image récupérée et une précision de localisation élevée, mais, elle reste à besoin des améliorations pour atteindre des résultats garantis compatibles avec la précision et l'importance de l'image médicale.

Conclusion Générale

Conclusion

Ce mémoire traite l'authentification du contenu des images médicales en utilisant le tatouage numérique qui attire beaucoup l'attention des chercheurs que les autres techniques de protection en raison de son efficacité de la résolution des problèmes concernant l'authenticité et l'intégrité des images.

Au cours de ce mémoire, nous avons présenté les techniques de protection des données, les exigences et le modèle général d'un système du tatouage numérique d'images. Ensuite, nous avons présenté les applications, la classification de ces systèmes. Après, nous avons concentré sur le tatouage des images médicales, nous avons commencé par les exigences, les applications et les classifications existantes des méthodes de ce tatouage avec quelques méthodes proposées. Ensuite, nous avons mis en évidence un système d'authentification d'image en présentant le modèle général, la classification de ces systèmes et quelques méthodes d'authentification d'image médicale.

Au niveau d'implémentation, nous avons implémenté un schéma du tatouage fragile pour l'authentification, la détection et la restauration de modification d'image couleur RVB basée sur la technique d'auto-insertion et utilisant la technique du filtrage chromatique CFA, et la permutation de Torus. Après, nous l'avons appliqué sur des images générales couleurs et sur des images médicales couleurs.

D'après les résultats expérimentaux, nous avons évalué les performances. Ce schéma a des bons résultats sur les images couleurs normales, il offre des images tatouées et récupérées à haute qualité avec une valeur PSNR supérieure à 44 (dB) pour une image tatouée et 34 (dB) pour une image récupérée et une précision de localisation élevée, mais pour les images médicales couleurs, il a des bons résultats avec quelques images et des mauvais résultats avec d'autres selon le taux de modification et les détails de l'image elle-même. Donc, nous avons constaté que ce schéma reste à besoin des améliorations pour atteindre des meilleurs résultats compatibles avec la précision et l'importance de l'image médicale.

Perspectives

À partir de ce travail réalisé, nous pouvons proposer quelques perspectives :

1. Généralement, les images médicales sont compressées lors de la transmission afin d'économiser la mémoire de la bande passante. Dans ce cas, le système d'authentification fragile (stricte) considère la compression comme une attaque non intentionnelle et déclare l'image comme non authentique, alors qu'elle est authentique. Donc, nous proposons qu'un système d'authentification des images médicales doit être tolérant avec la compression d'images.

2. En raison du rôle important d'image médicale dans le diagnostic, nous proposons qu'un système de tatouage pour l'authentification des images

médicales doit être réversible. Dans ce cas, le watermark extrait est supprimé et les valeurs originales des pixels sont restaurées afin d'obtenir une image récupérée très corrélée avec celle d'origine.

3. En cas des images médicales où on peut distinguer les régions d'intérêt ROI et les régions non d'intérêt RONI, il est très convenable d'utiliser un système de tatouage réversible pour l'authentification d'image en insérant les valeurs ou les LSBs des pixels originales qui seront remplacées par le watermark dans la RONI afin de l'utiliser plus tard pour récupérer les valeurs originales d'image, aussi, il est utile d'insérer le watermark dans la RONI et préserver la ROI qui contient les informations importantes pour le diagnostic.

Bibliographie

[Agung et al., 2012] Agung, T., Permana, BW, F. P., et al. (2012). Medical image watermarking with tamper detection and recovery using reversible watermarking with lsb modification and run length encoding (rle) compression. In *2012 IEEE International Conference on Communication, Networks and Satellite (ComNetSat)*, pages 167–171. IEEE.

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

[Al-Qershi and Khoo, 2011] Al-Qershi, O. M. and Khoo, B. E. (2011). Authentication and data hiding using a hybrid roi-based watermarking scheme for dicom images. *Journal of digital imaging*, 24(1) :114–125.

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

[Belferdi et al., 2018] Belferdi, W., Behloul, A., and Noui, L. (2018). A bayer pattern-based fragile watermarking scheme for color image tamper detection and restoration. *Multidimensional Systems and Signal Processing*.

[Benazzouz, 2014] Benazzouz, M. (2014). *analyse intelligente des images médicales : application aux images microscopiques de cytologie*. PhD thesis, Université d'Aboubekr belkaid-Tlemcen.

[Boreiry and Keyvanpour, 2017] 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.

[Boujemaa et al., 2016] Boujemaa, N., Yousef, E., Rachid, L., Aziz, B. M., et al. (2016). Fragile watermarking of medical image for content authentication and security. *IJCSN-International Journal of Computer Science and Network*, 5(5).

[Chao et al., 2002] Chao, H.-M., Hsu, C.-M., and Miaou, S.-G. (2002). A data-hiding technique with authentication, integration, and confidentiality for electronic patient records. *IEEE transactions on information technology in biomedicine*, 6(1) :46–53.

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

[Chikhi, 2008] Chikhi, S. (2008). *Contribution à l'authentification souple d'images digitales par des techniques de marquage numérique. Application aux images médicales*. PhD thesis, Université de Mentouri-Constantine.

[Coatrieux et al., 2006] Coatrieux, G., Lecornu, L., Sankur, B., and Roux, C. (2006). A review of image watermarking applications in healthcare. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 4691–4694. IEEE.

[Coatrieux et al., 2000] Coatrieux, G., Maître, H., Sankur, B., Rolland, Y., and Collorec, R. (2000). Relevance of watermarking in medical imaging. In *Proceedings 2000 IEEE EMBS International Conference on Information Technology Applications in Biomedicine. ITAB-ITIS 2000. Joint Meeting Third IEEE EMBS International Conference on Information Technol*, pages 250–255. IEEE.

[Cox et al., 2007] Cox, I., Miller, M., Bloom, J., Fridrich, J., and Kalker, T. (2007). *Digital watermarking and steganography*. Morgan kaufmann.

[Cox et al., 2000] Cox, I. J., Miller, M. L., and Bloom, J. A. (2000). Watermarking applications and their properties. In *Proceedings International Conference on Information Technology : Coding and Computing (Cat. No. PR00540)*, pages 6–10. IEEE.

[Cox et al., 1999] Cox, I. J., Miller, M. L., Linnartz, J., and Kalker, T. (1999). A review of watermarking principles and practices. *Digital signal processing for multimedia systems*, pages 461–482.

[CVG, 2014] CVG (2014). Cvg-ugr-base de données d'images. http://decsai.ugr.es/cvg/dbimagenes/.

[Das and Kundu, 2013] Das, S. and Kundu, M. K. (2013). Effective management of medical information through roi-lossless fragile image watermarking technique. *Computer methods and programs in biomedicine*, 111(3) :662–675.

[Eswaraiah and Reddy, 2014] Eswaraiah, R. and Reddy, E. S. (2014). Roi-based fragile medical image watermarking technique for tamper detection and recovery using variance. In *2014 Seventh International Conference on Contemporary Computing (IC3)*, pages 553–558. IEEE.

[Giakoumaki et al., 2006] Giakoumaki, A., Pavlopoulos, S., and Koutsouris, D. (2006). Multiple image watermarking applied to health information management. *IEEE Transactions on Information Technology in Biomedicine*, 10(4) :722–732.

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

[Haouzia and Noumeir, 2008] Haouzia, A. and Noumeir, R. (2008). Methods for image authentication : a survey. *Multimedia tools and applications*, 39(1) :1–46.

[Ho and Li, 2004] 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.

[Hu and Jeon, 2006] 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.

[ICIAR, 2018] ICIAR (2018). Images médicales microscopiques. https://iciar2018-challenge.grand-challenge.org/dataset/.

[Jimson and Hemachandran, 2018] Jimson, N. and Hemachandran, K. (2018). Dft based digital image watermarking : a survey. *International Journal of Advanced Research in Computer Science*, 9(2) :540.

[Karthigaikumar et al., 2012] 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.

[Kaur et al., 2012] Kaur, M., Jindal, S., and Behal, S. (2012). A study of digital image watermarking. *Journal of Research in Engineering and Applied Sciences*, 2(2) :126–136.

[Khurana, 2011] Khurana, S. (2011). Watermarking and information-hiding. *International Journal of Computer and Information Technology*, 2 :1679–1681.

[Lee et al., 2007] Lee, H., Battle, A., Raina, R., and Ng, A. Y. (2007). Efficient sparse coding algorithms. In *Advances in neural information processing systems*, pages 801–808.

[Ling and Ur-Rehman, 2015] Ling, C. and Ur-Rehman, O. (2015). Watermarking for image authentication. In *Robust image authentication in the presence of noise*, pages 43–73. Springer.

[Liu et al., 2006] 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.

[Lu, 2004] Lu, C.-S. (2004). *Multimedia security : steganography and digital watermarking techniques for protection of intellectual property : steganography and digital watermarking techniques for protection of intellectual property*. Idea Group Publishing.

[Memon and Gilani, 2011] Memon, N. A. and Gilani, S. A. M. (2011). Watermarking of chest ct scan medical images for content authentication. *International Journal of Computer Mathematics*, 88(2) :265–280.

[Mousavi et al., 2014] Mousavi, S. M., Naghsh, A., and Abu-Bakar, S. (2014). Watermarking techniques used in medical images : a survey. *Journal of digital imaging*, 27(6) :714–729.

[Navas and Sasikumar, 2007] Navas, K. and Sasikumar, M. (2007). Survey of medical image watermarking algorithms. In *Proc. Internation Conf. Sciences of Electronics, Technologies of Information and Telecommunications*, pages 25–29.

[Nyeem et al., 2014] Nyeem, H., Boles, W., and Boyd, C. (2014). Digital image watermarking : its formal model, fundamental properties and possible attacks. *EURASIP Journal on Advances in Signal Processing*, 2014(1) :135.

[Parah et al., 2017] Parah, S. A., Sheikh, J. A., Ahad, F., Loan, N. A., and Bhat, G. M. (2017). Information hiding in medical images : a robust medical image watermarking system for e-healthcare. *Multimedia Tools and Applications*, 76(8) :10599–10633.

[Pei and Tam, 2003] Pei, S.-C. and Tam, I.-K. (2003). Effective color interpolation in ccd color filter arrays using signal correlation. *IEEE Transactions on Circuits and Systems for video technology*, 13(6) :503–513.

[Potdar et al., 2005] Potdar, V. M., Han, S., and Chang, E. (2005). A survey of digital image watermarking techniques. In *INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.*, pages 709–716. IEEE.

[Qasim et al., 2018] Qasim, A. F., Meziane, F., and Aspin, R. (2018). Digital watermarking : Applicability for developing trust in medical imaging workflows state of the art review. *Computer Science Review*, 27 :45–60.

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

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

[RajaRao et al., 2015] RajaRao, C., Boddu, M., and Mandal, S. K. (2015). Single sensor color filter array interpolation algorithms. In *Information systems design and intelligent applications*, pages 295–307. Springer.

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

[Rey and Dugelay, 2001] Rey, C. and Dugelay, J.-L. (2001). Un panorama des méthodes de tatouage permettant d'assurer un service d'intégrité pour les images. *TS Traitement du Signal*, 18(4) :283–295.

[Rey and Dugelay, 2002] Rey, C. and Dugelay, J.-L. (2002). A survey of watermarking algorithms for image authentication. *EURASIP Journal on Advances in Signal Processing*, 2002(6) :218932.

[Saini and Shrivastava, 2014] Saini, L. K. and Shrivastava, V. (2014). A survey of digital watermarking techniques and its applications. *arXiv preprint arXiv :1407.4735*.

[Sathik and Sujatha, 2012] 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.

[Seitz, 2005] Seitz, J. (2005). *Digital watermarking for digital media*. Information Science Publishing (Idea Group Inc.).

[Shehab et al., 2018] Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., and Hou, G. (2018). Secure and robust fragile watermarking scheme for medical images. *IEEE Access*, 6 :10269–10278.

[Singh and Singh, 2017] 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.

[Singh et al., 2013] 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.

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

[Su et al., 2013] 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.

[Tao et al., 2014] Tao, H., Chongmin, L., Zain, J. M., and Abdalla, A. N. (2014). Robust image watermarking theories and techniques : A review. *Journal of applied research and technology*, 12(1) :122–138.

[Tareef et al., 2014] Tareef, A., Al-Ani, A., Nguyen, H., and Chung, Y. Y. (2014). A novel tamper detection-recovery and watermarking system for medical image authentication and epr hiding. In *2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 5554–5557. IEEE.

[Tefas et al., 2009] 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.

[Tirkel et al., 1993] Tirkel, A. Z., Rankin, G., Van Schyndel, R., Ho, W., Mee, N., and Osborne, C. F. (1993). Electronic watermark. *Digital Image Computing, Technology and Applications (DICTA'93)*, pages 666–673.

[Tsai, 2009] 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.

[Ur-Rehman and Zivic, 2018] Ur-Rehman, O. and Zivic, N. (2018). Digital watermarking for image authentication. In *Noise Tolerant Data Authentication for Wireless Communication*, pages 33–37. Springer.

[Voloshynovskiy et al., 2001] Voloshynovskiy, S., Pereira, S., Pun, T., Eggers, J. J., and Su, J. K. (2001). Attacks on digital watermarks : classification, estimation based attacks, and benchmarks. *IEEE communications Magazine*, 39(8) :118–126.

[Vongpradhip and Rungraungsilp, 2012] 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.

[Voyatzis and Pitas, 1996] Voyatzis, G. and Pitas, I. (1996). Applications of toral automorphisms in image watermarking. In *Proceedings of 3rd IEEE International Conference on Image Processing*, volume 2, pages 237–240. IEEE.

[Wu et al., 2007] 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.

[Yip et al., 2006] 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.

[Zain and Fauzi, 2006] Zain, J. M. and Fauzi, A. R. (2006). Medical image watermarking with tamper detection and recovery. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society*, pages 3270–3273. IEEE.

[Zehda, 2014] Zehda, F. (2014). *Tatouage d'images basé sur des transformées discrètes entières*. PhD thesis, Université de Ferhat Abbas –Setif 1–.