REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de Batna 2

Faculté des Mathématiques et de l'Informatique

Département d'Informatique

THESE

En vue de l'obtention du diplôme de

Doctorat en Sciences en Informatique

Présentée par

Nour El-Houda GOLEA

Approches Evolutionnaires Hybrides pour Le Tatouage Numérique des Images.

Soutenue publiquement le **12/07/2018** devant le jury formé de :

Dr. Hamouma MOUMEN	**Président**	M.C. Université de Batna2
Pr. Kamal Eddine MELKEMI	**Rapporteur**	Prof. Université de Batna2
Pr. Mohamed Chawki BATOUCHE	**Examinateur**	Prof. Université de Constantine2
Pr. Mohamed Khireddine KHOLLADI	**Examinateur**	Prof. Université d'ElOued

Remerciements

Je tiens tout d'abord à exprimer ma profonde gratitude à mon directeur de thèse, Mr Kamel Eddine Melkemi, professeur à l'université de Batna2 pour sa disponibilité ainsi, que pour ses conseils judicieux qui m'ont permis de surmonter les difficultés et de mener à bien ce travail.

J'exprime mes remerciements à Monsieur Hamouma Moumen, de l'Université de Batna2, qui me fait le grand honneur d'accepter la présidence du jury.

Je tiens à remercier très chaleureusement le Professeur Mohamed Chawki Batouche chef du département Informatique Fondamentale Et Ses Applications de l'université de Constantine2 et le Professeur Mohamed-Khireddine Kholladi de l'université d'ElOued ; d'avoir accepté de faire partie de ce jury malgré leurs occupations.

Je souhaiterais aussi adresser mes remerciements à Dr. Ali Behloul, Maître de conférences à l'université de Batna2 pour ses précieuses discussions.

Mes remerciements vont également à Dr. Celine Roudet de l'université de Bourgogne du laboratoire Le2i , pour m'avoir accueillir au sein de son équipe.

Je tiens à saisir cette occasion pour adresser mes profonds remerciements à Dr. Hamoudi Kalla, chef de département d'informatique et Dr Souhila Bouame Chef-Adjoint de la Post-Graduation pour leurs aides administratifs et leurs encouragements.

Mes sincères remerciements à ma petite famille, mon mari et ma fille adorable Norsine. J'adresse aussi mes vifs remerciements à mes très chers parents qui m'ont toujours aidé, soutenu et encouragé au cours de mon parcours. Je remercie aussi mes sœurs, frères et nom cher neveu Ilane.

Je n'oublie jamais d'adresser un remerciement spécial à ma grand-mère pour son encouragement et ses prières et je prie pour que le Dieu la guérisse.

Dédicace

A mes chers parents, que Dieu leur prête santé, bonheur et longue vie.
A mon cher mari, pour son soutien et ses encouragements durant les années de la thèse.
A ma fille adorable *Norsine Minnat-Allah*, que Dieu le tout puissant les garde pour moi.

ملخـــــص

مقاربات تطوريـــة هجينـــة من اجـــل الوشـــم الرقمـــي للصـور

في السنوات الأخيرة، الانتقال إلى العالم الرقمي يوفر للمستخدمين العديد من وسائل الراحة لاستخدام ومعالجة وتخزين ونقل البيانات الخاصة بهم. وبالإضافة إلى ذلك، فإن التطور السريع والمستمر لأنظمة اقتناء الصور قد سمح بنمو هائل في استخدام الصور الرقمية. في الواقع، الرقمنة هو سيف ذو حدين، فإنه يوفر العديد من الفوائد من جهة ويطرح مشاكل أمنية من ناحية أخرى. ولهذا السبب، من الضروري تصميم أنظمة حماية الصور الرقمية من التلاعب غير المشروع. في العقود الأخيرة، اقترح الوشم الرقمي كتقنية فعالة لمعالجة العديد من جوانب الأمن الرقمي. مبدأ هذه التقنية هو دس إشارة رقمية تسمى العلامة المائية في إشارة رقمية أخرى تسمى إشارة المضيف (النص، الصورة، الصوت، الفيديو، ...). وفي هذا السياق، نقترح في هذه الأطروحة مقاربات جديدة للوشم الرقمي للصور. المساهمة الأولى هي اقتراح مقاربة جديدة تقوم على خوارزميات جينية لحماية حقوق الطبع والنشر للصور الملونة. والهدف من هذه المقاربة هو تحسين متطلبين متناقضين للوشم: الشفافية والمتانة. وتستند هذه المقاربة على استخدام خوارزمية متعددة الأهداف المعروفة بفعاليتها. أما المساهمتان الثانية والثالثة فتصفان طرق وشم جديدة مطبقة على الصور الطبية . هاتان المقاربتان مستوحاتان من النقل الشبكي حيث يعتبر استخدام الكشف عن الأخطاء وتصحيحها أمر طبيعي. احدى هاتان المقاربتان يعتمد على استخدام رمز الكشف عن الخطأ (CRC) لضمان مصداقية المنطقة المهمة في الصورة الطبية. بينما تستخدم الاخرى رمز تصحيح الخطأ (RS) لضمان النزاهة بالإضافة إلى المصداقية. في المساهمة الرابعة، نقترح مقاربة جديدة لوشم الجيل الثاني تعتمد على Voronoi Diagrams ورمز CRC باستخدام كثير حدود ذو درجات عالية بخصائص رياضية خاصة مثل CRC-32 و CRC-16 و CRC-8 لتوليد العلامة المائية. يتم إدخال الأخير في كل منطقة من الصورة بعد تقسيمها باستخدام VDs.

كلمات البحث :النهج التطوري، متعدد الهدف الأمثل، الخوارزمية الجينية، الوشم الرقمي، الصورة الطبية.

Abstract

Hybrid Evolutionary Approaches for digital image Watermarking

In recent years, the transition to the digital world offers users several conveniences, to use, process, store and transmit their data. In addition, the rapid and continuous evolution of image acquisition systems has allowed a tremendous growth in the use of digital images. Indeed, digitization is a double-edged sword, it offers several benefits on the one hand and poses security problems on the other hand. For this reason, it is mandatory to design digital image protection systems against illegal manipulation. In recent decades, digital tattooing, a brilliant technique proposed to address several aspects of security. The principle of this technique is to implement a digital signal called watermark in another digital signal called host signal (text, image, audio, video, ...). In this context, we propose in this thesis new approaches of digital image watermarking. The first contribution is to propose a new evolutionary approach based on genetic algorithms for the copyright protection of RGB color images. The goal of this approach is to optimize the two contradictory demands of watermarking : imperceptibility and robustness. The second and third contributions describe new watermarking approaches applied to medical imaging. These two approaches are inspired from network transmission where the use of errors detecting and correcting codes appeared natural. One of these approaches relies on the use of the error detecting code (CRC) to guarantee the authentication of the region of interest of the medical image. While, the other uses error-correcting code to ensure in addition to authentication, integrity. In the fourth contribution, we propose a new second generation watermarking approach based on Voronoi diagrams (VD) and CRC code using standard high degree polynomials with special mathematical properties such as CRC-32, CRC-16 and CRC-8 to generate the watermark. The latter is inserted into each region of the image after decomposition usin VD.

Keywords : Evolutionary approaches, Multi-objective optimization, Genetic algorithm, Digital watermrking, Digital image, Medical imaging.

Résumé

Approches Evolutionnaires Hybrides pour Le Tatouage Numérique des Images

Résumé :

Au cours de ses des dernières années, le passage vers le monde numérique offre aux utilisateurs plusieurs commodités, pour utiliser, traiter, stocker et transmettre leurs données. En outre, l'évolution rapide et sans cesse des systèmes d'acquisition d'images a permis un formidable essor de l'utilisation de l'image numérique. En effet, la numérisation est une épée à double tranchant, elle offre plusieurs bénéfices d'une part et pose des problèmes de sécurité d'autre part. Pour cette raison, il est obligatoire de concevoir des systèmes de protection des images numériques contre toutes manipulations illégales. Dans ces dernières décennies, le tatouage numérique, une technique brillante proposée pour répondre à plusieurs aspects de la sécurité. Le principe de cette technique est d'implanter un signal numérique appelé watermark dans un autre signal numérique appelé signal hôte (texte, image, audio, vidéo, ...). Dans ce cadre, nous proposons dans cette thèse des nouvelles approches de tatouage numérique des images. La première contribution consiste à proposer une nouvelle approche évolutionnaire à base des algorithmes génétiques pour la protection de droit d'auteurs des images couleurs RGB. L'objectif de cette approche est d'optimiser les deux exigences contradictoires du tatouage : l'imperceptibilité et la robustesse. La deuxième et la troisième contributions décrient des nouvelles approches de tatouage appliquées à l'imagerie médicale. Ces deux approches sont inspirées de la transmission en réseau où l'utilisation des codes détecteur et correcteur des erreurs est apparu naturel. Une de ces approches repose sur l'utilisation du code détecteur des erreurs (CRC) afin de garantir l'authentification de la région d'intérêt de l'image médicale. Tandis que, l'autre utilise un code correcteur des erreurs (RS) pour assurer en plus de l'authentification, l'intégrité. Dans la quatrième contribution, nous proposons une nouvelle approche de tatouage de deuxième génération basée sur les Diagrammes de Voronoi VD et le code CRC en utilisant des polynômes standard de degré élevée ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans chaque région de l'image après une décomposition en utilisant VDs.

Mots clés : Approches évolutionnaire, Optimisation multi-objectif, Algorithme génétique, Tatouage numérique, image numérique, Imagerie médicale.

Table des matières

Table des figures

Liste des tableaux

Liste des Algorithmes

Liste des acronymes

ACR The American College of Radiology.
AEs Algorithmes évolutifs.
ARQ Automatic Repeat reQuest.

BE Barium Enema.

CRC Contrôle de Redondance Cyclique.
CT-Scan Computed Tomography-Scan.

DCT Discrete Cosine Transform.
DFT Discret Fourier Transform.
DWT Discret Wevelet Transform.

ECC Error Correcting Codes.
EDC Error Detecting codes.
EPR Electronic Patient Record.

FEC Forward Error Correction.
FGW First Generation Watermarking.
FPs Feature Points.
FS Facteur Scalaire.

HIS Hospital Information System.

IRM Imagerie par Résonance Magnétique.

JPEG Joint Photographic Experts Group.

LSB Least Significat Bits.
LWT Lifting Wavelet Transform.

MSE Mean Square Error.

NC Normalized Correlation.
NEMA National Electrical Manufactures Association.
NSGA-II Non-dominated Sorting Genetic Algorithm II.

PACS Picture Archiving and Communication System.

PN Pseudo-Noise.
PSNR Peak Signal to Noise Ratio.

RGB Reed Green Blue.
ROI Region Of Interest.
RONI Region Of Non Intereset.
RS Reed Solomon.

SGW Second Generation Watermarking.
SSIM Structural SIMilarity.
SV Singular Value.
SVD Singular Value Decomposition.

TIM Tatouage d'Imagerie Medicale.

UGI Upper Gastrointestinal.

VD Voronoi Diagram.

XR X-Ray.

Introduction générale

L'avènement du multimédia permet à différentes applications de mélanger le son, les images ainsi que la vidéo et d'interagir avec de grandes quantités d'informations (par exemple, dans le commerce électronique, l'enseignement à distance, etc.). L'industrie investit pour fournir aux clients des données audio, image et vidéo sous forme numérique et les sociétés de diffusion TV, les grandes entreprises et les archiveurs de photos convertissent leur contenu de l'analogique au format numérique. Le passage vers la numérisation est dû aux bénéfices des médias numérique par rapport aux médias traditionnels (documents papier et des enregistrements analogiques). Certains de ces avantages sont les suivants [Chun-Shien, 2005] :

— La qualité des signaux numériques est haute par rapport à celle de leurs signaux analogiques correspondants.
— Les données numériques peuvent être facilement transmises sur les réseaux de communication.
— La facilité de faire des copies exactes de données numériques. Ceci est très utile, mais il crée également des problèmes pour le propriétaire des données numériques de valeur.
— Il est possible de cacher des informations dans des données numériques d'une manière telle que ces modifications sont indétectables pour les sens humains (l'œil et l'oreille).

Le développement des technologies numériques permettant la transmission de données numériques sur Internet a soulevé des questions sur la façon dont les droits d'auteurs sont applicables dans ce nouvel environnement numérique. Comment la propriété intellectuelle numérique peut être mis à la disposition du public tout en garantissant la propriété des droits de la propriété intellectuelle par le titulaire des droits et l'accès libre à l'information par l'utilisateur ?

La cryptographie a été une première proposition pour sécuriser des transferts de documents numériques. Aujourd'hui les algorithmes de cryptage modernes, avec des clés de longueur importante, permettent d'assurer la confidentialité. Néanmoins, une fois décrypté, le document n'est plus protégé et il peut être distribué ou modifié malhonnêtement. La dissimulation d'information, et plus particulièrement l'insertion de données cachées peut être une réponse à ce problème. En effet, l'insertion d'un watermark dans un document permet de l'authentifier et de garantir son intégrité [Rey and Dugelay, 2002]. Cette technique est connue par le nom "*tatouage numérique*" (*digital watermarking* en Anglais). Cette technologie est très rapidement apparue comme une solution très efficace pour renforcer la sécurité des documents multimédia. L'idée de base du «watermarking» est de cacher dans un document numérique une information invisible ou inaudible suivant la nature du document permettant d'assurer un service de sécurité (copyright, intégrité, traçbilité, non répudiation, etc).

La conception d'un système de tatouage est modélisée généralement par deux phases : dans la première phase le watermak est implanté dans le document à protéger (nommé *document hôte* ou *document original*). Le document original, peut être un fichier texte, image, son ou un vidéo. Ensuite, le document tatoué est transmis via le réseau et il peut subir des modifications

intentionnelles ou accidentelles. Dans la deuxième phase, le watermark est extrait afin de prouver la propriété intellectuelle du document.

Tout système de tatouage numérique doit être conçu pour avoir certaines propriétés tout en satisfaisant les exigences fonctionnelles. Dans le cas des images, la phase d'insertion ne doit pas détériorer l'image hôte de façon perceptible, c'est à dire l'image tatouée doit être visuellement équivalente à l'image originale. Cette propriété est connue par les termes *imperceptibilité*, *invisibilité* ou encore *fidélité*.

D'autres propriétés doivent être prendre en considération : *la robustesse*, *la capacité*, *la sécurité* et *la complexité*. L'ensemble de ces propriétés dépend du domaine d'application du tatouage. Selon Zhao et al. [Zhao et al., 1998], ces domaines sont : la protection du droit d'auteurs, annotation cachée (hidden annotations), authentification et communication secrète invisible. Chacune de ces applications a ses propres exigences. Par exemple, si le tatouage est appliqué pour la protection des droits, la robustesse, l'imperceptibilité et la sécurité sont primordiales tandis que la capacité est moins importante.

La conception d'un tatouage optimal pour une application donnée implique toujours un compromis entre l'exigence d'imperceptibilité et l'exigence de robustesse. Par conséquent, le tatouage d'image peut être considéré comme un problème d'optimisation.

Alors que la plupart des problèmes du monde réel nécessitent l'optimisation simultanée de plusieurs critères (ou objectifs) souvent concurrents, la solution à ces problèmes est généralement calculée en les combinant en un seul critère à optimiser, selon une fonction d'utilité. Cependant, dans de nombreux cas, la fonction d'utilité n'est pas bien connue avant le processus d'optimisation. Tout le problème devrait alors être traité comme un problème multi-objectif. De cette façon, un certain nombre de solutions peuvent être trouvées pour fournir au décideur un aperçu des caractéristiques du problème avant qu'une solution finale soit choisie.

Les problèmes liés à des objectifs multiples se posent de façon naturelle dans la plupart des disciplines et leur solution constitue un défi pour les chercheurs depuis longtemps. Malgré la grande variété de techniques développées dans la recherche opérationnelle et d'autres disciplines pour s'attaquer à ces problèmes, la complexité de leur solution fait appel à des approches alternatives. L'utilisation des AEs pour résoudre des problèmes de cette nature a été motivée principalement en raison de la nature populationnelle des AEs qui permet la génération de plusieurs éléments de l'ensemble optimal de Pareto dans un seul cycle. De plus, la complexité de certains problèmes d'optimisation multi-objectifs (POM) (par exemple, très grands espaces de recherche, incertitude, bruit, courbes de Pareto disjointes, etc.) peut empêcher l'utilisation (ou l'application) des techniques traditionnelles de résolution des POM. Dans le cadre de notre travail, nous cherchons à optimiser le problème de tatouage numérique en utilisant les AEs.

Cette thèse décrit quatre contributions au domaine de tatouage numérique des images. La première contribution consiste à proposer une nouvelle approche évolutionnaire à base des AGs pour la protection de droit d'auteurs des images couleurs RGB. En effet, la méthode proposée s'inscrit dans le domaine fréquentiel en utilisant la décomposition SVD pour incorporer un watermark couleur dans les SVs d'une image hôte couleur. Plus précisément, nous avons proposé une nouvelle méthode pour maintenir l'ordre des SVs, une fois le watermark intégré dans l'une des SVs du milieu de chaque bloc en divisant la SV choisit par le FS. Dans cette méthode, le problème est le choix de deux paramètres : la meilleure SV du milieu et le FS de mise à l'échelle afin d'obtenir un bon compromis entre la robustesse et l'imperceptibilité car ces deux paramètres dépendent de l'image originale et du watermark. Ce problème peut être considéré comme un problème d'optimisation et il peut être modélisé en utilisant un AG.

Récemment, plusieurs approches basées sur les AGs ont été proposées pour le tatouage d'image. Dans [Veysel, 2008], un simple système de tatouage à base d'AG est proposé pour

résoudre le problème du choix d'un FS optimal. Les SVs de l'image niveaux de gris sont modifiées pour intégrer l'image de watermark en employant plusieurs FSs. Les modifications sont optimisées en utilisant l'AG pour obtenir la plus grande robustesse possible sans perdre l'imperceptibilité. La fonction fitness d'un individu est calculée par la différence entre deux fonctions : la première estime la robustesse (entre l'image originale et le watermark) et la seconde évalue l'imperceptibilité. Récemment, Chih-Chin Lai [Lai., 2011] a proposé une technique de tatouage d'image basée sur la SVD et Tiny-GA. Dans son approche, les SVs de l'image originale sont modifiées pour intégrer le watermark. Le Tiny-GA offre une manière systématique de considérer les améliorations des FSs qui sont utilisées pour contrôler la force du watermark intégré. Avec ce schéma, le watermark inséré peut survivre avec succès après avoir été attaqué par des opérations de traitement d'image. Les résultats de la simulation montrent que le schéma proposé surpasse les autres travaux similaires. La fonction de fitness utilisée est une concaténation de deux critères contradictoires : l'imperceptibilité et la robustesse. Vu que nous avons deux paramètres à optimiser, le tatouage d'image peut être considéré comme un problème d'optimisation bi-objectif. La présence d'objectifs multiples dans le problème de tatouage d'image, donne naissance à un ensemble de solutions optimales largement connues sous le nom de solutions pareto-optimales, au lieu d'une seule solution optimale. En l'absence de toute autre information, on ne peut pas dire que l'une de ces solutions pareto-optimales soit meilleure que l'autre. Cela demande à l'utilisateur de trouver autant de solutions pareto-optimales que possible. Les méthodes classiques d'optimisation suggèrent de convertir le problème d'optimisation multi-objectif en un problème d'optimisation à objectif unique [Veysel, 2008, Lai., 2011] en mettant l'accent sur une solution pareto-optimale particulière à la fois. Lorsqu'une telle méthode doit être utilisée pour trouver des solutions multiples, elle doit être appliquée plusieurs fois, en espérant trouver une solution différente à chaque simulation.

Dans cette première contribution, nous avons proposé une approche multi-objectif hybride pour le tatouage des images couleurs RGB afin d'optimiser les deux exigences contradictoires : l'imperceptibilité et la robustesse contre les attaques. L'objectif de notre approche est d'optimiser les deux exigences contradictoires d'un schéma de tatouage *aveugle* et *robuste* : l'imperceptibilité et la robustesse contre les attaques. Nous avons proposé d'utiliser l'algorithme NSGA-II. NSGA-II est un algorithme d'optimisation efficace repose sur l'idée d'une méthode de sélection basée sur des classes de dominance de toutes les solutions. Il utilise un algorithme de classement rapide non-dominé et un mécanisme de partage sans paramètre pour la diversification des solutions. La phase de test a prouvé que le système de tatouage aveugle basé sur le NSGA-II permet d'obtenir un très bon compromis entre l'imperceptibilité et la robuste à douze types d'attaques.

La deuxième et la troisième contributions décrient des nouvelles approches de tatouage appliquées à l'imagerie médicale. Les schémas proposés sont inspirés de la transmission en réseau, dans lequel le message à transmettre est divisé en paquets de taille fixe et des informations redondantes sont ajoutées à chaque paquet pour traiter les erreurs. En fonction des caractéristiques du canal de communication, deux stratégies ont été mises en pratique : une utilise les codes détecteurs des erreurs (EDC) et l'autre emploie les codes correcteurs des erreurs (ECC). La théorie des codes est attrayante pour la recherche de tatouage d'images. Ainsi, plusieurs approches de tatouage basées sur les codes sont proposées et divers EDC ou ECC sont utilisés tels que Reed Solomon (RS), Hamming (Ham), Bose-Chaudhuri-Hocquenghen (BCH), etc. La plupart des méthodes de tatouage d'image basées sur les codes ont éte effectuées sur la signature ou sur certaines caractéristiques de l'image [Terzija and Geisselhardt, 2004, Lin et al., 2004, Zhou et al., 2004]. Dans le cas de l'image médicale, les codes sont réalisés afin d'obtenir l'authentification de l'EPR [Mostafa et al., 2010, Hajjaji et al., 2011, Kumar et al.,

2015]. Dans le cadre de notre travail, nous avons exploité l'efficacité des codes à détecter les erreurs afin d'atteindre l'authentification et l'intégrité en appliquant les codes directement sur les pixels de la ROI. Une approche pour l'authentification et la détection des altérations dans la *Région d'intérêt* ROI des images médicales est proposée en utilisant le code détecteur des erreurs CRC, qui est connu comme l'un des EDC les plus utiles et les plus puissants utilisés dans divers systèmes de communication numérique.

Tandis que dans la troisième contribution, nous avons proposé un schéma de tatouage *zéro-bit* pour l'authentification et l'intégrité de la ROI. Le concept de tatouage zéro-bit est employé pour éviter d'insérer aucune information dans la ROI et préserver la fidélité de cette région. En plus de la détection des altérations, cette méthode permet de corriger les altérations dans la ROI en utilisant un code correcteur des erreurs RS. Les informations d'authentification et de reconstruction sont insérées dans le domaine fréquentiel de la RONI) utilisant la transformée LWT).

Dans la quatrième contribution, nous avons proposé une nouvelle approche de tatouage de deuxième génération basée sur les DVs et le code CRC en utilisant des polynômes standard de degré élevée ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans chaque région de l'image après une décomposition en utilisant les Diagrammes de Voronoi VD. La décomposition de Voronoi est employée car elle a de bonnes performances de récupération comparée à des algorithmes de décomposition géométrique similaires. Le détecteur de Harris est utilisé pour extraire les points d'intérêts (FPs) considérés comme des germes pour créer une décomposition de Voronoi de l'image. La méthode proposée peut être applicable dans le cas où la détection d'altération est critique et seules certaines régions d'intérêt doivent être retransmises si elles sont altérées, comme dans le cas des images médicales. L'aspect de sécurité de notre méthode proposée est atteint en utilisant le système de cryptage à clé publique RSA pour crypter les FPs. Les résultats expérimentaux prouvent l'impact de la décomposition VD sur la qualité des images tatouées par rapport à la décomposition en blocs. Nous avons aussi appliqué notre approche pour la détection des altérations des images médicales. Habituellement, les informations de détection d'altération et de récupération de la ROI sont stockées dans RONI qui accepte une dégradation de la qualité visuelle. Dans certaines situations, le récepteur est impuissant de changer ce partitionnement. Par exemple, lorsqu'il détecte des ROIs dans la RONI. Notre schéma proposé peut être applicable dans ce cas et le récepteur peut spécifier plusieurs ROIs et si elles sont altérées, seuls les paquets altérés dans ces régions sont retransmis par l'expéditeur.

Ce manuscrit est composé de six chapitres. Le premier chapitre expose une introduction aux approches évolutionnaires et l'optimisation génétique. Plus précisément, nous focalisons notre étude sur l'optimisation multi-objectif basée sur les algorithmes génétiques. Le second chapitre fournit un survol sur les aspects principaux et les terminologies liés aux évolutions des technologies du tatouage invisible des images numériques.

Le troisième chapitre décrit l'application du tatouage numérique à l'imagerie médicale. Nous présentons une introduction à l'imagerie médicale, les exigences de protection et les limitations des systèmes conventionnels de protection, les techniques du tatouage d'image médicales. Le concept du tatouage zéro-bit sera exposé à la fin de ce chapitre.

Le quatrième chapitre décrit une nouvelle approche de tatouage numérique basée sur l'utilisation des algorithmes évolutionnaires. Le cinquième chapitre exprime les deux approches du tatouage appliquées à l'imagerie médicale en utilisant la théorie des codes. Le dernier chapitre décrit une nouvelle approche de tatouage fragile de deuxième génération basée sur le Diagramme de Vororoi. Cette thèse est clôturée par une conclusion suivie par deux annexes.

Chapitre 1

Approches évolutionnaires et optimisation génétique

Sommaire

1.1 Introduction

La recherche d'une technique de recherche optimale a été l'objet de nombreux chercheurs, qui ont d'abord abordé le problème au moyen de méthodes mathématiques précises. Néanmoins, la nécessité de résoudre des problèmes plus complexes a donné lieu à des méthodes stochastiques. Certaines de ces techniques reposent principalement sur les principes de l'évolution naturelle et, plus précisément, sur le fait que les organismes capables d'acquérir des ressources auront tendance à avoir des descendants à l'avenir. Nous avançons que ces organismes sont plus adaptés à la survie, et leurs caractéristiques seront choisies pour leurs descendants naturels.

La modélisation algorithmique et la simulation numérique du processus d'évolution naturelle a donné naissance à la notion de *Calcul Evolutif* (CE) [Back et al., 1991].

Beaucoup de chercheurs ont développé des algorithmes inspirés par l'évolution naturelle [Bäck et al., 1997] dans le but de résoudre des des problèmes trop difficiles à résoudre avec d'autres méthodes analytiques.

Ces algorithmes d'évolution artificielle, également connus sous le nom d'*algorithmes évolutionnaires* (EAs), utilisent une *fonction objectif* appelée aussi *fonction d'adaptation* (*fitness* en anglais) qui détermine à quel point les solutions résolvent le problème prédéfini. Ces organismes, communément appelés *individus*, représentent des solutions candidates à un problème prédéfini, et le concept de la fonction de fitness est tout à fait différent de celui de l'évolution naturelle, où le fitness d'un individu est défini par son succès reproductif.

Les techniques existantes dans le domaine du CE permettent d'abstraire le processus d'évolution naturel en algorithmes utilisés pour rechercher des solutions optimales à un problème spécifique. Les AEs sont considérés comme des méthodes de recherche très flexibles et peuvent être utilisés pour résoudre de nombreux problèmes en considérant à la fois une bonne représentation individuelle (solution candidate) et une fonction de fitness précise qui décrit l'adéquation individuelle pour le problème.

Néanmoins, de nombreux chercheurs ont critiqué le concept d'évolution artificielle en raison de ses éléments de hasard et d'absence de preuve formelle de convergence [Gonzalez et al., 1997].

L'objectif de ce chapitre est d'introduire les approches évolutionnaires et l'optimisation génétique. Nous faisons référence à des notions pertinentes des approches évolutionnaires, leurs principes, leurs avantages et leurs domaines d'application. Nous énumérons aussi les paradigmes des AEs : stratégies évolutionnaires, programmation génétique, programmation évolutionnaire et algorithmes génétiques. Par la suite, nous focalisons la lumière sur les algorithmes génétiques en présentant les concepts et terminologies qui faciliteront la compréhension des notions utilisées dans le contexte de notre travail de thèse. Nous présentons aussi la notion d'optimisation mono-objectifs et multi-objectifs ainsi que la notion de Pareto. Par la suite, nous exposons certaines approches conventionnelles d'optimisation afin de mettre l'accent sur les avantages d'utilisation des AGs pour la résolution des problèmes d'optimisation multi-objectifs. Par ailleurs, nous avons orienté nos intérêts vers les approches populaires d'optimisation multi-objective comme le NSGA-II qui sera utiliser dans le chapitre 5 pour l'optimisation du processus de tatouage.

1.2 Algorithmes évolutionnaires

L'évolution de Charles Darwin en 1859 est intrinsèquement un mécanisme de recherche et d'optimisation. Le principe de Darwin "*survie des plus forts*" a capturé l'imagination populaire. Ce principe est utilisé comme point de départ pour l'introduction du CE et aux AEs [Bäck

et al., 2000]. En conséquence, les AEs sont d'un intérêt récent, en particulier pour la résolution de problèmes pratiques et ils sont avérés être des alternatives très efficaces aux méthodes classiques pour la résolution de nombreux problèmes d'optimisation.

1.2.1 Principe de base

Les AEs sont des méthodes stochastiques d'optimisation globale basées sur une imitation de l'évolution naturelle des populations [Sumathi et al., 2008, Bäck et al., 1997]. Le principe de base des AGs est de faire évoluer une population par transformation aléatoire de certains de ses éléments, et ensuite l'application du principe de la sélection naturelle. Ces algorithmes sont assimilés à un processus d'optimisation d'un problème donné où les individus d'une population évoluent dans le temps, afin de devenir de plus en plus adapté à l'environnement du problème à résoudre. Le principe général d'un AE est bien détaillé dans l'algorithme 1.1.

Algorithme 1.1 Procédure standard d'un AE

Étape 1 : *Initialisation*

- Initialisation du nombre de génération $t = 0$.
- Génération aléatoirement d'une population initiale $P(t)$.

Étape 2 : *Évaluation*

- Évaluation de chaque individu dans $P(t = 0)$ par calcul de la fonction de fitness.

Étape 3 : *Génération d'une nouvelle population* $P(t)$

- $t = t + 1$;
- Génération d'une nouvelle population $P(t)$ à partir de la population $P(t - 1)$ comme suit :
  - Sélection des individus les plus performants de $P(t - 1)$ au sens de la fonction de fitness.
  - Application des opérateurs de variation :
    - Recombinaison des parties de deux individus pour en obtenir deux nouveaux (opérateur de croisement).
    - Modification aléatoirement des individus (opérateur de mutation).
  - Évaluation la fonction de fitness de chaque individu de la nouvelle population.
  - Remplacement de certains individus de l'ancienne population par les meilleurs individus de la nouvelle population.

Étape 4 : *Critères d'arrêt*

Si la condition d'arrêt n'est pas vérifiée, aller vers l'étape 3, sinon, retourner le meilleur individu de $P(t)$.

1.2.2 Paradigmes des AEs

Dans le CE, il existe quatre paradigmes historiques [Sivanandam and Deepa, 2007] : Algorithmes génétiques, programmation génétique, stratégies évolutives et programmation évolutive. Les différences fondamentales entre les paradigmes reposent sur la nature des schémas de représentation, des opérateurs de reproduction et des méthodes de sélection.

- **Algorithmes génétiques (AG) :** Les AGs proposés par J. Holland [Holland, 1975] et popularisés D.E. Goldberg [Goldberg, 1989]. Ils mettent l'accent sur le croisement plus que la mutation, qui est couramment appliqué avec une très faible probabilité.

- **Les stratégies d'évolution (SE) :** Les SE appartiennent à un deuxième paradigme qui a été développé par I. Rechenberg [Rechenberg, 1973] comme une méthode pour résoudre des problèmes d'optimisation des paramètres réels. Ils utilisent généralement une représentation individuelle constituée d'un vecteur à valeur réelle. Les propositions des SE initiales ont utilisé la mutation en tant qu'opérateur principal, mais aujourd'hui, la mutation et le croisement sont considérées. Il convient de noter que, dans toute proposition de SE, la mutation modifie habituellement les individus selon une distribution normale [Back et al., 1991].
- **La programmation évolutive (PE) :**
  La programmation évolutive est un troisième paradigme, qui a d'abord été défini par .J. Fogel et al. [Fogel et al., 1966]. Dans la PE, les individus sont représentés par un vecteur à valeur réelle et ils sont évolués en considérant l'opérateur de mutation (le croisement n'est pas utilisé) avec une probabilité qui suit souvent une distribution normale [Beyer and Schwefel, 2002].
- **La programmation génétique (PG) :**
  La programmation génétique peut être considérée comme un AG avec un encodage spécial. Elle a été proposée par Koza [Koza, 1992] pour créer des programmes informatiques au moyen d'un langage de représentation complexe. L'objectif initial de la PG était de trouver une solution optimisée à partir d'un espace de recherche composé de tous les programmes informatiques possibles. Néanmoins, la PG est actuellement utilisée pour développer d'autres types de connaissances, comme les systèmes basés sur des règles [Espejo et al., 2010], car elle est considérée comme une technique heuristique évolutive et très flexible qui permet d'utiliser des représentations de motifs complexes.

1.2.3 Avantages des AEs

Les AEs offrent des avantages pratiques à plusieurs problèmes d'optimisation [Fogel, 1997] :

1. ***Simplicité conceptuelle :***
   Un avantage majeur du calcul évolutif est qu'il est conceptuellement simple. L'algorithme consiste en une initialisation, une variation itérative et une sélection en fonction de fitness. Sur les itérations de variation et de sélection aléatoires, la population peut être convertie en solutions optimales.
2. ***Large domaine d'application :***
   Les algorithmes évolutifs peuvent être appliqués à tous les problèmes qui peuvent être formulés en tant que problèmes d'optimisation d'une fonction prédéfini. Pour résoudre ces problèmes, il faut une structure de données pour représenter et évaluer des solutions à partir d'anciennes solutions. Les petits changements dans la structure des parents conduiront à de petits changements dans la progéniture, et de même des changements importants chez les parents entraîneront des modifications drastiques chez les descendants. Dans ce cas, des AEs sont développés, de sorte qu'ils soient syntonisés de manière auto-adaptative. Cela permet d'appliquer les AEs à de vastes zones, y compris des problèmes combinatoires discrets, des problèmes de nombres mixtes et ainsi de suite [Han and Kim, 2000, Rahmat-Samii and Michielssen, 1999].
3. ***Hybridation avec d'autres méthodes***
   Les AEs peuvent être combinés avec des techniques d'optimisation plus traditionnelles.
4. ***Robustesse aux changements dynamiques :***
   Les méthodes traditionnelles d'optimisation ne sont pas robustes aux changements dynamiques dans l'environnement et nécessitent un redémarrage complet pour fournir une

solution. Au contraire, le CE peut être utilisé pour adapter les solutions aux circonstances changeantes. La population générée à partir des solutions évoluées fournit une base pour une amélioration et dans de nombreux cas, il n'est pas nécessaire de réinitialiser la population au hasard.

5. ***Résolution des problèmes qui n'ont pas de solutions :***
   L'avantage des AEs comprend sa capacité à résoudre des problèmes pour lesquels il n'y a pas d'expertise humaine. Même si l'expertise humaine devrait être utilisée lorsqu'il est nécessaire est disponible ; il s'avère souvent moins adéquat pour les routines automatisées de résolution de problèmes. Certains problèmes existent avec un système expert : les experts ne sont peut-être pas d'accord, peuvent ne pas être qualifiés, peuvent ne pas être cohérents ou simplement provoquer une erreur.
6. ***Parallélisme***
   Lorsque les ordinateurs de traitement distribués deviennent plus populaires, il y aura un potentiel accru d'application du CE à des problèmes plus complexes. Cependant, le processus d'évolution est un processus très parallèle. [Ochi et al., 1998, Alba, 2002].

1.3 Algorithmes génétiques

Les AGs utilisent donc une terminologie similaire à celui de la génétique. Nous parlerons ainsi d'*individus* ou *chromosomes* dans une *population*. Chaque individu ou chromosome est constitué d'un ensemble d'éléments appelés *gènes* contenant les caractères héréditaires de l'individu. Ils utilisent un mécanisme de sélection naturelle, basée essentiellement sur *la reproduction* et sur *le codage génétique* qui stocke les informations décrivant l'individu sous forme de gènes imitant les systèmes naturels de l'évolution des espèces. Les éléments d'un AG sont présentés dans la Figure 1.1.

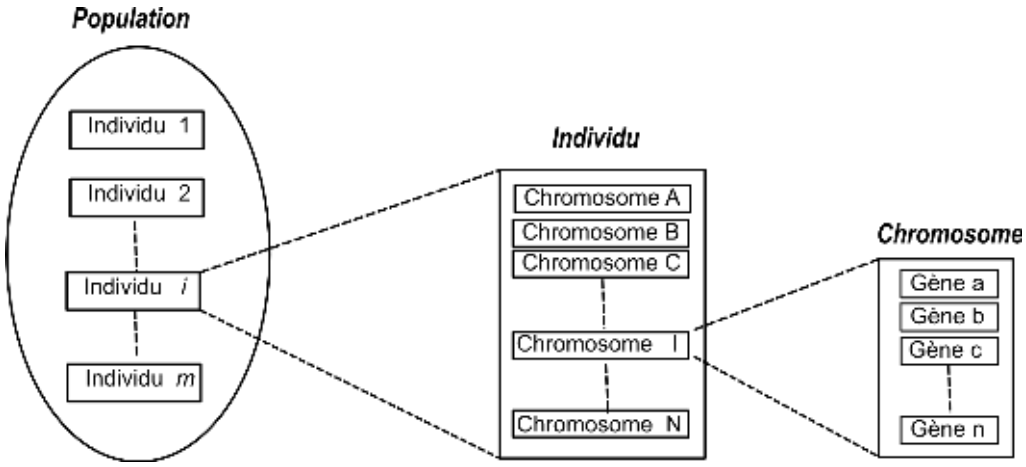


FIGURE 1.1: Éléments d'un AG.

1.3.1 Fonctionnement d'un AG

Selon Michalewicz [Michalewicz, 2013], un AG possédé cinq composants de base :

1. Une représentation des solutions du problème avec une méthode de codage.
2. Un mécanisme de génération d'une population initiale.

3. Une fonction de fitness pour évaluer la qualité des solutions.
4. Opérateurs génétiques pour diversifier la population.
5. Valeurs des paramètres des algorithmes génétiques tels que la taille de la population, le nombre total de générations ou critère d'arrêt de l'algorithme, etc.

L'AG maintient une population d'individus, nommée $P(t)$, pour la génération t. Chaque individu représente une solution potentielle au problème à résoudre. Chaque individu est évalué par calcule d'une fonction de fitness. Certains individus subissent des transformations stochastiques par des opérations génétiques pour former de nouveaux individus. Il existe deux types de transformation : *la mutation*, qui crée de nouveaux individus en faisant des changements dans un seul individu, et *un croisement*, ce qui crée de nouveaux individus en combinant des parties de deux individus. Les nouveaux individus, appelés progéniture $C(t)$, sont ensuite évalués. Une nouvelle population est formée en sélectionnant les individus les plus adaptés de la population mère et la population de progéniture. Après plusieurs générations, l'algorithme converge vers le meilleur individu, représente une solution optimale ou sous-optimale au problème. Le fonctionnement général des algorithmes génétiques est décrit par la Figure 1.2.

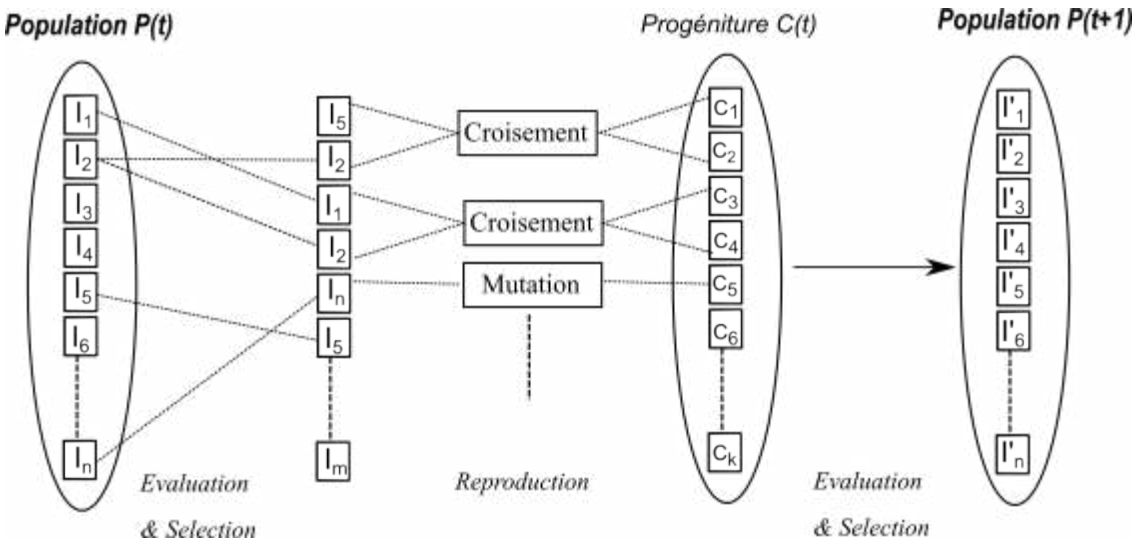


FIGURE 1.2: Principe général d'un AG [Michalewicz, 2013].

1.3.2 Fondations d'un AG

1.3.2.1 Mécanisme de codage

Le codage est le processus de représentation des gènes. Le codage dépend principalement du problème à résoudre. Nous pouvons distinguer différents types de codage [Sivanandam and Deepa, 2007] :

A. ***Codage binaire***
La manière la plus courante et la plus simple du codage est le codage binaire qui représente chaque gène par une chaîne de bits.

B. ***Codage octal***
Ce codage utilise une chaîne composée de nombres hexadécimales de 0 à 7.

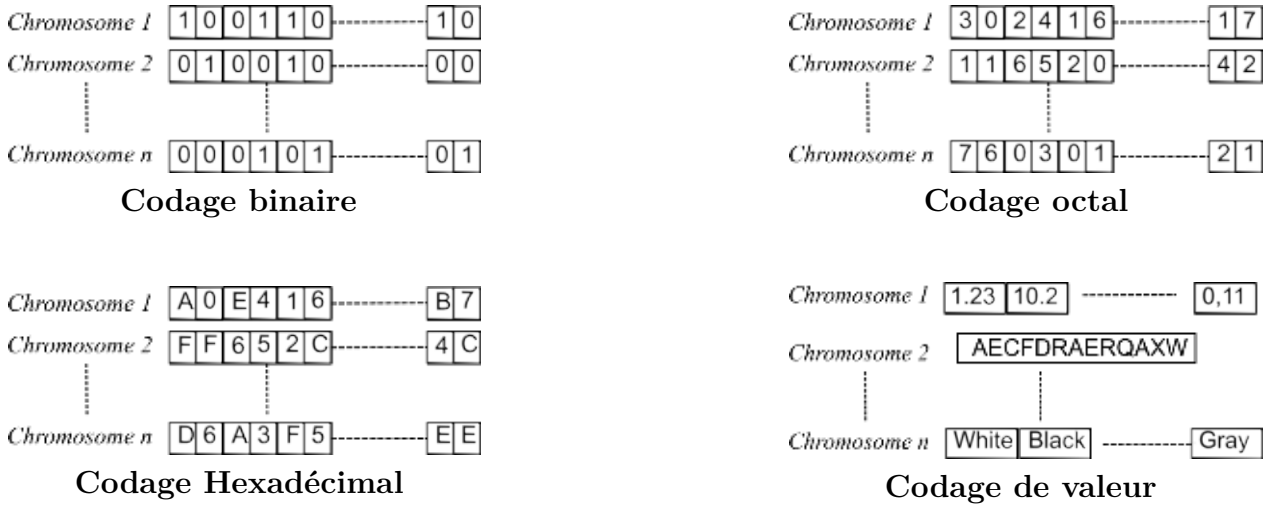


FIGURE 1.3: Différents types de codage.

C. ***Codage hexadécimal***
Ce codage utilise une chaîne composée de nombres octales de 0 à 9 et de A à F.

D. ***Codage de permutation (codage réel)***
En codage de permutation, chaque chromosome est une chaîne de valeurs entières/réelles, qui représente le nombre dans une séquence.

E. ***Codage de valeur***
Chaque chromosome est une chaîne de valeurs et les valeurs peuvent être liées au problème à résoudre. Ce type de codage produit les meilleurs résultats pour certains problèmes spéciaux.

F. ***Codage d'arbre***
Ce codage est principalement utilisé pour l'évolution des expressions de programme pour la programmation génétique. Chaque chromosome est un arbre de certains objets telles que les fonctions et les commandes d'un langage de programmation.

La Figure 1.3 illustre les différents types de codage.

1.3.2.2 Opérateur de sélection

La sélection est le processus de choix de deux parents de la population pour le passage à la reproduction. Après avoir décidé d'un codage, la prochaine étape consiste à décider de la sélection c'est-à-dire comment choisir des individus dans la population qui créeront une progéniture pour la prochaine génération et combien de descendants créeront chacun. Le but de la sélection est de mettre l'accent sur les personnes en pleine forme dans la population, dans l'espoir que leurs ressorts ont une meilleure forme de fitness.

Typiquement, nous pouvons distinguer deux types de schéma de sélection, une sélection proportionnelle et une sélection ordinale. La sélection proportionnelle choisit les individus en fonction de leurs valeurs de fitness par rapport à l'aptitude des autres individus dans la population. Par contre, la sélection ordinale sélectionne les individus en fonction de leurs rangs dans la population et non pas par rapport à de leurs fonctions de fitness.

De nombreux schémas de sélection ont été proposés dans la littérature. Nous décrivons , dans ce qui suit les méthodes les plus courantes [Mitchell, 1998].

A. ***Sélection par tirage de roulette (loterie biaisée)***
La sélection de la roulette est l'une des techniques traditionnelles de sélection de l'AG

proposée par Holland [Holland, 1975]. Elle s'inspire des roues de loterie. L'opérateur de reproduction couramment utilisé est l'opérateur de reproduction proportionnel où un individu est sélectionné dans le pool d'accouplement avec une probabilité proportionnelle à la fonction de fitness. Le principe de la sélection de la roulette est une recherche linéaire à travers une roulette avec les fentes de la roue pondérées proportionnellement aux valeurs de la fonction de fitness de l'individu.
Avec cette méthode chaque individu a une chance d'être sélectionné proportionnelle à sa performance, donc plus les individus sont adaptés au problème, plus ils ont de chances d'être sélectionné. Ainsi, un individu x_i dans une population de N individus a la probabilité suivante d'être sélectionné :

$$P(x_i) = \frac{fitness(x_i)}{\Sigma_{j=1}^{N} fitness(x_j)}$$

Le principe de cette technique est que chaque individu reçoit une tranche de la roulette, la taille de la tranche étant proportionnelle à son adaptation. La roulette est tournée N fois, où N est le nombre d'individus dans la population. À chaque tour, l'individu, sous le marqueur de la roue est sélectionné pour être dans le groupe de parents pour la prochaine génération.

B. *Sélection par rang*

La sélection par tirage de la Roulette aura un problème lorsque les valeurs de fitness diffèrent considérablement. Si la meilleure fonction de fitness est de 90%, sa tranche occupe 90% de la roulette, et les autres chromosomes ont trop peu de chances d'être sélectionnés. Backer [Baker, 1985] introduit la notion de la sélection par rang. Cette approche classe la population et chaque chromosome reçoit un rang du classement selon l'ordre donné par la fonction de fitness. Le meilleur individu dans une population de taille N prendra le rang N, par contre le plus mauvais prendra le rang 1. Cependant, la probabilité de sélectionner un individu x_i est :

$$P(x_i) = \frac{Rang(x_i)}{\Sigma_{j=1}^{N} Rang(x_j)}$$

Il en résulte une convergence lente, mais évite une convergence trop rapide. Il maintient également la pression de sélection lorsque la variance de la fonction de fitness est faible. Il préserve la diversité et mène à une recherche réussie. En effet, les parents potentiels sont sélectionnés et un tournoi est retenu pour décider lequel des individus sera le parent.

C. *Sélection par tournoi*

Une stratégie de sélection idéale devrait être capable d'ajuster la pression de sélection et la diversité de la population afin d'affiner la performance de la recherche des AG.
Contrairement à la sélection par la roulette, la stratégie de sélection du tournoi offre une pression sélective en organisant une compétition de tournoi parmi les N individus. Cependant, cette approche augmente les chances pour les individus de piètre qualité de participer à l'amélioration de la population.
Le principe du tournoi est de tirer aléatoirement plusieurs individus dans la population, ensuite sélectionner le meilleur pour créer une nouvelle population. Le meilleur individu du tournoi est celui qui a la valeur de fitness la plus grande, qui est le gagnant de N. Les concours de tournoi et le gagnant sont insérés par la suite dans le pool d'accouplement. La compétition du tournoi est répétée jusqu'à ce que le bassin d'accouplement, pour générer de nouveaux descendants, soit rempli. La différence de fitness fournit la pression de sélection, qui permet à l'AG d'améliorer l'aptitude des gènes suivants. Cette méthode est plus efficace et conduit à une solution optimale.

1.3.2.3 Opérateur de croisement

Après le processus de sélection, la population est enrichie de meilleurs individus. L'opérateur de croisement est appliqué au pool d'accouplement avec l'espoir qu'il crée une meilleure progéniture.

Le croisement procède en trois étapes :

— L'opérateur de reproduction sélectionne au hasard une paire de chaînes pour l'accouplement.
— Une position de croisement est sélectionnée au hasard le long de la longueur de la chaîne.
— Enfin, les chaînes sont échangées entre elles suite au site de croisement.

Nous présentons par la suite certaines techniques de croisement :

A. ***Croisement à un point***
Les AGs traditionnels utilisent un croisement à un seul point, où les deux chromosomes d'accouplement sont coupés une fois aux points correspondants et les sections après les coupures sont échangées.

B. ***Croisement à deux points***
Dans ce cas, deux points de croisement sont choisis et le contenu entre ces points est échangé entre deux parents accouplés.

C. ***Croisement multi-points (croisement à N-points)***
Plusieurs points de croisement sont sélectionnés et l'échange se fait sur les différentes parties des séquences cernées par ces points, entre les gènes des parents.

D. ***Croisement uniforme***
Un croisement uniforme est tout à fait différent du croisement à N points. Chaque gène est créé en copiant le gène correspondant de l'un ou de l'autre parent choisi selon un masque de croisement binaire généré aléatoirement de même longueur que les chromosomes. Lorsque la valeur du masque est 1, le gène est copié du premier parent et, lorsque sa valeur est 0, le gène est copié du second parent. Le masque est généré au hasard pour chaque paire de parents.

E. ***Croisement à trois parents***
Dans cette technique, trois parents sont choisis au hasard. Chaque bit du premier parent est comparé au bit du second parent. Si les deux sont identiques, ce bit est pris pour création d'un nouvel individu ; autrement dit le bit du troisième parent est pris pour la progéniture.

La Figure 1.4 illustre les différents types de mutation.

1.3.2.4 Opérateur de mutation

Après un croisement, les chaines sont soumises à une opération de mutation. Cet opérateur introduit de nouvelles structures génétiques dans la population en modifiant aléatoirement certains de ses éléments constitutifs. La mutation aide à échapper au piège des minima locaux et à maintenir la diversité dans la population. Elle joue aussi un rôle très important de récupération des matériaux génétiques perdus, c'est une police d'assurance contre la perte irréversible du matériel génétique.

Il existe de nombreuses formes de mutation pour les différents types de représentation.

A. ***Mutation par renversement (flipping)***
Pour la représentation binaire, une simple mutation peut consister à inverser la valeur de chaque gène avec une faible probabilité. Le renversement d'un bit implique de changer sa valeur de 0 à 1 et de 1 à 0 en fonction d'un chromosome de mutation généré aléatoirement. Le rôle du chromosome de mutation est d'indiquer les positions des bits à inverser. La

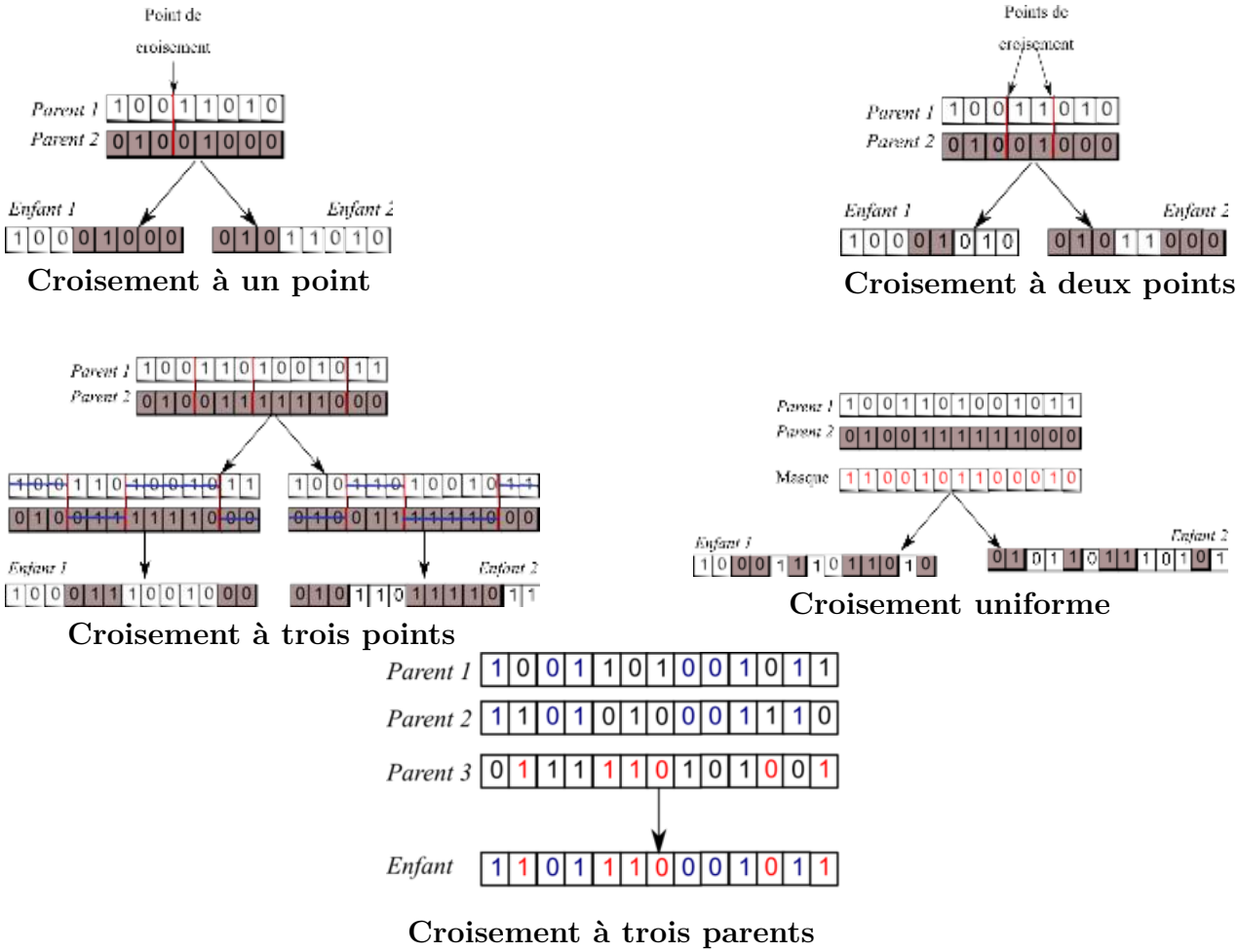


FIGURE 1.4: Différents types de mutation.

valeur 1 du chromosome de mutation signifie que le bit correspondant dans le chromosome parent est renversé (0 à 1 et 1 à 0) et le chromosome enfant est produit. La Figure 1.5 donne un exemple simple d'une mutation par renversement.

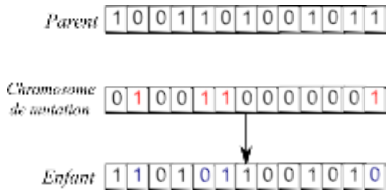


FIGURE 1.5: Exemple d'une mutation par renversement.

B. *Mutation par inter-changement*

Deux positions aléatoires de la chaîne sont choisies et les bits correspondant à ces positions sont échangés. Ceci est montré à la Figure 1.6.

1.3.2.5 Opérateur de remplacement

Le remplacement est la dernière étape d'une AG. Deux parents sont tirés d'une population de taille fixe, ils génèrent deux enfants, mais tous les quatre ne peuvent pas revenir à la

FIGURE 1.6: Exemple d'une mutation par inter-changement.

population, donc deux doivent être remplacés. Une méthode de remplacement doit être utilisée afin de déterminer lequel des membres actuels de la population, le cas échéant, devraient être remplacés par les nouvelles solutions. Fondamentalement, il existe deux types de méthodes pour maintenir la population : un remplacement générationnel et un remplacement stationnaire.

A. ***Les techniques de remplacement générationnel***

Les techniques de remplacement générationnel consistent à produire N enfants d'une population de taille N pour former la nouvelle population (génération), et cette nouvelle population d'enfants remplace complètement la sélection parentale.

B. ***Les techniques de remplacement stationnaire***

Dans le remplacement stationnaire, de nouveaux individus sont insérés dans la population dès qu'ils sont créés, par opposition aux techniques de remplacement générationnel où toute une génération est produite à chaque étape. L'insertion d'un nouvel individu nécessite habituellement le remplacement d'un autre membre de la population. L'individu à supprimer peut-être choisi selon une des méthodes suivantes [Sivanandam and Deepa, 2007] :

— Le pire membre de la population, cela entraîne une pression de sélection très forte.
— Le plus âgé de la population.
— Le remplacement du tournoi : c'est exactement identique à la sélection des tournois, sauf les solutions moins bonnes sont choisies.
— Le membre le plus similaire de la population existante.

1.4 Problème d'optimisation

L'optimisation consiste à trouver une ou plusieurs solutions qui correspondent à la minimisation (ou à la maximisation) d'un ou de plusieurs objectifs spécifiés et satisferont toutes les contraintes (le cas échéant). L'optimisation peut être appliquée à n'importe quelle discipline scientifique ou technique. Le but de l'optimisation est de trouver un algorithme qui résout une classe de problèmes donnés. Il n'existe aucune méthode spécifique, qui résout tous les problèmes d'optimisation.

D'une part, un problème d'optimisation mono-objectifs implique une fonction objectif unique et aboutit habituellement à une solution unique, appelée *solution optimale*. D'autre part, l'optimisation multi-objectifs considère simultanément plusieurs objectifs contradictoires. Dans ce cas, il n'y a habituellement pas de solution optimale, mais un ensemble d'alternatives avec différents compromis, appelés solutions optimales de *Pareto,* ou des *solutions non dominées*. Malgré l'existence de multiples solutions optimales de Pareto, dans la pratique, il ne faut généralement choisir qu'une de ces solutions [Branke et al., 2008].

Définition 1 ***Optimisation mono-objectif*** *[Coello et al., 2007]*
Un problème général d'optimisation mono-objectif est défini par une fonction de minimisation (ou maximisation) de $f(X)$ *soumis à* $g_i(X) \leq 0, i = \{1, ..., m\}$ *et* $h_j(x) = 0, j = \{1, ..., p\}, X \in \omega$. *Une solution minimise (ou maximise) le scalaire* $f(X)$ *où* X *est un vecteur de* n *variables de décision* $X = (x_1, ..., x_n)$ *à partir d'un univers* Ω.

Observez que $g_i(X) \leq 0$ et $h_j(x) = 0$ représentent les contraintes qui doivent être satisfaites en optimisant (minimisant ou maximisant) $f(X)$. Ω contient tous les X possibles qui peuvent être utilisés pour satisfaire une évaluation de $f(X)$ et de ses contraintes. La méthode pour trouver l'optimum global (peut ne pas être unique) de n'importe quelle fonction est appelée optimisation globale.

Le problème d'optimisation multi-objectif POM (également appelé optimisation multi-critère, ou multi-performance) peut alors être défini comme le problème de trouver un vecteur de variables de décision qui satisfait des contraintes et optimise une fonction vectorielle dont les éléments représentent les fonctions objectifs. Ces fonctions forment une description mathématique des critères de performance qui sont généralement en conflit les unes avec les autres. Par conséquent, le terme *optimiser* signifie trouver une telle solution qui donnerait au décideur les valeurs de toutes les fonctions objectifs [Osyczka, 1985].

Définition 2 ***Optimisation multi-objectif*** *[Coello, 2002]*
Un POM est défini par une fonction de minimisation (ou maximisation)

$$F(X) = (f_1(X), ..., f_k(X))$$

Où k est le nombre de fonctions objectifs à optimiser au sujet de $g_i(X) \leq 0, i = \{1, ..., m\}$ et $h_j(X) = 0, i = \{1, ..., p\}$ où $X \in \Omega$. Une solution d'un POM minimise (ou maximise) les composantes du vecteur $F(X)$ où X est un vecteur de variables de décision $X = (x_1, x_2, ..., x_n)$, $X \in \Omega$. Notant que $g_i(X) \leq 0$ et $h_j(X) = 0$ représenter les contraintes qui doivent être satisfaites en minimisant (ou en maximisant) $F(X)$ et Ω contient tous les X possibles qui peuvent être utilisés pour satisfaire une évaluation de $F(X)$.

Notion de Pareto

La notion d'*optimum* la plus couramment adoptée est celle proposée à l'origine par Francis Ysidro Edgeworth [Edgeworth, 1881] et plus tard généralisée par mathématicien italien Vilfredo Pareto [Stadler, 1988]. Bien que certains auteurs appellent cette notion l'optimum d'*Edgeworth-Pareto*, le terme le plus couramment accepté est l'*optimum de Pareto*.

Définition 3 ***Pareto Optimal*** *[Coello, 2002]*
La solution $X \in \Omega$ est dite Pareto Optimal par rapport à Ω si et seulement s'il n'y a pas une autre solution $X' \in \Omega$ pour que $v = F(x')$ domine $u = F(X)$.

Cette définition affirme que X' est l'optimum de Pareto s'il n'existe pas de vecteur X qui diminuerait un critère sans provoquer une augmentation simultanée d'au moins un autre critère (en supposant une minimisation).

De plus, il y a quelques autres définitions qui sont également adoptées dans l'optimisation multi-objectifs : Dominance de Pareto, ensemble d'optimums Pareto et Front de Pareto.

Définition 4 ***Dominance de Pareto*** *[Veldhuizen, 1999]*
Un vecteur $u = (u_1, u_2, ..., u_k)$ domine un autre vecteur $v = (v_1, v_2, ...v_k)$ noté par $u \preceq v$ si et seulement si u est partiellement inférieur à v, cela veut dire :

$$\forall i \in \{1, ..., k\}, u_i \leq v_i \wedge \exists i \in \{1, ..., k\} : u_i < v_i. \quad (1.1)$$

Les solutions optimales de Pareto (Figure 4.7) sont les solutions dans l'espace de recherche dont les composantes du vecteur objectif phénotype correspondant ne peuvent pas être toutes simultanément améliorées. Ces solutions sont également appelées *solutions non inférieures*, *admissibles* ou *efficaces*. L'ensemble complet étant représenté par $\mathcal{P}^*$. Leurs vecteurs correspondants sont appelés *solutions non-dénommés*, la sélection d'un ou de plusieurs vecteurs à

partir de cet ensemble de vecteurs (front de Pareto $\mathcal{FP}^*$) indique implicitement des solutions optimales de Pareto.

Définition 5 ***Ensemble d'optimums Pareto*** *[Veldhuizen, 1999]*
Pour un POM $F(x)$, l'ensemble d'optimums Pareto, $\mathcal{P}^*$, est défini comme suit :

$$\mathcal{P}^* := \{x \in \Omega | \neg \exists x' \in \Omega F(x') \preceq F(x)\}. \quad (1.2)$$

Lorsqu'ils sont tracés dans un espace objectif, les vecteurs non dominants sont connus collectivement comme le front de Pareto. Encore une fois, $\mathcal{P}^*$ est un sous-ensemble d'un ensemble de solutions. Ses vecteurs objectifs évalués forment $\mathcal{FP}^*$, dont chacun est non-dénominatif par rapport à tous les vecteurs objectifs produits en évaluant chaque solution possible dans Ω.

Définition 6 ***Front de Pareto***
Pour un POM $F(x)$ et un ensemble d'optimums Pareto $\mathcal{P}^*$, le front de Pareto $\mathcal{FP}^*$ est défini comme suit :

$$\mathcal{FP}^* := \{u = F(x) | x \in \mathcal{P}^*\}. \quad (1.3)$$

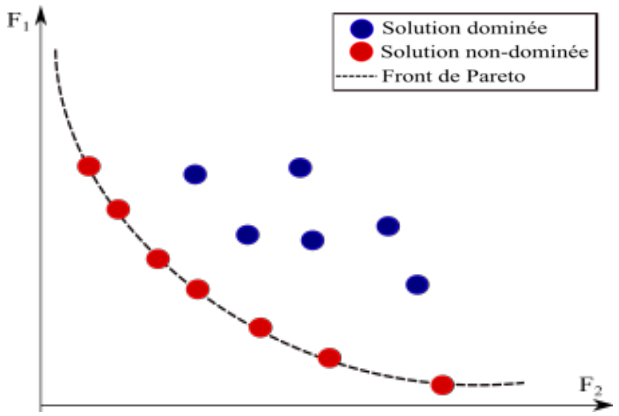


FIGURE 1.7: Concept de Pareto [Zitzler, 1999].

1.5 Approches d'optimisation multi-objectifs

L'utilisation d'AGs pour les tâches de recherche et d'optimisation est devenue très populaire ces dernières années avec le développement de nouvelles théories et de nouveaux domaines d'applications [Goldberg, 1989, Fonseca et al., 1993]. L'un des domaines de recherche émergents dans lesquels les AGs sont de plus en plus populaires est l'optimisation multi-objectifs (OMO). Dans les PMO , nous avons deux ou plusieurs fonctions objectifs à optimiser en même temps, au lieu d'en avoir une seule. En conséquence, il n'y a pas de solution unique aux PMO, mais nous cherchons plutôt à trouver toutes les bonnes solutions de compromis disponibles (l'ensemble optimal de Pareto).

La première implémentation d'un algorithme d'optimisation multiobjectif génétique (*Multi-Objective Genetic Alogrithm MOGA*) remonte au milieu des années 1980 [Schaffer, 1985].

Dans la littérature une grande variété de techniques MOGA a été proposée. Nous pouvons les regroupé en trois grandes catégories [Coello et al., 1999, Abraham and Jain, 2005] :

- Méthodes agrégées.
- Méthodes fondées sur la population.
- Méthodes fondées sur le Pareto.

1.5.1 Approches agrégées

L'approche la plus simple pour gérer plusieurs objectifs avec n'importe quelle technique est peut-être de combiner tous les objectifs en un seul en utilisant une addition, une multiplication ou toute autre combinaison d'opérations arithmétiques. En fait, les approches d'agrégation sont les plus anciennes méthodes de programmation mathématique pour l'optimisation multiobjectif, puisqu'elles peuvent être dérivées des conditions de Kuhn-Tucker pour les solutions non dominées [Kuhn,].

Les techniques agrégées les plus populaires sont :

- La méthode de la somme pondéré (weighted sum) [Kim and de Weck, 2005, Stanimirovic et al., 2011].
- La programmation des objectifs (goal programming) [Deb, 1999, Deb, 2001b].
- Méthode ϵ-contrainte [Mavrotas, 2009, Laumanns et al., 2006].
- L'algorithme min-max [Hajela and Lin, 1992, Coello and Christiansen, 1998].

1.5.2 Approches fondées sur la population

Dans ces techniques, la population d'un AG est utilisée pour diversifier la recherche, mais le concept de dominance de Pareto n'est pas directement incorporé dans le processus de sélection. L'exemple classique de ce type d'approche est le Vector Evaluated Genetic Algorithm (VEGA), proposé par Schaffer [Schaffer, 1985].

L'algorithme VEGA est un algorithme génétique simple avec un mécanisme de sélection modifié. A chaque génération, un certain nombre de sous-populations est généré en effectuant une sélection proportionnelle en fonction de chaque fonction objectif à son tour. Ainsi, pour un problème avec k objectifs, on génère k sous-populations de taille $\frac{M}{k}$ (M est la taille de population totale).

Dans la méthode VEGA le processus de sélection est opposé au concept de domination de Pareto. Si, par exemple, il y a un individu qui code une bonne solution de compromis pour tous les objectifs, mais ce n'est pas le meilleur dans aucun d'entre eux, il sera rejeté. Notez cependant que cet individu devrait vraiment être préservé car il code une solution Pareto-optimale. Schaffer a suggéré quelques heuristiques pour traiter ce problème. Par exemple, utiliser une approche de préférence de sélection heuristique pour les individus non dominants dans chaque génération, afin de protéger les individus qui codent pour des solutions Pareto-optimales mais ne sont pas les meilleurs dans une fonction objectif unique. De plus, le croisement entre les individus pourrait être encouragé en ajoutant quelques heuristiques de sélection de contraintes au lieu d'utiliser la sélection de contraintes aléatoires de l'AG traditionnelle. Néanmoins, le fait que la dominance de Pareto ne soit pas directement incorporée dans le processus de sélection de l'algorithme reste son principal inconvénient. Malgré les limites de ces approches, leur simplicité a attiré plusieurs chercheurs pour développer d'autres variantes de VEGA ou d'autres approches basées sur la population comme par exemple la méthode lexicographique qui consiste à ranger tous les objectifs par ordre d'importance ensuite l'optimum est obtenu pour chaque fonction objectif [Fourman, 1985].

1.5.3 Approches fondées sur le Pareto

Goldberg [Goldberg, 1989] a proposé un moyen pour résoudre les problèmes posés par les approches fondées sur la population. L'approche proposée consiste en un schéma de sélection basé sur le concept d'optimalité de Pareto. Goldberg a non seulement suggéré ce qui deviendrait

le standard d'optimisation mutlti-objectif à base des approches évolutionnaires (MOEA) pendant plusieurs années, mais a également indiqué que le bruit stochastique rendrait de tels algorithmes inutiles à moins qu'un mécanisme spécial n'ait été adopté pour bloquer la convergence. Le *nichage* ou le *partage de fitness* a été suggéré par Deb et Goldberg [Deb and Goldberg, 1989] comme un moyen de maintenir la diversité et d'éviter la convergence de l'AG vers une solution unique.

Les approches basées sur le Pareto peuvent être historiquement étudiées comme couvrant deux générations. La première génération est caractérisée par l'utilisation du partage de la fonction de fitness et du nichage combiné avec le classement de Pareto (défini par Goldberg ou en adoptant une légère variation).

La deuxième génération de MOEA est née avec l'introduction de la notion d'*élitisme*. Dans le contexte de l'optimisation multi-objectif, l'élitisme désigne habituellement l'utilisation d'une population externe (également appelée population secondaire) pour retenir les individus non dominés.

1.5.3.1 Approches de nichage

1. **Multiobjective Genetic Algorithm (MOGA)**

   Fonseca et Fleming (1993) [Fonseca et al., 1993] sont les premiers qui ont introduit le principe de l'optimisation multi-objectif à base d'AG (appelée MOGA) qui repose sur la classification non dominée de la population. Ils ont proposé pour la première fois une stratégie d'AG multi-objectif qui vise explicitement à mettre l'accent sur des solutions non dominées et à maintenir simultanément la diversité dans les solutions non dominées. Le MOGA diffère d'un AG standard dans la façon dont la fonction objectif est assignée à chaque individu dans la population. Le reste de l'algorithme est le même que celui de l'AG classique.

   Le principe de cette méthode est de ranger chaque individu de la population selon un rang qui lui est affecté. Le rang d'une solution i est égal à un plus le nombre de solution n_i qui dominent la solution i :

   $$r_i = 1 + n_i. \tag{1.4}$$

   De cette manière, les solutions non dominées se voient attribuer un rang égal à 1, car aucune solution ne dominerait une solution non dominée en population.

2. **Niched-Pareto Genetic Algorithm (NPGA)**

   L'algorithme NPGA est proposé par Horn et al. [Horn et al., 1994]. Cette approche utilise un système de sélection de tournois basé sur la domination de Pareto. L'idée de base de l'algorithme est la suivante :

   - Deux individus sont choisis au hasard et comparés à un sous-ensemble de la population entière (typiquement, environ 10% de la population).
   - Si l'un d'entre eux est dominé (par les individus choisis au hasard parmi la population) et l'autre ne l'est pas, alors l'individu non dominé gagne.
   - Lorsque les deux compétiteurs sont dominés ou non (c'est-à-dire qu'il y a égalité), le résultat du tournoi est décidé par une fonction de partage de fitness.

   La méthode NPGA utilise la sélection de tournique binaire, contrairement à la méthode de sélection proportionnelle utilisée dans VEGA, NSGA et MOGA. Le choix de la sélection de tournoi par rapport à la sélection proportionnelle est motivé par les études théoriques de Goldberg and deb 1991 [Goldberg and Deb, 1991] sur les opérateurs de sélection utilisés dans l'optimisation mono-objectif. Ils ont démontré que la sélection tournique

a de meilleures propriétés de croissance et de convergence par rapport à la sélection proportionnelle.

3. **Non-dominated Sorting Genetic Algorithm (NSGA)**

   Cet algorithme a été proposé par Srinivas et Deb [Srinivas and Deb, 1994]. L'approche est basée sur le classement non dominé. Avant la sélection, la population est classée sur la base de la non-dominance : tous les individus non dominés sont classés en une seule catégorie (avec une valeur de fitness factice, proportionnelle à la taille de la population, pour offrir un potentiel de reproduction égal à ces individus).

   NSGA ne diffère d'un AG simple que par le fonctionnement de l'opérateur de sélection. Les opérateurs de croisement et de mutation restent comme d'habitude. Avant que la sélection ne soit effectuée, la population est classée en fonction de la non-domination d'un individu. Les individus non dominants présents dans la population sont d'abord identifiés à partir de la population actuelle. Alors tous ces individus sont supposés constituer le premier front non dominé de la population et se voient attribuer une grande valeur de fitness factice. La même valeur de fitness est assignée pour donner un potentiel de reproduction égal à tous les individus non-dominés.

   Pour maintenir la diversité dans la population, ces individus classés sont ensuite partagés avec leurs valeurs factices. Le partage est réalisé en effectuant une opération de sélection en utilisant des valeurs de fitness dégradées qui sont obtenues en divisant la valeur de fitness initiale d'un individu par une quantité proportionnelle au nombre d'individus qui l'entourent. Cela entraîne la coexistence de plusieurs points optimaux dans la population. Après partage, ces individus non-dominants sont temporairement ignorés pour traiter le reste de la population de la même manière pour identifier les individus pour le second front non-dominé. Ces points non dominants se voient alors assigner une nouvelle valeur de fitness fictive qui est maintenue plus petite que la valeur de fitness minimale factice partagée du front précédent. Ce processus se poursuit jusqu'à ce que toute la population soit classée en plusieurs fronts (Figure 1.8).

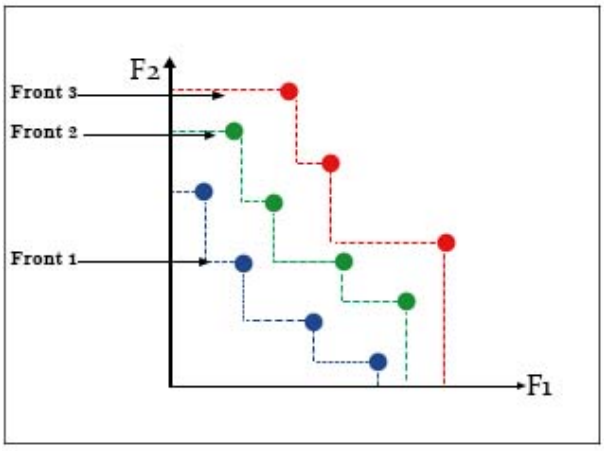


FIGURE 1.8: Classement par fronts (NSGA) [Zitzler, 1999].

Puisque les individus du premier front ont la valeur maximale de la fonction de fitness, ils ont toujours plus de copies que le reste de la population. Cela permet de rechercher des régions non dominées et aboutit à une convergence de la population vers de telles régions. Le partage, de son côté, aide à répartir la population sur cette région (c'est-à-dire le front

de Pareto du problème).

1.5.3.2 Approches basées sur l'élitisme

A l'inverse des approches non élitistes, les approches élitistes comportent une ou plusieurs stratégies permettant de conserver les meilleures solutions trouvées au cours du processus de reproduction.

1. **Distance-Based Pareto Genetic Algorithm (DPGA)**
   Osyczka et Kundu (1995) [Osyczka and Kundu, 1995] ont proposé un AG avec une stratégie d'élitisme basée sur la distance nommée Distance-Based Pareto GA (DPGA). Ils visent à mettre l'accent sur les progrès vers le front optimal de Pareto et la diversité le long du front obtenu en utilisant une seule mesure de fitness. Cet algorithme maintient deux populations : une population d'AG standard P_t où les opérations génétiques sont effectuées, et une autre population élite E_t contenant toutes les solutions non dominées trouvées.
   La population initiale P_0 de taille N est créée au hasard. Le premier membre de la population reçoit une valeur de fitness positive générée aléatoirement F_1. Il est automatiquement ajouté à l'ensemble élite E_0. Par la suite, nous attribuons à chaque solution une valeur de fitness basée sur sa distance par rapport à l'ensemble élite, $E_t = \{e^{(k)} : k = 1, 2, ..., K\}$, où K est le nombre de solutions dans l'ensemble élite. Chaque solution élite $e^{(k)}$ a M valeurs de la fonction objectif, $e^{(k)} = \left(e_1^{(k)}, e_2^{(k)}, ..., e_M^{(k)}\right)^T$. La distance d'une solution x de l'ensemble d'élite est calculée comme suit :

$$d^k\{x\} = \sqrt{\sum_{m=1}^{M} \left(\frac{e_m^{(k)} - f_m(x)}{e_m^{(k)}}\right)^2} \tag{1.5}$$

2. **Strength Pareto Evolutionnary Algorithm (SPEA)**
   Zitzler et Thiele en 1998 [Zitzler and Thiele, 1998] ont proposé un algorithme évolutif élitiste, qu'ils ont appelé *Strength Pareto Evolutionnary Algorithm*. Cet algorithme introduit l'élitisme en maintenant explicitement une population externe $\overline{P}$. Cette population stocke un nombre fixe de solutions non dominées trouvées jusqu'au début d'une simulation. À chaque génération, les solutions non dominées nouvellement trouvées sont comparées à la population externe existante et les solutions non dominées qui en résultent sont préservées. Le SPEA fait plus que simplement préserver les élites, il utilise aussi ces derniers pour participer aux opérateurs génétiques avec la population actuelle dans l'espoir d'influencer la population à se diriger vers de bonnes régions dans l'espace de recherche.
3. **Non-dominated Sorting Genetic Algorithm II (NSGA-II)**
   En 2000 Deb et al [Deb et al., 2000], ont suggéré une stratégie de tri élitiste non-dominée (appelée NSGA-II). Contrairement à la méthode ci-dessus qui utilise seulement une stratégie de préservation d'élite, NSGA-II utilise une stratégie de préservation d'élite et un mécanisme explicite de préservation de la diversité. Dans la plupart des aspects, cet algorithme n'a pas beaucoup de similitude avec NSGA-I, mais les auteurs ont gardé le nom NSGA-II pour mettre en évidence les origines de la méthode.
   Dans NSGA-II, la population de la progéniture Q_t est d'abord créée en utilisant la population parente P_t. Cependant, au lieu de trouver seulement les fronts non dominés de Q_t, les deux populations sont d'abord combinées pour former R_t de taille $2 \times N$. Ensuite,

un tri non dominé est utilisé pour classer toute la population R_t. Bien que cela nécessite plus d'efforts que d'effectuer un tri non dominé sur Q_t mais il permet un contrôle global de non-domination entre les solutions parentes et enfants.

Une fois le tri non dominé est terminé, la nouvelle population P_{t+1} est comblée par des solutions de différents fronts non dominés, un à la fois. Le remplissage commence par le meilleur front non dominé et continue avec les solutions du deuxième front non dominé, suivi par le troisième front, et ainsi de suite. Il est impossible de prendre en compte tous les fronts dans les créneaux N disponibles dans la nouvelle population P_{t+1}. Cependant, les fronts qui n'ont pas pu être accommodés sont simplement supprimés. Lorsque le dernier front autorisé commence à poindre, il peut exister plus de solutions dans le dernier front que les créneaux restants dans la nouvelle population. Ce scénario est illustré à la Figure 1.9.

Au lieu de rejeter arbitrairement certains membres du dernier front, une stratégie de nichage est utilisée pour choisir les membres du dernier front, qui résident dans la région la moins peuplée de ce front. Une stratégie comme celle-ci n'affecte pas beaucoup le déroulement de l'algorithme dans la population combinée. Il est probable que les solutions de plusieurs fronts non dominants sont déjà incluses dans la nouvelle population, avant qu'elles ne s'ajoutent à N. Peu importe alors quelle solution est incluse pour remplir la population. Cependant, durant les dernières étapes de la simulation, il est également probable que la plupart des solutions dans la population se situent dans le meilleur front non dominé. Il est également probable que dans la population combinée R_t de taille $2N$, le nombre de solutions dans le premier front non dominé dépasse N.

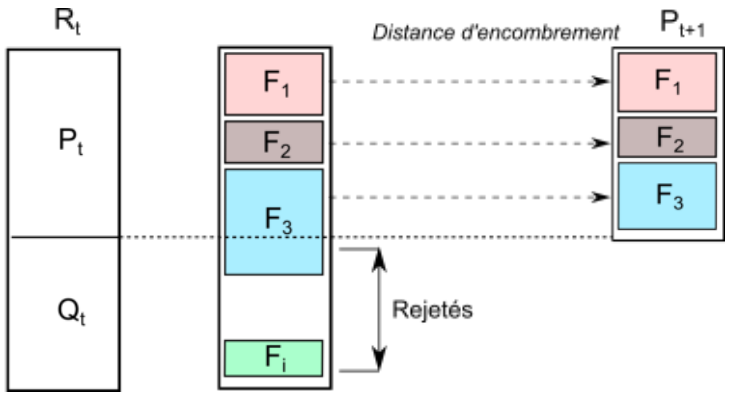


FIGURE 1.9: Principe générale de l'algorithme NSGA-II [Deb, 2001a].

Dans la suite, nous décrivons l'algorithme NSGA-II. Initialement, une population aléatoire P_0 est créée. La sélection de tournois binaires (avec un opérateur de tournoi à enchaînements décrit plus tard), les opérateurs de recombinaison et de mutation sont utilisés pour créer une population de descendants Q de taille N. La procédure NSGA-II est par l'algorithme 1.2 .

Algorithme 1.2 Procédure NSGA-II

Étape 1 :

- Création d'une population R_t en combinant la population parent P_t et la population enfant Q_t : $R_t = P_t \cup Q_t$.
- Classement de la population R_t et identification des fronts non-dominés $\mathcal{F}_i$, $i = 1, 2, ...$

Étape 2 :

- Posant $P_{t+1} = \phi$ et $i = 1$;
- Jusqu'à ce que $|P_{t+1}| + |\mathcal{F}_i| < N$ faire :
  - $P_{t+1} = P_{t+1} \cup \mathcal{F}_i$.
  - $i = i + 1$.

Étape 3 :

- Exécution de la procédure de tri d'encombrement *crowding-sort* (Voir l'algorithme 1.3).
- Inclusion des solutions les plus répandues $N - |P_{t+1}|$ en utilisant les valeurs de distance d'encombrement dans le front $\mathcal{F}_i$.

Étape 4 :

- Création d'une population d'enfants Q_{t+1} à partir de P_{t+1} en utilisant la sélection tournique d'encombrement, le croisement et la mutation.

A l'étape 3, le tri des solutions de front i (le dernier front qui n'a pas pu être complètement intégré) est effectué en utilisant une métrique de distance d'encombrement, que nous décrirons un peu plus loin. La population est classée par ordre décroissant d'amplitude des valeurs de distance d'encombrement. À l'étape 4, un opérateur de sélection de tournoi d'encombrement, qui utilise également la distance d'encombrement, est employé.

Sélection tournique d'encombrement (*Crowded Tournament Selection* CTS) :

L'opérateur de comparaison ($<$) compare deux solutions et retourne le gagnant du tournoi. Il suppose que chaque solution i a deux attributs :

- Un rang de non-domination r_i dans la population.
- Une distance d'encombrement locale d_i dans la population : la distance d'encombrement est une mesure de l'espace de recherche autour de i qui n'est pas occupée par aucune autre solution dans la population.

Sur la base de ces deux attributs, l'opérateur de sélection tournique d'encombrement est défini comme suit :

Une solution i gagne un tournoi avec une autre solution j si l'une des conditions suivantes est remplie :

- Si la solution i a un meilleur rang, c'est-à-dire $r_i > r_j$.
- Si elles ont le même rang mais la solution i a une meilleure distance d'encombrement que la solution j, c'est-à-dire $r_i = r_j$ et $d_i > d_j$.

La première condition fait en sorte que la solution choisie repose sur un meilleur front non dominé. la seconde condition résout le fait que les deux solutions se trouvent sur le même front non dominé en décidant de leur distance surpeuplée. Celui qui réside dans une zone moins encombrée (avec une plus grande distance d'encombrement d_i) gagne.

La distance d'encombrement :
Pour estimer de la densité de solutions entourant une solution particulière i dans la population, nous prenons la distance moyenne de deux solutions de chaque côté de la solution i le long de chacun des objectifs. Cette quantité d_i sert d'estimation du périmètre d'un hypercube formé en utilisant les voisins les plus proches comme des sommets (nous appelons cela la distance d'encombrement). Dans la Figure 1.10, la distance d'encombrement de la solution i dans son front (est la longueur latérale moyenne de l'hypercube montrée par une boîte en pointillé). L'algorithme 1.3 est utilisé pour calculer la distance d'encombrement de chaque point de l'ensemble $\mathcal{F}$.

Algorithme 1.3 Procédure de tri d'encombrement (*Crowding-sort*)

Étape 1 :
- Pour chaque solution i dans $\mathcal{F}$ posant $d_i = 0$.

Étape 2 :
- Pour chaque fonction objectif f^m où $m = 1, 2, ..., M$ faire
  - — Classement de l'ensemble dans l'ordre pire de f_m.

Étape 3 :
- Pour $m = 1, 2, ..., M$ faire
  - — Affectation d'une grande distance aux solutions limites : $d_{I_1^m} = d_{I_l^m} = \infty$, où l est le nombre de solution dans le front.
  - — Pour toutes les autres solutions $j = 2$ jusqu'à $(l-1)$ faire :
    - — Affectation de la distance $d_{I_j^m}$ calculé comme suit :

$$d_{I_j^m} = d_{I_j^m} + \frac{f_m^{(I_{j+1}^m)} - f_m^{(I_{j+1}^m)}}{f_m^{max} - f_m^{min}} \tag{1.6}$$

L'index I_j dénote l'index de la solution j dans la liste triée. Ainsi, pour tout objectif, I_1 et I_l désignent les valeurs de la fonction objectif les plus basses et les plus élevées, respectivement. Le second terme du côté supérieur de l'équation 1.6 est la différence entre les valeurs de la fonction objectif entre deux solutions voisines de chaque côté de la solution I_j. Ainsi, cette métrique désigne la moitié du périmètre du l'hypercube incluant la solution i avec la solution voisine la plus proche placée sur les sommets du l'hypercube (Figure 1.10).
Il est intéressant de noter que pour toute solution i les deux solutions $(i+1)$ et $(i-1)$ n'ont pas besoin d'être voisins dans tous les objectifs, en particulier pour $M >= 3$. Les paramètres f_m^{max} et f_m^{min} peuvent être définis comme les valeurs maximum et minimum de la fonction objectif m.

1.6 Conclusion

Dans ce chapitre, nous avons présenté les approches évolutionnaires d'une manière générale. Nous avons exposé leurs avantages et leurs domaines d'application ainsi que leurs différents paradigmes (algorithmes génétiques, stratégies évolutionnaires, programmation génétique et

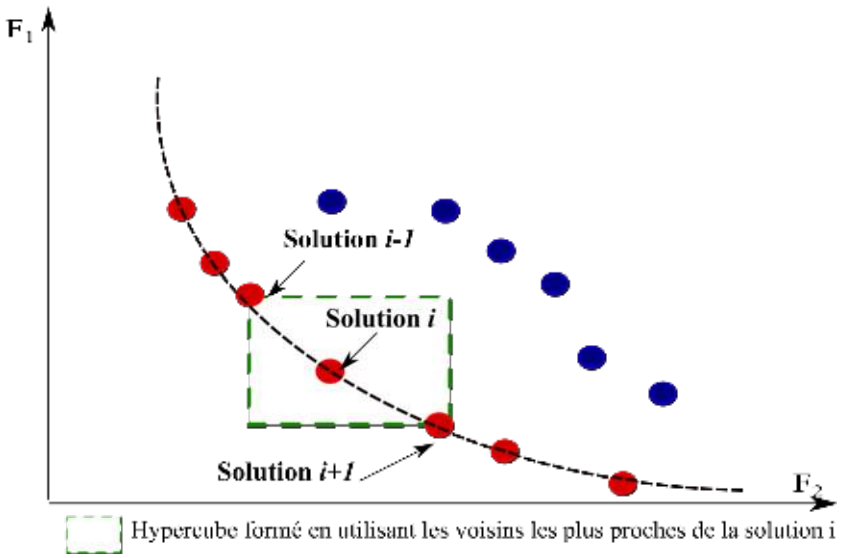


FIGURE 1.10: Calcul de la distance d'encombrement [Deb et al., 2002].

programmation évolutionnaire). Nous avons mis l'accent principalement sur les algorithmes génétiques. Nous nous sommes intéressés aux terminologies et aux notions pertinentes dans le domaine des AGs telles que la population, le chromosome, etc.

Nous nous sommes focalisés par la suite sur le concept d'optimisation. Nous avons donné un aperçu sur certaines notions pertinentes comme l'optimisation mono-objectifs, multi-objectifs ainsi que la notion de Pareto. A la fin, nous nous sommes intéressés en particulier à l'utilisation des AGs pour la résolution des problèmes d'optimisation multi-objectifs. Par ailleurs, nous avons orienté nos intérêts vers les approches populaires d'optimisation multi-objective comme le NSGA-II qui sera utiliser dans le chapitre 4 pour l'optimisation du processus de tatouage.

Chapitre 2

Tatouage numérique pour la protection des images

Sommaire

2.1 Introduction

Un facteur important qui ralentit la croissance des services en réseau multimédia est que les auteurs, les éditeurs et les fournisseurs de données multimédia sont réticents à autoriser la distribution de leurs documents dans un environnement réseau.

En effet, la facilité de reproduction de données numériques dans leur forme originale exacte est susceptible d'encourager la violation du droit d'auteur, le détournement de données et la distorsion du contenu.

Par conséquent, les créateurs et les distributeurs de données numériques recherchent activement des solutions fiables aux problèmes liés à la protection du droit d'auteur des données multimédia.

En outre, le développement des systèmes multimédias en réseau, en particulier sur les réseaux ouverts comme l'Internet, est conditionné par la mise au point de stratégies efficaces pour protéger les propriétaires de données contre toutes activités illégales.

La cryptographie a été la première proposition pour sécuriser des transferts de documents multimédia. Cette technique a fourni un contrôle sur l'accès aux données et les a rendues illisibles pour les utilisateurs non autorisés. Cependant, les systèmes de cryptage ne résout pas complètement le problème, car une fois décrypté, le document n'est plus protégé et il peut être distribué ou modifié malhonnêtement. Une stratégie complémentaire a été envisagée : le tatouage numérique dérivé de la stéganographie. Dans ce chapitre, nous introduisons les techniques de protection des données numériques : la cryptographie et la stéganographie. Ensuite, nous nous concentrons sur les différents concepts liés à la protection par tatouage numérique.

2.2 Techniques de protection des données numérique

La stéganographie et la cryptographie sont utilisées dans la protection de données. La cryptographie est la science qui consiste à protéger les données en les brouillant pour que personne ne puisse les lire sans des méthodes ou des clés données. Il permet à un individu de crypter des données de sorte que le destinataire soit la seule personne capable de le déchiffrer. La stéganographie est la science consistant à obscurcir le message dans un objet hôte (porteur) dans l'intention de ne pas attirer la suspicion sur le contexte dans lequel le message a été transféré.

2.2.1 La cryptographie

Historiquement, le terme *cryptographie* a été associé au problème de la conception et de l'analyse de schémas de cryptage qui fournissent une communication secrète sur des supports de communication non sécurisés. Cependant, depuis les années 1970, des problèmes telles que la construction de signatures numériques infalsifiables et la conception de protocoles tolérants aux pannes ont également été considérées comme relevant du domaine de la cryptographie. En fait, la cryptographie peut être considérée comme étant concernée par la conception de tout système devant résister à des tentatives malveillantes d'en abuser.

Un schéma de cryptage (ou chiffrement) est un protocole permettant à deux parties (communiquant sur un canal qui peut éventuellement être exploité par un adversaire) de communiquer secrètement entre elles. Typiquement, le schéma de chiffrement consiste en une paire d'algorithmes. Un algorithme, appelé *cryptage*, est appliqué par l'expéditeur, tandis

que l'autre algorithme, appelé *décryptage*, est appliqué par le récepteur. Par conséquent, afin d'envoyer un message, l'expéditeur applique d'abord l'algorithme de cryptage au message puis il envoie le résultat, appelé le *texte chiffré* (ou crypté), sur le canal. Lors de la réception d'un texte chiffré, le destinataire applique l'algorithme de décryptage et récupère le message d'origine (appelé le *texte en clair*) [Vaudenay, 2006]. Pour que ce système fournisse une communication secrète, les parties communicantes doivent connaître quelque chose qui n'est pas connue par l'adversaire sinon, il pourrait décrypter le texte chiffré exactement comme fait par le récepteur. Cette connaissance supplémentaire prend la forme de l'algorithme de déchiffrement lui-même ou de certains paramètres et/ou entrées auxiliaires utilisés par l'algorithme de déchiffrement. Nous appelons cette connaissance supplémentaire *la clé de déchiffrement*. Dans les schémas de cryptage classiques, les deux algorithmes dépendent de la même *clé secrète*. Cette clé est utilisée à la fois pour le cryptage et le décryptage. Ces méthodes de chiffrement sont donc appelées *symétriques*. En 1976, W.Diffie and M.E. Hellman [Diffie and Hellman, 1976] ont introduit le concept révolutionnaire de la cryptographie à clé publique. Ils ont fourni une solution au problème d'échange de clés et ont montré la voie aux signatures numériques. Les méthodes de cryptage à clé publique sont *asymétriques*.

2.2.2 La stéganographie

Le terme stéganographie (en anglais : steganography) tire son origine d'une étymologie grecque : *steganos* signifiant cacher et *graphos* signifiant écriture. Cela veut dire que la stéganographie est l'art de cacher des messages secrets. Ce terme apparaît d'abord dans un manuscrit de Johannes Trithemius en 1499 et aussi dans un livre de Caspar Schott publié en 1665 [Schott, 1665]. La stéganographie est l'art de dissimulation d'information privée ou secrète dans un signal, apparemment anodin. Le signal porteur porte le nom *stégo-médium* peut être un fichier texte, image, audio ou vidéo. La propriété primordiale est que le fichier porteur doit sembler ne contenir aucune information secrète c'est-à-dire que personne ne puisse distinguer un médium vierge d'un stégo-médium. La stéganographie numérique repose sur les caractéristiques du système auditif ou visuel humain qui ne sont pas assez sensibles pour détecter de petites modifications ou distorsions introduites dans les documents multimédia [Shih, 2007].

2.2.2.1 Modèle classique de la stéganographie

Le premier modèle de stéganographie est proposé par Simmons [Simmons, 1984] et représenté dans la Figure 2.1. Dans ce modèle deux personnes A et B ont été emprisonnés séparément et ils désirent trouver une stratégie d'évasion. Toutes les communications entre eux sont contrôlées par le gardien C qui n'accepte aucune communication défiante. La stratégie utilisée afin de communiquer discrètement est de cacher les messages significatifs dans un support choisi (image, son,...). Ce support sera ensuite envoyé par A à B. A la réception du média, B extrait le message envoyé à l'aide d'une clé connue par les deux entités. Donc, A et B utilisent la stéganographie. Le rôle du gardien est d'inspecter tous les messages envoyés. Deux approches sont possibles pour les inspectées : *passive* ou *active*. La première approche, consiste à contrôler le support afin de déterminer s'il contient un message caché, puis de mener une action appropriée. Par contre, dans l'approche active, le gardien a modifié les messages, même s'il n'a perçu aucune trace de contenu caché. Des exemples de la méthode active seraient des opérations de traitement d'image tels que la compression avec perte, la conversion de format, la modification de la palette, et le filtrage passe-bas. Il s'agit là de stéganoanalyse.

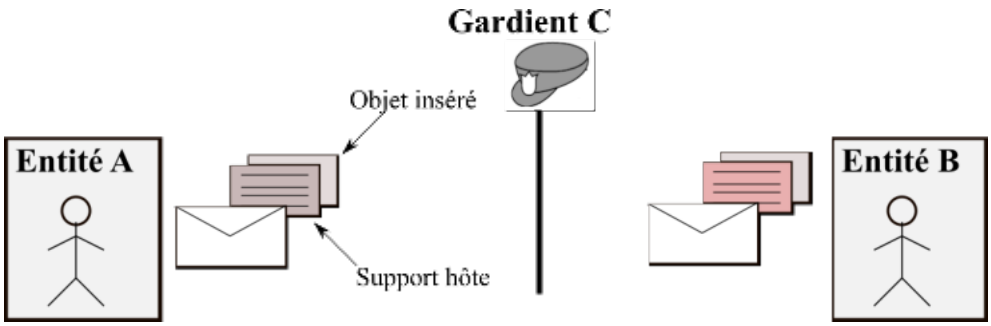


FIGURE 2.1: Modèle classique de la stéganographie [Shih, 2007].

2.2.2.2 Concepts liées à la stéganographie

Deux directions générales peuvent être distinguées dans la stéganographie : la protection contre la détection et la protection contre la suppression comme le montre la Figure 2.2.

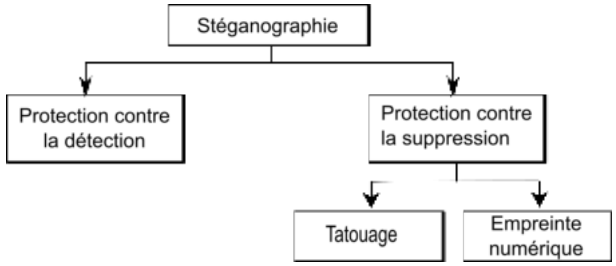


FIGURE 2.2: Techniques liées à la stéganographie [Popa, 1998].

La protection contre la détection repose sur l'utilisation des schémas qui ne modifient pas de façon visible l'objet original, les modifications doivent être invisibles par les systèmes visuels ou auditifs humains ou par les ordinateurs. Par contre, la protection contre la suppression suppose que le schéma devrait être robuste aux attaques communes, il est impossible de supprimer les données cachées sans dégrader la qualité de l'objet et le rendre inutile. Nous pouvons distinguer trois principaux concepts liés à la stéganographie [Popa, 1998] :

- ***Data Hiding*** : consiste à insérer secrètement un message secret dans un médium de sorte que personne ne puisse distinguer un médium vierge d'un stégo-médium.
- ***Tatouage numérique*** : cherche à répondre au problème de la protection des droits d'auteur [O'Ruanaidh et al., 1996]. La marque cachée permettra de protéger le support contre la copie ou contre toute modification ou falsification du support. A la différence du data hiding, l'attaquant ne cherche pas à découvrir le message caché, mais plutôt à le détruire.
- ***Fingerprinting*** *:* cherche à permettre la détection des copies illégales d'un stégo-médium. Chaque utilisateur authentifié possède sa propre copie du médium qui contient son identifiant (empreinte).

2.3 Tatouage numérique

2.3.1 Description formelle

Un système de tatouage est composé de deux sous-systèmes : un codeur et un décodeur. Formellement, ce système peut être décrit par $(\mathcal{O}, \mathcal{W}, \mathcal{K}, E_k, D_k, C_\tau)$, où $\mathcal{O}$ est l'ensemble des données originales, $\mathcal{W}$ est l'ensemble des watermarks et $\mathcal{K}$ est l'ensemble des clés à utiliser. La fonction d'insertion du watermark (codeur) est décrite comme suit [Memon and Wong, 1998] :

$$\begin{aligned} E_k : \mathcal{O} \times \mathcal{W} \times \mathcal{K} &\longrightarrow \mathcal{O} \\ E_k(I_o, w, k) &= I_w \end{aligned} \tag{2.1}$$

Cette fonction prend en entrée un document original I_o, un watermark w et une clé privée ou publique k pour générer en sortie un document tatoué I_w (voir la Figure 2.3).

Le document original, peut être un fichier texte, image, son ou un vidéo. Dans le reste de ce manuscrite, nous nous focalisons sur le tatouage d'images numériques.

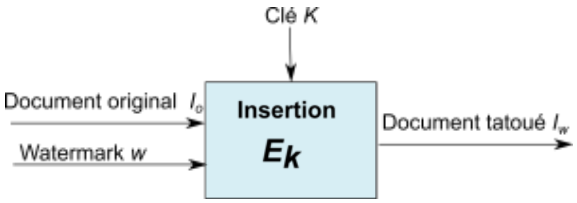


FIGURE 2.3: Fonction d'insertion (codeur).

La fonction d'extraction du watermark (décodeur) est définie comme suit [Memon and Wong, 1998] :

$$\begin{aligned} D_k : \mathcal{O} \times \mathcal{K} &\longrightarrow \mathcal{W} \\ D_k(I'_w, k) &= w' \end{aligned} \tag{2.2}$$

La fonction D_k prend en entrée un document tatoué et éventuellement attaqué I'_w et la clé k pour extraire en sortie le watermark w'. Selon la technique utilisée, l'algorithme d'extraction peut exiger aussi le document original (Figure 5.15).

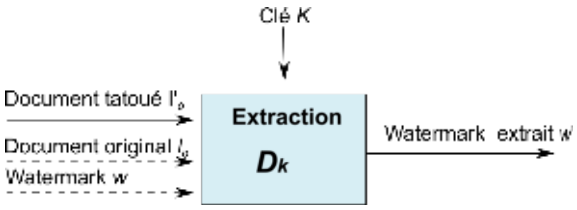


FIGURE 2.4: Fonction d'extraction (décodeur).

Le watermark extrait w' diffère en général du watermark original w en raison de différentes manipulations possibles. Afin de juger de la correspondance entre les deux watermarks, on définit la fonction de comparaison $\mathcal{C}_\tau$ comme suit :

$$\mathcal{C}_\tau : W^2 \longrightarrow \{0, 1\} \tag{2.3}$$

La fonction $\mathcal{C}_\tau$ permet de comparer le watermark extrait avec le watermark original, en utilisant un seuil de comparaison τ :

$$\mathcal{C}_\tau = \begin{cases} 1 & \text{si } c \geq \tau \\ 0 & \text{si } c < \tau \end{cases} \tag{2.4}$$

Le seuil τ dépend de l'algorithme utilisé.

2.3.2 Classification des algorithmes de tatouage

En se basent sur la description présentée au-dessus, les techniques de tatouage peuvent être classifié selon trois critères : la technique d'insertion, les données nécessaires pour l'extraction et la clé utilisée (Figure 2.5).

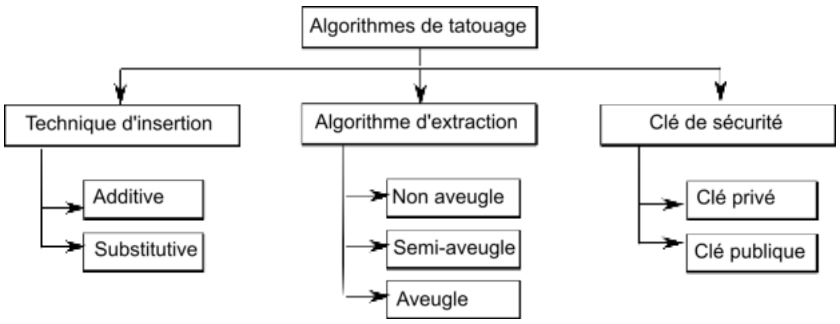


FIGURE 2.5: Classification des algorithmes de tatouage.

2.3.2.1 Classification selon la technique d'insertion

Il existe deux différentes techniques pour insérer le watermark w dans l'image originale I_o : *additive* et *substitutive*.

Dans le tatouage additif [Kwitt et al., 2011], le watermark est directement ajouté au signal hôte avec une puissance uniforme, tandis que dans le tatouage substitutif [Kalantari et al., 2009], la puissance du watermark par composant est proportionnelle à la valeur du signal hôte.

2.3.2.2 Classification selon l'algorithme de détection

Selon les données nécessaires pour l'extraction du watermark, les techniques de tatouage sont divisées en trois catégories : *non-aveugle*, *semi-aveugle*, et *aveugle* [Podilchuk and Delp, 2001].

A) ***Tatouage non aveugle (privé)*** :

Les systèmes de tatouage privé exigent au moins l'image originale. Deux schémas sont possibles :

— *Schéma 1* : le watermark est extrait à partir de l'image tatouée et éventuellement attaquée I'_o, en utilisant l'image originale I_o (Figure 2.6 (a)). La fonction de détection est décrite comme suit :

$$D_k(I'_o, I_o, k) = w'. \tag{2.5}$$

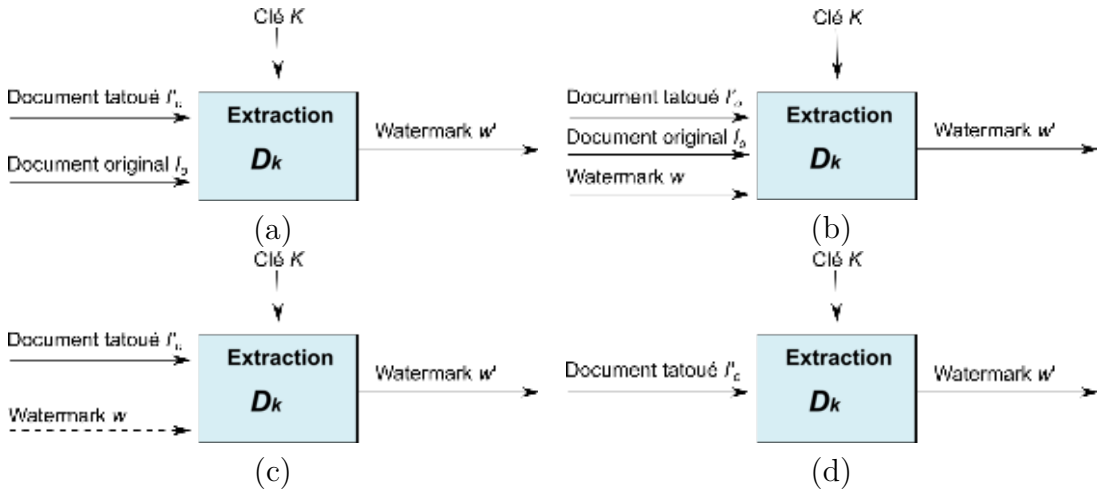


FIGURE 2.6: Classification selon l'algorithme d'extraction : (a) Tatouage non aveugle- Schéma 1. (b) Tatouage non aveugle- Schéma 2. (c) Tatouage semi-aveugle. (d) Tatouage aveugle.

— *Schéma 2* : en plus de l'image originale une copie du watermark w est nécessaire pour répondre à la question : *le watermark est présent ou non ?* (Figure 2.6 (b)). La fonction de détection est définie comme suit :

$$D_k(I'_o, I_o, w, k) = w'. \tag{2.6}$$

B) ***Tatouage semi-aveugle (semi-privé)*** **:**
Le tatouage semi-privé n'utilise pas l'image originale mais seulement une copie du watermark pour répondre à la même question : *le watermark est présent ou non ?* (Figure 2.6 (c)). La fonction de détection est définie comme suit :

$$D_k(I'_o, w, k) = w'. \tag{2.7}$$

C) ***Tatouage aveugle (publique)*** :
Le watermark est extrait à partir de l'image tatouée sans utilisation des données originales (I_o et/ ou w) ((Figure 2.6 (d)). La fonction de détection est définie comme suit :

$$D_k(I'_o, k) = w'. \tag{2.8}$$

2.3.2.3 Classification selon la clé appliquée

Selon la clé appliquée pour insérer et extraire le watermark, trois différentes catégories du systèmes sont citées dans la littérature : *système à clé privée*, *système à clé publique* et *système à clé publique asymétrique* [Shih, 2007].

A) ***Système à clé privée*** :
Dans ce cas, seul les utilisateurs autorisés peuvent détecter le watermark. En d'autres termes, ces techniques investissent tous les efforts pour empêcher les utilisateurs non autorisés d'extraire le watermark, par exemple en utilisant une clé privée générée aléatoirement.
Cette clé privée indique généralement l'emplacement du watermark dans l'image hôte, ou un paramètre utilisé pour l'insertion et l'extraction du watermark [Wong and Memon, 2001].

B) ***Système à clé publique*** *:*

En revanche, les techniques de tatouage qui permettent à tout le monde de lire le watermark sont les systèmes à clé public. Les systèmes de tatouage insèrent le watermark dans un emplacement connu de tous, de sorte que le logiciel d'extraction peut facilement extraire le watermark en balayant l'image entière.

En général, les techniques à clé privée sont plus robustes que les techniques à clé publique, dans lesquelles un attaquant peut facilement supprimer ou détruire le watermark une fois que le code intégré est connu [Wong, 1998, Hartung and Girod, 1997].

C) ***Système à clé publique asymétrique :***

Il y a aussi la forme asymétrique de tatouage à clé publique, par lequel tout utilisateur peut lire le watermark sans pouvoir l'enlever.

C'est ce que l'on appelle un crypto-système asymétrique. Dans ce cas, le processus de détection (et en particulier la clé de détection) est entièrement connu de tous, donc seule une clé publique est nécessaire pour la vérification et une clé privée est utilisée pour l'insertion [Eggers et al., 2000].

2.3.3 Propriétés du tatouage

Tout système de tatouage numérique doit être conçu pour avoir certaines propriétés tout en satisfaisant les exigences fonctionnelles.

Dans cette partie, nous présentons les propriétés principales des systèmes de tatouage qui sont *la fidélité*, *la robustesse*, *la capacité*, *la sécurité* et *la complexité*.

L'ensemble de ces propriétés dépend du domaine d'application du tatouage. Selon Zhao et al. [Zhao et al., 1998], ces domaines sont : la protection du droit d'auteurs, l'annotation cachée (hidden annotations), l'authentification et la communication secrète invisible.

Chacune de ces applications a ses propres exigences (voir Figure 2.7). Par exemple, si le tatouage est appliqué pour la protection des droits, la robustesse, l'imperceptibilité et la sécurité sont primordiales tandis que la capacité est moins importante.

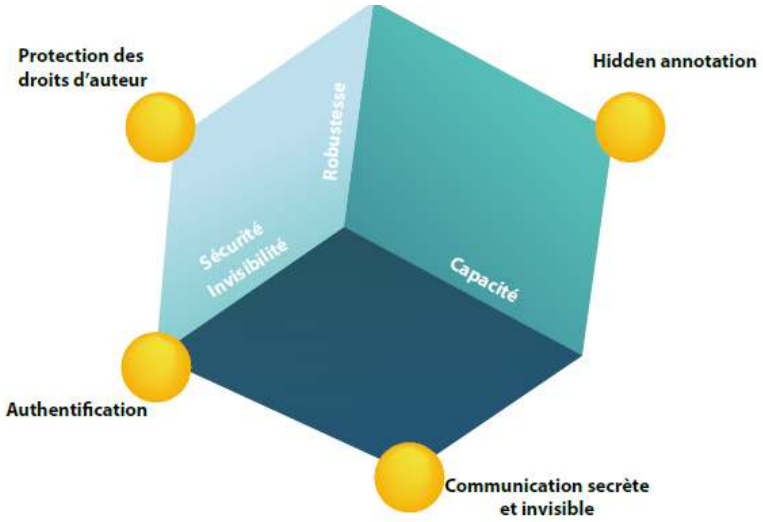


FIGURE 2.7: Dépendance entre l'application et les propriétés du tatouage [Zhao et al., 1998].

Selon Cox et al. [Cox et al., 2000], il est difficile, voire impossible de concevoir un système de tatouage en respectant toutes ces propriétés au plus haut degré. Généralement, nous essayons

de faire des compromis entre ces exigences, tout dépend des exigences de l'application du système de tatouage.

2.3.3.1 Fidélité

Le watermark inséré ne doit pas être perceptible par l'être humain et il ne doit pas dégrader la qualité de l'image originale. Cette propriété est désignée aussi par le terme *imperceptibilité* ou *invisibilité* [Kirovski, 2006].

Cependant, pour concevoir un système de tatouage imperceptible, il faut se baser sur le modèle visuel humain (SVH). Par exemple, les algorithmes de compression avec perte peuvent introduire ou supprimer des informations supplémentaires qui dépassent le seuil de visibilité.

2.3.3.2 Robustesse

La robustesse définit la résistance du watermark face aux différentes distorsions fréquentielles (comme la compression avec perte, filtrage, etc.) ou opérations géométriques (redimensionnement, rotation, ...). En effet, le watermark doit être détecter après toutes transformations.

Afin d'obtenir un système de tatouage robuste aux distorsions, il est préférable d'insérer le watermark dans des régions de perception significatives [Ruanaidh et al., 1996]. Par exemple, le watermark inséré dans des régions de perception insignifiantes est susceptible de ne pas survivre à la compression avec perte. Nous pouvons alors remarquer que cette propriété est contradictoire avec l'imperceptibilité.

La robustesse traite deux problèmes différents, à savoir la présence et la détection du watermark après une certaine opération de traitement. Il n'est pas nécessaire de retirer un watermark pour le rendre inutile, si le récepteur ne peut pas signaler la présence de la marque alors l'attaque peut être considérée comme réussitse.

Cela signifie qu'un schéma de tatouage est robuste lorsqu'il est capable de résister à une série d'attaques qui tentent de dégrader la qualité du watermark incorporé, jusqu'au point où il est supprimé.

Selon la contrainte de robustesse, nous pouvons classifier les algorithme de tatouage en trois catégories :

- ***Tatouage robuste :***
  Les techniques de tatouage robuste disposent d'un large champ de théories et de résultats. Un système de tatouage est dit *robuste* s'il résiste aux altérations possibles (compression, filtrage, rotation, ...). Ce type de tatouage sert généralement à protéger la copyright [Chae and Manjunath, 1997].
- ***Tatouage fragile :***
  Dans ce type de tatouage, le watermark est fortement sensible aux modifications de l'image tatouée et il devrait détecter toute altération. Ces techniques sont généralement utilisées pour garantir un service d'authentification et d'intégrité d'un fichier tatoué [Lin and Delp, 1999].
- ***Tatouage semi-fragile :***
  Tatouage semi-fragile combine la fragilité contre les perturbations malveillantes et la robustesse à certaines classes de dégradations légères de l'image, comme la compression [Lin and Chang, 2000].

2.3.3.3 Capacité

La capacité désigne la quantité d'informations qui peuvent être insérées dans un document hôte sans affecter la qualité de ce dernier.

Cette propriété est liée à l'application visée. Dans le contexte de protection des droits d'auteurs, la capacité n'est pas primordiale. Tandis que dans des applications de data hiding, cette propriété est très importante.

2.3.3.4 Sécurité

La conception d'un système de tatouage sécurisé exige le respect de principe d'Auguste Kerckhoff [Kerckhoffs, 1883] : « I*l faut que le système n'exige pas le secret, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi* ». Cela signifie que le système lui-même doit être connue de tous et ce sont les clefs qui sont secrètes.

Cette propriété concerne la génération des clés, ainsi que les protocoles d'échange de clés. Afin d'atteindre cette propriété, les méthodes de tatouage reposent généralement sur l'utilisation des algorithmes de cryptage symétrique ou asymétrique. La sécurité est liée à la complexité, c'est-à-dire que l'algorithme de tatouage devrait fonctionner avec suffisamment de clés longues pour décourager la recherche de la clé secrète appropriée ce qui influe directement sur la complexité de l'approche de tatouage [Tao et al., 2014].

2.3.3.5 Complexité

Le coût de calcul est un facteur important dans la conception des applications du tatouage. Afin de réduire le coût de calcul, une méthode de tatouage doit être moins complexe. Les méthodes de tatouage basées sur des algorithmes complexes sont gourmandes en matière de ressources logiciels et matérielles. Donc plus de coûts de calcul. Généralement, la simplicité de calcul est habituellement préférée dans les environnements à ressources limitées comme les appareils mobiles [Singh and Chadha, 2013].

2.4 Techniques de tatouage

Les techniques actuelles de tatouage décrites dans la littérature peuvent être regroupées en trois classes principales (Figure 2.8). La première classe comprend les techniques travaillant dans *le domaine spatial.* Ceux-ci intègrent le watermark en modifiant directement les valeurs des pixels de l'image originale.

La seconde comprend les méthodes travaillant dans *le domaine fréquentiel* (ou transformé). Elles insèrent les données en modulant les coefficients d'une transformée de signal original. Le tatouage dans le domaine fréquentiel est plus robuste aux attaques par rapport au tatouage dans le domaine spatial.

La troisième classe comprend les techniques *fondées sur le contenu.* Ces techniques prennent en compte les caractéristiques des régions, des bordures et des objets. De telles méthodes de tatouage peuvent présenter des avantages supplémentaires en termes de détection et de récupération du watermark après des attaques géométriques par rapport aux approches précédentes.

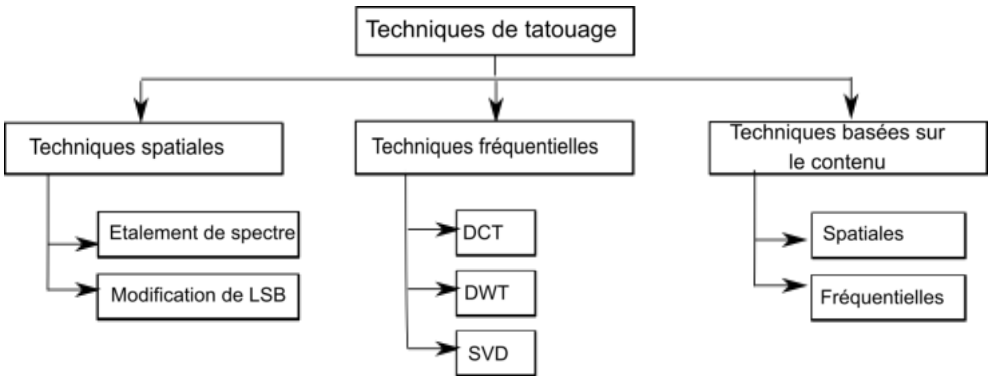


FIGURE 2.8: Techniques de tatouage [Chun-Shien, 2005].

2.4.1 Tatouage dans le domaine spatial

2.4.1.1 Techniques avec étalement de spectre

De nombreuses techniques spatiales sont basées sur l'ajout d'une séquence de bruit pseudo-aléatoire d'amplitude fixe PN à l'image hôte [Cox et al., 1997, Fridrich, 1998, Pérez-Freire and Pérez-González, 2009]. Dans ce cas, la procédure d'insertion et d'extraction sont simplement des opérateurs d'addition et de soustraction, respectivement.

Les séquences PN sont également utilisées comme *clé d'étalement* lorsque nous considérons le support hôte comme un bruit dans un système d'étalement de spectre, où le watermark est le message à transmettre. Dans ce cas, la séquence PN est utilisée pour répartir les bits de données sur le spectre afin de cacher les données.

En général, le watermark w est intégré dans les composantes d'image I_o en utilisant un facteur α (force de tatouage) qui permet d'amplifier les valeurs du watermark afin d'obtenir le meilleur résultats. L'image tatouée est définie tel que :

$$I_w = I_o + \alpha \times w. \tag{2.9}$$

La détection du watermark est basée sur les principes de corrélation. Dans ce cas, un détecteur spécifique compare l'image tatouée et éventuellement attaquée I'_o avec l'image originale I_o et décide automatiquement, en fonction d'un niveau de corrélation spécifique, si le watermark existe ou non [Hanjalic et al., 2000].

2.4.1.2 Techniques avec modification des bits LSB

Ces approches modifient les bits de poids faible LSB de l'image hôte. L'imperceptibilité du watermark est réalisée en supposant que les données LSB sont visuellement insignifiantes. Le watermark est généralement récupéré en utilisant la connaissance de la séquence PN (et peut-être d'autres clés secrètes, comme l'emplacement du watermark) et les propriétés statistiques du processus d'insertion.

Deux techniques LSB sont décrites par Schyndel, Tirkel et Osborne [Van Schyndel et al., 1994]. La première remplace le bit LSB de l'image par une séquence PN, tandis que la seconde ajoute une séquence PN au bit LSB des données.

Afin d'illustrer comment insérer le watermark dans le domaine spatial d'une image, nous décrivons une simple méthode de tatouage numérique proposée par Schyndel et al. dans [Van Schyndel et al., 1994]. Cette technique combine l'insertion dans les bits LSB avec une

procédure d'étalement du spectre. L'algorithme 2.1 illustrent le principe d'insertion de cette méthode.

Algorithme 2.1 Tatouage dans le domaine LSB [Van Schyndel et al., 1994]

1. Génération du watermark :
   - Génération aléatoirement d'une séquence m en utilisant une clé secrète.
   - Arrangement de la séquence binaire générée dans un tableau de deux dimensions qui représente le watermark.
2. Insertion du watermark généré pixel par pixel dans le dernier bit LSB de l'image originale.

Puisque le watermark est inséré dans les LSB, il est invisible. Pour la même raison, il n'est pas robuste, en ce sens qu'il peut être enlevé facilement.

2.4.2 Tatouage dans le domaine fréquentiel

Le principe de base des techniques travaillant dans le domaine fréquentiel est d'utiliser une transformation vers une représentation fréquentielle. Ensuite, le watermark sera inséré dans les coefficients de la transformée utilisée (voir 2.9). Dans la littérature plusieurs transformées ont été appliquées pour le tatouage comme DCT, DFT,DWT, SVD, etc.

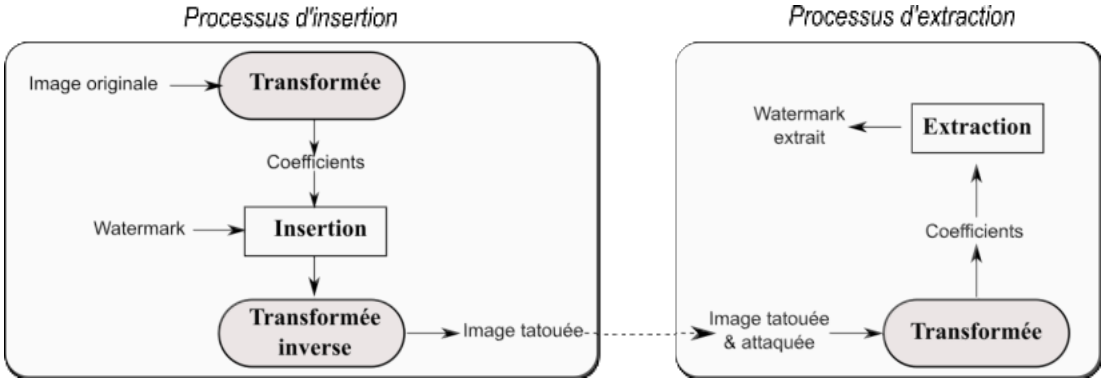


FIGURE 2.9: Schéma de tatouage dans le domaine fréquentiel.

2.4.2.1 Techniques basées sur la DCT

De nombreux algorithmes de compression vidéo et image appliquent la DCT pour transformer une image en domaine fréquentiel et effectuer une quantification pour la compression de données. Cela permet de séparer une image en parties (ou sous-bandes spectrales) d'importance hiérarchique (par rapport à la qualité visuelle de l'image). La technologie JPEG utilise la DCT pour compresser les images. La transformée DCT ainsi que son inverse sont décrits par la définition 7 et 8.

Définition 7 ***La Transformée DCT*** *[Khayam, 2003]*
Soit $f(x,y)$ l'image dans le domaine spatial et $F(u,v)$ représente l'image dans le domaine fréquentiel, l'équation générale de la transformée 2D DCT est :

$$F(u,v) = C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y) \times \cos(\frac{u\pi(2x+1)}{2N}) \times \cos(\frac{v\pi(2y+1)}{2N}) \quad (2.10)$$

Avec :

$$C(u) = C(v) = \begin{cases} \sqrt{\frac{1}{N}} & si\ u = v = 0 \\ \sqrt{\frac{2}{N}} & sinon \end{cases} \quad (2.11)$$

Définition 8 ***La Transformée DCT inverse****[Khayam, 2003]*
La transformée DCT inverse est donnée par la formule :

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} C(u)C(v)F(u,v) \times \cos(\frac{u\pi(2x+1)}{2N}) \times \cos(\frac{v\pi(2x+1)}{2N}). \quad (2.12)$$

La DCT souvent calculée sur des blocs de taille 8×8 ou 64×64. Les coefficients de la transformée sont répartis sur trois bandes de fréquence : basses, moyennes et hautes fréquences, comme indiqué sur la Figure 2.10.

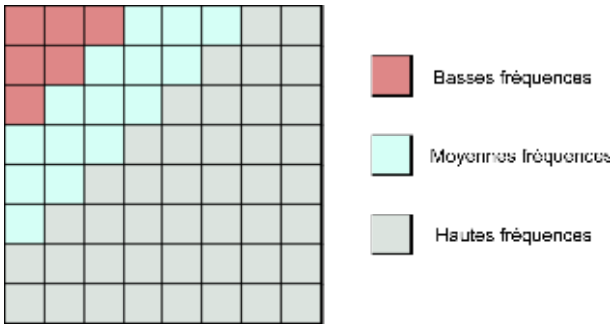


FIGURE 2.10: Répartition des coefficients d'un bloc DCT de taille 8×8 sur trois bandes de fréquence.

Plusieurs algorithmes de tatouage ont été proposés pour utiliser la DCT. Parmi les techniques basées sur la DCT les plus connues, nous citons ici la méthode proposée par Cox et al. [Cox et al., 1997]. Cette méthode est décrite par l'algorithme 2.2.

Algorithme 2.2 Tatouage basé sur la DCT [Cox et al., 1997]

Procédure d'insertion

Entrées :

— W : le watermark est une séquence PN de taille n : $w = \{w_1, w2, \ldots, w_n\}$.

— I_o : l'image originale.

Sortie :

— L'image tatouée I_w.

Etapes :

1. Application de la transformée DCT sur l'image originale I_o.
2. Sélection d'un ensemble C de coefficients les plus significatifs $C = \{c(1), c(2), ..., c(n)\}$.Le premier coefficient (DC) sera exclu du processus l'insertion.
3. Insertion de watermark dans les coefficients de la DCT par la formule :

$$c_w(i) = c(i) + \alpha \times w(i).$$

   Où α est un facteur scalaire qui détermine la force de tatouage $\alpha \in [0, 1]$
4. Application de la DCT inverse pour obtenir l'image tatouée I_w.

Procédure d'extraction

1. Application la transformé DCT sur l'image tatouée et éventuellement attaquée I'_w.
2. Extraction de watermark à partir des coefficients $c'_w(i)$ de la DCT de I'_w comme suit :

$$w'(i) = \frac{c'_w(i) - c(i)}{\alpha}.$$

Nous constatons que cette méthode et non aveugle car elle nécessite l'image originale pour extraire le watermark.

2.4.2.2 Techniques basées sur la DWT

La transformée en ondelettes discrètes (DWT) est aussi une approche de transformation simple et rapide qui transforme une image du domaine spatial au domaine fréquentiel. Elle est utilisée dans la compression JPEG 2000, et elle est devenu de plus en plus populaire. Cette transformée consiste à analyser le signal à l'aide d'une fonction bien localisée, de moyenne nulle, que nous appelons *ondelette*.

Comme les sinus et les cosinus dans la transformée de DCT, les ondelettes sont utilisées comme fonctions de base pour la représentation du signal et de l'image. Ces fonctions de base sont obtenues par dilatation et translation d'une ondelette mère (*mother wavelet*) $\psi(x)$ par des quantités s et τ, respectivement [Shih, 2007] :

$$\psi_{\tau,s}(x) = \{\psi(\frac{x-\tau}{s}), (\tau, s) \in R \times R^+\}. \tag{2.13}$$

Où τ est le paramétrer de translation et s est le paramètre d'échelle.

La translation et la dilatation permettent de localiser la transformée en ondelettes en temps et en fréquence. En outre, les fonctions de base d'ondelettes peuvent représenter des fonctions avec des discontinuités et des pointes d'une manière plus compacte que les sinus et cosinus.

Définition 9 ***La transformée en ondelettes continue*** *[Burrus et al., 1998, Meyer, 1995]*
La transformée en ondelette continue CWT d'une fonction $f(t)$ est définie par la formule suivante :

$$cwt_\psi(\tau, s) = \frac{1}{\sqrt{|s|}} \int f(t)\psi^*_{\tau,s}(t)\mathrm{d}t; \tag{2.14}$$

Avec : $\psi^*_{\tau,s}$ est le conjugué complexe de $\psi_{\tau,s}$

Définition 10 ***La transformée en ondelettes continue inverse*** *[Burrus et al., 1998, Meyer, 1995]*
La transformée en ondelette continue inverse iCWT est définie par la formule suivante :

$$x(t) = \frac{1}{C^2_\psi} \int_s \int_\tau cwt_\psi(\tau, s) \frac{1}{s^2} \psi_{\tau,s}(t)\mathrm{d}\tau\mathrm{d}s \tag{2.15}$$

Avec C^2_ψ est un constant dépend de l'ondelette utilisée.

Pour discrétiser la CWT, le cas le plus simple est l'échantillonnage uniforme du plan temps-fréquence. Cependant, l'échantillonnage pourrait être plus efficace en utilisant la règle de Nyquist :

$$N_2 = \frac{s_1}{s_2} N_1, \tag{2.16}$$

N_1 et N_2 dénotent le nombre d'échantillons sur l'échelle s_1 et s_2, respectivement, et $s_2 > s_1$.

Cette règle signifie que pour des échelles plus élevées (fréquences plus basses), le nombre d'échantillons peut être diminué. Le taux d'échantillonnage obtenu est le taux minimum qui permet de reconstruire le signal original à partir d'un ensemble discret d'échantillons.

Une transformée dyadique satisfait la règle de Nyquist en discrétisant le paramètre d'échelle en une série logarithmique, et le paramètre de temps est ensuite discrétisé par rapport aux paramètres d'échelle correspondants. Les équations suivantes fixent la translation et la dilatation à l'échelle dyadique avec des séries logarithmiques de base 2 pour $\psi_{k,j}$:

$$\tau = k2^j, s = 2^j. \tag{2.17}$$

Nous pouvons voir ces coefficients comme des filtres qui sont classés en deux types. Un ensemble, L, fonctionne comme un filtre passe-bas, et l'autre, H, comme un filtre passe-haut.

Ces deux types de coefficients sont appelés filtres miroir en quadrature (quadrature mirror filters) et sont utilisés dans des algorithmes pyramidaux. Pour un signal 2D, la transformée en ondelettes 2D peut être décomposée en utilisant la combinaison de transformées d'ondelettes 1D.

Définition 11 ***La transformée en ondelettes 2D***
La transformation 1D peut être appliquée individuellement à chacune des dimensions de l'image. En utilisant des filtres miroirs en quadrature, nous pouvons décomposer une image I de taille $n \times n$ en coefficients d'ondelettes, comme ci-dessous.
Les filtres L et H sont appliqués sur les lignes d'une image, divisant l'image en deux sous-images de dimensions $\frac{n}{2} \times n$ (la moitié des colonnes) chacune. Une de ces sous-images, L_r (où l'indice r désigne la ligne), contient les informations de passe-bas ; L'autre, H_r, contient l'information passe-haut. Ensuite, les filtres L et H sont appliqués aux colonnes des deux sous-images. Enfin, on obtient quatre sous-images de dimensions $\frac{n}{2} \times \frac{n}{2}$. Les sous images L_cL_r, H_cL_r, L_cH_r et H_cH_r (où c dénote les colonnes) contiennent respectivement les fréquences bas-bas, haut-bas, bas-haut et haut-haut (Figure 2.11).

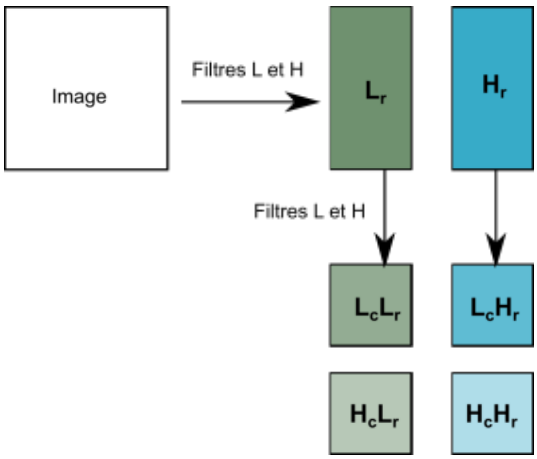


FIGURE 2.11: Décomposition en ondelette 2D d'une image.

FIGURE 2.12: Décomposition DWT en un seul niveau de l'image *Lala Fatma Nessoumer*.

Les mêmes procédures sont appliquées de façon itérative à la sous-image contenant les informations les plus basses jusqu'un certain niveau. La Figure 2.12 montre l'image de *Lala Fatma Nessoumer* décomposée en un seul niveau. Chacune des sous-images résultantes est appelée sous-bande.

Nous présentons par la suite une technique de tatouage basée sur l'insertion dans les coefficients DWT. Cette approche est décrite par l'algorithme 2.3 et la Figure 2.13.

Algorithme 2.3 Tatouage basé sur la DWT [Chae and Manjunath, 1997].

1. Décomposition de l'image originale et le watermark en utilisant la transformée DWT.
2. Pour chaque coefficient X de la transformée du watermark faire :
   - Représentation de coefficient X par A (les bits les plus significatifs), B (les bits moyens significatifs) et C (les bits moins significatifs).
   - Construction des nouveaux coefficients A', B' et C' en prenant compte seulement les bits les plus significatifs.
   - Construction d'un bloc de taille 2×2 comme suit : $\begin{vmatrix} A' & B' \\ C' & A' \end{vmatrix}$
3. Insertion de watermark dans l'image hôte : $\mathcal{CF}_{I_w} = \alpha \times \mathcal{CF}_{I_o} + \mathcal{CF}_W$
   Où $\mathcal{CF}_{I_o}$ sont les coefficients de l'image originale, $\mathcal{CF}_W$ sont les coefficients du watermark et α est la force de tatouage.
4. Application de la DWT inverse sur les coefficients modifiés $\mathcal{CF}_{I_w}$ pour obtenir l'image tatouée.

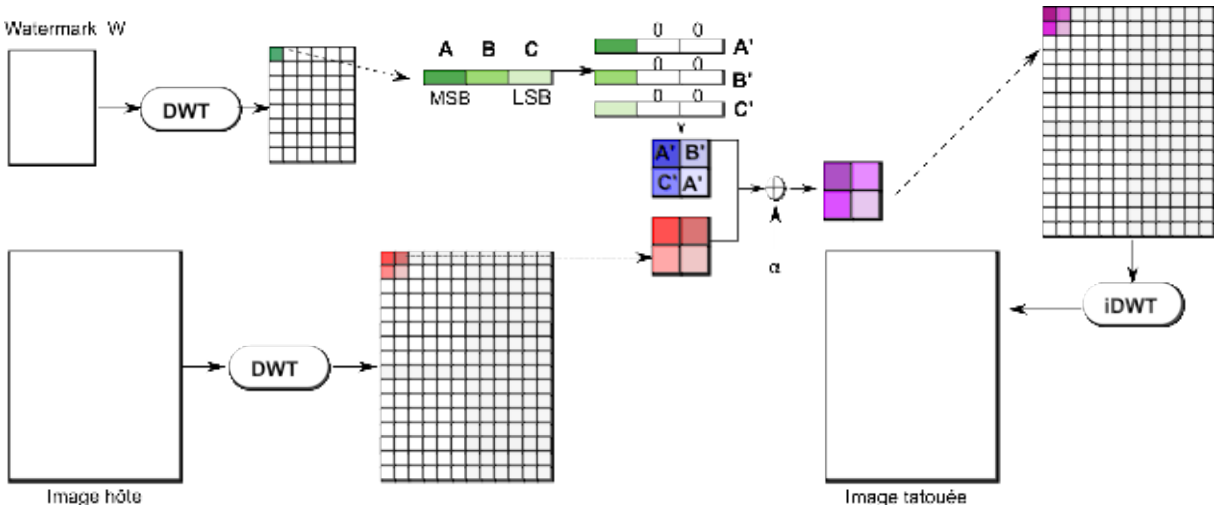


FIGURE 2.13: Approche de tatouage basée sur la DWT [Chae and Manjunath, 1997].

2.4.2.3 Lifting Wavelet Transform (LWT)

La transformée en ondelette conventionnelle appelée aussi première génération d'ondelettes (FGW) a d'excellentes performances dues à l'analyse multi-résolution d'une part et présente des inconvénients d'autre part :

- Le temps de calcul élevé provoqué par le calcul de la convolution.
- Augmenter les besoins en mémoire dues à la manipulation de nombres flottants.
- Non recommander pour le schéma de tatouage d'authentification réversible en raison de la perte de reconstruction lors de l'arrondissement des valeurs flottantes en entiers [Kamstra and Heijmans, 2005].

Par conséquent, une ondelette de seconde génération (SGW) est développée pour résoudre ces problèmes et augmenter l'efficacité. La transformée LWT est une sorte de SGW qui a des propriétés distinctives par rapport aux transformées de la première génération. Contrairement

aux ondelettes traditionnelles, la LWT effectue des valeurs entières et n'a pas besoin d'un tableau temporaire dans le calcul, ce qui réduit le temps de calcul et les besoins en mémoire.

Les principales étapes de LWT sont les suivantes [Sweldens, 1996] :

- Diviser (Lazy transform) : les données sont décomposées en composants pairs et impairs.
- Prédire (dual lifting) : les composants impairs sont prédits à partir des composants pairs.
- Mettre à jour (primal lifting) : les composants pairs sont remplacés par des valeurs moyennes.

L'ondelette est simplement reconstruite en miroir de la transformation vers l'avant. Le principe de LWT et son inverse sont illustrés sur la Figure 2.14.

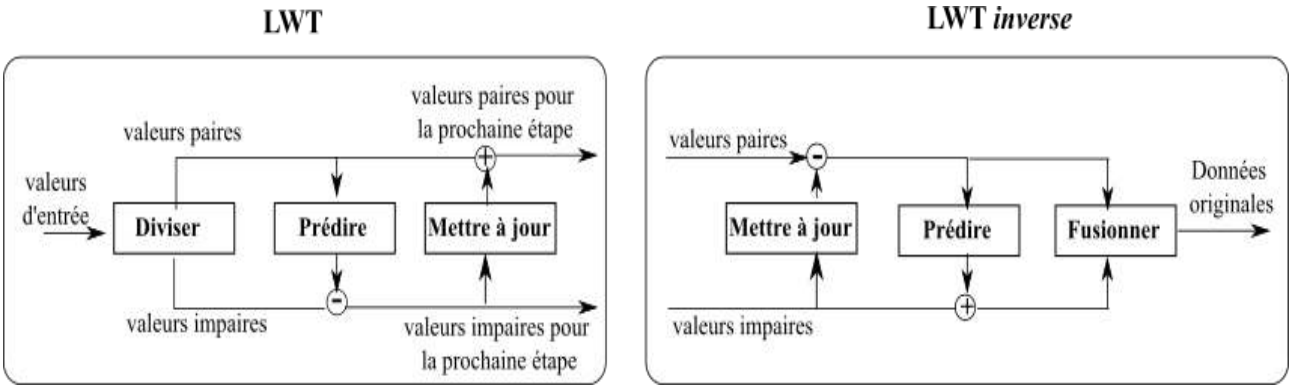


FIGURE 2.14: La transformée LWT et son inverse [Devi et al., 2009].

2.4.2.4 Techniques basées sur la SVD

La SVD s'avère être non seulement un outil puissant d'analyse de l'efficacité des méthodes numériques d'inversion mais permet également d'introduire la notion de pseudo-inverse. Cette notion sera en particulier utilisée pour les problèmes de reconstruction avec des données incomplètes ou encore de détermination dans le cas de problèmes sur-déterminés (comme par exemple l'interpolation polynomiale en deux dimensions et plus).

Définition 12 ***La décomposition en valeurs singulières*** *[Liu and Tan, 2002]*
Toute matrice A, de taille $m \times n$, peut se décomposer en produit de trois matrices de la manière suivante :

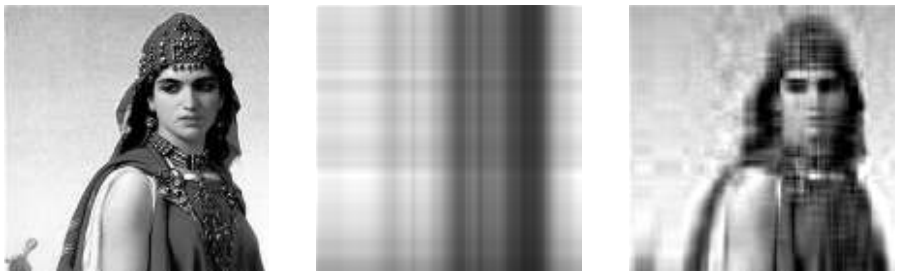
$$A = USV^T = \sum_{i=1}^{r} \lambda_i U_i V_i^T. \tag{2.18}$$

Où U et V sont des matrices orthogonales, respectivement de dimensions $m \times m$ et $n \times n$. On a : $U^TU = I$ et $V^TV = I$.
S est une matrice diagonale de taille $n \times n$ composée des valeurs singulières λ_i, dans l'ordre décroissant, sur la diagonale et T est l'opérateur de transposition. On peut aussi écrire : $S = diag(\lambda_1, \lambda_2, ..., \lambda_r)$, telles que $\lambda_1 \geq \lambda_2 \geq .... \geq \lambda_r > 0$ où $r = min(m, n)$ le rang de la matrice A est égal au nombre de valeurs singulières (SVs) non nulles que possède la matrice A.

La SVD est très utilisée dans le domaine du tatouage numérique pour deux raisons :

— les valeurs singulières (SVs) sont très stables, i.e., lorsque de petites informations (perturbations) sont ajoutées à l'image, leurs SVs ne changent pas significativement.
— la SVD range le maximum d'énergie de l'image dans un minimum de valeurs singulières, la compression est obtenue donc intuitivement en forçant les valeurs singulières les plus faibles à zéro.

La Figure 2.15 illustre le résultat de l'application de la SVD sur l'image *Lala Fatma Nessoumer*. La Figure (b) présente la première image singulière et de sa troncature de rang 10 (i.e. on reconstruit l'image avec les 10 premières valeurs singulières (c)). Nous remarquons que la première image singulière est plutôt basse fréquence alors que la dixième est haute fréquence.



(a) (b) (c)

FIGURE 2.15: Image originale (a), sa première image singulière (b), et sa troncature de rang 10 (c).

Nous expliquons dans cette section un algorithme de tatouage basé sur la SVD proposé par R.Liu et T. Tan [Liu and Tan, 2002]. La Figure 2.16 illustre le schéma de cet algorithme.

Algorithme 2.4 Tatouage basé sur la SVD [Liu and Tan, 2002].

Procédure d'insertion

1. Décomposition de l'image hôte I_o en valeurs singulières : $I_o = U \times S \times V^T$;
2. Insertion de watermark w à la matrice S comme suit : $D = S + \alpha \times w$;
3. Décomposition de D en valeurs singulières : $D = U_w \times S_w \times V_w$;
4. L'image tatouée I_w est obtenue en utilisant les SVs modifiées (S_w) de l'image originale : $I_w = U \times S_w \times V^T$.

Procédure d'extraction

1. Décomposition de l'image tatouée et éventuellement attaquée I'_w en valeurs singulières : $I'_w = U' \times S' \times V'^T$;
2. Le calcul de la matrice D' qui contient le watermark en utilisant U_w et V_w : $D' = U_w \times S' \times V_w^T$.
3. Le watermark w' est obtenu en utilisant S : $w' = \frac{D'-S}{\alpha}$.

Nous remarquons que cet algorithme est non aveugle car il utilise les matrices originales S, U_w et V_w.

2.4.3 Tatouage fondé sur le contenu (Deuxième génération)

En général, les méthodes de tatouage numérique peuvent être considérées comme des systèmes de communication numérique. La plupart des méthodes utilisent une sorte de modulation et de démodulation. Habituellement, le watermark est pondéré, pour diminuer sa perception lorsqu'il est inséré dans l'image originale. Les schémas de la première génération (FGW) ne font pas explicitement usage des caractéristiques perceptuelles importantes dans les données.

Les techniques de la deuxième génération (SGW) ont été développées afin d'augmenter la robustesse et l'invisibilité et de surmonter les faiblesses des techniques de la FGW.

Cette classe de tatouage implique la notion de caractéristiques perceptuellement significatives dans les données originales. Les caractéristiques peuvent être abstraites ou peuvent être des

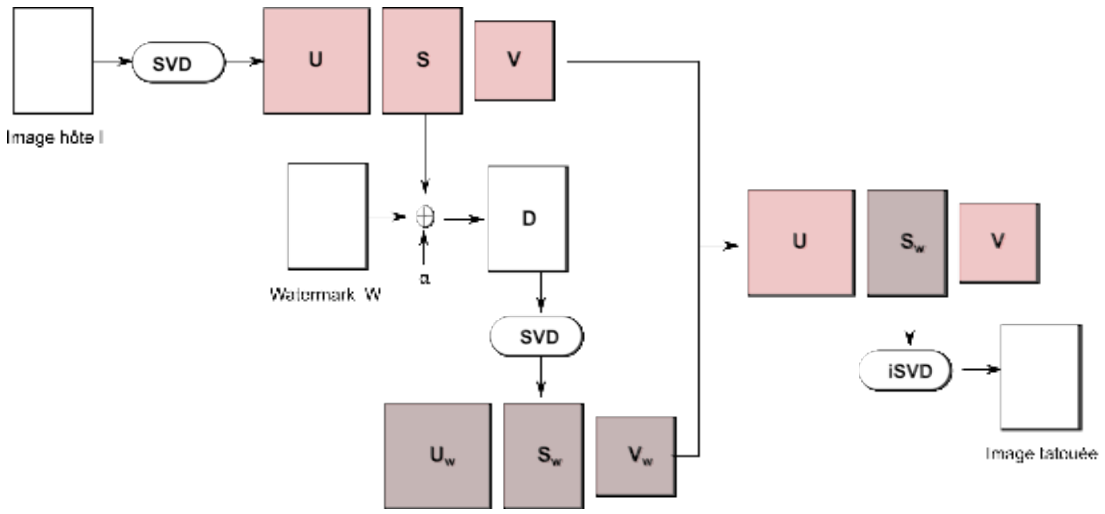


FIGURE 2.16: Approche de tatouage basée sur la SVD proposée par R.Liu et T. Tan [Liu and Tan, 2002].

caractéristiques sémantiquement significatives. Pour les images, les éléments peuvent être des bordures, des coins, des zones texturées, points ou objets d'intérêt. Certaines caractéristiques ne conviennent pas pour le tatouage. Par exemple, la zone d'une région uniforme dans une image n'est pas une bonne caractéristique car elle changera si l'image est mise à l'échelle. Les caractéristiques adaptées au tatouage doivent avoir les propriétés suivantes [Kutter et al., 1999] :

— Invariance au bruit (compression avec perte, bruit additif ou multiplicatif, ...).
— Covariance aux transformations géométriques (rotation, changement de formats, sous-échantillonnage, ...).
— Localisation (par exemple le cropping ne doit pas modifier les points d'intérêt restants).

La première propriété assure que seules les caractéristiques significatives sont choisies. Ces caractéristiques ne sont pas préférées par les attaques car la valeur commerciale de données originales sera perdue par la modification de ces caractéristiques. La deuxième propriété désigne le comportement des caractéristiques utilisées si les données originales sont géométriquement déformées. Des modifications géométriques modérées ne devraient pas détruire ou modifier les caractéristiques utilisées. La dernière propriété implique que l'utilisation de telles caractéristiques rend le watermark robuste contre le cropping.

Les méthodes de la deuxième génération apportent des avantages supplémentaires en termes de détection et de récupération du watermark après des attaques géométriques par rapport aux méthodes de la première génération. Ceci est réalisé en exploitant les propriétés des régions ou des objets de l'image. En outre, les méthodes de la deuxième génération peuvent être conçues de manière à obtenir une robustesse sélective pour différentes classes d'attaques.

Le modèle général d'une technique de tatouage de deuxième génération est décrit par la Figure 2.17.

Ce modèle est composé de trois phases : l'extraction des caractéristiques, insertion du watermark et extraction du watermark.

Pour les techniques de tatouage fondées sur le contenu, avant d'insérer le watermark, la première phase consiste à extraire les caractéristiques pertinentes.

Les caractéristiques extraites peuvent être utilisées de deux façons. Dans la première façon les caractéristiques servent comme phase auxiliaire qui aide le processus de tatouage. Par exemple, les caractéristiques peuvent être utilisées comme emplacements de référence et

orientation pour un schéma de tatouage. Le but d'un tel schéma est essentiellement d'augmenter la robustesse contre des altérations géométriques, bien que d'autres objectifs puissent également être envisagés.

La deuxième façon consiste à utiliser les caractéristiques directement dans le processus d'insertion. Autrement dit, les caractéristiques extraites sont directement modifiées pour incorporer les informations de tatouage.

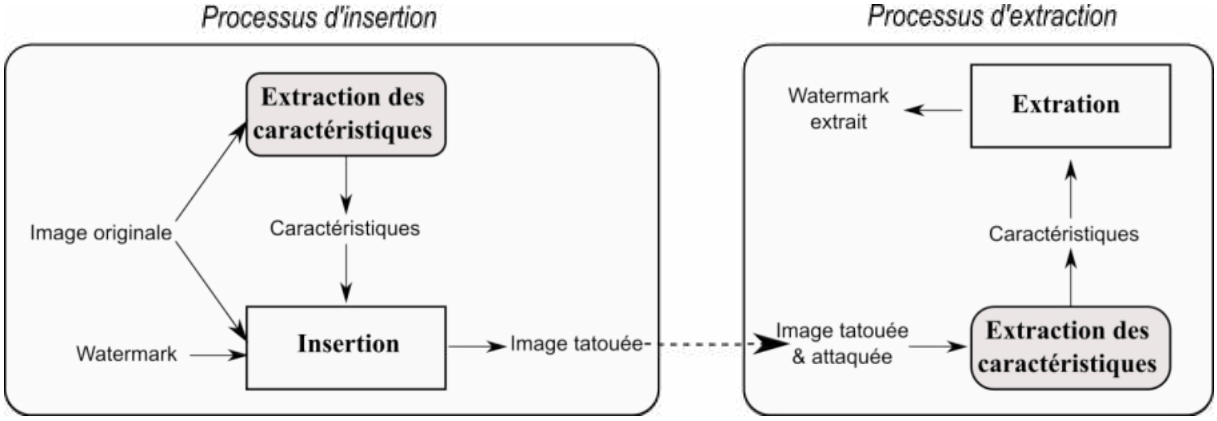


FIGURE 2.17: Modèle générale du tatouage fondé sur le contenu.

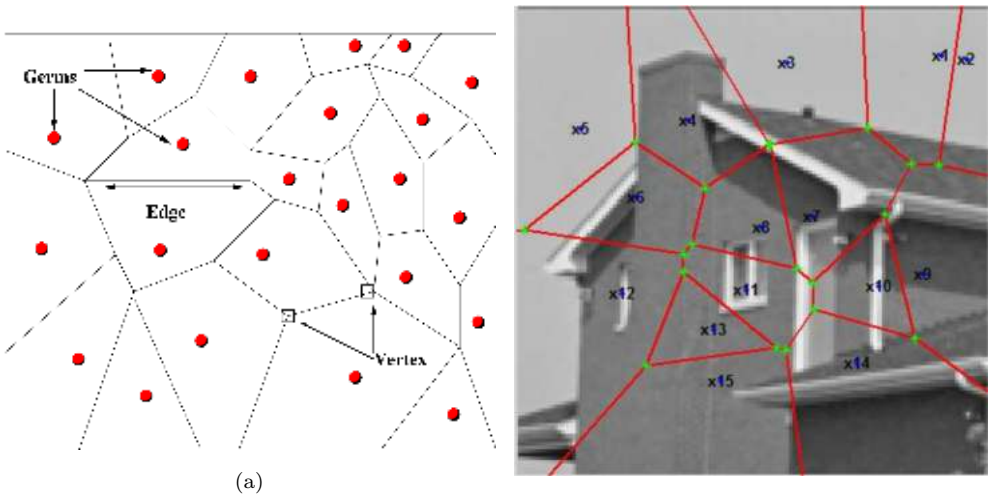
Le premier papier dans la catégorie des techniques de SGW est publié par Kutter et al. (1999) [Kutter et al., 1999]. Les auteurs proposent d'utiliser les *points d'intérêt* FPs comme caractéristiques pertinentes et **le diagramme de Voronoi** pour définir la région d'intérêt (ROI) à tatouer. Le processus d'extraction des caractéristiques est basé sur une décomposition de l'image à l'aide d'une ondelettes mère appelée *Mexican Hat*.

2.4.3.1 Diagramme de Voronoi

Le Diagramme de Voronoi est définie comme une partition du plan en polygones ou régions selon le principe du plus proche voisin.

Étant donné un ensemble de points $P = \{p_1, p_2, \ldots, p_n\}$. La région de Voronoi pour un point p_i est définie comme l'ensemble de tous les points plus proches de p_i que de tous les autres points. Les points p_i sont appelées *générateurs de Voronoi* (*germs*). Les bordures communes à deux régions de Voronoï s'appelle *Bordures de Voronoi* (*edge*). Les sommets où se rencontrent trois bordures de Voronoï ou plus sont nommés *Sommets de Voronoi* (*vertex*). Nous disons qu'un générateur de Voronoï p_i est adjacent à p_j quand leurs régions de Voronoi partagent une bordure commune [Wang et al., 201].

La Figure 2.18 illustre les concepts de la décomposition de l'image *House* utilisant le DV.



(a) (b)

FIGURE 2.18: (a) Concepts de VD. (b) Image *House* décomposée en utilisant le DV.

2.5 Conclusion

Dans ce chapitre, nous avons présenté les deux techniques de protection des données numériques : la cryptographie et la stéganographie. Nous nous sommes intéressés aux terminologies et notions liées aux tatouage numérique qui est dérivé de la stéganographie. Nous avons présenté une classification des techniques du tatouage selon différents critères : le type de l'algorithme d'insertion, les informations nécessaires à la détection et la clé utilisée. Nous avons aussi jeté la lumière sur les trois différents techniques de tatouage : ceux travaillant dans le domaine spatial, ceux travaillant dans le domaine fréquentiel et ceux fondés sur le contenu. Les différents concepts et terminologies présentés dans ce chapitre seront utiles pour les chapitres suivants.

Chapitre 3

Tatouage numérique appliqué à l'imagerie médicale

Sommaire

3.1 Introduction

Durant ces dernières années, le développement rapide des technologies d'Internet et des multimédia a facilite la reproduction d'information numérique. Les progrès de ces technologies ont permis de créer, de reproduire, de transmettre et de distribuer du contenu numérique de manière facile et sans effort. Cependant, la protection et l'application des droits de propriété intellectuelle pour les médias numériques est devenue une question cruciale.

Au cours de ces dernières années, le tatouage numérique est apparu comme une solution brillante pour la protection du contenu numérique. Parmi de nombreuses applications, le service de santé électronique (e-health) assure et transmet des transcriptions médicales via internet.

La télémédecine est l'utilisation des technologies de l'information et de la communication a permet de fournir des systèmes de santé modernes où les patients et les participants sont séparés par une distance géographique. Les systèmes modernes de santé intégrés tels que le Système d'information sur l'hôpital HIS, Archivage d'image et le système de communication PACS fournissent un accès facile, une manipulation et une distribution efficace des données médicales [Priya and Sadasivam, 2014].

Les images médicales nécessitent une protection stricte en raison de son importance dans le diagnostic clinique, le traitement, l'éducation et la recherche. De nombreux hôpitaux dispersés géographiquement partagent des images médicales pour le diagnostic électronique, traitement électronique, etc. De plus, les HIS et PACS génèrent un énorme volume de données cliniques comme les données démographiques, les images et les rapports. Ces énormes données acquises devraient être stockées, traitées et gérées, ce qui soulève des problèmes de sécurité comme la confidentialité, l'intégrité et l'authenticité.

Le problème de l'authenticité et l'intégrité des images médicales est abordé en 1995 par Wong et al. [Wong et al., 1995]. Mais seulement après 1999, la recherche sur la sécurité des images médicales a attiré l'attention des chercheurs.

L'objectif de ce chapitre est d'introduire la protection des images médicales par le tatouage numérique.

3.2 Exigences de la sécurité des images médicales

Récemment, la réalisation du diagnostic médical correct devient une décision très difficile en raison du développement rapide des maladies qui nécessitent la coopération de plusieurs organisations médicales. Les progrès importants dans le secteur de la santé introduisent divers moyens d'imagerie médicale en radiologie, des HIS et systèmes de gestion de l'information dans les hôpitaux. Plusieurs techniques d'imagerie médicale sont utilisées dans les décisions diagnostiques telles que : IRM, la tomodensitométrie, l'échographie et les radiographies. En outre, la disponibilité de la connectivité Internet à large bande passante peu coûteuse et la croissance rapide des technologies de l'information et de la communication ont donné lieu à de grandes opportunités pour la création, l'accès, la gestion et la distribution de contenu numérique par des utilisateurs habituelles. Cela conduit à l'émergence de services de santé en ligne qui introduisent de nouvelles pratiques pour les professions ainsi que pour les patients en permettant l'accès à distance, la transmission et l'interprétation des images médicales à des fins de diagnostic. En outre, la technologie de la télémédecine a offert de nombreuses applications tels que le diagnostic à distance, la consultation à distance, la surveillance à distance et le fonctionnement à distance. Ces progrès considérables dans le domaine de la communication et de la technologie de l'information ainsi que de la télémédecine s'accompagnent d'une foule de

problèmes. Le problème principal est que le contenu numérique peut être copié, manipulé et redistribué facilement à faible coût et sans perte de fidélité. L'échange de données médicales sur les canaux ouverts afin d'obtenir un diagnostic médical correct les expose à de nombreuses menaces. De plus, les images médicales peuvent passer par différents systèmes de traitement de l'information sur les réseaux et, par conséquent, les images peuvent être menacées tout au long de leur vie de différentes façons.

La sécurité de l'information médicale nécessite trois caractéristiques [Coatrieux et al., 2006a] :

1. *La confidentialité* : garantit que seuls les utilisateurs ont accès à l'information car certains patients ne souhaitent pas exposer leurs informations au public.
2. *La fiabilité* : qui comprend :
   (a) *L'intégrité* : les informations n'ont pas été modifiées par des personnes non autorisées.
   (b) *L'authenticité :* une preuve que l'information appartient au patient correct et émis de la bonne source.
3. *La disponibilité* : signifie l'accès à l'information pour les personnes autorisées.

Afin de garantir la confidentialité des informations du patient, la norme a été développé en 1983 par une collaboration entre ACR et NEMA afin de fournir un guide facultatif pour la production d'images médicales.

DICOM représente des années d'efforts pour créer le standard le plus universel et le plus fondamental dans l'imagerie médicale numérique. Il fournit tous les outils nécessaires pour la représentation et le diagnostic précis des données d'imagerie médicale. DICOM n'est pas seulement un format d'image ou de fichier. Il s'agit d'un protocole de transfert, de stockage et d'affichage entièrement intégré, conçu pour couvrir tous les aspects fonctionnels de la médecine contemporaine (c'est pourquoi beaucoup considèrent le DICOM comme un ensemble de normes plutôt qu'un seul standard) [Pianykh, 2009].

Le fichier DICOM est décomposé de deux parties : l'en-tête et le corps. L'en-tête du DICOM contient l'information du patient, les détails du médecin et les informations sur les hôpitaux, où ils sont connus sous le nom de définition de l'objet d'information (IOD). Le corps du DICOM comprend les informations importantes sur le cas du patient. Il est décomposé généralement en deux régions : la ROI et la RONI.

Plusieurs techniques de sécurité existantes sont actuellement utilisées, mais l'application de ces techniques dans la protection des données médicales est caractérisée par certaines limitations. Les techniques de sécurité conventionnelles et leurs limites sont résumées dans le Tableau 3.1.

3.3 Protection par tatouage numérique

Les informations médicales sont des informations très sensibles, de sorte qu'il faut non seulement une protection avec intégrité et une grande confidentialité, mais aussi une gestion appropriée par le biais de différents services de santé.

Afin d'éviter toutes manipulations illégales des informations privées du patient et des images médicales, le tatouage peut être utilisé pour cacher l'EPR à l'intérieur de l'image médicale. Cela empêche les attaquants de changer facilement l'image médicale ou l'information du patient.

Système de sécurité	Limitation
Cryptographie	Outil efficace pour le stockage et la transmission, mais après réception et décryptage, les données ne sont plus sécurisées.
En-tête du fichier DICOM	Le fichier DICOM contient une image médicale et l'information du patient est stockée dans l'en-tête de fichier. Cette séparation peut entraîner une inadéquation qui entraîne une erreur de diagnostic. L'en-tête peut être perdue en raison de toute opération de traitement du signal. L'intrus peut briser la confidentialité du patient en accédant à l'en-tête du fichier.
Pare-feu	Un outil d'isolement entre l'Intranet et l'Internet, ne protège que l'information jusqu'au point des réseaux internes.
Fonction d'hachage	Prend un bloc arbitraire de données et renvoie une chaîne de bits de taille fixe (valeur de hachage), de sorte qu'une modification accidentelle ou intentionnelle des données modifie la valeur de hachage. Ce système ne peut pas indiquer l'endroit où les images ont été falsifiées. C'est un peu sensible à l'entrée.

TABLE 3.1: Limitations des systèmes de sécurité conventionnelles [Yassin, 2015].

3.3.1 Importance du TIM

Le TIM dans le domaine médical comporte de nombreuses applications pratiques, y compris le télédiagnostic, les téléconférences et l'apprentissage à distance. L'échange d'images médicales entre cliniciens, spécialistes et radiologues fournit une plateforme pour discuter et consulter des mesures diagnostiques et thérapeutiques. Dans ce cas, le EPR et les images médicales sont envoyés séparément à la destination. L'utilisation de techniques de tatouage pour l'implantation de l'EPR dans les images médicales garantiront non seulement la confidentialité et la sécurité des données envoyées, mais aussi l'intégrité des images médicales. En outre, l'authentification des watermarks et les méthodes de détection d'altération (Tamped detection) peuvent être utilisées respectivement pour identifier la source des images médicales et localiser les régions altérées [Mousavi et al., 2014, Navas and Sasikumar, 2007].

3.3.2 Avantages du TIM

Le tatouage numérique présente de nombreuses caractéristiques qui les rendent supérieures aux systèmes traditionnels de la sécurité dans les domaines de la protection du droit d'auteur et de la télé-médecine.

Le tatouage numérique appliqué à l'imagerie médicale traite principalement deux problèmes. L'un consiste à aborder les contraintes de sécurité (l'authentification, le contrôle de l'intégrité, la confidentialité et la non répudiation) et l'autre pour aborder les considérations du système (absence de détachement, réduction des exigences de stockage et de transmission, etc.).

Contraintes de sécurité

La propriété fondamentale et la plus attrayante du tatouage est la capacité de dissimulation de données [Fallahpour et al., 2009]. La confidentialité peut être maintenue en cachant les données privées dans les images.

Le fait de conserver les informations médicales nécessaires dans les images médicales peut fournir une meilleure sécurité contre les manipulations malveillantes, en supposant que les images médicales ne seraient pas de l'intérêt des personnes sans l'information du patient [Ulutas et al., 2011].

Dans le cas d'une falsification intentionnelle ou involontaire, les informations altérées peuvent être détectées et récupérée en utilisant un système de tatouage approprié [Zain and Fauzi, 2006, Faoziyah et al., 2013].

Selon Coatrieux et al. [Coatrieux et al., 2000], les objectifs des systèmes de tatouage numérique appliqués pour l'imagerie médicale sont : la dissimulation des données, le contrôle de l'intégrité et l'authentification, qui peuvent fournir la sécurité requise des images médicales. Par exemple, l'objectif de la dissimulation des données permet d'insérer des méta-données (EPR) et d'autres informations afin que l'image soit plus utile ou plus facile à utiliser [Chao et al., 2002], [Navas et al., 2008]. L'objectif du contrôle de l'intégrité est de vérifier que l'image n'a pas été modifiée d'une manière non autorisée [Coatrieux et al., 2013, Pan et al., 2010]. Le tatouage numérique permet une association permanente du contenu de l'image avec des preuves de sa fiabilité en modifiant certaines valeurs de pixels d'image, indépendamment du format du fichier image [Memon and Gilani, 2011]. En outre, l'authentification trace l'origine d'une image.

Non répudiation

Le tatouage est également prometteur pour soutenir la non répudiation dans diverses applications multimédia [Zhou et al., 2002]. Par conséquent, l'utilisation d'un système de tatouage à base de clé peut faciliter la non répudiation de la teléradiologie, de sorte que les deux parties pourraient être en sécurité lorsque la clé utilisée par l'hôpital pourrait être leur logos ou leurs signatures numériques [Nyeem et al., 2013].

Absence de détachement (Avoiding detachment)

La propriété de dissimulation du tatouage numérique facilite davantage l'annotation des informations nécessaires pour éviter tout problème de transmission séparée ou de détachement. L'EPR ou l'information du patient est vitale pour le processus de diagnostic et de traitement. Si l'EPR et l'image sont transmises séparément, le détachement peut se produire et cette séparation peut entraîner une inadéquation qui entraîne une erreur de diagnostic. Afin d'éviter cette situation, intégrer l'EPR dans l'image correspondante à l'aide du tatouage est une bonne solution [Chao et al., 2002, Zhang et al., 2006, Münch et al., 2004].

Réduction des exigences de stockage et de transmission

L'espace de stockage et les exigences de bande passante sont un facteur décisif important pour l'économie financière des petits hôpitaux. L'espace de stockage peut être réduit dans une certaine mesure dans HIS en intégrant l'EPR dans l'image [Navas et al., 2008]

D'autre part, une grande quantité de bande passante est requise pour la transmission des données d'image en télé-radiologie. L'exigence supplémentaire de bande passante pour la transmission des méta-données peut être évitée si les données sont cachées dans l'image elle-même [Das and Kundu, 2012].

3.3.3 Exigences de conception des approches de TIM

Les exigences des systèmes conventionnels de tatouage sont la capacité, l'imperceptibilité et la robustesse (voir Chapitre 2). Pour les images médicales, en plus de ces exigences, la ROI de l'image doit être particulièrement maintenue intacte. C'est un défi supplémentaire pour les chercheurs dans ce domaine [Navas and Sasikumar, 2007]. Les exigences de conception des approches de TIM sont principalement définies en termes de sécurité, confidentialité, fidélité et complexité de calcul. Par conséquent, les exigences en matière de sécurité et de confidentialité. Ils ont pour objectif la dissimulation des données, la vérification de l'intégrité et d'authenticité. Les exigences de fidélité garantissent que les images médicales tatouées sont utilisables pour le diagnostic et d'autres utilisations cliniques. En outre, les exigences de calcul permettent de déterminer le coût et la faisabilité de la mise en œuvre pratique d'un système de tatouage.

Fidélité

En général, la fidélité d'un système de tatouage fait référence à la similitude perceptive entre l'image originale et tatouée [Cox et al., 2002]. L'insertion du watermark dans une image hôte présente des dégradations visuelles. Cependant, le processus d'insertion ne doit pas affecter les caractéristiques essentielles de l'image originale. Cette propriété s'appelle aussi imperceptibilité ou transparence perceptuelle. Un système de tatouage devrait avoir un niveau d'imperceptibilité raisonnable afin que l'image tatouée ne soit pas inutile et que le watermark ne soit pas visible à l'œil humain [Singh et al., 2016]. Dans le cas d'imagerie médicale, le maintien d'une haute similitude perceptive est essentiel pour éviter tout risque de diagnostic erroné.

Robustesse

La robustesse, une propriété importante pour la phase de détection du watermark. Elle est définie comme le degré de résistance d'un système de tatouage à des modifications du signal hôte en raison des opérations du traitement de signal ou des opérations spécialement conçues pour rendre le watermark indétectable [Cox et al., 2002]. Sur la base de cette propriété, les systèmes de tatouage peuvent être robustes, fragiles et semi-fragiles.

Dans un tatouage robuste, un watermark contient habituellement des informations concernant le propriétaire afin de valider à qui appartient l'image (par exemple, le PER.) [Shih and Wu, 2005]. Ainsi, ces schémas de tatouage sont utilisés à des fins d'authentification de contenu dans diverses applications d'images numériques (par exemple, protection des droits d'auteur).

Les techniques semi-fragiles et fragiles sont utilisés pour transporter de nombreuses informations sur lui-même, les méta-données de son propriétaire, sa distribution, etc., et sont donc utilisées pour la dissimulation de PER [Chao et al., 2002] et le contrôle de l'intégrité [Lin et al., 2005, Pan et al., 2009, Coatrieux et al., 2013].

Capacité d'insertion

La capacité d'insertion, généralement mesurée par le nombre de bits inséré dans l'image hôte, signifie le nombre de bits qui peuvent être modifiés ou intégrés de manière appropriée dans une image. L'augmentation de la capacité d'insertion dans la conception des approches de contrôle d'intégrité et d'annotation est un problème fondamental, qui sont généralement de nature fragile ou semi-fragile [Al-Qershi and Khoo, 2011b]. L'obtention d'une capacité d'intégration élevée introduit souvent plus de distorsions sur une image tatouée et, par conséquent, il est souvent difficile de préserver une imperceptibilité élevée. Un tatouage robuste pour la protection

des droits d'auteur nécessite une capacité plus faible que celle requise pour un tatouage fragile ou semi-fragile [Zhang and Zhang, 2004].

Une capacité d'insertion élevée est également requise dans les schémas de tatouage fragiles ou semi-fragiles pour la détection et la récupération de falsification.

Sécurité

Selon le principe de Kerchoff's [Kerckhoffs, 1883], la sécurité d'un système de cryptage ne doit pas dépendre de la confidentialité de la mise en œuvre du système. Il doit être impossible pour un attaquant d'extraire, détecter, modifier, intégrer ou supprimer le watermark sans connaissances complètes sur l'implémentation du système et les clés secrètes [Menezes et al., 1996].

La sécurité d'un schéma de tatouage se réfère à sa capacité à résister aux attaques hostiles. Une attaque hostile est un processus spécifiquement destiné à déjouer le but du watermark. Les attaques sont divisés en trois grandes catégories [Cox et al., 2007] :

— Suppression non autorisée ;

— Insertion non autorisée ;

— Détection non autorisée.

La suppression et l'insertion non autorisées sont appelées des attaques *actives* parce que ces attaques modifient le document tatoué. Par contre, la détection non autorisée ne modifie pas le document tatoué et est donc appelée une attaque *passive*.

Détection aveugle

La tatouage aveugle désigne la capacité d'une fonction (par exemple, la génération du watermark et la détection) à fonctionner sans aucune version originale d'entrée (par exemple, image ou watermark, etc.). La génération non aveugle du watermark est importante alors qu'un watermark dépend d'une image originale est requis. Un watermark généré à partir d'une image originale, l'image est utile pour traiter les attaques d'ambiguïté (par exemple, attaques de copie) [Nyeem et al., 2013]. Par contre, un watermark ne dépend pas de l'image originale, il peut être facilement copié sur une autre image ou forgé pour produire une image tatouée invalide. Le caractère aveugle est très primordial pour la phase de détection, où la disponibilité de l'image d'origine ou du watermark sur le détecteur peut déjouer les objectifs de tatouage [Golpira and Danyali, 2009].

Une détection non aveugle est parfois utilisée dans le développement de systèmes de tatouage de récupération de manipulation, où la récupération de régions altérées est souvent difficile à obtenir à partir de l'image tatouée elle-même.

Réversibilité

Un système de réversible a la propriété que la fonction de détection est l'inverse de la fonction d'insertion. Le tatouage réversible (ou parfois appelé *inversible* ou *sans perte*) s'intéresse particulièrement aux applications d'images numériques où aucune distorsion de l'image originale n'est autorisée. Par conséquent, une image originale doit être restaurée à partir des images tatouées respectives par le détecteur.

La réversibilité n'intervient généralement pas pour la détection non-aveugle, car la détection nécessite l'image originale, bien que le développement d'un détecteur aveugle ou d'un tatouage

réversible soit plus difficile, en particulier lorsque l'on souhaite une capacité d'insertion élevée. Le développement d'un système de tatouage réversible a reçu beaucoup d'attention pour les applications d'images médicales afin d'éviter tout diagnostic erroné [Golpira and Danyali, 2009, Coatrieux et al., 2009].

3.4 Classification des techniques du TIM

Les techniques de tatouage d'images médicales peuvent être regroupées selon deux critères : la méthode d'insertion et le domaine d'application.

3.4.1 Classification selon la méthode d'insertion

Selon la méthode d'insertion du watermark, Coatrieux et al. [Coatrieux et al., 2006a] regroupent les techniques de tatouage des images médicales en trois catégories :

3.4.1.1 Techniques basées sur l'insertion dans la RONI

Cette première classe regroupe des méthodes qui intègrent le watermark dans une région de non-intérêt (RONI) afin de ne pas compromettre la capacité de diagnostic [Wakatani, 2002].

De nombreuses expériences suggèrent que la RONI correspond en général aux parties noires de l'image, mais parfois, elle peut inclure des portions de niveau de gris peu intéressantes [Shih and Wu, 2005], laissant ainsi un espace pour insérer le watermark dans l'image.

Comme il n'y a pas d'interférence avec le contenu pertinent de l'image, l'invisibilité est moins stricte, par conséquent, nous pouvons revenir à des méthodes à plus grande capacité et robustesse. Même si aucune interférence ne se produit avec les données potentiellement utiles pour le diagnostic, il a été souligné que changer le fond noir avec un bruit du sel et poivre comme un modèle bruyant peut gêner le médecin. Par conséquent, l'amplitude du signal du watermark à insérer doit être correctement sélectionnée.

Les approches d'insertion dans la RONI laisseront intactes les informations de diagnostic, mais elles ne peuvent être appliquées que si un RONI existe. En outre, la capacité d'insertion dépend de la taille de la zone RONI.

3.4.1.2 Techniques réversibles

Une fois que le contenu intégré est lu, le watermark peut être retiré de l'image afin de récupérer le contenue original [Macq and Dewey, 1999]. Un grand effort a été récemment fourni dans le développement de ce type de méthode, mais la capacité est encore bien inférieure à la capacité d'intégration avec les techniques non réversible. En raison de la fragilité des méthodes réversibles, ces méthodes sont utilisées pour le but de contrôle d'intégrité et la dissimulation des données.

Le tatouage réversible facilite la mise à jour du contenu du watermark, l'image reste non protégée une fois que le watermark a été supprimé. Il s'agit d'une situation similaire au cryptage.

Néanmoins, l'avantage du tatouage réversible par rapport au cryptage est qu'au moins l'image est authentifiée. Néanmoins, certaines méthodes sans distorsion ont été proposées [Coatrieux et al., 2006b]. Il faut s'attendre à ce que le watermark soit conservé dans l'image et invisible à l'analyse d'image.

3.4.1.3 Techniques basées sur les méthodes traditionnelles de tatouage

La troisième approche consiste à utiliser des méthodes classiques de tatouage tout en minimisant la distorsion. Dans ce cas, le watermark remplace certains détails de l'image tels que le bit le moins significatif de l'image [Shih and Wu, 2005, Wakatani, 2002] ou les détails perdus après une compression avec perte [Li et al., 2005].

Dans [Piva et al., 2005], un tatouage robuste a été considéré après que le médecin ait sélectionné la puissance maximale du watermark juste sous le niveau d'interférence avec le diagnostic. Néanmoins, il faut considérer que l'image originale capturée subit souvent un certain traitement, comme l'amélioration et l'étirement du contraste avec des paramètres variant d'un utilisateur à l'autre. Par conséquent, le watermark peut devenir plus ou moins visible. Cet effet est souligné par la diversité des images médicales avec des pixels codés sur plus de 8 bits.

3.4.2 Classification selon l'application

Les techniques de tatouage numérique sont classifiées selon leurs applications en trois catégories : dissimulation des informations du patient (EPR), authentification de contenu et contrôle d'intégrité [Nyeem et al., 2013].

3.4.2.1 Techniques de dissimulation des informations du patient

Les applications de la télémédecine nécessitent le transfert des enregistrements électroniques des patients (EPR) ainsi que des images médicales pour un diagnostic ultérieur. Il est essentiel de protéger à la fois l'EPR et les images. L'insertion d'EPR dans l'image médicale sans dégradations perceptives est une solution prometteuse pour répondre aux exigences de sécurité et réduire l'espace de stockage ainsi que la vitesse de transmission.

Navas et al. [Navas et al., 2007] ont proposé trois exigences clés pour la dissimulation et la transmission du EPR :

1. L'extraction du EPR doit être aveugle en raison de l'indisponibilité de l'image originale ;
2. Le taux de bit erreur BER [1] doit être zéro ;
3. L'imperceptibilité ne devrait pas être affectée.

Ces exigences suggèrent que les critères nécessaires pour le tatouage numérique d'image médicale soient invisibles, aveugles et réversibles. Un tel modèle de tatouage peut être soit robuste, soit semi-fragile.

Pour une capacité plus élevée, le système de tatouage peut être semi-fragile, bien qu'il nécessite de définir l'ensemble des opérations / traitements appropriés auxquels le système doit être robuste ou ne pas être robuste. Des techniques de correction des erreurs peuvent être utilisées pour obtenir un BER nul et améliorer les performances du système [Zinger et al., 2001]. Afin de renforcer la confidentialité, l'EPR peut être également crypté par les techniques traditionnelles de cryptage [Machkour et al., 2009].

Chao et al [Chao et al., 2002] ont présenté une technique à base de nombre bipolaire pour insérer les données relatives à l'EPR (tels que les rapports de diagnostic, l'électrocardiogramme et les signatures numériques des médecins ou de l'hôpital) dans une image de marque. L'image de marque pourrait être la marque de l'hôpital utilisée pour identifier l'origine d'un EPR. Les signatures numériques de médecins et de l'hôpital pourraient être appliquées pour l'authentification de l'EPR. Ainsi, différents types de données médicales peuvent être intégrées dans la

1. Bit Error Ration

même image de marque. La confidentialité est finalement obtenue en déchiffrant les données relatives à l'EPR et les signatures numériques avec une copie exacte de l'image de marque d'origine.

Acharya et al [Acharya et al., 2004] ont présenté un schéma de tatouage pour cacher les données des patients et les signaux graphiques au sein d'une image médicale. L'image est transformée en domaine fréquentiel en utilisant la DCT. Les coefficients sont compressés avec l'algorithme Run Length Encoding (RLE). Le codage Huffman à longueur variable est utilisé pour économiser de l'espace mémoire. Le fichier texte qui doit être caché est composé de caractères ASCII et crypté et les bits du nombre binaire équivalent sont insérés dans les bits LSB des coefficients DCT à haute fréquences. Les données graphiques tels que les signaux ECG ou EEG sont également cachées dans l'image après la conversion en binaire. L'insertion dans les LSB des coefficients DCT est plus robuste que l'insertion directe dans les LSB des pixels.

3.4.2.2 Techniques d'authentification

L'authentification a suscité beaucoup d'intérêt dans la recherche de tatouage pour l'authentification d'origine et/ ou de contenu d'images médicales. Les détails importants peuvent être conservés dans les images de manière imperceptible, sans causer de dommages dans la ROI. De telles descriptions brèves peuvent être cachées dans les images immédiatement après la production des images dans les départements de la radiologie.

Cela peut se faire en incorporant un processus de tatouage dans différents appareils d'imagerie, comme les scanners par exemple. En utilisant l'association permanente et automatique des watermarks, la sécurité des bases de données médicales peut être assurée.

Ce type de tatouage doit remplir les exigences suivantes [Nyeem et al., 2013] :

1. Le tatouage devrait être invisible, aveugle et robuste ;
2. Le système devrait intégrer les informations minimales requises pour l'authentification d'origine ;
3. L'insertion dans la RONI ;
4. La validation du système de tatouage afin que l'intégration permanente du watermark soit fiable et sécurisée pour le diagnostic.

Pour la validation d'un schéma de tatouage, bien qu'il soit généralement requis pour tout projet de conception d'une approche de tatouage, il est nécessaire de prendre soin de la qualité de l'image tatouée pour une technique de tatouage irréversible. En outre, ce type de tatouage doit insérer le watermark dans la RONI pour ne pas affecter la ROI. Cependant, dans le cas du tatouage réversible, les exigences de sécurité doivent être reconsidérées car le tatouage réversible suppose un environnement sécurisé.

3.4.2.3 Techniques de contrôle d'intégrité

Les images médicales dans différentes modalités radiologiques contiennent des informations médicales pertinentes qui peuvent être facilement altérées avec des opérations de traitement d'image. Ainsi, leur protection et leur authentification revêtent une grande importance, ce qui avancera avec la future normalisation de l'échange de données entre les hôpitaux, ou entre les patients et les médecins [Fotopoulos et al., 2008].

L'intégrité d'une image médicale peut être vérifiée dans trois niveaux [Huang et al., 2008]

1. Détection de l'altération,

2. Localisation de l'altération,
3. Récupération de la région falsifiée (si c'est possible).

L'atteinte de ces exigences nécessite le développent d'un système de tatouage fragile, aveugle et réversible ou à base d'insertion dans la RONI. Par conséquent, le tatouage fragile aide à localiser les régions altérées après toute modification malveillante ou involontaire de l'image tatouée.

Si l'authentification d'origine d'une image médicale est obtenue par un tatouage robuste, le tatouage fragile (sous la forme d'un tatouage multiple) peut être utilisé pour localiser et éventuellement récupérer toute région altérée de l'image tatouée. Cela permettra à l'utilisateur de vérifier l'authenticité et l'intégrité des images médicales en même temps. Dans ce cas, si le tatouage est basé sur la RONI plutôt que réversible, il faut tenir compte de la limite de distorsion supplémentaire.

3.5 Tatouage zéro-bit pour la protection des images médicales

Dans les techniques traditionnelles de tatouage, deux problèmes sont posés : le premier est la dégradation de la qualité des données originales introduites par le processus d'incorporation du watermark. En effet, dans certaines applications, comme dans le cas de l'image médicale, toute distorsion n'est pas acceptable. Le deuxième problème, est le compromis entre l'imperceptibilité et la robustesse. La technique de tatouage zéro-bit [2] (ou sans watermark) est une bonne solution à ces problèmes [Chang et al., 1999].

L'idée du tatouage zéro-bit consiste simplement à créer un *partage secret* (*Secret Share* SS) à partir de certaines caractéristiques uniques et invariantes de l'image originale et de l'image du watermark. Lors du processus d'extraction, le watermark est récupéré en combinant les entités du SS et les entités extraites de l'image tatouée.

La technique du zéro-bit est d'abord présenté dans le travail de Chang et al. [Chang et al., 1999]. Dans leur méthode, l'image originale est décomposée en blocs en fonction de la taille du watermark. Un modèle binaire appelé *Master Share* (MS) a été généré à partir de la variance des blocs. Le partage secret (SS) est créé avec une opération XOR entre *MS* et le watermark. Le modèle typique de tatouage zéro est illustré dans la Figure 3.1. Dans le processus d'insertion, l'image hôte et le watermark sont utilisés pour construire le *MS* et le *SS*.

En effet, certaines caractéristiques invariantes doivent être extraites de l'image hôte. Dans la littérature différentes caractéristiques invariantes sont utilisées telles que : les coefficients DWT [Jian-hu and Jia-xing, 2007, Yang et al., 2012], les coefficients DCT [Dong et al., 2011, Li et al., 2012, Shang and Kang, 2013], les matrices SVD [Tian-yu, 2011, Seenivasagam and Velumani, 2013], caractéristiques de similarité de la quantification vectorielle [Huang et al., 2001, Charalampidis, 2005], réseaux de neurones [Sang et al., 2006], etc.

Au cours du processus d'extraction, le *MS* est d'abord extrait de l'image tatouée, puis il est combiné avec le *SS* pour récupérer le watermark [Seenivasagam and Velumani, 2013].

Au cours des dernières années, le concept de tatouage zéro-bit est très adopté dans le domaine de l'image médicale, car il préserve la fidélité de l'image médicale. Dans [Dong et al., 2011], Dang et al. utilisent sept coefficients DCT basse fréquence comme vecteur *MS*. Le *SS* est créé en exécutant la fonction de hachage sur le *MS* et le watermark. Afin de préserver la propriété de l'image originale, le *SS* est stocké dans une troisième partie. Au cours du processus

2. en anglais Zero watermarking

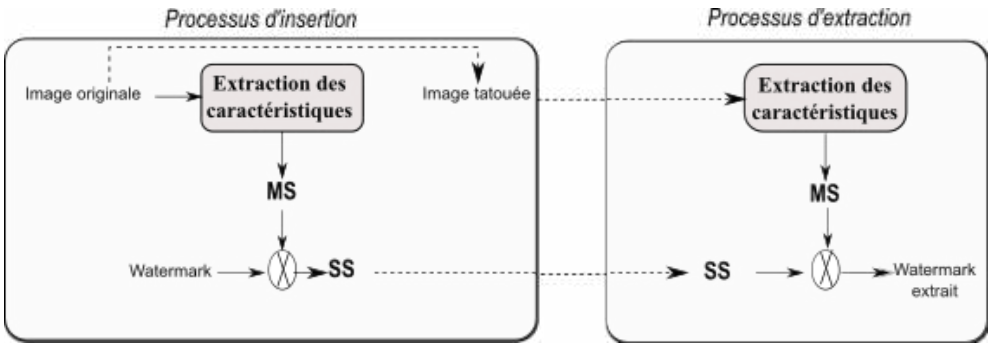


FIGURE 3.1: Modèle typique du tatouage zéro-bit.

d'extraction, le watermark est reconstruit par la fonction de hachage du vecteur stocké *SS* et extrait de l'image tatouée.

Le MS est construit en utilisant cinq coefficients DWT-DFT à basse fréquence dans un autre schéma similaire proposé par Li et al. [Li et al., 2011].

Shang et al. [Shang and Kang, 2013] génère le *MS* en utilisant la transformation DCT de l'image médicale. Un *SS* binaire est généré par la fonction de hachage du watermark crypté et le *MS*. La technologie de brouillage est utilisée pour crypter le watermark.

Dans [Seenivasagam and Velumani, 2013], le code de réponse rapide (Quick Response code) est utilisé pour coder l'information du patient. Le *MS* est construit en utilisant les moments invariants de *Hu* et le *SS* est généré en effectuant la fonction de génération de nombres triangulaires (TNG) sur le *MS* et le watermark.

In [Roček et al., 2016], Roček et al. présentent une approche hybride réversible et zéro-bit pour l'image médicale. Le *SS* est créé à partir du watermark et du *MS* généré à partir du ROI. Ce *SS* est considéré comme un watermark à incorporer dans la RONI.

Cependant, toutes ces techniques de tatouage zéro-bit sont conçues pour préserver la fidélité des images médicales et aboutit à une bonnes robustesse face à certaines manipulations de traitement du signal ou attaques malveillantes.

3.6 Conclusion

Dans ce chapitre, nous avons introduit les notions de base du tatouage numérique appliqué à l'imagerie médicale. Nous avons exposé d'abord les exigences de sécurité et les limitations des systèmes classiques de protection d'imagerie médicale. Par la suite, nous sommes focalisés sur la protection par le tatouage numérique et nous avons présenté ses avantages, ses exigences et une classification des différentes techniques de TIM. Le concept du tatouage zéro-bit est aussi introduit car une approche basée sur ce concept est proposée dans le contexte de notre travail et elle sera présentée, par la suite dans le chapitre 5.

Chapitre 4

Nouvelle approche d'optimisation multi-objectif hybride pour le tatouage aveugle des images couleurs RGB

Sommaire

4.1 Introduction

La conception d'un tatouage optimal pour une application donnée implique toujours un compromis entre l'exigence d'imperceptibilité et l'exigence de robustesse. Par conséquent, le tatouage d'image peut être considéré comme un problème d'optimisation multi-objectif.

Dans le cadre de notre travail de thèse, nous avons développé une nouvelle approche d'optimisation multi-objectif (MOO) utilisant l'approche NSGA-II pour la conception d'un système de tatouage aveugle et robuste afin de protéger les droits d'auteurs des images couleur RGB. En effet, la méthode proposée s'inscrit dans le domaine fréquentiel en utilisant la décomposition SVD.

La technique mathématique SVD fournit une manière élégante d'extraire des caractéristiques algébriques d'une image. Elle est largement appliquée au traitement d'image numérique. En effet, les principales propriétés de la SVD du point de vue des applications du traitement d'image sont [Liu and Tan, 2002] :

— Les valeurs singulières (SVs) d'une image ont une très bonne stabilité, c'est-à-dire lorsqu'une petite perturbation est ajoutée à une image, ses valeurs singulières ne changent pas de manière significative ;
— Les SVs représentent les propriétés intrinsèques de l'image algébrique.

Dans [Golea et al., 2010], nous avons proposé un schéma de tatouage aveugle basé sur une décomposition en bloc (Block-SVD) pour incorporer un watermark couleur RGB dans une image hôte couleur RGB. Plus précisément, nous avons proposé une nouvelle méthode pour maintenir l'ordre des SVs une fois le watermark intégré dans l'une des SVs du milieu de chaque bloc en divisant la valeur singulière choisit par un facteur scalaire. Dans cette méthode, le problème est le choix d'une meilleure SV du milieu et le facteur scalaire (SF) de mise à l'échelle car ces deux paramètres dépendent de l'image originale et du watermark. Ce problème peut être considéré comme un problème d'optimisation et il peut être modélisé en utilisant un algorithme génétique. D'ailleurs, plusieurs approches basées sur les AGs ont été proposées pour le tatouage d'image récemment.

Dans [Veysel, 2008], un simple système de tatouage à base d'AG est proposé pour résoudre le problème du choix d'un facteur scalaire optimal. Les SVs de l'image niveaux de gris sont modifiées pour intégrer l'image de watermark en employant plusieurs SFs. Les modifications sont optimisées en utilisant l'AG afin d'obtenir la plus grande robustesse possible sans perdre l'imperceptibilité. La fonction de fitness d'un individu est calculée comme la différence entre deux fonctions : la première estime la robustesse (entre l'image originale et le watermark) et la seconde évalue l'imperceptibilité.

Chih-Chin Lai [Lai., 2011] a proposé une technique de tatouage d'image basée sur la SVD et Tiny-GA. Dans son approche, les SVs de l'image originale sont modifiées pour intégrer le watermark. Le Tiny-GA offre une manière systématique de considérer les améliorations des SFs qui sont utilisées pour contrôler la force du watermark intégré. Avec le schéma proposé, le watermark inséré peut survivre avec succès après avoir été attaqué par des opérations de traitement d'image. Les résultats de la simulation montrent que le schéma proposé surpasse les autres travaux similaires. La fonction de fitness utilisée est une concaténation de deux critères contradictoires : l'imperceptibilité et la robustesse.

Parce que nous avons deux paramètres à optimiser, le tatouage d'image peut être considéré comme un problème d'optimisation bi-objectif. La présence d'objectifs multiples dans le problème de tatouage d'image, donne naissance à un ensemble de solutions optimales largement connues sous le nom de solutions pareto-optimales, au lieu d'une seule solution optimale. En

l'absence de toute autre information, on ne peut pas dire que l'une de ces solutions pareto-optimales soit meilleure que l'autre. Cela demande à l'utilisateur de trouver autant de solutions pareto-optimales que possible. Les méthodes classiques d'optimisation suggèrent de convertir le problème d'optimisation multi-objectif en un problème d'optimisation à objectif unique en mettant l'accent sur une solution pareto-optimale particulière à la fois. Lorsqu'une telle méthode doit être utilisée pour trouver des solutions multiples, elle doit être appliquée plusieurs fois, en espérant trouver une solution différente à chaque simulation.

Dans [Golea et al., 2011], nous avons proposé une approche multi-objectif hybride pour le tatouage des images couleurs RGB afin d'optimiser les deux exigences contradictoires : l'imperceptibilité et la robustesse contre les attaques. L'approche proposée est décomposée en deux modules : le tatouage à base de SVD et le tatouage à base de NSGA-II. La Figure 4.1 illustre le modèle proposé.

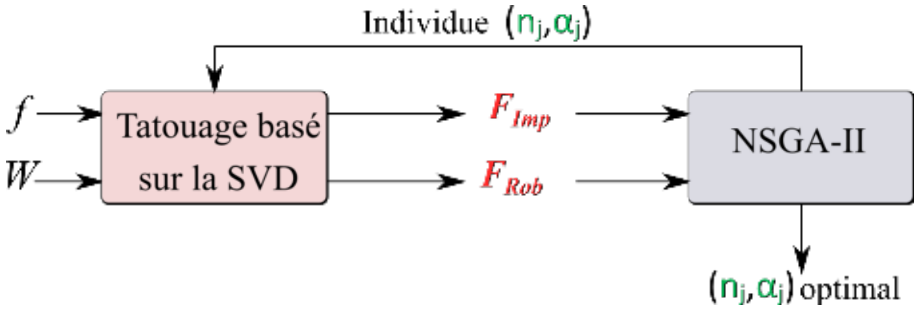


FIGURE 4.1: Modélisation de l'approche proposée.

Dans ce qui suit, nous présentons en détail les deux modules de l'approche proposée. Nous commençons d'abord par la technique de tatouage basée sur la SVD puis nous exposons l'optimisation de cette dernière en utilisant l'algorithme NSGA-II.

4.2 Tatouage aveugle basé sur la SVD

4.2.1 Algorithme d'insertion

Dans cette section, nous présentons l'algorithme d'insertion du watermark (Algorithme 4.1) dans les valeurs singulières d'une image couleurs RGB. Le résultat dépend de deux constantes n et α où :

— n : est l 'ordre de la SV du milieu utilisé ;

— α : est un facteur scalaire SF choisit pour maintenir la qualité de l'image tatouée.

Elles sont choisies expérimentalement et elles peuvent être vues comme clés privées (elles ne seront connues que par des personnes ayant droit d'extraire le watermark). Un schéma démonstratif de l'algorithme d'insertion est présenté dans la Figure 6.3.

Algorithme 4.1 Algorithme d'insertion de tatouage aveugle basé sur la SVD

Entrées :

— f : image hôte (une image couleur RGB de taille $w_f \times h_f$) ;
— W : watermark (une image couleur RGB de taille $w_W \times h_W$).
— La clé secrète (n,α).

Sortie :

— f_w : image tatouée (une image couleur RGB de taille $w_f \times h_f$).

Étapes :

1. Pour chaque composante de couleur $C \in \{R, G, B\}$ faire :
   (a) Décomposition de la composante C en blocs B_i de taille :

$$T = \frac{w_f}{w_W} \times \frac{h_f}{h_W}. \tag{4.1}$$

   (b) Pour chaque bloc B_i faire :
      i. Décomposition de B_i en valeurs singulières :

$$B_i = U_i S_i V_i^T; \tag{4.2}$$

      λ_i sont les SVs de B_i (éléments diagonaux de S_i).
      ii. Insertion de pixel i de la composante C du watermark $W_C(i)$ directement dans une des SVs du milieu λ_n comme suit :

$$\lambda_n = \frac{W_C(i)}{\alpha}; \tag{4.3}$$

      iii. Maintenance de l'ordre des SVs comme suit :
      — $j = n - 1$, Tant que $\lambda_n > \lambda_j$ faire : $\lambda_j = \lambda_n$; $j = j - 1$;
      — $j = n + 1$, Tant que $\lambda_n < \lambda_j$ faire : $\lambda_j = \lambda_n$; $j = j + 1$;
      iv. Construction des blocs tatoués Bw_i en utilisant les SVs modifiées (la matrice Sw_i) :

$$Bw_i = U_i S w_i V_i^T; \tag{4.4}$$

   (c) Reconstruction de la composante tatouée C_w en utilisant les blocs tatoués.
2. Création de l'image tatouée f_w à partir des trois composantes R_w, G_w et B_w

4.2.2 Algorithme d'extraction

Dans cette section, nous présentons l'algorithme d'extraction (voir Figure 4.3).

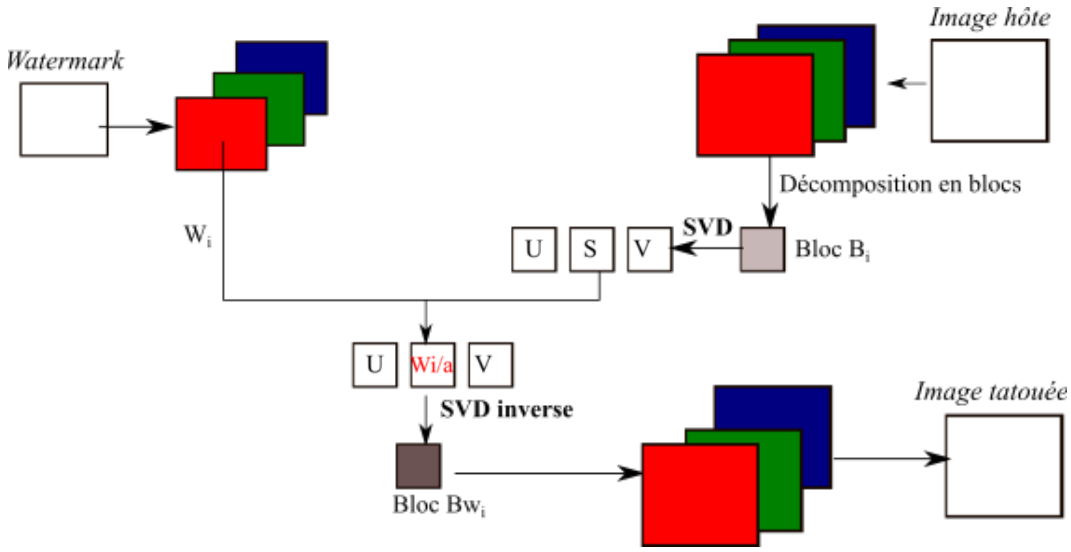


FIGURE 4.2: Algorithme d'insertion basé sur la SVD.

Algorithme 4.2 Algorithme d'extraction de tatouage aveugle basé sur la SVD

Entrées :

— f_w^* : image tatouée et éventuellement attaquée (une image couleur RGB de taille $w_f \times h_f$) ;
— La clé secrète (n,α) : la même clé utilisée par l'algorithme d'insertion.
— T : la taille du bloc.

Sortie :

— W^* : watermark extrait (une image couleur RGB de taille $w_W \times h_W$).

Étapes :

1. Pour chaque composante de couleur $C_w^* \in \{R_w^*, G_w^*, B_w^*\}$ faire :
   (a) Décomposition de la composante C_w^* en blocs Bw_i^* de taille $T \times T$;
   (b) Pour chaque bloc Bw_i^* faire :
      i. Décomposition de Bw_i^* en valeurs singulières :

$$Bw_i^* = U_i^* S_i^* V_i^{*T}; \tag{4.5}$$

      ii. Extraction du pixel $W_C^*(i)$ du watermark à partir de la SV du milieu λw_n^* du bloc correspondant Bw_i^* comme suit :

$$W_C^*(i) = \lambda w_n^* \times \alpha. \tag{4.6}$$

   (c) Construction de la composante W_C^* à partir des pixels extraits $W_C^*(i)$.
2. Construction de watermark extrait W^* à partir des trois composantes W_R^*, W_G^* et W_B^*.

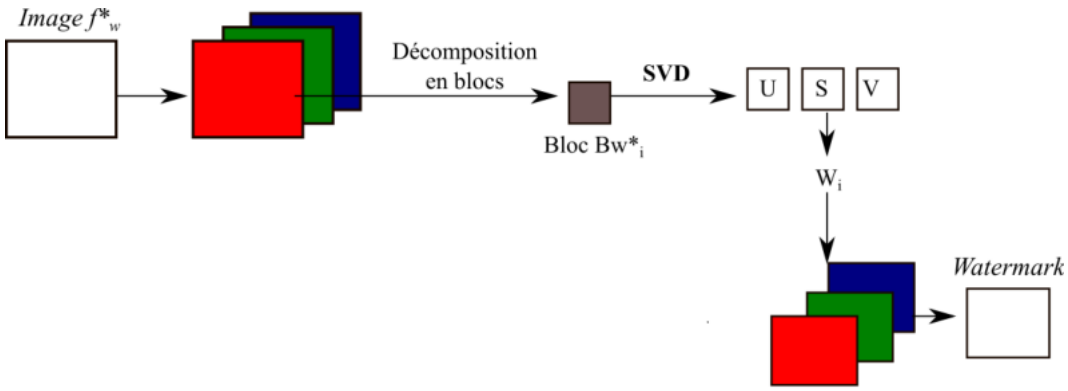


FIGURE 4.3: Algorithme d'extraction basé sur la SVD.

4.3 Algorithme d'optimisation multi-objectif pour le tatouage numérique

Cette section illustre le principe d'utilisation des AGs afin d'optimiser le processus d'insertion du watermark par rapport aux deux exigences contradictoires : l'imperceptibilité et la robustesse. Un bloc de taille $T \times T$ peut avoir $\frac{T}{3}$ SVs du milieu qui peuvent révéler une tolérance différente à la modification. Comme nous n'avons aucune idée sur la sensibilité de l'image à différentes valeurs de (n, α), un algorithme est nécessaire pour obtenir l'optimum (n, α) qui produisent une imperceptibilité et une robustesse maximales.

Par conséquent, un algorithme d'optimisation efficace et puissant est requis pour ces objectifs. Pour cette raison, nous proposons d'utiliser l'algorithme d'optimisation multi-objectif NSGA-II (voir Chapitre 1).

4.3.1 Critères d'optimisation

Nous présentons ici les critères d'optimisation que nous avons choisi pour quantifier les qualités des fonctions objectifs considérées. Nous avons utilisé deux critères d'optimisations pour évaluer les deux fonctions objectifs (l'imperceptibilité F_{Imp} et la robustesse F_{Rob}).

Pour la première fonction objectif F_{Imp}, nous avons employé la métrique MSE entre l'image originale et tatouée. Cette fonction est définie comme suit :

$$F_{Imp} = MSE; \tag{4.7}$$

$$MSE = \frac{1}{NM} \sum_{n,m} (I_{n,m} - I^*_{n,m})^2 \tag{4.8}$$

Pour la deuxième fonction objective F_{Rob}, nous utilisons le NC entre le watermark original W et le watermark extrait W^* après X types d'attaque.

$$F_{Rob} = 1 - \frac{1}{X} \sum_{i=1}^{X} NC(W, W^*_i) \tag{4.9}$$

Où $NC(W, W^*_i)$ est le NC entre le watermark original et le watermark extrait après le $i^{ième}$ attaque.

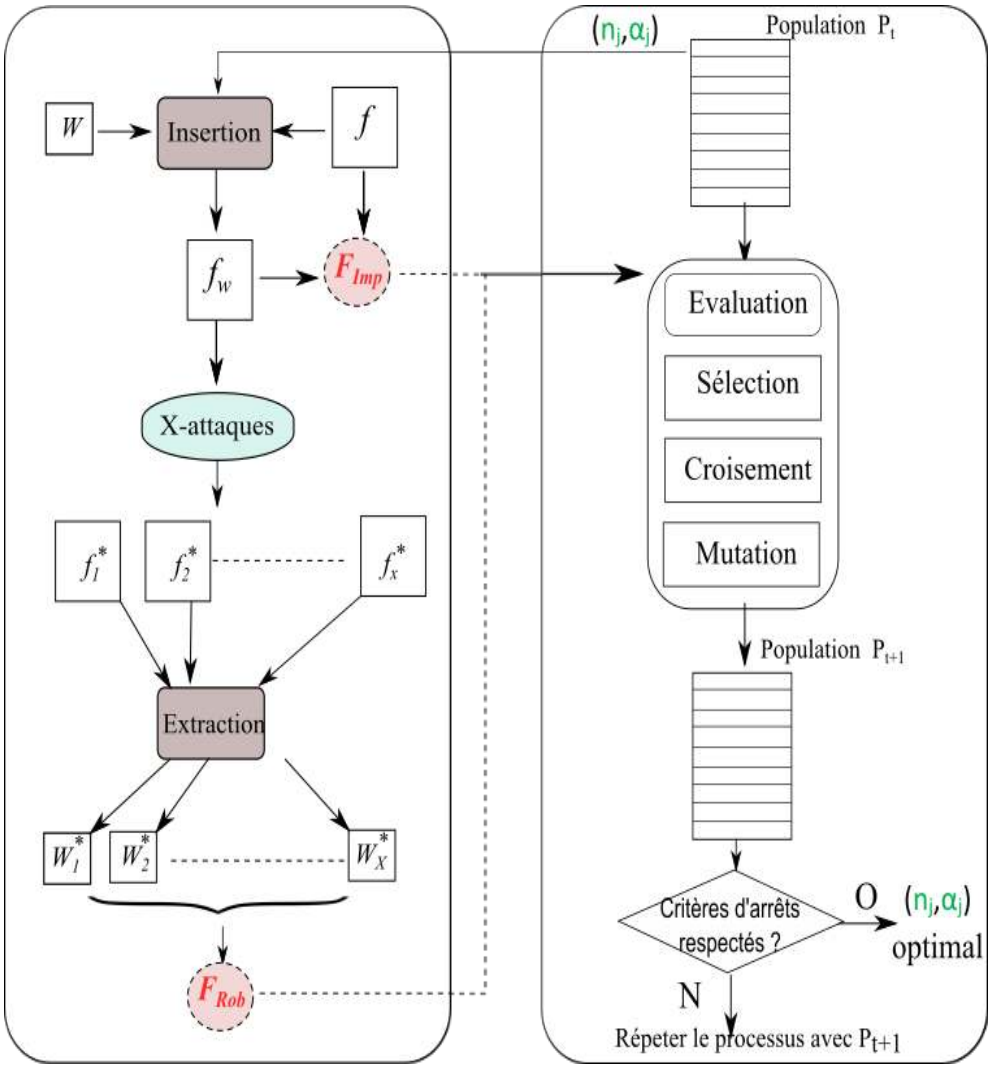


FIGURE 4.4: Approche de tatouage aveugle basée sur la SVD et NSGA-II.

$$NC(W, W_i^*) = \frac{\sum_h \sum_j W(h,j) \times W^*(h,j)}{\sqrt{\sum_i \sum_j W(h,j)^2} \times \sqrt{\sum_h \sum_j W^*(h,j)^2}}. \tag{4.10}$$

Les valeurs de NC sont dans l'intervalle $[0, 1]$, des valeurs plus proches de 1 indiquent plus de similarité entre les watermarks incorporés et les watermarks extraits.

4.3.2 Algorithme proposé

Algorithme 4.3 Algorithme de tatouage basé sur la NSGA-II

Entrées :

— f : image couleurs RGB.
— W : le watermark (image couleurs RGB).

Sortie :

— Le couple (n, α) optimal.

Étapes :

Étape 1 : Initialisation

— Création de la population initiale P_0 de taille N (génération aléatoire de (n, α)).
— Initialisation de l'archive A_0 de taille N.
— Initialisation de nombre de génération $t = 0$.

Étape 2 : Processus d'insertion et d'extraction du watermark

— Pour chaque chromosome j dans la population P_t.
  — Insertion de watermark dans l'image hôte utilisant le chromosome j pour produire l'image tatouée $f_w(j)$.
  — Application de X types d'attaques sur l'image tatouée pour produire X images tatouées et attaquées.
  — Extraction de watermark $W_i^*(j)$ après l'attaque i où $i \in [1 - X]$.

Étape 3 : Évaluation

— Calculer F_{Imp} entre l'image originale et l'image tatouée et attaquée (équation 4.7).
— Calculer F_{Rob} entre le watermark originale et les watermarks extraits après chaque attaque $\{W_1^*, W_2^*, ..., W_X^*\}$ (équation 4.9).
— Évaluation des solutions en utilisant la distance d'encombrement (voir Chapitre 2).

Étape 4 : Création d'une nouvelle population P_{t+1}

— Création d'une nouvelle population en répétant les étapes suivantes jusqu'à ce que la nouvelle population soit complète.
  — *Sélection* : sélectionner deux chromosomes parents de la population P_t en fonction de la distance d'encombrement.
  — *Croisement* : avec une probabilité de croisement sur les parents pour former une nouvelle progéniture (enfants). Si aucun croisement n'a été effectué, la progéniture est la copie exacte des parents.
  — *Mutation* : avec une probabilité de mutation, muter une nouvelle progéniture à chaque locus.
  — *Acceptation* : placer une nouvelle progéniture dans la nouvelle population.

Étape 5 : Test

— Si les conditions sont satisfaites, arrêter la procédure itérative et retourner la meilleure solution dans la population.

Étape 7 : Boucle $t = t + 1$; Aller à l'étape 2.

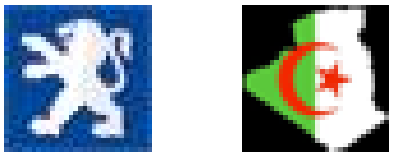
4.4 Résultats expérimentaux

Afin d'évaluer notre méthode de tatouage, plusieurs images couleurs RGB de taille 512×512 sont tatouées avec deux watermarks de taille 32×32 : le logo de Lion et la carte d'Algérie (voir Figure 4.5). Les images hôtes sont présentées dans la Figure 4.6.

Nous avons pris en considération douze attaques : (1) Average Filter (AF), (2) Bluring Filter (BF) , (3) Croping (CR), (4) Resize (RS) , (5) Gausien Filter (GF), (6) Laplacien Filter (LF), (7) Median Filter (MF), (8) Wiener Filter (WF), (9) JPEG (JP) Q=80%, (10) JPEG Q=50%, (11) Salt & pepper noise (SP), (12) Guasian noise (GN).

Paramètres de l'algorithme NSGA-II

- Taille de la population : 50 ;
- Nombre de génération : 20 ;
- Probabilité de mutation : 0.9 ;
- Probabilité de mutation polynomiale : 0.1.



(a) (b)

FIGURE 4.5: Watermarks W : (a) *Logo de Lion*, (b) *Carte Algérie*.

Lena House Tree

Fatma Nessoumer Emir Timgad

FIGURE 4.6: Images hôtes f.

La Figure 4.7 présente les fronts de Pareto pour les différentes images hôtes.

Nous avons choisi trois solutions à partir des fronts du pareto. Elles sont illustrées à la Figure 4.7 par des cercles rouges, verts et magenta. En utilisant les solutions sélectionnées, les images tatouées et les watermarks extraits sont illustrés dans la Figure 4.8. Les valeurs de PSNR et de NC après les différentes attaques sont présentées dans le Tableau 4.1.

Nous pouvons noter à partir des valeurs PSNR que la distorsion entre les images tatouées et les images originales est imperceptible. Nous pouvons également voir à partir des valeurs NC que notre méthode est très robuste contre plusieurs attaques.

Les watermarks extraits à partir des images tatouées *House* et *Nessoumer* après différentes attaques, ont été illustrés respectivement dans la Figure 4.9 et la Figure 4.10.

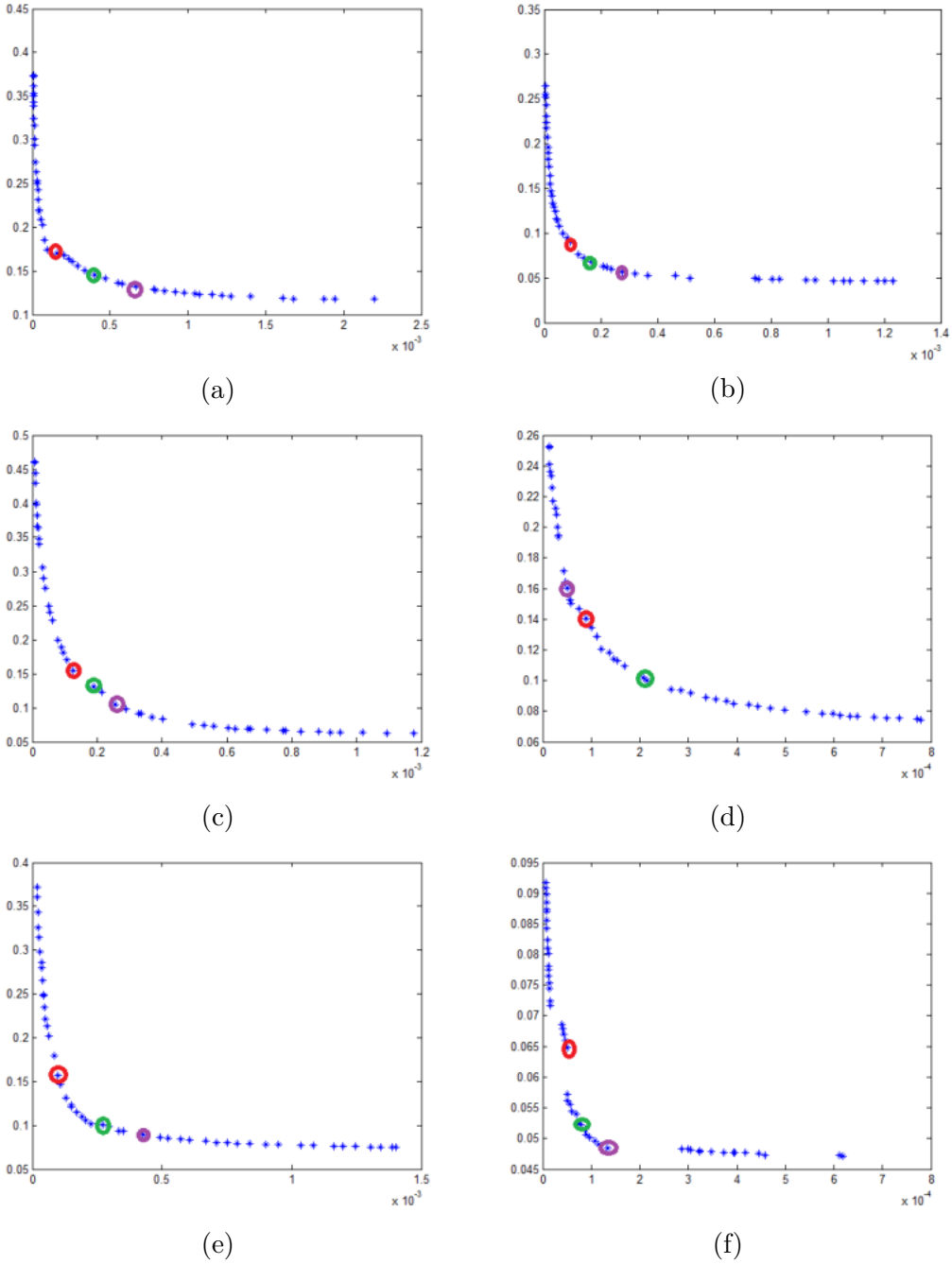


FIGURE 4.7: Fronts de Pareto pour les différentes images hôtes :(a) Lena, (b) House, (c) Tree, (d) Fatema Nessoumer, (e) Emir et (f) Timgad.

4.5 Conclusion

Dans ce chapitre, nous avons présenté une approche de tatouage multi-objectif basée sur les algorithmes génétiques pour la protection des droits d'auteur des images couleur RGB. En effet, l'approche proposée est un algorithme combiné de tatouage aveugle des images couleur RGB et la méthode d'optimisation NSGA-II, qui est considérée comme l'un des cadres d'optimisation multi-objectifs robustes.

Ainsi, l'approche développée repose sur l'utilisation des SVs d'une image afin d'intégrer

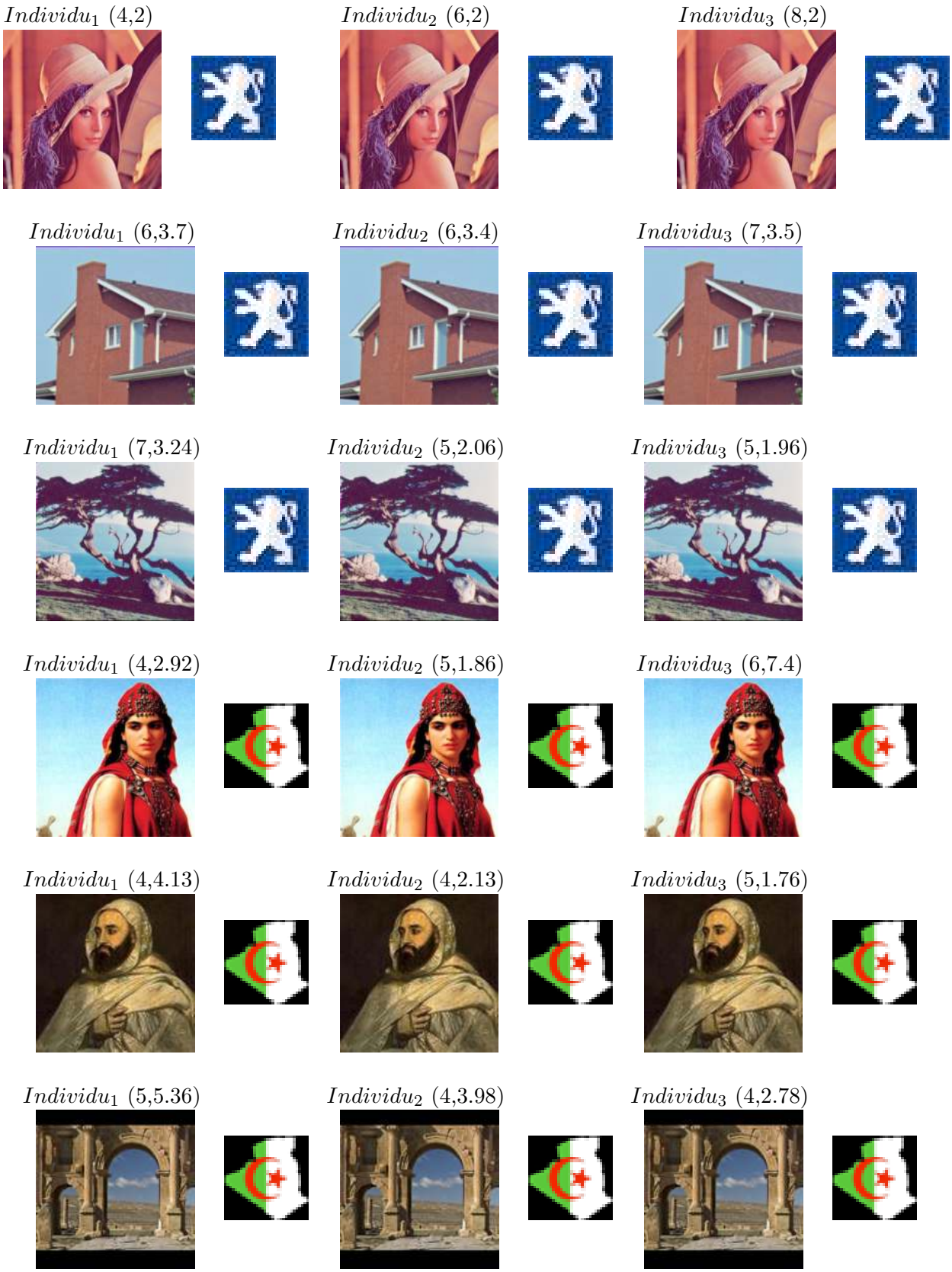


FIGURE 4.8: Images tatouées avec les meilleures individus sélectionnés (n, α) et les watermarks extraits à partir des images tatouées correspondantes.

Lena

Solution	(4,2)	(6,2)	(8,2)
Imperceptibilité PSNR	38.9288	36.2861	33.9333
Exactitude NC	0.9996	0.9989	0.9972
Robustesse NC			
AF	0.7222	0.7248	0.8000
BF 0.1	0.9996	0.9989	0.9972
BF 1.0	0.8185	0.7970	0.7967
CR	0.9663	0.9595	0.9547
RS	0.7138	0.6453	0.5536
GF	0.9418	0.9546	0.9732
JP 80%	0.8857	0.9008	0.9225
JP 50%	0.8306	0.8218	0.8269
LF	0.7750	0.8287	0.8829
MF	0.6761	0.6537	0.6864
SF	0.9317	0.9805	0.9814
WF	0.8237	0.8477	0.8798

House

Solution	(6,3.7)	(6,3.4)	(7,3.5)
Imperceptibilité PSNR	40.8365	39.8582	38.6803
Exactitude NC	0.9993	0.9994	0.9993
Robustesse NC			
AF	0.9993	0.9994	0.9229
BF 0.1	0.9076	0.9120	0.9993
BF 1.0	0.9740	0.9550	0.9803
CR	0.9550	0.9753	0.9504
RS	0.9483	0.9506	0.9597
GF	0.9954	0.8892	0.9968
JP 80%	0.8772	0.9957	0.8680
JP 50%	0.8673	0.8780	0.8731
LF	0.8101	0.7933	0.8406
MF	0.7681	0.9821	0.8242
SF	0.9810	0.8266	0.9861
WF	0.8375	0.8620	0.8769

Tree

Solution	(7,3.24)	(5,2.06)	(5,1.96)
Imperceptibilité PSNR	38.9565	37.2018	36.6739
Exactitude NC	0.9991	0.9987	0.9986
Robustesse NC			
AF	0.8844	0.8389	0.8473
BF 0.1	0.9991	0.9987	0.9986
BF 1.0	0.9713	0.9581	0.9601
CR	0.9506	0.9608	0.9604
RS	0.9406	0.9140	0.9185
GF	0.9955	0.9925	0.9928
JP 80%	0.7657	0.8721	0.8793
JP 50%	0.7198	0.8274	0.8364
LF	0.6056	0.6352	0.6560
MF	0.6082	0.6506	0.6735
SF	0.9717	0.9384	0.9480
WF	0.7275	0.8426	0.8588

Nessoumer

Solution	(4,2.92)	(5,1.86)	(6,7.4)
Imperceptibilité PSNR	39.9862	35.4220	47.7627
Exactitude NC	0.9723	0.9604	0.9739
Robustesse NC			
AF	0.9723	0.8994	0.7213
BF 0.1	0.8548	0.9604	0.9739
BF 1.0	0.9723	0.9379	0.8746
CR	0.9720	0.9604	0.9737
RS	0.8948	0.9113	0.7767
GF	0.9604	0.9555	0.9515
JP 80%	0.8087	0.8438	0.6696
JP 50%	0.7671	0.8133	0.5342
LF	0.6388	0.8686	0.5924
MF	0.8339	0.8733	0.5845
SF	0.8577	0.9221	0.8707
WF	0.8737	0.8871	0.6724

Emir

Solution	(4,4.13)	(4,2.13)	(5,1.76)
Imperceptibilité PSNR	40.7363	36.4787	33.6836
Exactitude NC	0.9902	0.9876	0.9820
Robustesse NC			
AF	0.6969	0.8432	0.8637
BF 0.1	0.9902	0.9876	0.9820
BF 1.0	0.8871	0.9341	0. 0.9280
CR	0.9884	0.9860	0.9820
RS	0.7721	0.8616	0.8467
GF	0.9695	0.9763	0.9738
JP 80%	0.8818	0.9141	0.9099
JP 50%	0.8446	0.8976	0.8934
LF	0.5604	0.7757	0.8700
MF	0.6175	0.7816	0.8069
SF	0.8390	0.8991	0.9458
WF	0.7953	0.9198	0.9286

Timgad

Solution	(5,5.36)	(4,3.98)	(4,2.78)
Imperceptibilité PSNR	42.9986	42.2499	38.6953
Exactitude NC	0.9950	0.9958	0.9936
Robustesse NC			
AF	0.9310	0.9472	0.9500
BF 0.1	0.9950	0.9958	0.9936
BF 1.0	0.9630	0.9743	0.9746
CR	0.9950	0.9958	0.9937
RS	0.9142	0.9478	0.9504
GF	0.9907	0.9912	0.9504
JP 80%	0.8782	0.8792	0.8922
JP 50%	0.7839	0.8458	0.8730
LF	0.9387	0.9045	0.9194
MF	0.9184	0.9343	0.9397
SF	0.9854	0.9580	0.9653
WF	0.9241	0.9607	0.9716

TABLE 4.1: Analyse de l'imperceptibilité, l'exactitude et la robustesse contre les attaques en utilisant les trois individus sélectionnés.

le watermark. En fait, nous avons proposé un nouveau tatouage basé sur la décomposition de l'image hôte en blocs et l'application de la SVD sur chaque bloc de la SVD. L'algorithme NSGA-II est utilisé pour optimiser les deux exigences contradictoires : l'imperceptibilité et la robustesse contre les attaques. Enfin, nous avons montré que le système de tatouage aveugle basé sur le NSGA-II est robuste à douze attaques.

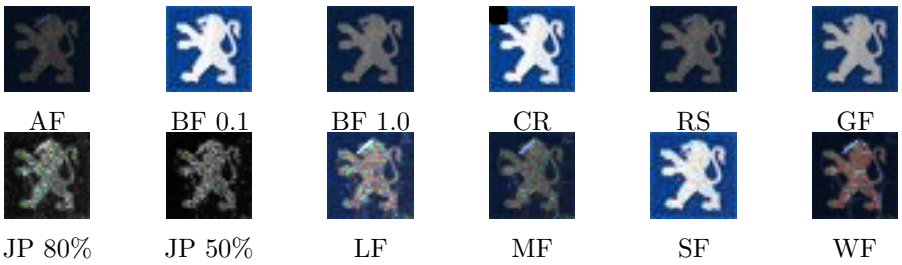


FIGURE 4.9: Watermarks extraits à partir de l'image tatouée *House* après différentes attaques.

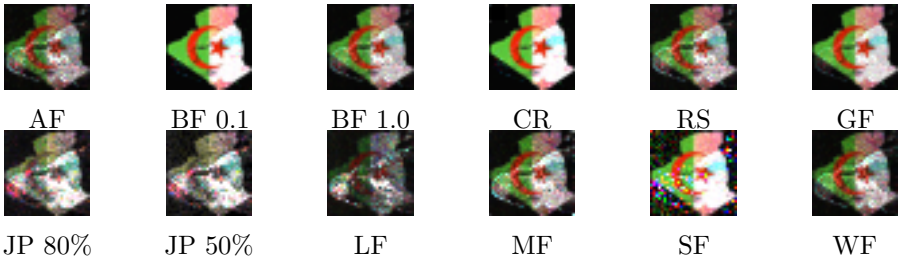


FIGURE 4.10: Watermarks extraits à partir de l'image tatouée *Nessoumer* après différentes attaques.

Chapitre 5

Approches de tatouage numérique appliquées à l'imagerie médicale utilisant les codes détecteurs et correcteurs des erreurs

Sommaire

5.1 Introduction

Les schémas proposés sont inspirés de la transmission en réseau, dans lequel le message à transmettre est divisé en paquets de taille fixe et des informations redondantes sont ajoutées à chaque paquet pour traiter les erreurs. En fonction des caractéristiques du canal de communication, deux stratégies ont été mises en pratique : la stratégie de *la correction d'erreur directe* FEC et *la stratégie de demande de répétition automatique* ou *la retransmission* ARQ. La stratégie FEC utilise les *codes de correction des erreurs* ECC pour corriger les erreurs causées par les canaux qui font beaucoup d'erreurs (comme les liens sans fil). Tandis que, l'ARQ est basé sur *des codes de détection des erreurs* EDC qui permettent au récepteur de détecter qu'une erreur s'est produite et il demande une retransmission. Cette dernière stratégie est utilisée dans le cas de la fibre optique ou d'un canal de haute qualité où des erreurs apparaissent occasionnellement et la détection ainsi que la retransmission des erreurs sont généralement plus efficaces [Tanenbaum, 2003]. Généralement, la technique ARQ est préférée dans la pratique pour la raison que la taille d'information redondante requise est plus petite que dans le cas de FEC. Ce dernier est surtout utilisé lorsque la retransmission est difficile à appliquer [Ramabadran and Gaitonde, 1988].

Dans ce chapitre, nous exposons deux approches de tatouage appliquées à l'imagerie médicale pour la protection de la Région d'intérêt (ROI). La première approche [Golea and Melkemi, 2017] repose sur l'utilisation d'un code détecteur des erreurs nommé CRC qui est connu comme l'un des EDC les plus utiles et les plus puissants utilisés dans divers systèmes de communication numérique. Cependant, la deuxième approche [Golea et al.,] est basée sur le code de correction RS afin de reconstruire la région d'intérêt. Les caractéristiques de ces deux approches sont illustrées dans le Tableau 5.1.

Caractéristiques	**Première méthode**	**Deuxième méthode**
Domaine d'insertion	Spatial (LSB)	Fréquentiel (LWT)
Insertion dans la ROI	Oui	Non (tatouage Zéro-bit à la ROI)
Objectif	Authentification	Contrôle d'intégrité
Fonctions	Détection des altérations	Détection et correction des altérations
Code	Détecteur des erreurs (CRC)	Détecteur et correcteur des erreurs (RS)
Technique	Fragile	Hybride (fragile et robuste)
Algorithme d'extraction	Aveugle	Aveugle

Table 5.1: Caractéristiques des deux techniques de tatouage proposées.

5.2 Tatouage numérique basé sur la théorie de codes

La théorie des codes est attrayante pour la recherche de tatouage d'images. Ainsi, plusieurs approches de tatouage basées sur les codes sont proposées et divers EDC ou ECC sont utilisés tels que Reed Solomon (RS), Hamming (Ham), Bose-Chaudhuri-Hocquenghen (BCH), etc. Le Tableau 5.2 présente un résumé de la littérature de différentes approches de tatouage basées sur la théorie des codes.

Schéma	Adopter à l'imagerie médicale	Type	Code	Information codée par le code	Domaine d'insertion
[Lee and Won, 2000]	Non	Fragile	RS	signature générée.	Spatial
[Terzija and Geisselhardt, 2004]	Non	Robuste	RS	watermark (texte)	Fréquentiel
[Lin et al., 2004]	Non	Fragile	CRC	signature générée	Spatial
[Nayak et al., 2004]	Oui	Robuste	RS	information du patient	Spatial
[Zhou et al., 2004]	Non	Semi-fragile	BCH	Signature extraite de l'image	Fréquentiel
[Chemak et al., 2007]	Oui	Robuste	Turbo code	information du patient	Fréquentiel
[Qi and Qi, 2007]	Non	Robuste	Ham	watermark (texte)	Frequency
[Nayak et al., 2009]	Oui	Robuste	RS, BCH, Ham	information du patient	Spatial
[Al-Qershi and Khoo, 2009]	Oui	Fragile	RS	information du patient & signature	Spatial
[Mostafa et al., 2010]	Oui	Robuste	BCH	information du patient	Fréquentiel
[Hajjaji et al., 2011]	Oui	Robuste	BCH	information du patient	Fréquentiel
[Kumar et al., 2015]	Oui	Robuste	BCH	information du patient	Fréquentiel

TABLE 5.2: Résumé de la littérature de différents codes basés sur des techniques de tatouage.

A partir de ce tableau, nous pouvons noter que toutes les méthodes de tatouage d'image basées sur les codes sont effectuées sur la signature ou sur certaines caractéristiques de l'image. Dans le cas de l'image médicale, les ECC sont réalisés afin d'obtenir la robustesse de l'EPR. Nous avons proposé d'utiliser les codes directement sur les pixels de la ROI pour atteindre l'authentification et l'intégrité. Les concepts des codes CRC et RS sont présentés dans l'Annexe A et Annexe B.

5.3 Première approche basée sur le code CRC pour la détection des altérations

5.3.1 Méthodologie proposée

Dans cette section, nous décrivons notre schéma qui s'étale sur deux étapes : la génération/ insertion du watermark et l'étape de détection des altérations. La première étape exécute la procédure du codage CRC pour générer un watermark qui sera incorporé dans les LSB. À la deuxième étape, le watermark est extrait et une procédure de décodage CRC est effectuée pour détecter les paquets altérés.

5.3.1.1 Algorithme de génération et d'insertion du watermark

Algorithme 5.1 met en évidence les détails de notre schéma. En particulier, le schéma génère un watermark en utilisant le codeur CRC et l'incorpore par la suite dans les LSB de chaque pixel dans la ROI. La première étape effectuée par l'Algorithme 5.1 est la segmentation de l'image originale f en deux régions : ROI (*Région d'intérêt*) et RONI (*Région de non intérêt*). La segmentation peut être effectuée manuellement ou automatiquement. Cette dernière est généralement destinée à des modalités spécifiques. Par exemple, l'approche proposée dans [Liu et al., 2015] est une segmentation de masse efficace dans les mammographies. Afin d'appliquer notre approche pour différentes modalités, nous proposons de donner la main à l'utilisateur pour sélectionner la ROI. Cette région est définie par un polygone car elle n'est pas régulière dans la plupart des cas. Les coordonnées des sommets de ce polygone sont stockées dans un vecteur $Vert_{roi}$ et chiffrées en utilisant une clé secrète Key_1 pour créer un vecteur $Vert_{Encry}$ qui est utilisé plus tard dans le processus de détection. La Figure 5.1 illustre un exemple de construction du vecteur $Vert_{roi}$. Pour la simplicité de la description, nous nous sommes concentrés sur une ROI unique. Les mêmes algorithmes peuvent s'étendre sur plusieurs ROIs.

Par la suite, les pixels du ROI extrait sont stockés dans le vecteur roi qui sera permuté en utilisant la deuxième clé secrète Key_2. Ce vecteur permuté est décomposé sur des paquets P_i de 16 pixels, où i est le nombre de paquets. Les six bits de poids fort MSBs de chaque paquet sont concaténées pour créer un vecteur binaire M_{P_i} de taille 16×6. Un exemple de paquet P_i et le vecteur M_{P_i} est montré dans la Figure 5.2. Le codage $CRC(128, 96)$ est effectuée à chaque vecteur M_{P_i} pour créer un checksum de taille 32. Le checksum généré est considéré comme un watermark W qui sera intégré dans le domaine spatial (premier et deuxième LSBs) de chaque pixel correspondant pour reconstruire la ROI tatouée, notée ROI_w. Enfin, l'image tatouée est créée en combinant ROI_w et $RONI$. La Figure 5.3 illustre le block de diagramme de génération et insertion du watermark.

Algorithme 5.1 Procédure de génération et d'insertion du watermark

Input :

- f : Image médicale originale.
- Key_1 et Key_2 : Clés secrètes.

Output :

- f_w : image tatouée ;
- $Vert_{Encry}$: Vecteur qui contient les sommets chiffrés du ROI.

Steps :

1. Sélection de la ROI de l'image originale f.
2. Les coordonnées des sommets de la ROI sont stockées dans le vecteur $Vert_{roi}$. La taille de ce vecteur est $2 \times N$ où N est le nombre de sommets. Le vecteur $Vert_{roi}$ est ensuite chiffré en utilisant un nombre pseudo-aléatoire Key_1 pour retourner le vecteur $Vert_{Encry}$.
3. Les pixels de ROI sont stockés dans le vecteur roi qui est permuté de manière aléatoire en utilisant une clé Key_2.
4. Décomposition de vecteur permuté en paquets P_i de taille fixe (16 pixels).
5. Pour chaque paquet P_i faire :
   - Extraction des six bits MSB de chaque pixel.
   - Concaténation de ces bits ensemble pour créer un vecteur M_{P_i} de taille 16×6.
   - Application de codage $CRC(128, 96)$ à M_{P_i} utilisant le polynôme générateur CRC-32.
   - Le checksum généré est considéré comme un watermark W_{P_i}.
   - Insertion de chaque deux bits de W_{P_i} dans le premier et deuxième LSBs du pixel correspondant pour créer le paquet tatoué P_i^w.
6. Reconstruction de roi_w en utilisant les paquets tatoués P_i^w.
7. Combinaison de $RONI$ et ROI_w pour créer l'image tatouée f_w.

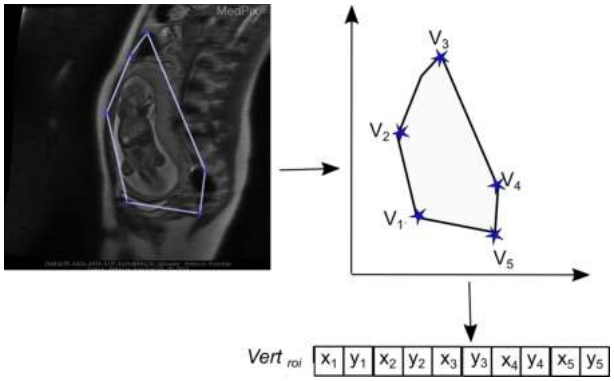


FIGURE 5.1: Exemple de vecteur $Vert_{roi}$.

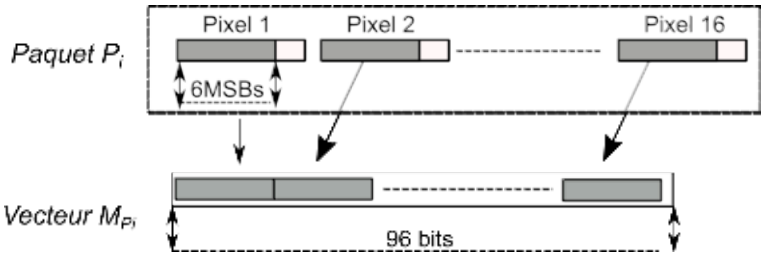


FIGURE 5.2: Exemple de construction du paquet P_i et le vecteur M_{P_i} .

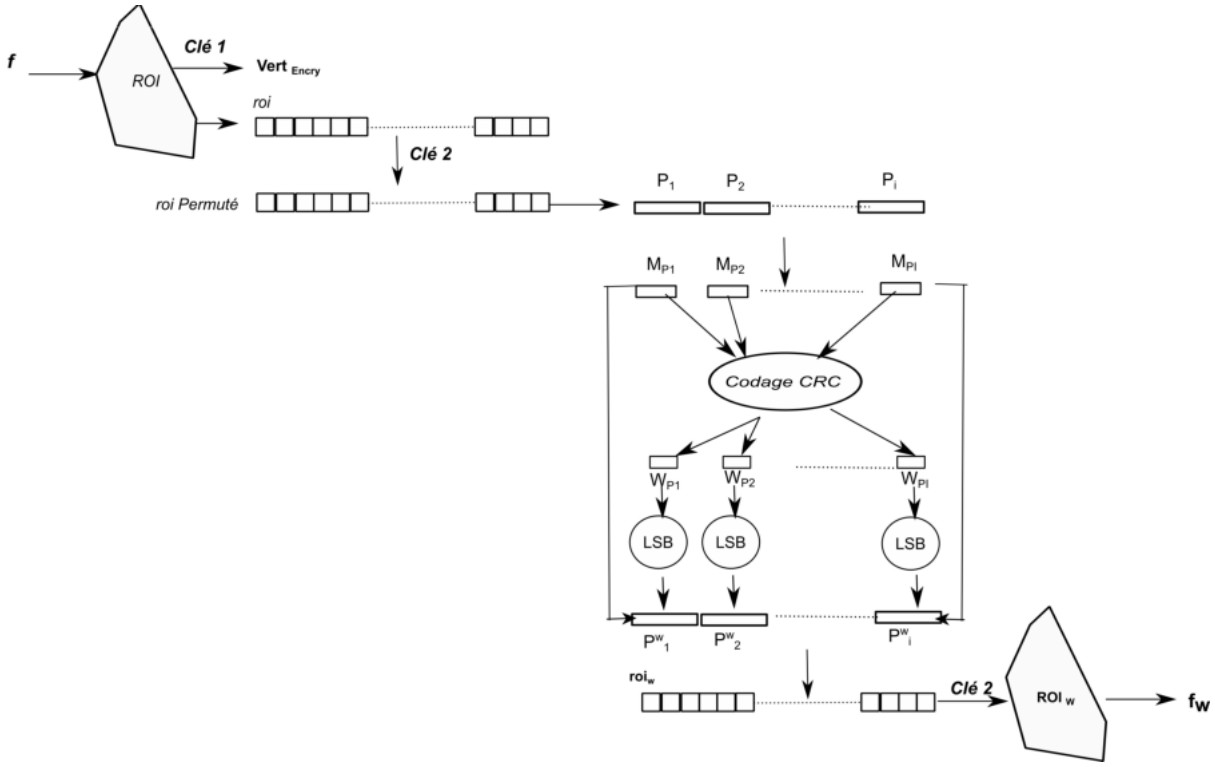


FIGURE 5.3: Diagramme de la génération et l'insertion du watermark.

5.3.1.2 Algorithme de détection des altérations

L'extraction et la détection des altérations est juste inverse du processus d'insertion. Les détails sont reportés dans l'algorithme 5.2.

Algorithme 5.2 Procédure d'extraction et de détection des altérations

Input :

- f_w : image tatouée.
- Key_1 et Key_2 : clés secrètes.
- $Vert_{Encry}$: vecteur contient les sommets chiffrés de la ROI.

Output :

- Carte de détection des altérations (*Tamper Detection Map* TDM).

Steps :

1. Extraction des sommets de la ROI en déchiffrant $Vert_{Encry}$ utilisant Key_1.
2. Décomposition de l'image tatouée en ROI et $RONI$ en utilisant les sommets extraits.
3. Les pixels de ROI sont stockés dans le vecteur roi_w.
4. Permutation aléatoirement du vecteur roi_w utilisant Key_2.
5. Décomposition de vecteur permuté en paquets P_i^w de taille fixe (16 pixels).
6. Pour chaque paquet P_i^w faire :
   - Extraction des six bits MSBs de chaque pixel.
   - Concaténation de ces bits ensemble pour créer un vecteur M'_{p_i} de taille 16×6.
   - Extraction des deux bits LSB de chaque pixels pour créer le watermark extrait W'_{p_i}.
   - Adjonction de W'_{p_i} à la fin de M'_{p_i} pour créer le vecteur WM_{p_i} comme représenté sur la Figure 5.4.
   - Application de décodage $CRC(128, 96)$ à cette séquence en utilisant le polynôme générateur de degré 32.
   - Si le reste est null alors
     - $TDM = 1$: ce qui indique que le paquet n'est pas altéré.

     Sinon
     - $TDM = 0$: le paquet est altéré.

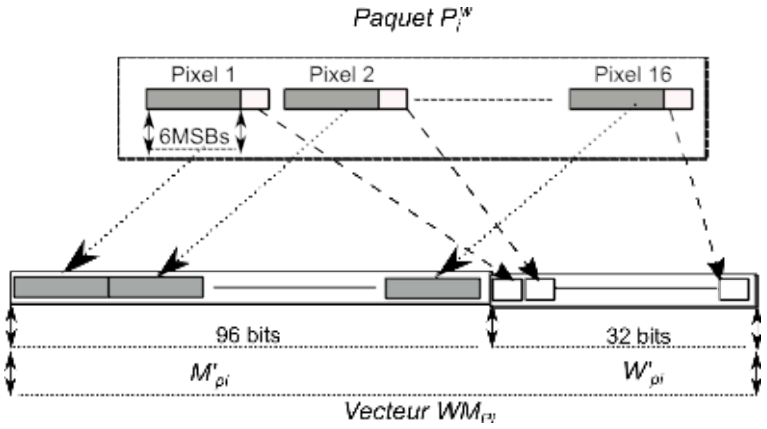


FIGURE 5.4: Example of extracting the watermark W'_{p_i} and constructing the vector WM_{P_i} .

5.3.2 Résultats expérimentaux

Dans cette section, nous nous concentrons sur l'évaluation de l'efficacité du système proposé en termes d'imperceptibilité et de capacité de détection. Par conséquent, les tests ont été séparés en deux parties : la première est destinée à tester la propriété d'imperceptibilité et la seconde est destinée à évaluer la fragilité (ou les capacités de détection des altérations.

Les expériences sont réalisées sur un ensemble de données composé de six modalités différentes d'imagerie médicale : CT-Scan, IRM,XR, glsUS, UGI et BE. Ces images sont téléchargées à partir de la base de données d'images médicales MedPix [MedPix, 2017] et elles sont illustrées à la Figure 5.5. Les tailles des images de tests et les ROIs sont présentées dans le Tableau 5.3.

Dans nos expériences, un ordinateur portable avec un processeur Intel i3 2.GHZ, 4 Go de RAM, Windows 7 est utilisé comme plateforme de simulation.

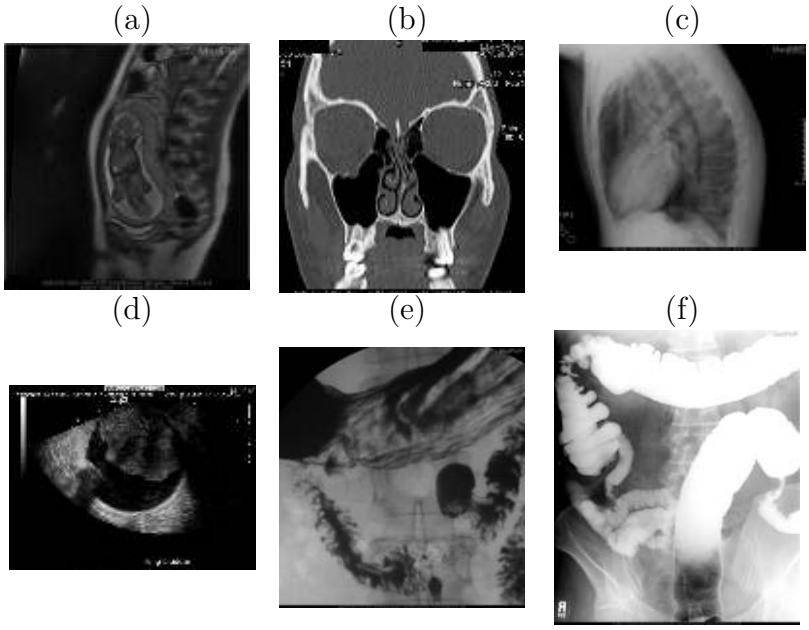


FIGURE 5.5: Images medicale originales : (a) MRI scan, (b) CT , (c) XR , (d) US, (e) UGI et (f) BE.

Modalités	Taille de l'image	Taille de la ROI (%)
MRI	513×512	15
CT	571×500	25
XR	637×760	43
US	720×960	9
UGI	1024×1085	43
BE	1001×1200	63

TABLE 5.3: Description de l'ensemble des données utilisées dans les expériences.

5.3.2.1 Analyse de l'imperceptibilité

La propriété d'imperceptibilité signifie que le processus d'insertion du watermark ne doit pas dégrader la qualité de l'image originale. La Figure 5.6 montre les ROIs sélectionnées et les images tatouées f_w.

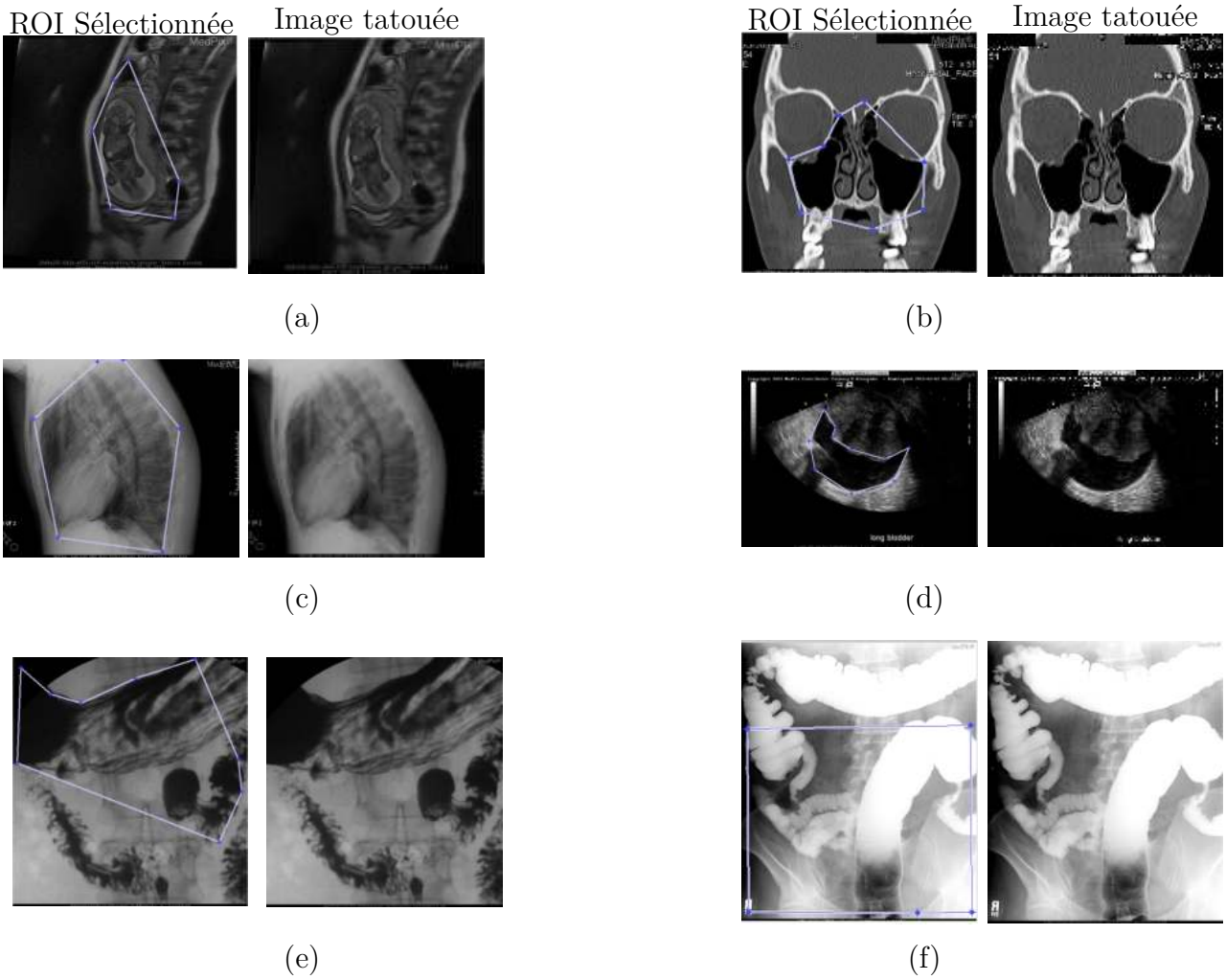


FIGURE 5.6: ROI sélectionnées et images tatouées : (a) MRI scan, (b) CT, (c) XR, (d) US, (e) UGI et (f) BE.

Afin de tester la qualité des images tatouées, deux mesures mathématiques différentes sont utilisées : PSNR (rapport signal sur bruit maximum) et SSIM (indice de similarité structurelle).

Le PSNR estime la distorsion entre deux images f et f_w. Considérant que, le SSIM évalue la similitude entre eux et ses valeurs sont $\in [-1, 1]$. La valeur 1 signifie que les images originales et tatouée sont similaires. Supposons que N_1 et N_2 sont la hauteur et la largeur des images, PSNR et SSIM sont définis comme suit [Roček et al., 2016] :

$$PSNR = 10 \log_{10} \left(\frac{N_1 \times N_2 \times \max(f(i,j))^2}{\sum_{i=1}^{N_1} \sum_{j=1}^{N_2} (f(i,j) - f_w(i,j))^2} \right). \tag{5.1}$$

$$SSIM = \frac{(2 \times \mu_f \times \mu_{f_w} + C_1)(2 \times \sigma_{ff_w} + C_2)}{(\mu_f^2 + \mu_{f_w}^2 + C_1)(\sigma_f^2 + \sigma_{f_w}^2 + C_2)}. \tag{5.2}$$

Où μ_f et μ_{f_w} sont les moyens locaux, σ_f, σ_{f_w} sont les écarts-types et σ_{ff_w} est la covariance. C_1 et C_2 sont des constantes incluses pour éviter un dénominateur nul lorsque $\mu_f^2 + \mu_{f_w}^2 = 0$ et/

ou $\sigma_f^2 + \sigma_{f_w}^2 = 0$.

	Notre méthode		La méthode [Eswaraiah and Reddy, 2014]	
Modalités	PSNR	SSIM	PSNR	SSIM
MRI	55.5628	0.9969	50.1560	0.9839
CT	56.0244	0.9965	-	-
XR	50.8052	0.9882	-	-
US	57.8021	0.9970	52.4634	0.9824
UGI	50.8508	0.9861	-	-
BE	48.0818	0.9815	-	-

TABLE 5.4: Qualité des images tatouées via PSNR et SSIM.

Les résultats rapportés dans le Tableau 5.4 montrent des résultats satisfaisants du schéma proposé. Dans tous les cas, les valeurs PSNR sont supérieures à $48dB$ et les valeurs SIMM supérieures à 0.98, sont meilleures que celles de Eswaraiah. Dans le cas des modalités CT, XR, UGI et BE, le schéma de Eswaraiah ne fonctionne pas car la taille du ROI est supérieure à 25%.

Une autre approche a également été utilisée pour estimer l'imperceptibilité qui est le tracé d'histogramme permettant d'observer la distribution tonale d'une image. Par conséquent, en comparant les histogrammes des images originales et tatouées, nous pouvons juger de l'imperceptibilité.

A partir des histogrammes de la Figure 5.7, nous pouvons voir qu'ils sont superposés, ce qui indique que la différence entre les images originales et les images tatouées n'est pas perceptible au système visuel humain.

Nous évaluons également l'impact de l'augmentation de la taille du ROI sur la qualité de l'image tatouée. Les résultats sont montrés dans la Figure 5.8. A partir des graphes de PSNR, nous pouvons observer que les valeurs PSNR sont très bonnes (sont dans la gamme de 60 dB) pour de petites tailles de la ROI et elles sont encore bonnes en augmentant la taille de la ROI à protéger. Lorsque la taille du ROI est de 100% de l'image originale (toute l'image est considérée comme ROI), le PSNR est égal à 46 dB, ce qui est considéré comme bon. Les graphiques SSIM indiquent également qu'en augmentant la taille du ROI, les valeurs SSIM vont de $0,96$ à 1.

5.3.2.2 Analyse de la fragilité

Pour examiner l'efficacité de l'approche proposée à détecter les altérations, nous calculons le taux de détection TD en utilisant l'équation suivante :

$$TD = \frac{N_d}{N_{total}} \times 100. \tag{5.3}$$

Où N_d est le nombre des paquets altérés et détectés et N_{total} est le nombre total des paquets altérés.

La variation de la détection des altérations de différentes modalités altérées, en ce qui concerne le pourcentage d'altération, est présentée dans la Figure 5.9. A partir de cette figure, il est tout à fait évident que les méthodes proposées détectent des paquets altérés de 100% indépendamment du pourcentage de falsification et qu'elle fonctionne de façon assez similaire avec différentes modalités.

Nous testons également la capacité de détection au niveau du paquet. Par conséquent, nous estimons la capacité de détection si le paquet est altéré ou non par rapport au nombre de pixels

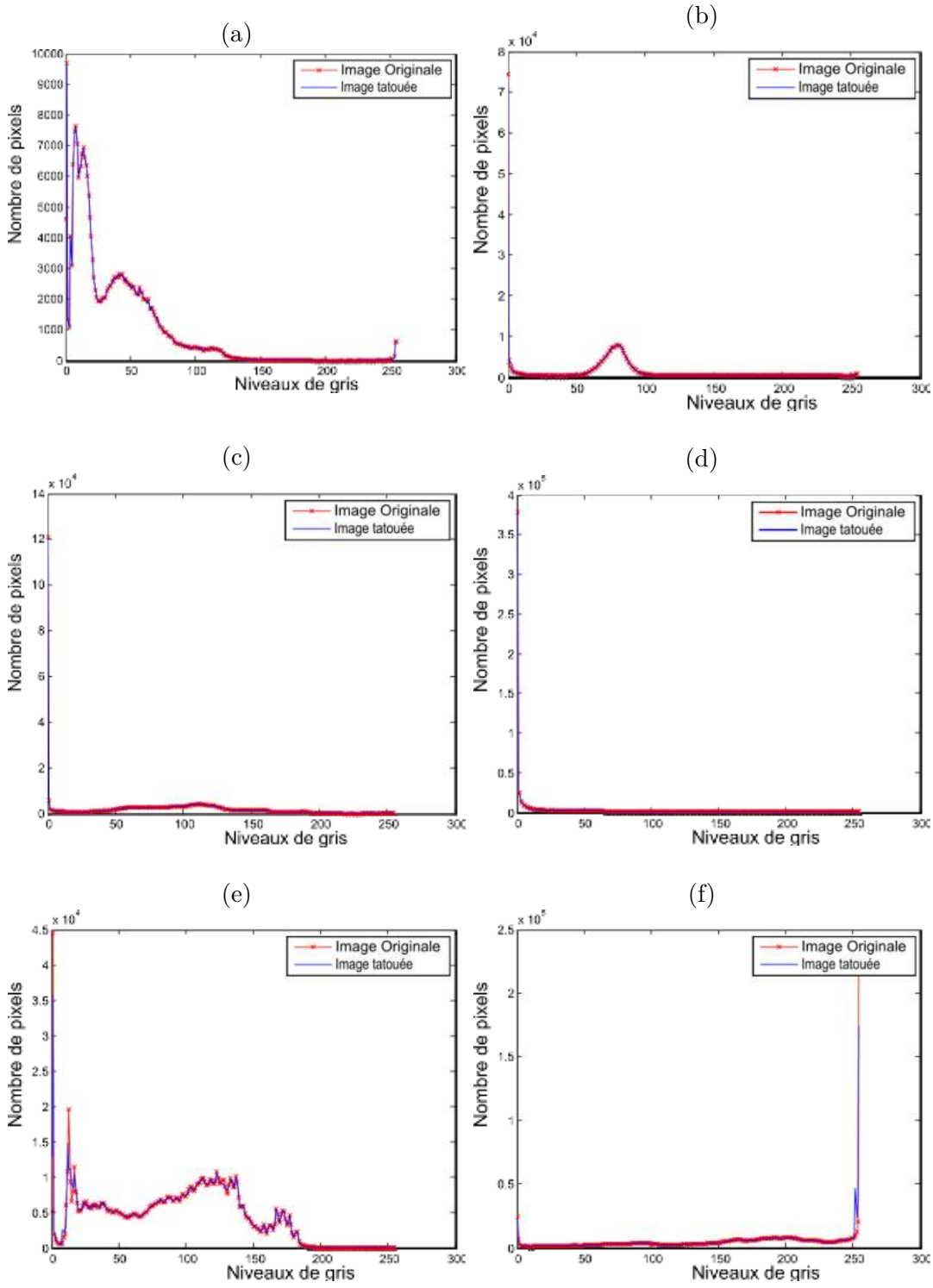


FIGURE 5.7: Évaluation de l'imperceptibilité à travers des histogrammes pour différentes modalités : (a) MRI scan, (b) CT, (c) XR, (d) US, (e) UGI et (f) BE.

altérés dans le paquet (de 1 pixel à 16 pixels). La Figure 5.10 montre la capacité de détection au niveau du paquet.

Pour présenter visuellement l'exactitude et la fragilité du schéma proposé, nous utilisons l'image TDM (Tamper Detection Map) pour indiquer les paquets altérés dans la ROI. Les

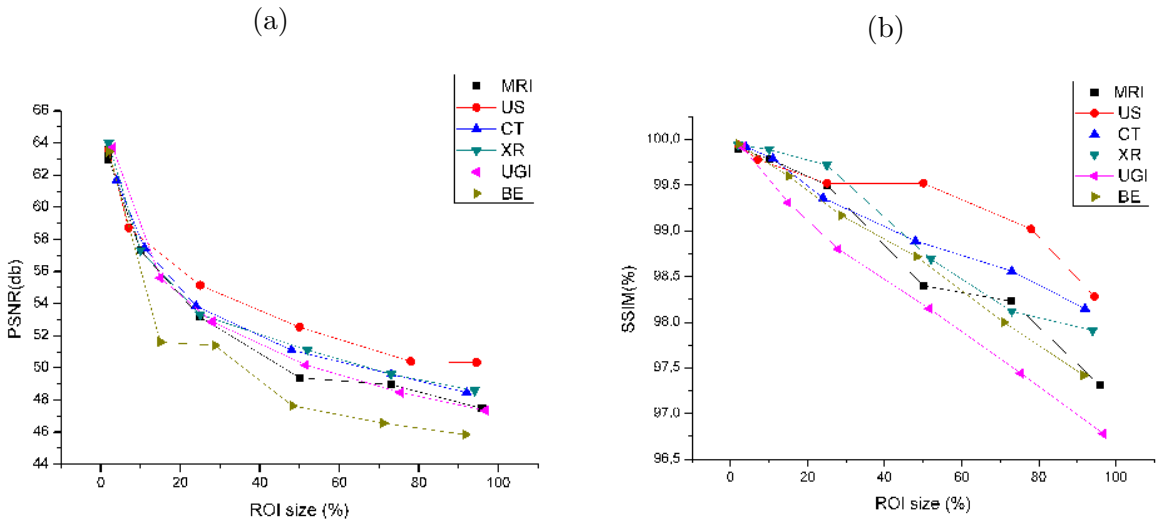


FIGURE 5.8: Impact de l'augmentation de la taille du ROI sur la qualité des images tatouées : (a) graphe de PSNR and (b) graphe de SSIM.

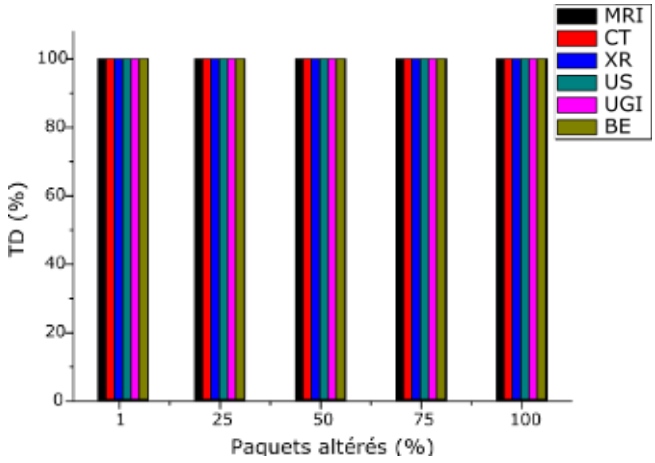


FIGURE 5.9: Variation du taux de détection des altérations pour différentes modalités par rapport au pourcentage des paquets altérés.

pixels noirs dans TDM illustrent les pixels altérés. La Figure 5.11 illustre la carte de détection d'altération extraite de différentes images tatouées en cas d'absence d'attaque.

Pour mettre en évidence la fragilité de notre méthode, nous avons pris en compte plusieurs types d'attaques. La Figure 5.12 montre les images attaquées et leurs cartes de détection d'altérations correspondantes.

Il est clair que l'approche proposée est capable de détecter des attaques fiables (comme une modification d'un bit et d'un pixel) et des attaques fortes qui altèrent plusieurs ou tous les pixels (comme le bruit et le filtre).

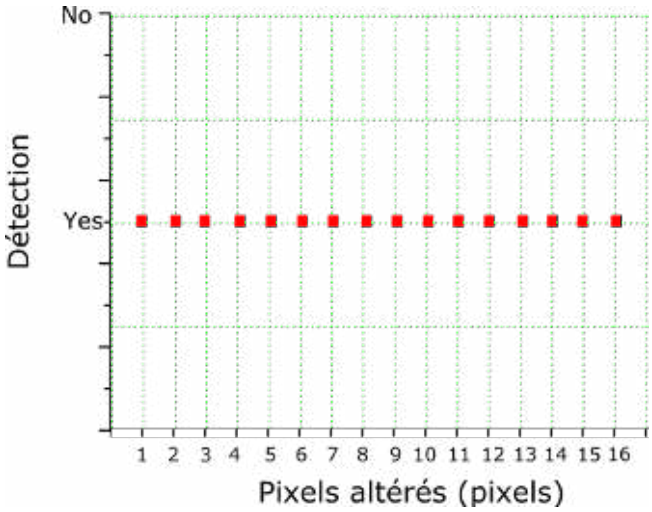


FIGURE 5.10: Détection des altérations au niveau paquet.

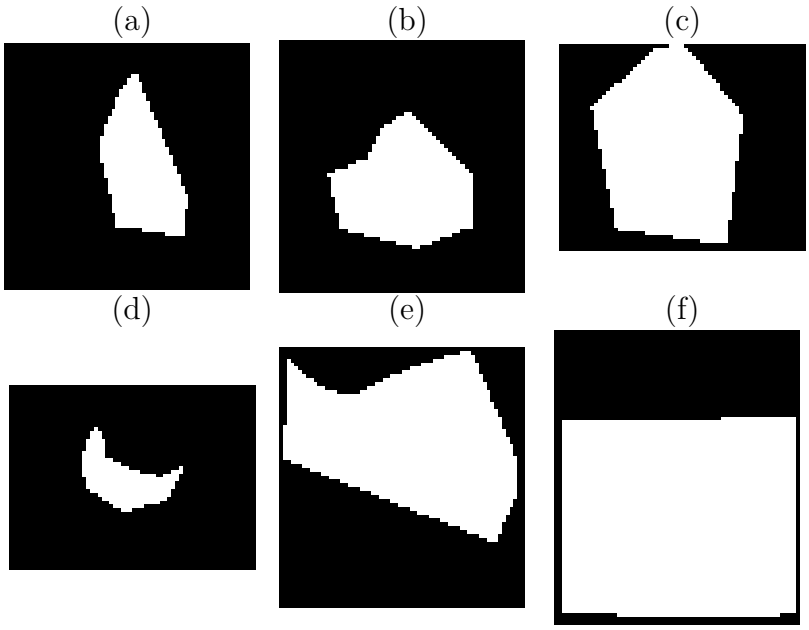


FIGURE 5.11: Carte de détection des altérations (TD) extraite à partir d'images tatouées sans aucune attaque : (a) MRI scan, (b) CT, (c) XR, (d) US, (e) UGI et (f) BE.

5.4 Deuxième approche basée sur le code RS pour la détection et la récupération des altérations

Les points suivants sont pris en compte dans le choix du code RS :

- Reed-Solomon est l'un des ECC les plus utiles, il est applicable dans différents périphériques durs (comme les CD et DVD) et sur différents systèmes de communication (ADSL et DTV) [Clarke, 2002, Wicker and Bhargava, 1999].
- C'est un sous-ensemble significatif de codes BCH non binaires. Il est prouvé, que ce code a une distance maximale séparable par rapport aux autres codes BCH [Wicker, 1995].
- C'est la meilleure solution recommandée dans la communication mobile [Wicker and Bhar-

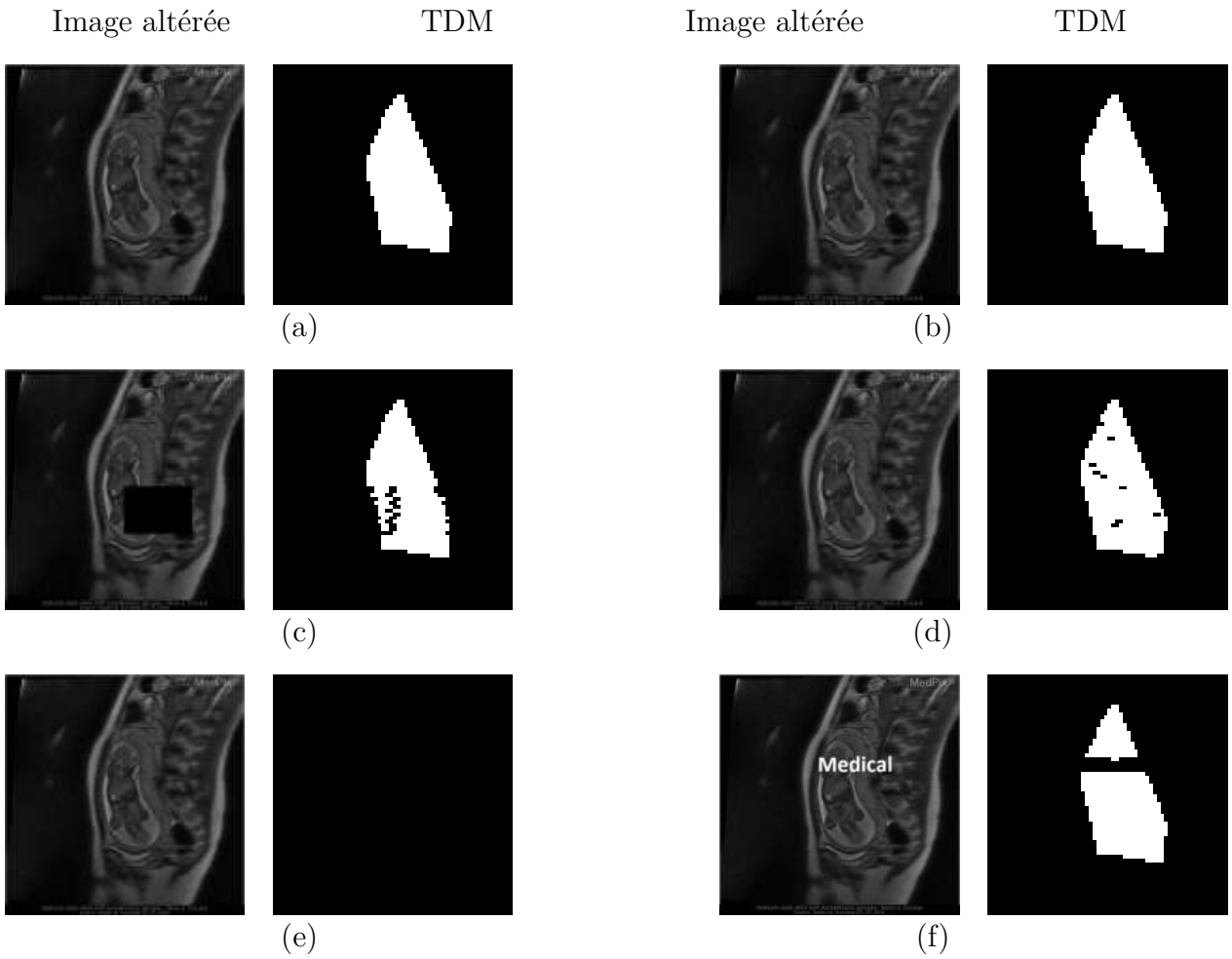


FIGURE 5.12: Fragilité contre les attaques : (a) Un bit corrompu. (b) Un pixel corrompu. (c) Attaques de re-cadrage. (d) Bruit de sel et de poivre. (e) Le bruit gaussien. (f) Copie de texte.

gava, 1999].

5.4.1 Méthodologie proposée

L'approche proposée est décomposée en trois algorithmes : algorithme de génération de la clé secrète SS (*Secret Share*) considéré comme un watermark, algorithme d'insertion de ce dernier et algorithme d'extraction/ récupération. Le premier algorithme exécute le concept du tatouage zéro-bit sur la ROI pour générer une SS qui sera utilisée comme information de détection et de récupération. Cette SS est générée en exécutant un codage RS sur des pixels de ROI. Dans l'algorithme d'insertion, les SS sont intégrées dans le domaine fréquentiel de la RONI en utilisant LWT. À l'algorithme d'extraction et de récupération, le SS est extrait de la RONI et combiné avec le MS (*Master Share*) de la ROI. Le décodage RS est exécuté à cette séquence pour détecter et récupérer la ROI.

5.4.1.1 Algorithme de génération du watermark

Algorithme 5.3 Génération de SS utilisant le code RS

Entrées :
- f : image médicale originale.
- (n, k) : paramètres de RS.

Sorties :
- SS : Secret Share.
- $\mathcal{K}$: clé secrète.

Étapes :
1. Sélectionne de la ROI de l'image originale f .
2. Les sommets du ROI sont sauvegardés comme une clé secrète $\mathcal{K}$.
3. Les pixels de ROI sont stockés dans le vecteur V_{roi}.
4. Création de MS en permutant le vecteur V_{roi}.
5. Décomposition du vecteur de caractéristiques MS en paquets de taille k.
6. Pour chaque paquet P_i où $i \in \left[1, \frac{size(ROI)}{k}\right]$ faire :
   - Application de codage RS : codage $RS(n, k)$.
   - Génération d'un checksum Ch_i de taille $(n - k)$.
7. Création de SS en combinant les valeurs du checksum générés.

Le diagramme de l'algorithme de génération de la SS est présenté dans la Figure 5.13.

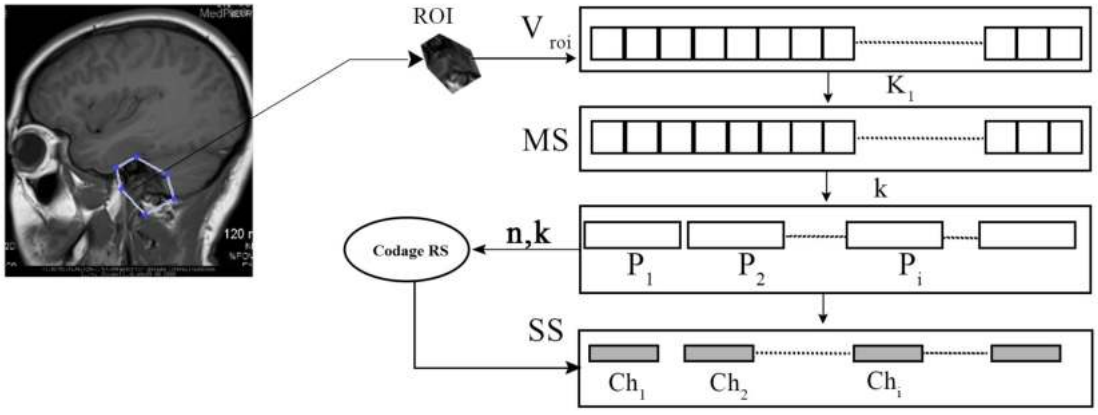


FIGURE 5.13: Le processus de génération de SS basé sur RS code.

5.4.1.2 Algorithme d'insertion

Algorithme 5.4 Insertion du watermark dans le domaine fréquentiel utilisant la transformée LWT

Entrées :
- f : image médicale Originale.
- SS : Secret Share.

Sortie :
- f_w : image tatouée.

Étapes :
1. Représentation de SS en binaire pour créer le watermark W.
2. Décomposition de $RONI$ en blocs de taille $N \times N$.
3. Pour chaque bloc faire :
   - Application de la transformée LWT à trois niveaux pour générer à chaque niveau quatre sous-bandes .
   - Insertion des bits de W dans les deux LSBs de tous les coefficients.
   - Application de la transformée inverse $iLWT$ pour obtenir les blocs tatoués.
4. Combinaison des blocs tatoués pour créer la $RONI$ tatouée.
5. Reconstruction de l'image tatouée f_w en combinant ROI et $RONI$ tatouée.

Un schéma démonstratif de cet algorithme est illustré dans la Figure 5.14.

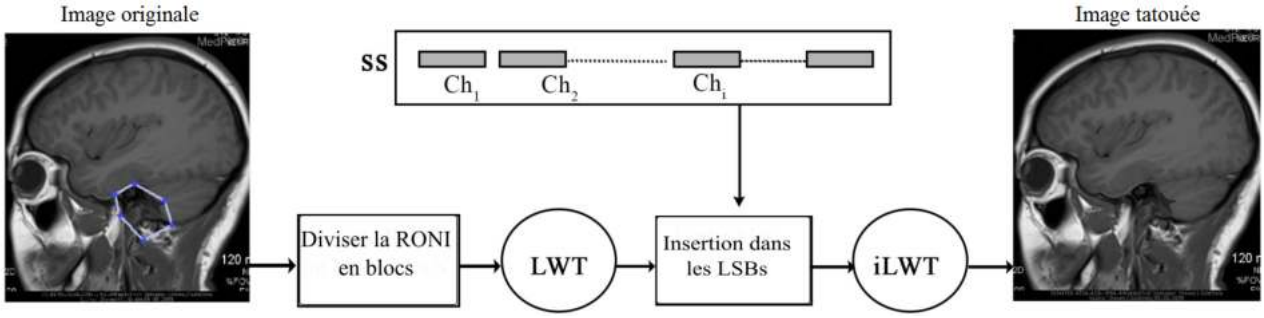


FIGURE 5.14: Processus d'insertion basé sur la transformée LWT.

5.4.1.3 Algorithme d'extraction et de reconstruction

Algorithme 5.5 Extraction et reconstruction de la ROI utilisant la transformée LWT et le code RS.

Entrées :

- f_w^* : image tatouée et éventuellement attaquée ;
- $\mathcal{K}$: clé secrète.

Sorties :

- ROI reconstruite.

Étapes :

1. Extraction des sommets du ROI en utilisant $\mathcal{K}$.
2. Utilisation des sommets pour décomposer f_w^* en ROI et RONI.
3. Extraction de watermark :
   - Décomposition de RONI en blocs de taille $N \times N$.
   - Application de la transformée LWT sur chaque bloc et extraire les bits du watermark du LSB de tous les coefficients.
   - Représentation de W en nombres entiers pour créer le SS^*.
4. Extraire le MS^* :
   - Stockage des pixels de ROI dans un vecteur V_{roi}^*.
   - Permutation du vecteur V_{roi}^* pour créer MS^*.
5. Combinaison de MS^* et SS^* :
   - Décomposition de MS^* en paquets de taille k.
   - Pour chaque paquet P_i faire :
     - Adjonction de SS_i^* à la fin du paquet.
     - Application de décodage RS sur cette séquence. S'il y a des erreurs, corriger les et passer au paquet suivant.

La Figure 5.15 illustre le schéma fonctionnel de l'algorithme de vérification et de récupération.

5.4.2 Résultats expérimentaux

Dans cette section, nous nous concentrons sur la démonstration de l'efficacité de notre méthode en termes d'imperceptibilité, d'exactitude du watermark extrait et de capacité de récupération. L'analyse de ces propriétés dépend des paramètres RS sélectionnés. En effet, nous devons d'abord sélectionner les paramètres RS.

5.4.2.1 Paramètres du RS

A partir de la définition de RS, il est clair que toutes les erreurs dans le paquet de taille k peuvent être récupérées si la somme de contrôle est $2 \times k$. Si $2t = 2k$ alors $n = 2k + k$. Donc $RS(3k, k)$ est un code parfait : $RS(15, 5)$, $RS(120, 30)$, $RS(210, 70)$ et $RS(255, 85)$.

Le temps de calcul est le point critique sur lequel nous sommes basé pour choisir les paramètres du code. Pour $m = 8$, nous testons le temps total (codage RS + décodage RS) obtenu avec différents codes parfaits. Ces résultats sont illustrés dans la Figure 5.16. Nous pouvons voir que le temps de calcul dépend de la taille du message à transmettre (dans notre

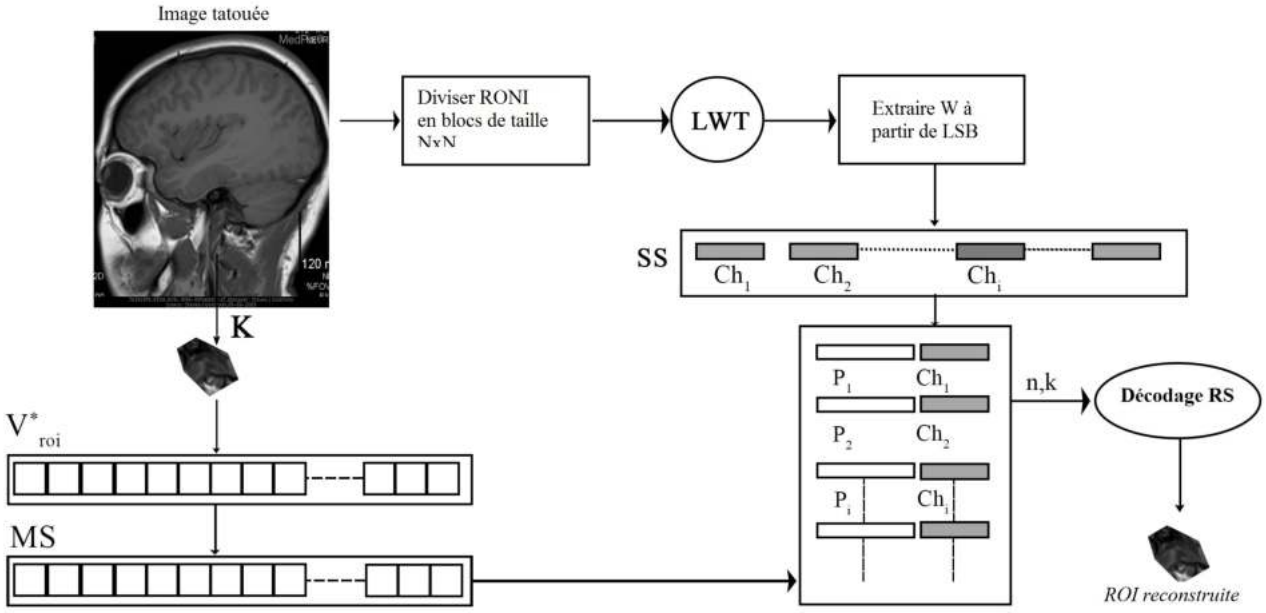


FIGURE 5.15: Processus d'extraction et reconstruction basé sur la transformée LWT et le code RS.

cas la ROI) et de la taille des paquets (k). Pour un message de taille petite (jusqu'à 1000 pixels), le RS avec de petits paquets (k = 5 et k = 30) est préférable à de gros paquets. Pour les messages de taille moyenne (entre 2000 et 4000), nous remarquons que les codes $RS(120, 30)$, $RS(210, 70)$ et $RS(255, 85)$ ont presque le même temps de calcul. Dans le cas de messages plus volumineux, $RS(255, 85)$ donne des performances supérieures aux autres codes et les RS $(15, 5)$ sont les plus mauvais. Dans nos prochaines expériences, nous utilisons $RS(255, 85)$ car la taille du ROI est généralement grande.

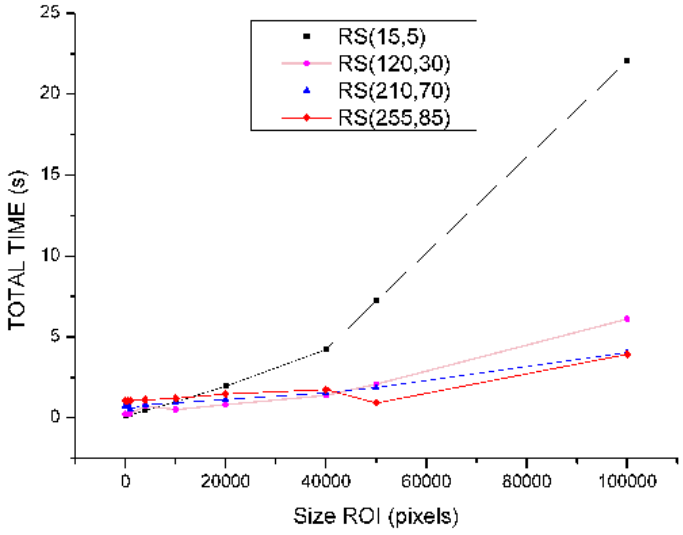


FIGURE 5.16: Temps de calcul en fonction de la taille du ROI et de la taille du paquet(k) pour différents codes parfaits $RS(3k, k)$ où $k = 5, 30, 70$ et 85.

Modalités	Taille d'image	Taille de ROI (pixels)	Taille W (bits)	capacité d'insertion (bpp)	PSNR	SSIM	NC
MRI	548×500	29,597	474,640	1.94	48.15	0.9723	1.00
US	720×960	52,826	845,920	1.33	47.80	0.9281	1.00
CT	571×500	27,139	435,200	1.50	47.96	0.9523	1.00
XR	637×760	47.525	761,600	1.62	48.52	0.9822	1.00
UGI	733×964	49.509	792.880	1.23	49.60	0.9804	1.00

TABLE 5.5: Qualité des images tatouées (PSNR et SSIM) et exactitude des watermarks extraits (NC) pour différentes modalités.

5.4.2.2 Analyse de l'imperceptibilité

Afin d'évaluer notre méthode, différentes modalités d'images médicales sont utilisées comme CT, IRM, US, UGI et XR. Ces images sont téléchargeables à partir de la base de données d'images médicales gratuite MedPix[1]. Les images originales, les ROIs sélectionnées et leurs images tatouées correspondantes sont présentées dans la Figure 5.17.

Deux métriques sont utilisées pour évaluer la propriété d'imperceptibilité, PSNR (Peak Signal to Noise Ratio) et SSIM (Structural Similarity Metric Index).

Les valeurs PSNR et SSIM obtenues pour les différentes modalités sont illustrées dans le Tableau 5.5.

A partir du Tableau 5.5, il est clair que les valeurs PSNR et SSIM sont très bonnes indiquant que la méthode proposée peut atteindre une bonne qualité des images tatouées.

L'histogramme est aussi employé pour juger l'imperceptibilité. A partir des histogrammes de la Figure 5.18, il est clair que la différence entre les images originales et les images tatouées n'est pas perceptible par le système visuel humain.

5.4.2.3 Analyse de l'exactitude

La corrélation normalisée (NC) est utilisée pour examiner la proximité entre le watermark original W et extrait W^* :

$$NC = \frac{\sum_i \sum_j W(i,j) \times W^*(i,j)}{\sqrt{\sum_i \sum_j W(i,j)^2} \times \sqrt{\sum_i \sum_j W^*(i,j)^2}}. \tag{5.4}$$

Les valeurs NC pour différentes images testées sont également présentées dans le Tableau 5.5. Pour toutes les modalités, les valeurs de NC sont égales à 1, ce qui indique que les watermarks extraits (SS) sont identiques aux watermarks originales. Cela signifie que les ROI sont authentiques et qu'il n'y a pas d'erreurs à récupérer.

5.4.2.4 Analyse de la capacité de reconstruction

Afin d'estimer la capacité de la méthode proposée à corriger les pixels altérés, nous calculons la capacité de récupération T_R en utilisant l'équation suivante :

$$T_R = \frac{N_R}{N_{total}} \times 100. \tag{5.5}$$

1. https ://medpix.nlm.nih.gov/

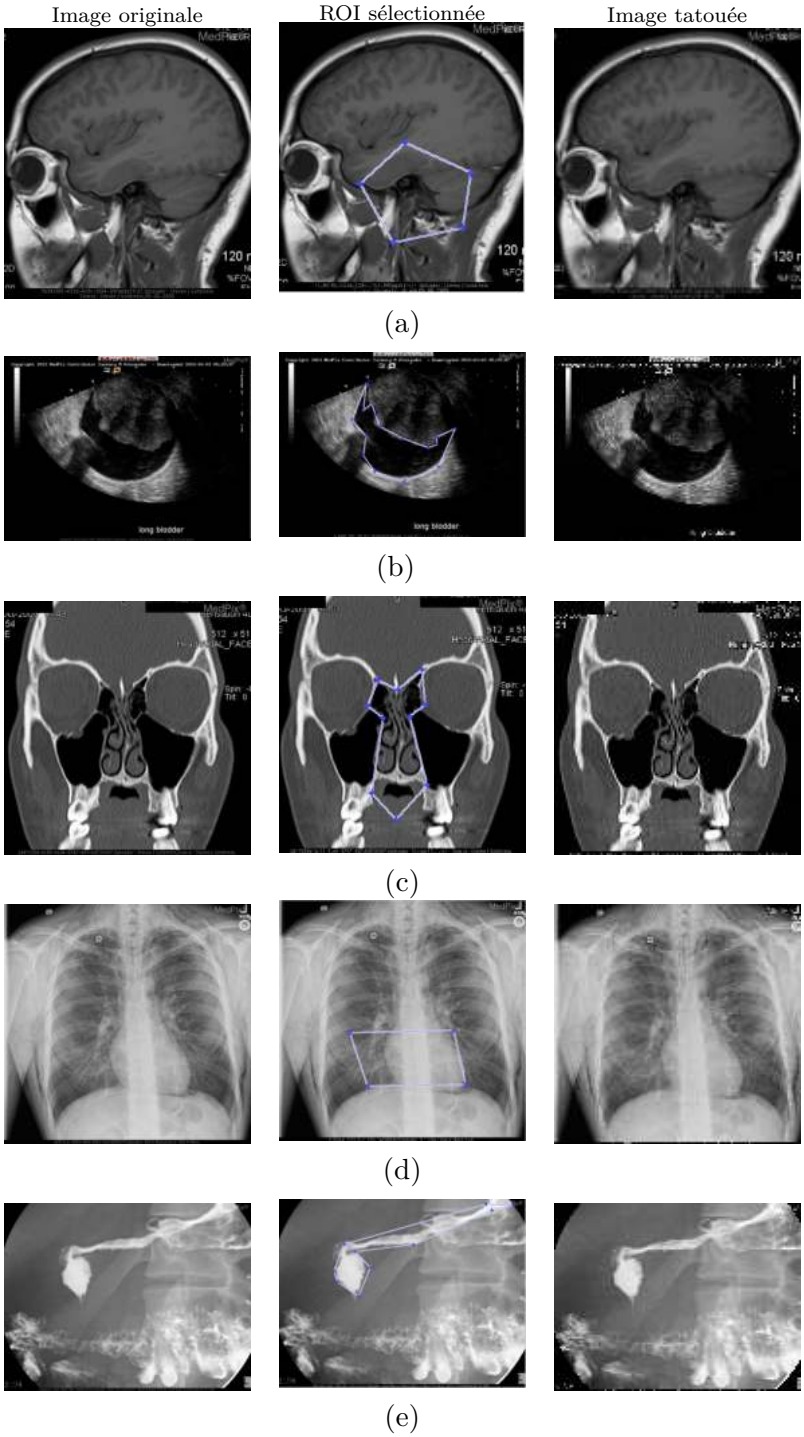


FIGURE 5.17: Images médicales originales, ROI sélectionnées et images tatouées : (a) MRI scan , (b) US , (c) CT , (d) XR et (e) UGI.

Où N_R est le nombre de paquets altérés et reconstruits et N_{total} est le nombre total des paquets altérés.

La capacité de la méthode proposée à extraire le watermark (NC) et à récupérer la ROI (T_R) après différents types de bruit est illustrée dans la Figure 5.19. Ces graphiques montrent la relation entre l'augmentation du nombre d'erreurs et la capacité d'extraire le watermark et de récupérer les pixels altérés dans le ROI.

Les résultats démontrent que pour différentes modalités, les courbes NC descendent le plus

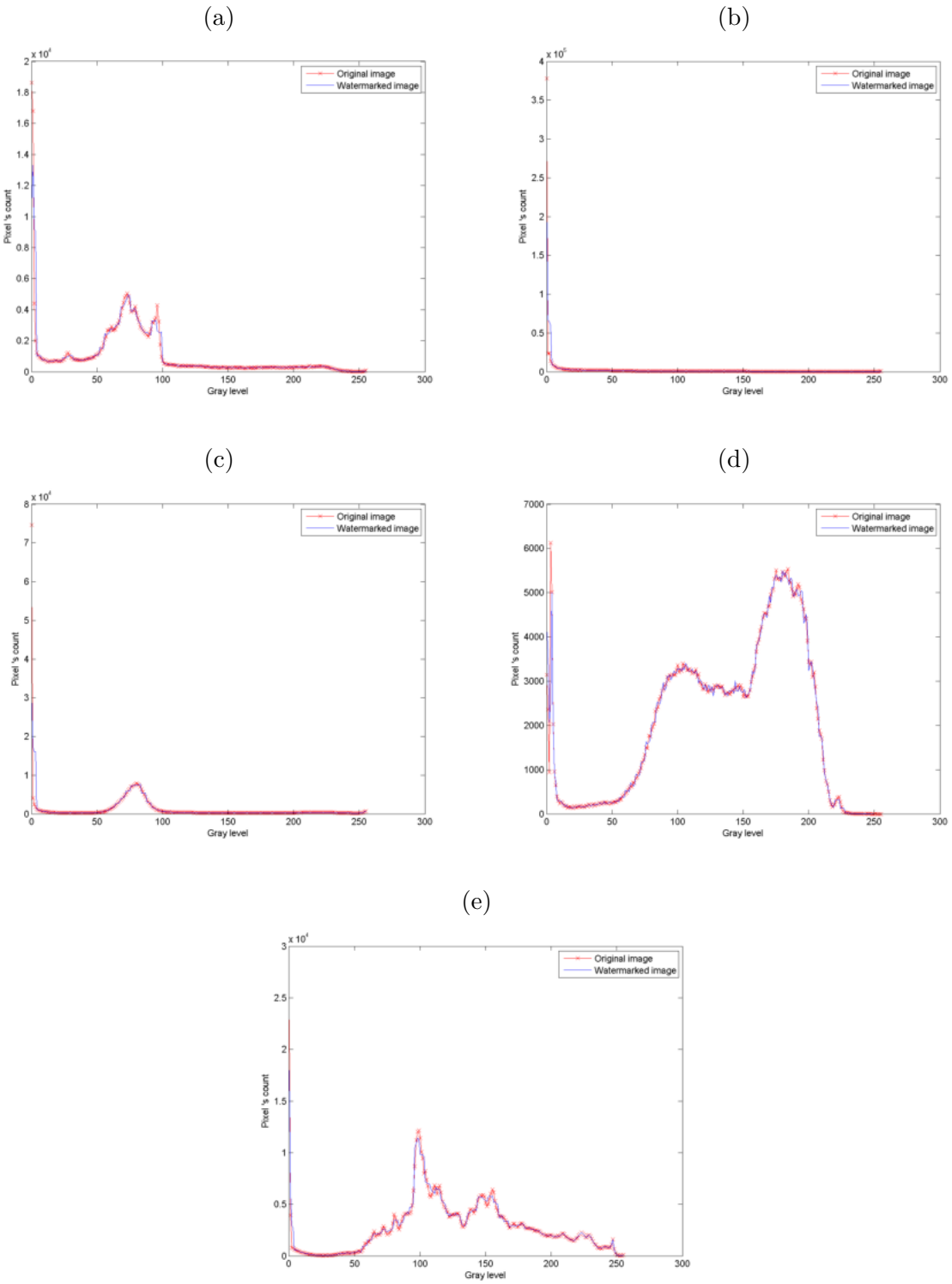


FIGURE 5.18: Analyse de l'imperceptibilité à travers des histogrammes pour différentes modalités : (a) MRI scan , (b) US , (c) CT , (d) XR et (e) UGI.

lentement en augmentant la distorsion dans RONI. Donc, cette descente lente est interprétée par une bonne robustesse contre les attaques de bruit.

Jusqu'à un taux de distorsion égal à 15%, en général le schéma proposé peut récupérer exactement le retour sur investissement ($T_R = 100\%$) après le bruit du sel et des poivrons. Pour

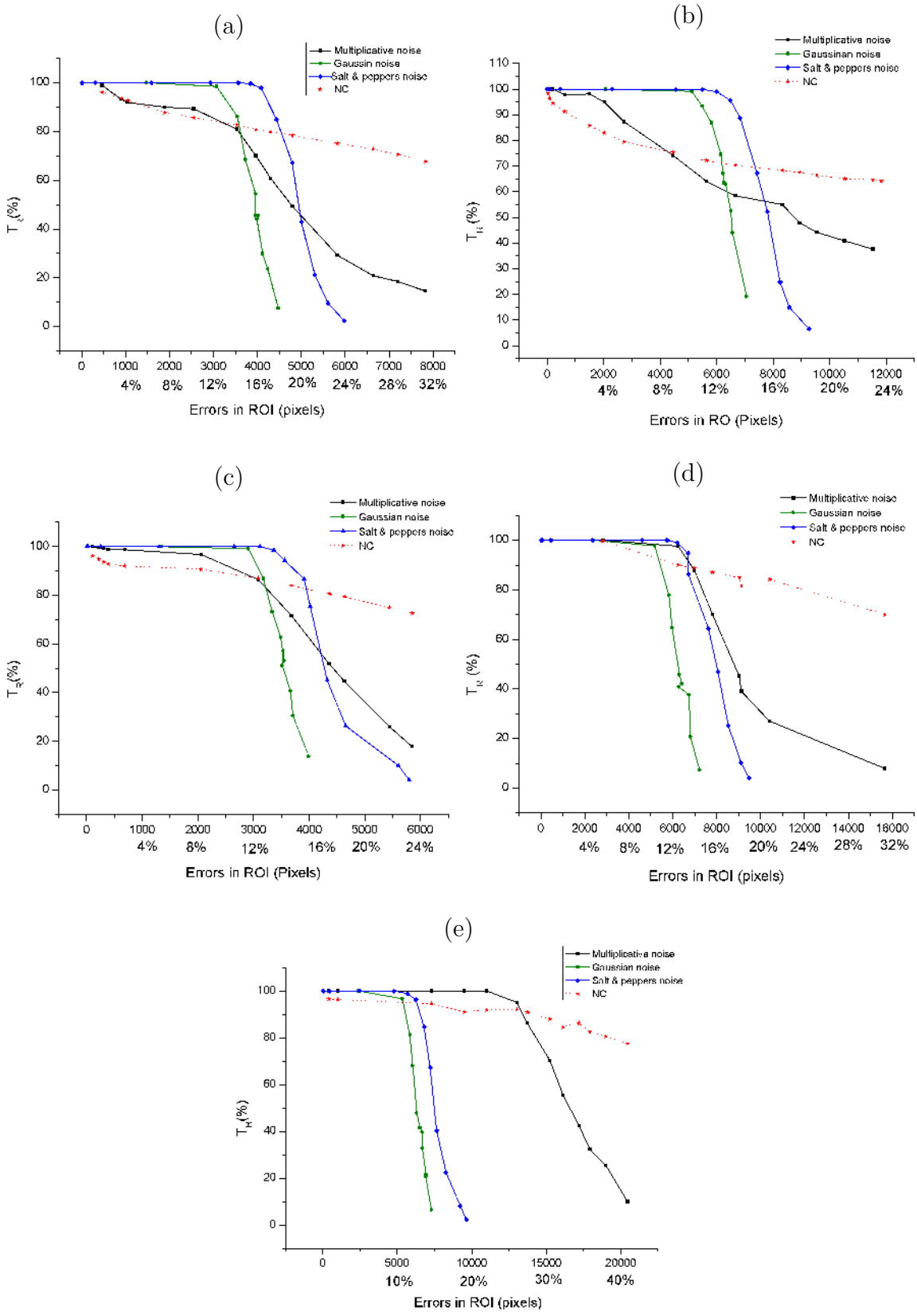


FIGURE 5.19: Performances contre différents types de bruit pour différentes modalités :(a) MRI scan , (b) US , (c) CT , (d) XR et (e) UGI.

les autres types de bruit, le système a une bonne capacité de récupération ($T_R \in [70 - 100]$). Après ce taux de distorsion (15%), le T_R diminue avec l'augmentation de la distorsion et il peut récupérer 50% de la ROI à 20% de distorsion. Nous pouvons observer que jusqu'à 15 % de distorsion, la capacité de récupération de la ROI sous le bruit de sel et de poivre est meilleure que le bruit gaussien et le bruit multiplicatif. Après ce taux, la capacité de récupération contre le bruit multiplicatif devient meilleure que les autres.

Afin de présenter visuellement la performance contre les attaques de bruit, la Figure 5.20 illustre les images attaquées, les cartes de détection des altérations et les ROIs récupérées après certaines attaques. La carte de détection affiche avec une couleur noire les pixels altérés dans la ROI et avec une couleur blanche les pixels non altérés.

Le système proposé peut également récupérer la ROI après des opérations de copie, re-cadrage et certaines attaques de traitement. La Figure 5.21 présente les performances contre ces attaques.

5.4.2.5 Analyse comparative

Nous comparons les capacités de notre système avec les approches similaires. Le Tableau 5.6 illustre une analyse comparative des schémas de tatouage des images médicales basées sur la ROI.

	Méthode proposée	Eswaraiah [Eswaraiah and Reddy, 2014]	Memon [Memon et al., 2011]	Al-Qershi [Al-Qershi and Khoo, 2011a]
Objectif	Détection d'altérations	Détection d'altérations	Dissimulation d'information & Détection d'altérations	Dissimulation d'information & Détection d'altérations
Fonction de reconstruction	✓	✓	✗	✓
Reconstruction de la ROI	Exactement	Exactement (lorsque la RONI n'est altérée)	✗	Forme compressée
Intégrité de la ROI	✓	✓	✗	✗
Domaine d'insertion	LWT	LSB	IWT	DWT
Imperceptibilité	Bonne	Bonne	très bonne	Acceptable pour les images 8-bits
Robustesse	✓ différent types de bruit noise, copie , re-cadrage	✗ -	✗ -	✓ Sel et poivre & cropping
Sécurité	Clé secrète	Clé secrète	Clé secrète	RSA
Capacité	2 bpp	2 bpp	Adaptative 1 to 4 bpp	0.48 bpp
Taille ROI	Plus petit que la RONI	Plus petit que la RONI	Plus petit que la RONI	Plus petit que la RONI

TABLE 5.6: Analyse comparative des approches de tatouage d'images médicales basées sur la ROI.

Nous pouvons observer que le schéma [Al-Qershi and Khoo, 2011a] est robuste contre

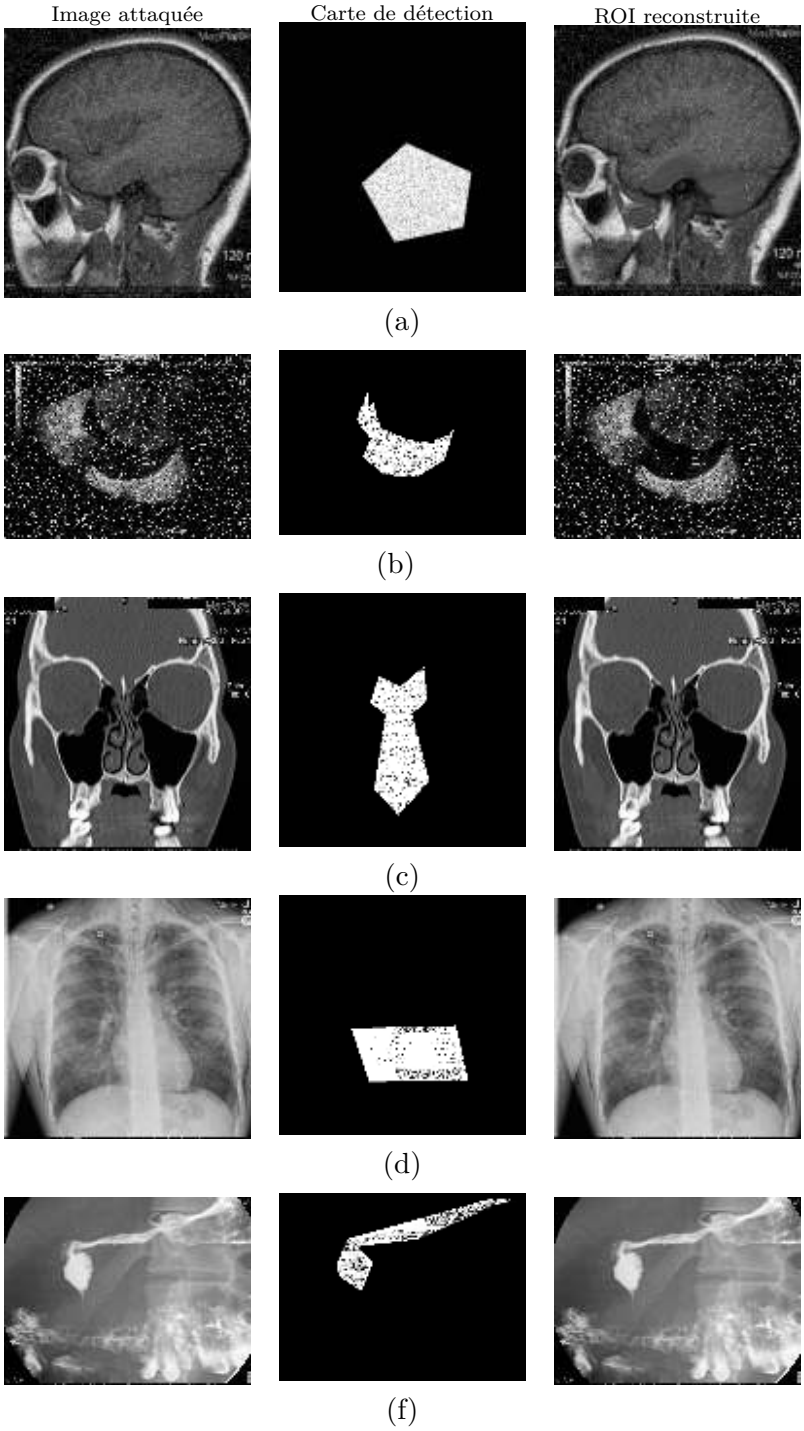


FIGURE 5.20: ROIs récupérées après les attaques de bruit : (a) Bruit Salt & Peppers : $NC = 0.8672$, $T_R = 100\%$. (b) Bruit Salt & Peppers : $NC = 0.8037$, $T_R = 85.59\%$, (c) Bruit Gaussian : $NC = 0.7793$, $T_R = 62.8422\%$, (d) Bruit Multiplicatif : $NC = 0.7010$, $T_R = 42.05\%$ et (e) Bruit Multiplicative : $NC = 0.7576$, $T_R = 66.56\%$.

certaines attaques mais il est basé sur la moyenne de chaque bloc pour déceler les altérations. Ce dernier problème est résolu dans [Eswaraiah and Reddy, 2014] en utilisant également la variance de chaque bloc pour détecter les blocs altérés. Le schéma [Eswaraiah and Reddy, 2014] a une bonne imperceptibilité mais il n'est pas robuste contre les attaques.

Le point fort de notre travail est de combiner tous ces schémas afin d'obtenir de meilleures

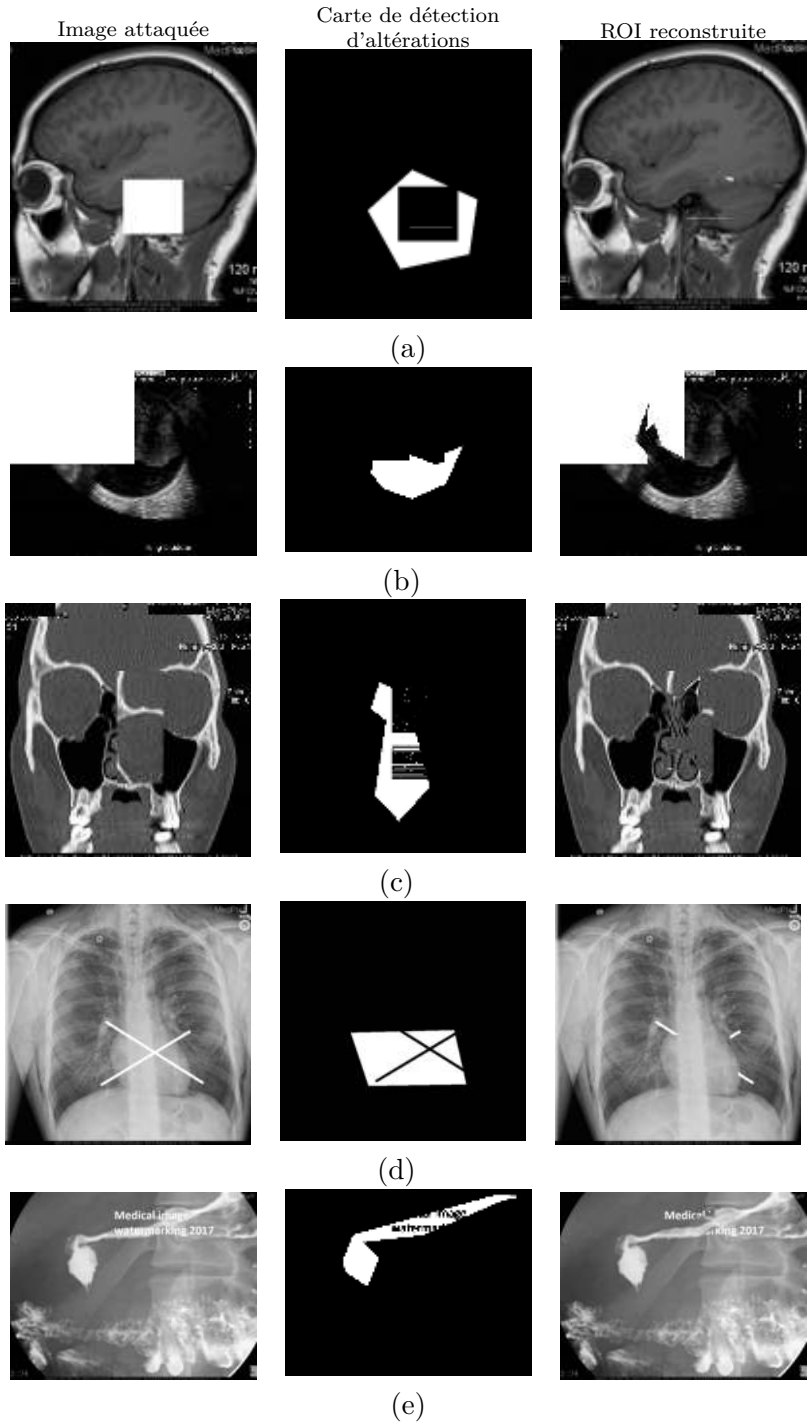


FIGURE 5.21: ROI récupérée après les opérations de re-cadrage, de copie et de traitement : (a) Re-cadrage 8% : NC=0.9992, $T_R = 99.36\%$, (b) Re-cadrage25% : NC=0.5459, $T_R = 80.67\%$, (c) Copie 8% : NC= 0.9454, $T_R = 100\%$ (d) et (e) Opérations de traitement.

performances en termes de :

- L'imperceptibilité : le watermark est intégré dans le LSB de chaque coefficient. Donc, de bonnes valeurs de PSNR sont obtenues.
- La robustesse contre les attaques en intégrant le watermark dans les coefficients LWT.
- La capacité d'insertion : 2 bpp.
- La reconstruction : capacité de tolérer une grande modification dans la ROI.

- L'intégrité de la ROI : la ROI n'est pas affectée par le processus d'insertion.
- Travailler sur différentes modalités avec différentes tailles.
- Flexibilité de sélection de la ROI.

5.5 Conclusion

Dans ce chapitre, nous avons proposé deux nouvelles approches de tatouage numérique utilisant le code CRC et RS. La première approche est une technique de tatouage fragile qui permet de détecter les altérations dans la ROI. Dans cette stratégie, l'utilisateur sélectionne tout d'abord la ROI à protéger. Ensuite, cette région est décomposée en paquets et la procédure de codage CRC est exécutée sur chaque paquet pour générer le checksum considéré comme un watermark à insérer dans des LSB de chaque pixel correspondant dans ROI. A la réception, le récepteur extrait le watermark et exécute le décodage CRC pour détecter les pixels altérés. La performance de notre méthode dépend du degré de polynôme générateur. Nous avons choisi le générateur standard de degré 32 (CRC-32) qui est connu par sa bonne capacité à détecter les erreurs. Les résultats expérimentaux montrent que notre schéma donne un bon compromis entre l'imperceptibilité et la fragilité.

Une deuxième approche de tatouage zéro-bit est proposée pour la détection et la récupération de la ROI. Tout d'abord, l'utilisateur sélectionne la ROI à protéger et stocke les sommets comme clé secrète. Ensuite, cette région est décomposée en paquets et un codage RS est effectué sur chaque paquet pour générer le SS qui est utilisé comme watermark à incorporer dans le domaine fréquentiel de RONI en utilisant la transformée LWT. A la réception, le récepteur décompose l'image en ROI et RONI en utilisant la même clé secrète. Les SS sont extraits de RONI et combinés avec la MS correspondante. Le codeur RS est exécuté à cette nouvelle séquence.

Les résultats expérimentaux montrent que cette approche produit une bonne performance en termes d'imperceptibilité où la valeur de PSNR est dans la gamme de 47 dB et de robustesse contre une altération importante où elle peut récupérer strictement le ROI après l'insertion de bruit dur.

Dans les prochains travaux, nous nous attendons à renforcer la robustesse contre d'autres types d'attaques comme JPEG et augmenter la capacité de tatouage dans le but d'élargir également la taille du la ROI.

En outre, nous allons également travailler davantage sur notre système pour protéger la transmission d'images médicales dans un environnement mobile, car RS est très recommandé dans la communication mobile.

Chapitre 6

Nouvelle approche de tatouage de deuxième génération basée sur VD

Sommaire

6.1 Introduction

Le développement des réseaux de communication et des supports numériques a encouragé l'utilisation des réseaux informatiques pour la transmission des informations numériques. Plusieurs organisations, à la fois publiques et privées, ont remplacé leurs dossiers, dispersés et tenus manuellement, par des systèmes informatiques leur offrant un meilleur accès aux données. Ce qui a posé le problème de la sécurité de ces données.

Dans ce contexte un schéma de tatouage fragile de permière génération appliqué à images couleurs est proposé [Golea, 2010, Golea, 2012]. Le principe de ce schéma est basé sur l'utilisation du code CRC pour détecter les pixels modifiés. Le contrôle de redondance cyclique (noté CRC, ou en anglais Cyclic Redundancy Check) est un moyen de contrôle d'intégrité des données puissant et facile à mettre en œuvre. Il représente la méthode principale de détection d'erreurs utilisée dans les télécommunications. Pour ces raisons, nous avons choisi de l'utiliser dans le contexte du tatouage fragile dans le but de savoir si l'image a subi des modifications ou pas.

En utilisant le CRC, les séquences binaires sont traitées comme des polynômes dont les coefficients correspondents à la séquence binaire. Nous ajoutons à la séquence binaire le reste d'une division polynomiale par un polynôme générateur. A la réception, le reste de la division reçu et le reste de la division calculé doit être null ou alors il y a erreur de transmission.

Notre schéma de tatouage de première génération est composé de trois phases. La première phase consiste à générer un watermark de taille 6 qui dépend des 18 bits MSB des trois pixels R,G et B en utilisant une clé secrète K. La deuxième phase consiste à insérer respectivement deux bits du watermark dans les deux bits LSB des pixels R, G et B. La dernière phase consiste à détecter si l'image tatouée a subi des modifications. Si le reste de la division du message reçu (18 bits MSB des trois pixels R,G et B concaténés avec les 6 bits du CRC) sur la clé secrète K est égale à zéro, alors l'image est authentique à l'image originale, sinon elle ne l'est pas.

En fait, le paramètre le plus important dans la détection des erreurs d'un flux de messages est la sélection du polynôme générateur. Pour pallier le problème de génération d'un polynôme générateur de petit degré, nous proposons une nouvelle approche de tatouage de deuxième génération en utilisant le VD et des polynômes standard de degré élevée ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans chaque région de l'image après une décomposition en utilisant les Diagrammes de Voronoi VD. nous avons proposé une nouvelle approche de tatouage de deuxième génération basée sur les DVs et le code CRC en utilisant des polynômes standard de degré élevée ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans chaque région de l'image après une décomposition en utilisant les Diagrammes de Voronoi VD. La décomposition de Voronoi est employée car elle a de bonnes performances de récupération comparée à des algorithmes de décomposition géométrique similaires. Le détecteur de Harris est utilisé pour extraire les points d'intérêts (FPs) considérés comme des germes pour créer une décomposition de Voronoi de l'image. La méthode proposée peut être applicable dans le cas où la détection de altération est critique et seules certaines régions d'intérêt doivent être retransmises si elles sont altérées, comme dans le cas des images médicales. L'aspect de sécurité de notre méthode proposée est atteint en utilisant le système de cryptage à clé publique RSA pour crypter les FPs. Les résultats expérimentaux prouvent l'impact de la décomposition VD sur la qualité des images tatouées par rapport à la décomposition en blocs.

Dans ce chapitre, nous présentons le principe du schéma proposé, les résultats expérimentaux ainsi que l'approche basée sur les DVs proposée.

6.2 Approche de tatouage fragile de première génération basée sur le CRC

La méthode proposée est décomposée de quatre algorithmes : Algorithme de génération de P_x (polynôme générateur), algorithme de génération du watermark, algorithme d'insertion du watermark et algorithme d'extraction & détection. Le modèle général de notre méthode est présenté dans la Figure 6.1.

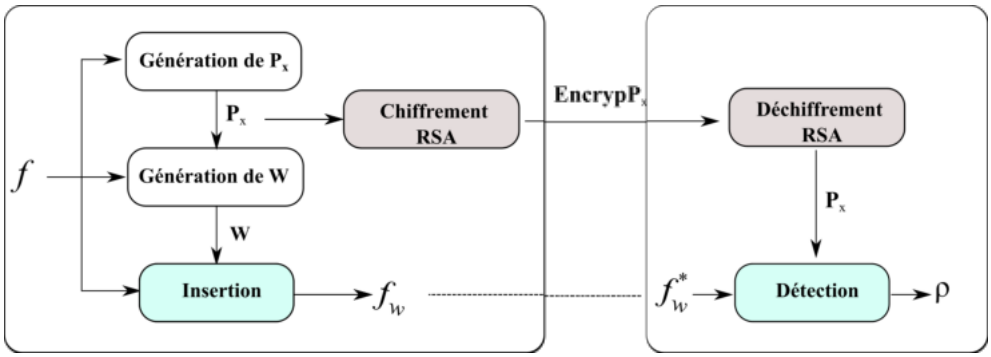


FIGURE 6.1: Modèle proposé

L'algorithme de génération de P_x crée une matrice P_x de même taille que l'image originale f. Cette fonction est décrite par $Generator_Px$:

$$P_X = Generator_{P_X}(f, d). \tag{6.1}$$

Chaque élément de P_x est un polynôme de degré d où $d \leq 6$.

L'algorithme de génération du watermark génère une signature qui contient les informations du watermark, en prenant l'image hôte originale f et un polynôme générateur P_X. Cet algorithme est décrit par la fonction $GeneratorW$:

$$W = Generator_W(f, P_X) \tag{6.2}$$

L'algorithme d'insertion prend la signature W et l'image hôte f, et génère l'image tatouée f_w, décrite par la fonction E :

$$f_w = E(f, W). \tag{6.3}$$

L'algorithme de détection prend l'image tatouée et éventuellement attaquée f_w^* et P_X, et calcule la mesure ρ. Le processus est décrit par la fonction D :

$$\rho = D(f_w^*, P_X) \tag{6.4}$$

si $\rho = 0$ alors le pixel n'est pas altéré, sinon il est altéré. Le polynôme générateur P_X doit être chiffré à l'aide d'une clé secrète K_S et en exécutant l'algorithme de chiffrement à clé asymétrique (RSA). A la réception, le récepteur doit déchiffrer le polynôme générateur P_{cryp} en utilisant la clé publique K_P et en exécutant l'algorithme *Decrypted*.

6.2.1 Méthodologie proposée

6.2.1.1 Génération de générateur polynômial

L'Algorithme 6.1 permet de créer une matrice P_X de même taille de l'image hôte f, chaque élément $P_X(i,j)$ de cette matrice est un polynôme générateur utilisé pour calculer le checksum CRC correspondant au pixel $f(i,j)$.

Algorithme 6.1 Génération de la matrice P_X

Entrées :

- $n \times m$: taille de l'image originale f ;
- d : dégrée du générateur polynomial, c'est à dire le nombre maximal de bits utilisés pour insérer le watermark (dans ce cas $d \leq 6$).

Sorties :

- P_X : matrice des générateurs polynomiaux de taille $n \times m$.

Étapes :

- Pour $i = 1$ à n faire :
  - Pour $j = 1$ à m faire :
    1. Génération aléatoirement d'une séquence binaire g de taille $d+1$:

$$g = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7\}.$$

    2. Calculer P_X comme suit :

$$P_X(i,j) = g_1X^6 + g_2X^5 + g_3X^4 + g_4X^3 + g_5X^2 + g_6X^1 + g_7X^0. \quad (6.5)$$

Pour crypter et décrypter la matrice P_X, nous proposons d'utiliser l'algorithme RSA (nommé pour ses inventeurs, Ron Rivest, Adi Shamir, et Leonard Adleman). Le système cryptographique RSA est l'algorithme de cryptographie à clé publique le plus largement utilisé. Il peut être utilisé pour crypter un message sans avoir besoin d'échanger une clé secrète séparément. L'algorithme RSA peut être utilisé pour le chiffrement à clé publique et les signatures numériques. Sa sécurité est basée sur la difficulté de factoriser de grands entiers.

6.2.1.2 Algorithme de génération du watermark

Cette phase génère un watermark de taille 6 bits qui dépend des 18 bits MSB des trois pixels R, G et B correspondants (voir Figure 6.2). Le détail de cet algorithme est présenté par l'Algorithme 6.2.

Algorithme 6.2 Génération du watermark W

Entrées :

- f : Image hôte (une image couleur RGB de taille $n \times m$).
- P_X : matrice de taille $n \times m$.

Sortie :

- W : matrice de taille $n \times m$, où chaque élément $W(i,j)$ est une séquence binaire de taille 6 bits $\{W_1, \cdots, W_6\}$.

Étapes :

- Pour chaque pixel $R(i,j)$, $G(i,j)$ et $B(i,j)$ faire :
  1. Construction de message M à transmettre à partir des trois pixels $R(i,j)$, $G(i,j)$ et $B(i,j)$ par la concaténation des 6 bits MSB.
  2. Application de l'algorithme CRC :
     - Adjonction de d bits nuls à M (dans notre cas en ajoute 6 bits)
     - Le watermark $W(i,j)$ est égal au reste de la division (en binaire = opération XOR) de $M(i,j)$ par $P_X(i,j)$.

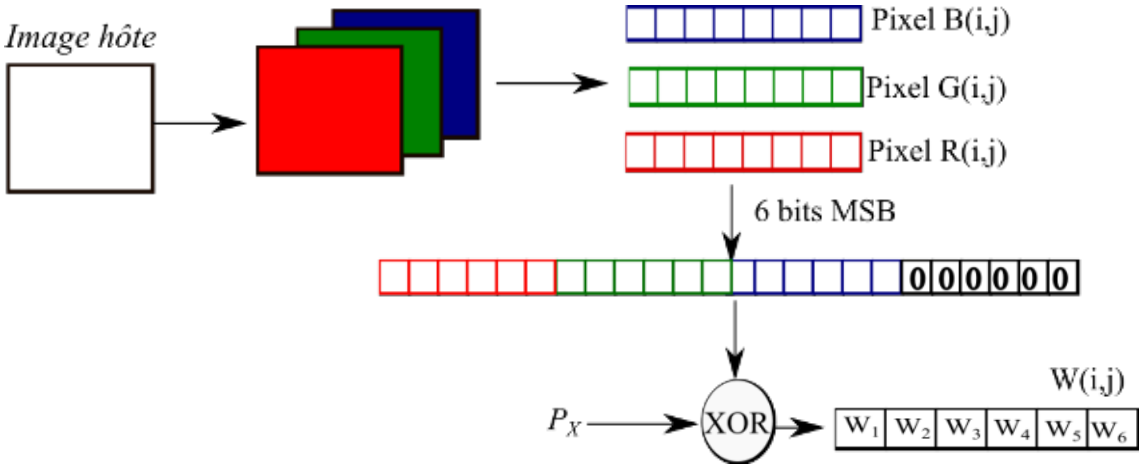


FIGURE 6.2: Processus de génération du watermark.

6.2.1.3 Algorithme d'insertion

Dans l'algorithme 6.3, le watermark généré précédemment est inséré dans les deux bits LSB des trois pixels R, G et B correspondants (voir Figure 6.3). Le principe de cet algorithme est présenté ci-dessous.

Algorithme 6.3 Insertion du watermark

Entrées :

- f : Image hôte (image couleur RGB) de taille $n \times m$.
- W : watermark de taille $n \times m$.

Sortie :

- f_w : image tatouée de taille $n \times m$.

Étapes :

- Pour chaque pixel $R(i,j)$, $G(i,j)$ et $B(i,j)$ faire :
  1. Remplacer les deux bits LSB de $R(i,j)$ par les deux premiers bits de $W(i,j)$.
  2. Remplacer les deux bits LSB de $G(i,j)$ par les deux bits suivants de $W(i,j)$.
  3. Remplacer les deux bits LSB de $B(i,j)$ par les deux derniers bits de $W(i,j)$.

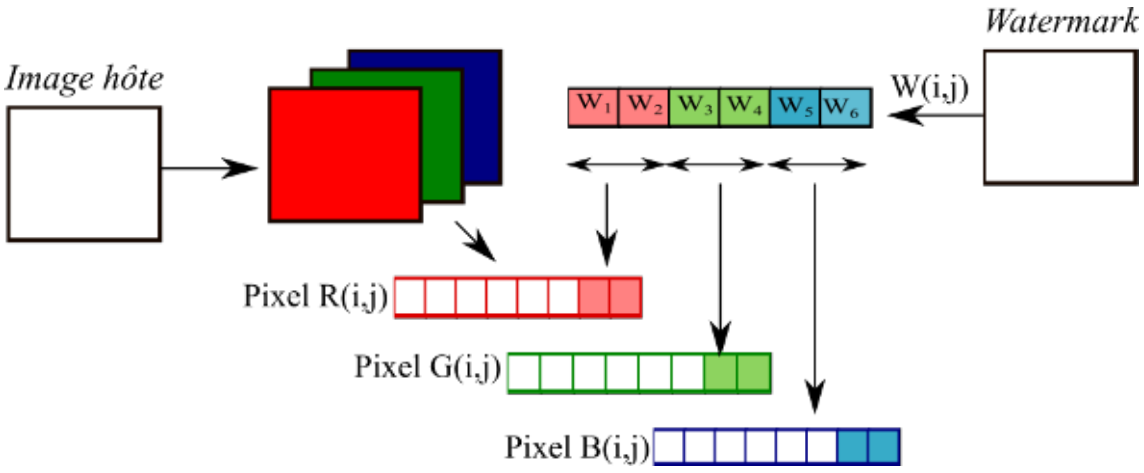


FIGURE 6.3: Processus d'insertion du W.

6.2.1.4 Algorithme de détection

Dans la phase d'extraction (Algorithme 6.4), les 6 bits MSB des trois pixels R, G et B concaténés avec le CRC sont divisés sur la clé k, si le reste de cette division est égale à 0 alors le pixel n'est pas attaqué, sinon il est attaqué (voir Figure 6.4).

Algorithme 6.4 Extraction du watermak et détection des altérations

Entrées :

- f_w : Image tatouée (image couleur RGB de taille $n \times m$).
- P_X : matrices du polynôme générateur $n \times m$.

Sortie :

- ρ : mesure de confidentialité.

Étapes :

- Pour chaque pixel $R(i,j)$, $G(i,j)$ et $B(i,j)$ faire :
  1. Construction de message M^* reçu à partir des trois pixels $R(i,j)$, $G(i,j)$ et $B(i,j)$ par la concaténation des 6 bits MSBs de chacun d'eux.
  2. Extraction du watermark $W(i,j)$: IL est obtenu par la concaténation des 2 bits LSB de chaque pixel.
  3. Application de l'algorithme CRC :
     - Adjonction des d bits de $W(i,j)$ à M^*.
     - Calculer ρ : le reste de la division de M^* par P_X.
       - Si $\rho = 0$ alors le pixel (i,j) n'est pas altéré.
       - Sinon, il est altéré.

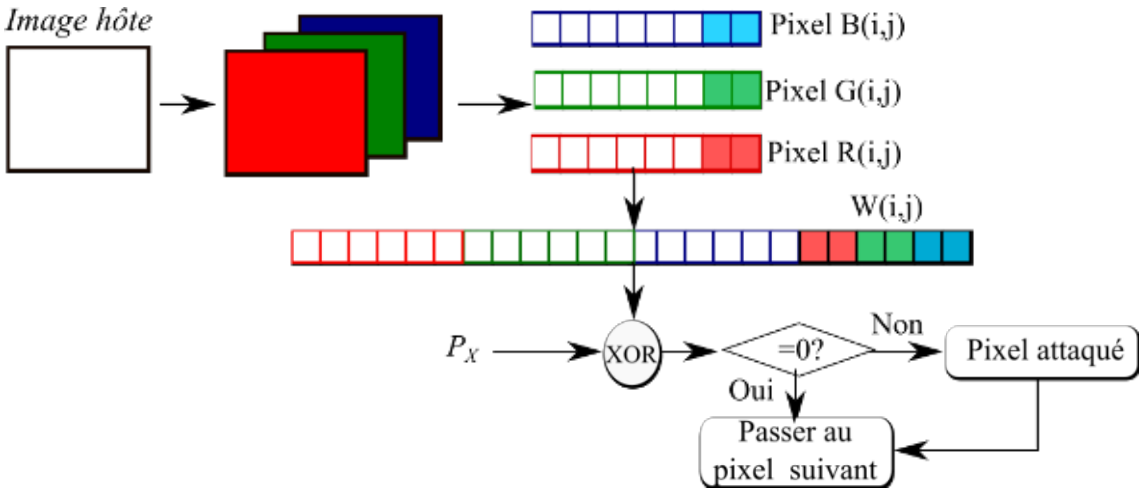


FIGURE 6.4: Processus d'extraction du W et détection des altérations.

6.2.2 Résultats expérimentaux

Dans cette section, nous démontrons principalement l'imperceptibilité et la fragilité de notre méthode de tatouage. Les résultats expérimentaux rapportés ici ont été séparés en deux parties : la première est pour tester la propriété d'imperceptibilité et l'autre est pour évaluer la fragilité à des manipulations malveillantes.

6.2.2.1 Analyse de l'imperceptibilité

Afin de tester la propriété d'imperceptibilité de notre méthode de tatouage, plusieurs images couleur RGB avec différentes tailles 128×128, 256×256 et 1024×1024 ont été tatouées. Ces images hôtes originales avec leurs images tatouées ont été respectivement représentées sur la Figure 6.5 et la Figure 6.6. A partir de ces images, nous pouvons remarquer que les différences entre les images originales et leurs images tatouées correspondantes sont difficiles à percevoir par les yeux humains.

FIGURE 6.5: Images hôtes f.

Nous avons jugé utile de présenter aussi le PSNR entre les images originales et tatouées afin de déterminer le degré de dégradation de l'image tatouée. Le Tableau 6.1 présente les valeurs de PSNR.

Host image	PSNR	Host image	PSNR
Lena	47.2578	House	47.4048
Tree	47.2048	Airplane	47.2914
Splash	47.0813	Peppers	47.2557
Jelly beans	47.1444	Girl	47.2048
Sailboat on lake	47.2407	Baboon	47.2633
Fatma Nessoumer	47.2853	Benbadis	47.4061
Emir Abedel Kader	47.2658	Logo	47.2109

TABLE 6.1: Qualité des images tatouées via les métriques $PSNR$ et $SSIM$.

D'après cette dernière table 6.1, il est claire que les valeurs de PSNR sont très bonnes, ce qui signifie que notre méthode de tatouage maintient une haute qualité d'images tatouées.

FIGURE 6.6: Images tatouées f_w.

6.2.2.2 Analyse d'exactitude et de la fragilité

La validité de toute technique de tatouage ne peut prendre de l'importance que si elle résiste à différents types d'attaques. Pour ceci, nous avons choisi de faire subir à chaque image tatouée un ensemble d'attaques et de vérifier la sensibilité aux modifications ainsi que son aptitude de détecter toute transformation dans l'image.

L'image CRC est la matrice des restes de la division, elle est calculée afin de montrer si l'image est modifiée ou non (si la matrice est égale à 0 donc l'image n'est pas modifiée, sinon elle est modifiée).

La Figure 6.7 présente certaines images CRC extraites à partir des trois premières images tatouées *Lena*, *House* et *Tree* dans le cas d'absence d'attaque.

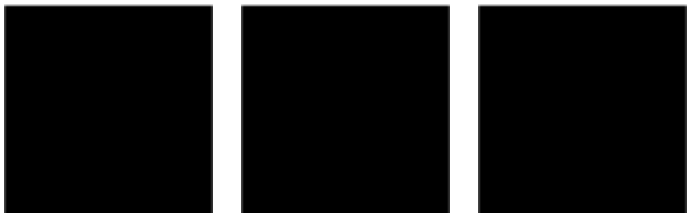


FIGURE 6.7: Images CRC extraites à partir des trois premières images tatouées *Lena*, *House* et *Tree* dans le cas d'absence d'attaque.

En effet, nous avons appliqué des attaques de natures diverses sur l'image tatouée *House* et nous avons mesuré l'efficacité de notre technique et son aptitude à détecter toute anomalie dans l'image. La Figure 6.8 présente la fragilité contre deux attaques géométriques : la rotation et le redimensionnement.

Les images CRC contient des pixels blancs ce qui signifie les pixels altérés. Nous pouvons noter que notre méthode est très efficace contre les opérations de redimensionnement et de

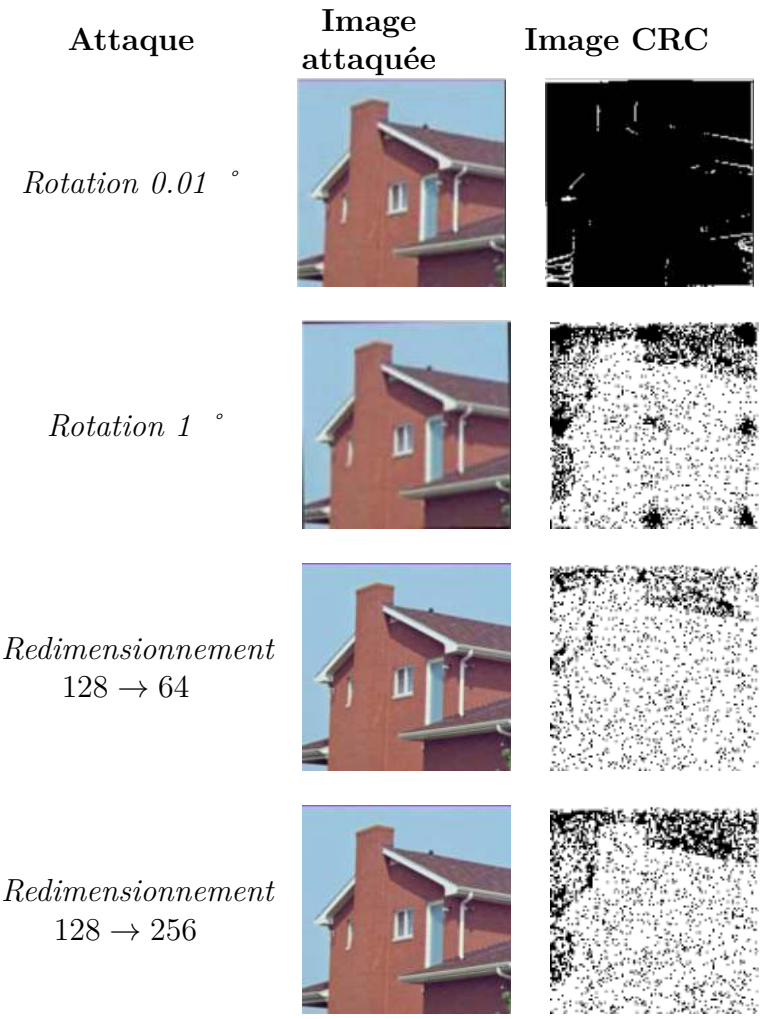


FIGURE 6.8: Fragilité contre les attaques géométriques *Rotation* et *Redimensionnement*.

rotation, même avec de très petits angles de rotations.

L'image tatouée est compressée avec divers facteurs pour tester la fragilité de notre méthode contre la compression JPEG. La Figure 6.9 illustre les images CRC extraites après une compression JPEG.

6.3 Nouvelle approche de tatouage fragile de deuxième génération basée sur le CRC et les Diagrammes de Voronoi

L'approche décrite précédemment authentifie les images RGB en utilisant le code CRC. Cependant, le degré du polynôme générateur est très petit et ne dépasse pas six. En fait, le paramètre le plus important dans la détection des erreurs d'un flux de messages est la sélection du polynôme générateur.

Pour pallier cette insuffisance et élargir le degré de polynôme générateur, nous proposons une technique de tatouage fragile par blocs utilisant un générateur polynomial standard $G(x)$ ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans de petits blocs de l'image après une décomposition

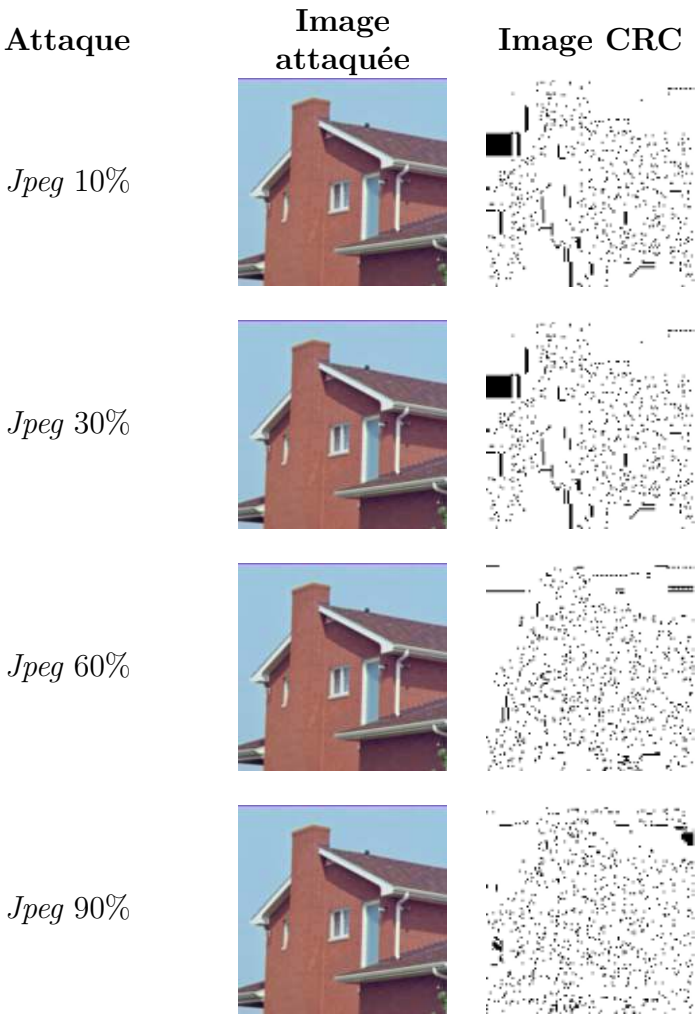


FIGURE 6.9: Fragilité contre la compression JPEG.

en bloc. Nous avons montré par des tests que la décomposition en bloc pose un problème de dégradation de la qualité des images tatouées. Pour cette raison, nous avons proposé une nouvelle décomposition en utilisant les Diagramme de Voronoi [Golea and Melkemi,].

Nous avons commencé d'abord par une approche à base d'une décomposition en blocs.

La Figure 6.10 présente l'image *Lena* tatouée en utilisant le CRC-32, différentes tailles ont été prises en considération 128×128, 256×256 et 512×512.

128×128	256×256	512×512
PSNR=32.00%	$PSNR = 33.25\%$	$PSNR = 35.23\%$

FIGURE 6.10: Tatouage fragile avec CRC-32, impact de la décomposition en blocs sur la qualité de l'image tatouée.

Il est clair que la décomposition en blocs génère les effets de mosaïque. Pour résoudre ce problème, nous avons proposé une nouvelle décomposition en utilisant les Diagrammes de Voronoi.

Notre système génère des segments liés aux valeurs d'intensité en utilisant les informations des sommets de la frontière externe de VD. Ainsi, l'image est décomposée en un ensemble de polygones, où les points d'intérêts (FPs) extraits sont les germes. Le Watermark généré est intégré dans chaque pixel de chaque segment.

6.3.1 Méthodologie proposée

La méthode proposée est décrite par trois algorithmes : les algorithmes de génération du watermark, d'insertion et de vérification. Ces algorithmes sont basés sur le CRC pour générer, insérer et extraire le watermark.

6.3.1.1 Algorithme de génération du watermark

Algorithme 6.5 Algorithme de génération du watermark utilisant le DV

Entrée :

- f : image originale.

Sorties :

- W : watermark.
- FP_{Cryp} : ensemble de FPs chiffré.

Étapes :

1. Sélectionner un ensemble de N points d'intérêt $FP = \{p_1, p_2, \ldots, p_N\}$ utilisant le détecteur de Harris
2. Chiffrer cet ensemble avec RSA.
3. Décomposer l'image f par la création de N région de voronoi (VR) utilisant FP comme germes. Chaque région $VR(p_i)$ est considérée comme un message à transmettre.
4. Pour chaque message $VR(p_i)$ faire :
   - Diviser le message $VR(p_i)$ en X paquets de taille $S_j = \{16, 8, 4, 2 \text{ or } 1\}$, où j est le nombre de paquets.
     Par exemple, si le premier message $VR(p_1)$ est composé de 47 pixels, $VR(p_1) = \{f_1, \ldots, f_{47}\}$. Les X paquets sont :
     - $X_1 = \{f_1, \ldots, f_{16}\}$ de taille $S_1 = 16 \Rightarrow G(x)$ de degré 32, CRC(32) ;
     - $X_2 = \{f_{17}, \ldots, f_{32}\}$ de taille $S_2 = 16 \Rightarrow G(x)$ de degré 32, CRC(32) ;
     - $X_3 = \{f_{33}, \ldots, f_{40}\}$ de taille $S_3 = 8 \Rightarrow G(x)$ de degré, CRC(16) ;
     - $X_4 = \{f_{41}, \ldots, f_{44}\}$ de taille $S_4 = 4 \Rightarrow G(x)$ de degré, CRC(8) ;
     - $X_5 = \{f_{45}, \ldots, f_{46}\}$ de taille $S_5 = 2 \Rightarrow G(x)$ de degré, CRC(4) ;
     - $X_6 = \{f_{47}\}$ de taille $S_6 = 1 \Rightarrow G(x)$ de degré, CRC(2) ;
   - Pour chaque paquet X_j de taille S_j faire :
     - Extraire les six bits MSB de chaque pixel.
     - Concaténer ces bits ensemble pour créer la séquence m.
     - Ajouter $2 \times S_j$ zéros bits à la fin de m pour créer m'. Cela est équivalent à $m' = m \times x^{2 \times S_j}$
     - Le watermark W_j^i est le reste de la division de m' par un CRC normalisé de degré $d = 2 \times S_j$.

6.3.1.2 Algorithme d'insertion

L'algorithme suivant décrit la façon dont le watermark W est inséré dans l'image hôte f (Figure 6.12).

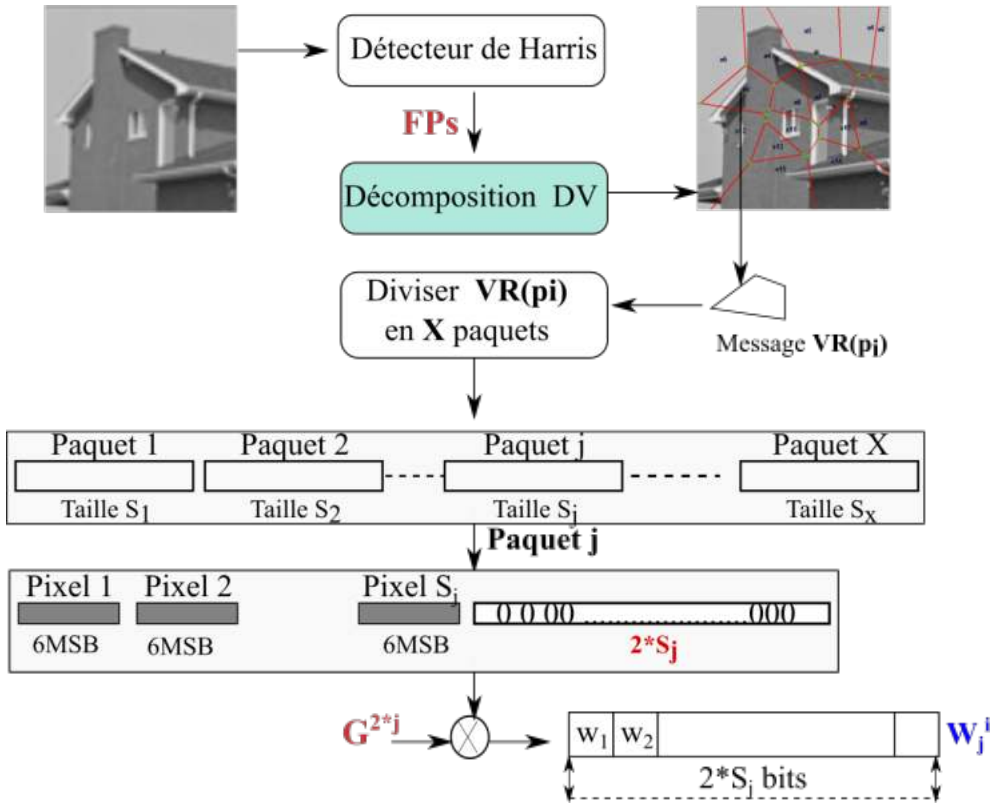


FIGURE 6.11: Processus de génération du Watermark utilisant la décomposition de DV.

Algorithme 6.6 Algorithme d'insertion basé sur la DV.

Entrées :

- f : image originale.
- W : watermark généré.

Sortie :

- f_w : image tatouée.

Étapes :

1. Décomposer f par la création de N region de voronoi Region (VR) utilisant les FP comme germes.
2. Pour chaque message $VR(p_i)$ faire :
   - Diviser le message en X paquets de taille $S_j = \{16, 8, 4, 2 \text{ or } 1\}$, où j est le nombre de paquets.
   - Pour chaque paquet P_j de taille S_j faire :
     - Insérer chaque deux bits du watermark W_j^i dans les deux bits LSB de chaque pixel.
   - Reconstruire le paquet tatoué WP_j utilisant les pixels tatoués.
   - Réarranger les X paquets tatoués pour reconstruire le message tatouée $VR_w(p_i)$.
3. Réarranger les N messages tatoués(segments) VR_w pour reconstruire l'image tatouée f_w.

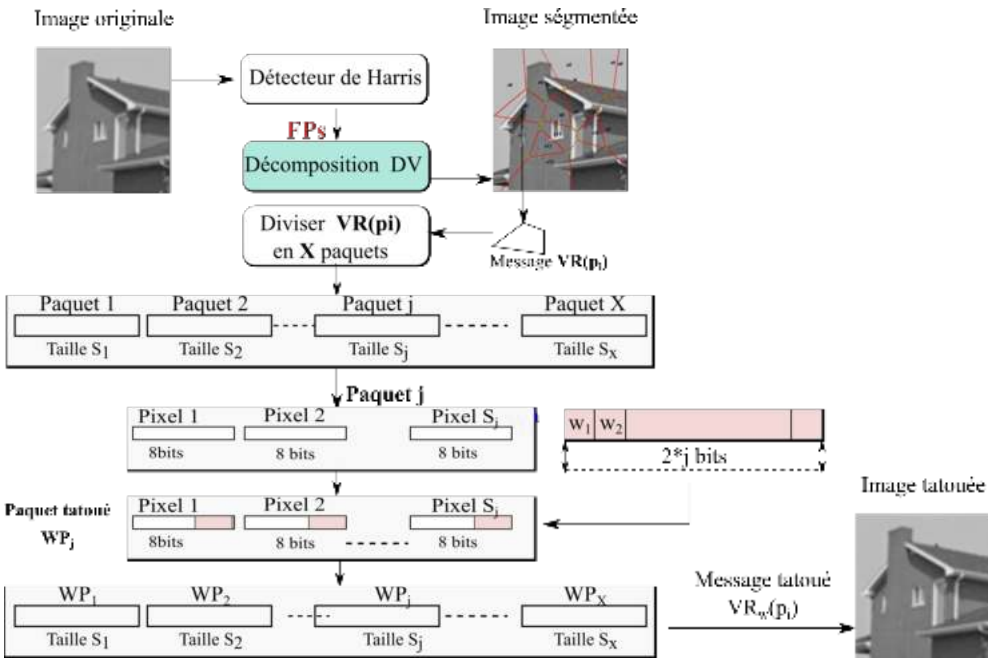


FIGURE 6.12: Processus d'insertion du Watermark.

6.3.1.3 Algorithme de vérification

Algorithme 6.7 Algorithme de vérification basé sur la décomposition de DV.

Entrées :

- f_w^* : image tatouée et éventuellement attaquée.
- FP_{Cryp} : ensemble de FPs chiffré.

Sortie :

- TDM : la carte de détection des altérations.

Étapes :

1. Créer N région (VR_w) utilisant FP comme germes.
2. Pour chaque message $VR_w(p_i)$ faire :
   - Diviser chaque message tatoué $VR_w(p_i)$ en X^* paquets de pixels de taille $S_j = \{16, 8, 4, 2 \text{ ou } 1\}$.
   - Pour chaque paquet tatoué WP_j^* de taille S_j faire :
     - Extraire les deux bits LSB de chaque pixel.
     - Concaténer ces bits ensemble pour créer le checksum extrait $W_j^{i^*}$.
     - Extraire les six bits MSB de chaque pixel.
     - Concaténer ces bits ensemble pour créer la séquence m_w^*.
     - Ajouter $W_j^{i^*}$ à la fin fe m^* to create m_w^*.
     - Diviser m_w^* par un CRC normalisé de degré $d = 2 \times S_j$.
     - Si le reste de la division n'est pas null alors le paquet WP_j^* est altéré.
   - Si l'un des paquets est corrompu, alors le message $VR_w(p_i)$ est aussi.

   En fonction du degré d'altération et de l'intérêt de la région, le récepteur envoie un accusé de réception négatif (NAK) à l'expéditeur, demandant que le message soit retransmis.

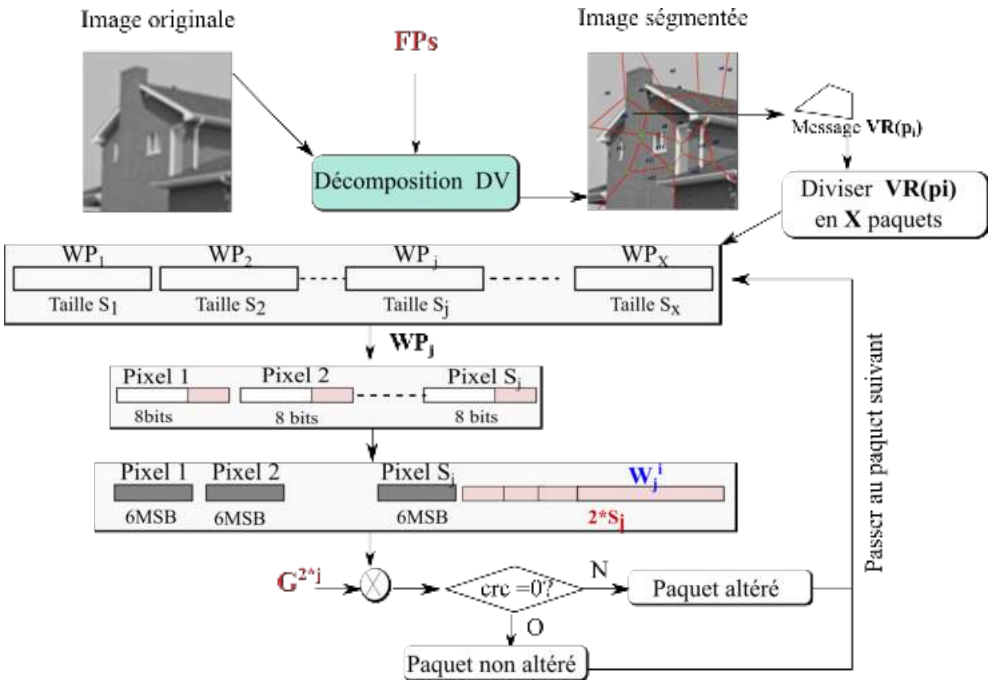


FIGURE 6.13: Processus de détection des altérations.

6.3.2 Résultats expérimentaux

Dans cette section, quelques expériences préliminaires ont été réalisées pour évaluer l'efficacité de notre approche de tatouage. Ces tests sont basés sur l'imperceptibilité, la fragilité, la capacité, le temps de calcul. Nous avons aussi comparé notre schéma avec une méthode de tatouage fragile similaire [Durgesh et al., 2013].

6.3.2.1 Analyse de l'imperceptibilité

Plusieurs images typiques avec différente taille (64×64, 128×128, 256×256 and 512×512) ont été tatouées, afin d'évaluer la propriété d'imperceptibilité de notre méthode de tatouage (voir Figures 6.14 et 6.15).

Les valeurs de PSNR et SSIM pour différentes tailles d'images hôtes obtenues par notre système par rapport à la méthode [Durgesh et al., 2013] ont été illustrées dans Table 6.2.

Les résultats rapportés dans le tableau 6.2 montrent des résultats satisfaisants du schéma proposé. Dans tous les cas, les valeurs PSNR sont supérieures à $47dB$ et sont meilleures que la méthode [Durgesh et al., 2013]. La taille de l'image hôte dans la méthode [Durgesh et al., 2013] est limitée à 256×256, car la position du pixel (colonne et ligne) est convertie en représentation binaire de sur 8 bits. Les histogrammes entre les images originales et tatouées sont présentés dans la Figure 6.16 A partir de ces plots, il est clair que les histogrammes sont similaires, ce qui démontre l'imperceptibilité de notre schéma.

Par conséquent, la différence entre les images originales et les images intégrées n'est pas perceptible dans le système visuel humain.

FIGURE 6.14: Images hôtes.

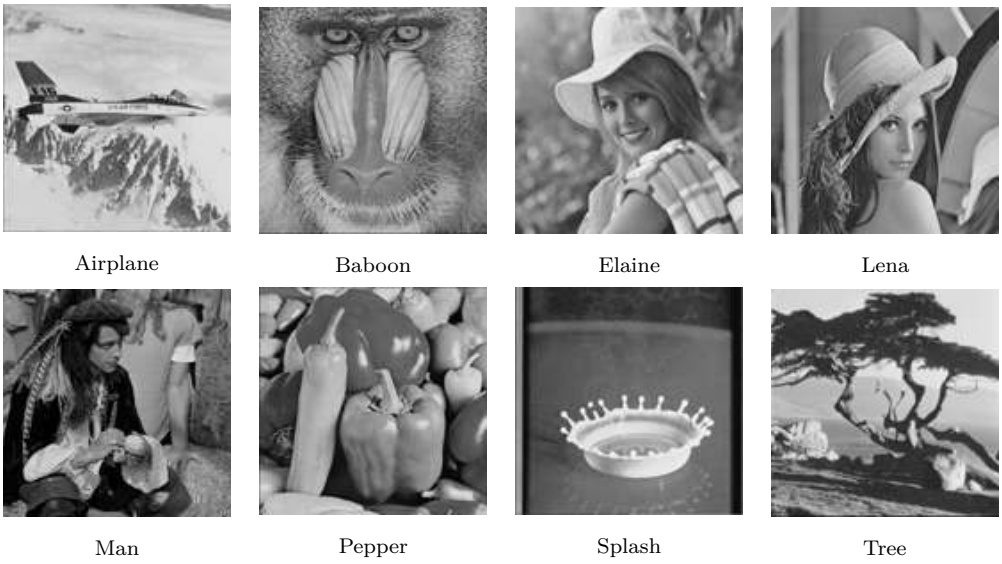


FIGURE 6.15: Images tatouées.

6.3.2.2 Analyse de l'exactitude et la fragilité

Pour estimer l'exactitude et la fragilité du schéma proposé, nous utilisons une image TDM (Tamper Detection Map) pour indiquer les paquets corrompus dans chaque région. S'il n'y a pas d'attaque, le TDM est une image noire, sinon les pixels blancs indiquent les pixels corrompus. La Figure 6.17 illustre la carte de détection des altérations pour différentes images tatouées dans le cas d'absence d'attaque. A partir de ces images, nous pouvons voir que la propriété de correction est satisfaite.

L'analyse de la capacité de détection des altérations est similaire à évaluation de la capacité de détecter les erreurs. A ce stade, nous étudions plusieurs scénarios des altérations au niveau des bits des pixels tatouées. En plus de la comparaison de notre méthode avec la technique [Durgesh et al., 2013], nous avons également comparé le schéma proposé avec l'utilisation d'un générateur polynomial de degré 3 (CRC-3). Ainsi, le watremark généré est inséré directement dans les trois bits LSB comme dans la méthode de Durgesh. La Tableau 6.3 illustre les différents

		Approche proposée				Approche[Durgesh et al., 2013]			
Host image		64×64	128×128	256×256	512×512	64×64	128×128	256×256	512×512
Air-plane	PSNR	47.04	47.02	47.15	47.37	41.51	41.27	40.95	-
	SSIM	0.990	0.986	0.981	0.979	0.970	0.958	0.945	-
Baboon	PSNR	47.61	47.19	47.16	47.17	41.40	41.02	40.99	-
	SSIM	0.995	0.994	0.993	0.993	0.981	0.978	0.975	-
Elaine	PSNR	49.26	47.07	47.12	47.16	41.07	41.07	41.02	-
	SSIM	0.995	0.991	0.985	0.985	0.983	0.968	0.948	-
Lena	PSNR	47.10	47.18	48.18	47.15	41.01	41.04	40.98	-
	SSIM	0.996	0.990	0.984	0.980	0.985	0.968	0.9480	-
Man	PSNR	47.22	47.18	47.23	49.23	41.20	41.18	41.13	-
	SSIM	0.997	0.994	0.990	0.986	0.990	0.976	0.962	-
Peppers	PSNR	47.04	47.08	47.19	47.16	41.48	41.34	40.97	-
	SSIM	0.996	0.990	0.984	0.981	0.987	0.969	0.946	-
Splash	PSNR	48.28	47.22	47.66	49.17	41.13	41.27	41.19	-
	SSIM	0.9888	0.9820	0.9803	0.9752	0.956	0.9413	0.928	-
Tree	PSNR	47.24	47.14	47.23	47.23	41.16	40.93	41.07	-
	SSIM	0.9969	0.991	0.987	0.984	0.9889	0.9725	0.960	-

TABLE 6.2: Estimation de la qualité des images tatouées (PSNR et SSIM).

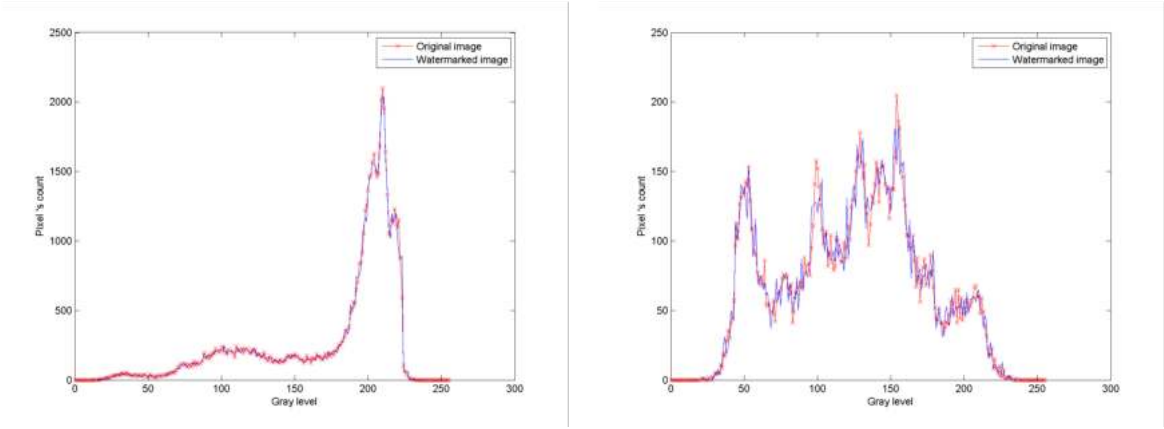


FIGURE 6.16: Présentation de l'imperceptibilité à travers des histogrammes pour les images *Airplane* (256×256) et *Lena* (128×128) .

scénarios des altérations au niveau des bits des pixels tatoués et la capacité des approches de tatouage à détecter des erreurs.

Pour mettre en évidence la fragilité de notre méthode, nous avons pris en compte plusieurs types d'attaques. La Figure 6.18 montre les images attaquées et leurs cartes de détection des altérations extraites.

6.3.2.3 Analyse de la capacité

La capacité du système de tatouage proposé pour une image de taille $N \times M$ est calculée comme suit :

$$Capacite = N \times M \times \frac{N_w}{8} \times 100. \tag{6.6}$$

Nw : est le nombre de bits tatoués.

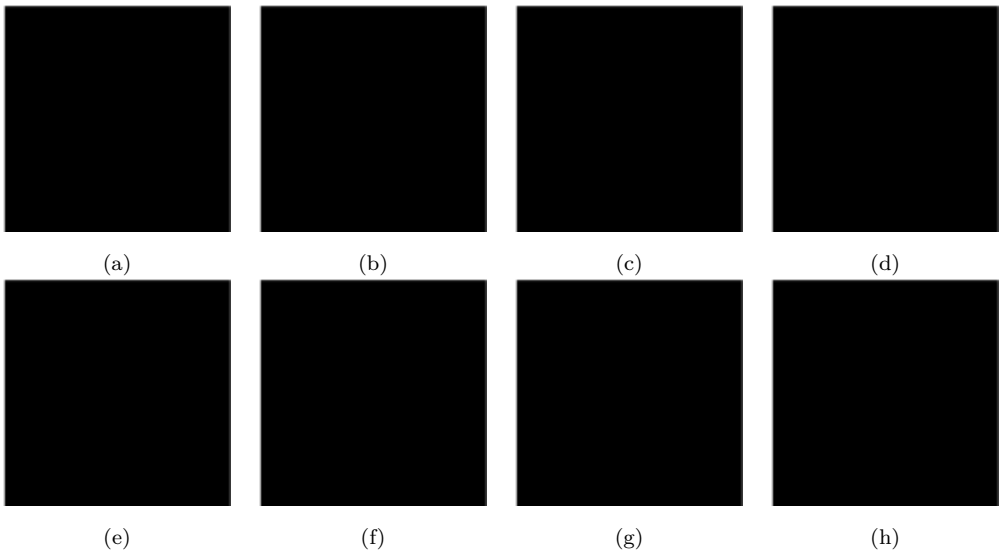


FIGURE 6.17: Cartes de détection des altérations extraites à partir des images tatouées, en cas d'absence d'attaque : (a) Airplane, (b) Baboon, (c) Elaine, (d) Lena, (e) Man, (f)Pepper, (g) Splash et (h) Tree.

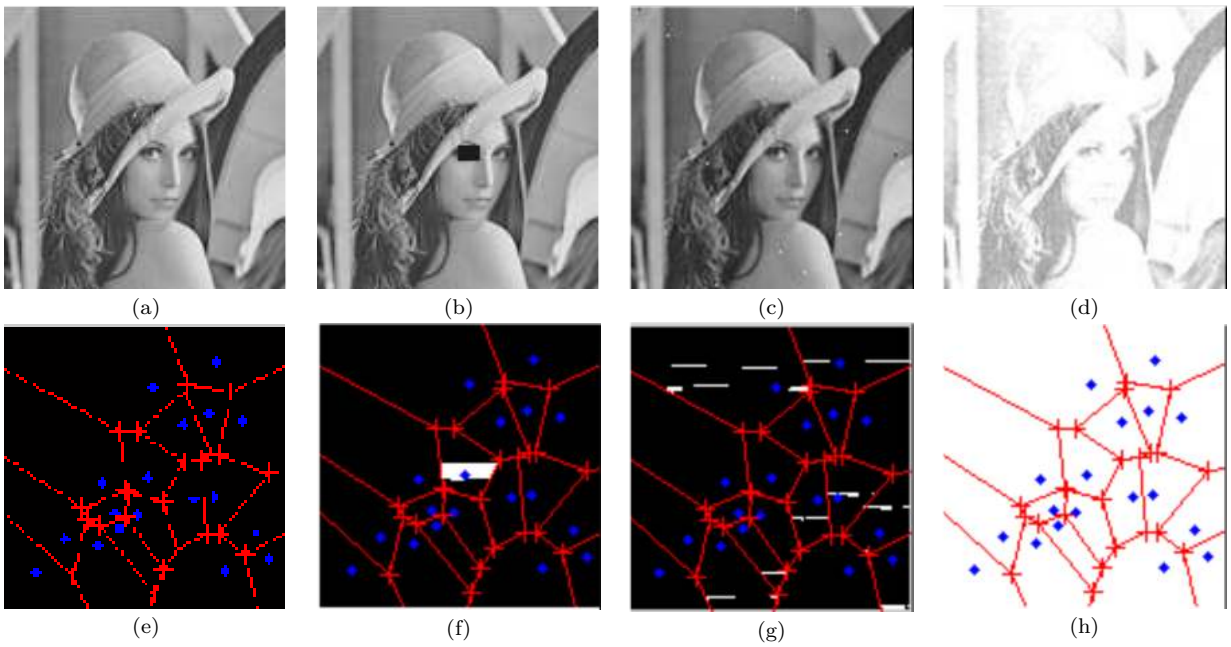


FIGURE 6.18: Fragilité contre les attaques : (a) Un pixel altéré. (b) recadrage. (c) Bruit sel et poivre. (d) Bruit Gaussian. (e-h) Cartes de détection des altérations : paquets altérés détectes dans chaque région après différentes attaques .

Dans notre approche, $N_w = 2$ alors la capacité d'insertion est 25% de la taille de l'image originale. Cette capacité est élevée. Dans le schéma [Durgesh et al., 2013], $N_w = 3$ et la capacité est de 37.5% de la taille de l'image hôte. Cette capacité est meilleure que la capacité atteinte par notre système, mais dans [Durgesh et al., 2013] la taille de l'image hôte est limitée à 256×256.

	Approche [Durgesh et al., 2013]			Approche basée sur le CRC-3			Notre approche		
Pixel original	1 0 0 1 1 0 1 1	155		1 0 0 1 1 0 1 1	155		1 0 0 1 1 0 1 1	155	
Pixel tatouée	1 0 0 1 1 0 1 0	154		1 0 0 1 1 0 0 1	153		1 0 0 1 1 0 0 0	152	
Bits altérés									
Bits LSB									
1	1 0 0 1 1 0 1 1	155	-	1 0 0 1 1 0 0 0	152	+	1 0 0 1 1 0 0 1	153	+
2	1 0 0 1 1 0 0 0	152	+	1 0 0 1 1 0 1 1	155	+	1 0 0 1 1 0 1 0	154	+
3	1 0 0 1 1 1 1 0	158	-	1 0 0 1 1 1 0 1	157	+	1 0 0 1 1 1 0 0	156	+
1-2	1 0 0 1 1 0 0 1	153	+	1 0 0 1 1 0 1 0	154	+	1 0 0 1 1 0 1 1	155	+
1-3	1 0 0 1 1 1 1 1	159	-	1 0 0 1 1 1 0 0	156	+	1 0 0 1 1 1 0 1	157	+
2-3	1 0 0 1 1 1 0 0	156	+	1 0 0 1 1 1 1 1	157	+	1 0 0 1 1 1 1 0	158	+
1-2-3	1 0 0 1 1 1 1 1	157	+	1 0 0 1 1 1 0 1	158	+	1 0 0 1 1 1 1 1	159	+
Bits MSB									
4	1 0 0 1 0 0 1 0	146	+	1 0 0 1 0 0 0 1	145	+	1 0 0 1 0 0 0 0	144	+
5	1 0 0 0 1 0 1 0	138	-	1 0 0 0 1 0 0 1	137	+	1 0 0 0 1 0 0 0	138	+
6	1 0 1 1 1 0 1 0	186	-	1 0 1 1 1 0 0 1	185	+	1 0 1 1 1 0 0 0	184	+
7	1 1 0 1 1 0 1 0	218	+	1 1 0 1 1 0 0 1	117	+	1 1 0 1 1 0 0 0	216	+
8	0 0 0 1 1 0 1 0	26	-	0 0 0 1 1 0 0 1	25	+	0 0 0 1 1 0 0 0	24	+
8-7	0 1 0 1 1 0 1 0	90	-	0 1 0 1 1 0 0 1	89	+	0 1 0 1 1 0 0 0	88	+
8-6	0 0 1 1 1 0 1 0	58	+	0 0 1 1 1 0 0 1	57	+	0 0 1 1 1 0 0 0	56	+
8-5	0 0 0 0 1 0 1 0	10	+	0 0 0 0 1 0 0 1	9	+	0 0 0 0 1 0 0 0	8	+
8-4	0 0 0 1 0 0 1 0	18	-	0 0 0 1 0 0 0 1	17	-	0 0 0 1 0 0 0 0	16	+
7-6	1 1 1 1 1 0 1 0	250	-	1 1 1 1 1 0 0 1	249	+	1 1 1 1 1 0 0	248	+
7-5	1 1 0 0 1 0 1 0	202	-	1 1 0 0 1 0 0 1	201	+	1 1 0 0 1 0 0 0	200	+
7-4	1 1 0 1 0 0 1 0	210	+	1 1 0 1 0 0 0 1	209	+	1 1 0 1 0 0 0 0	208	+
6-5	1 0 1 0 1 0 1 0	170	+	1 0 1 0 1 0 0 1	169	+	1 0 1 0 1 0 0 0	168	+
6-4	1 0 1 1 0 0 1 0	178	-	1 0 1 1 0 0 0 1	177	+	1 0 1 1 0 0 0 0	176	+
5-4	1 0 0 0 0 0 1 0	130	-	1 0 0 0 0 0 0 1	129	+	1 0 0 0 0 0 0 0	128	+
8-7-6	0 1 1 1 1 0 1 0	122	-	0 1 1 1 1 0 0 1	121	+	0 1 1 1 1 0 0 0	120	+
8-7-5	0 1 0 0 1 0 1 0	74	-	0 1 0 0 1 0 0 1	73	+	0 1 0 0 1 0 0 0	72	+
8-7-4	0 1 0 1 0 0 1 0	82	+	0 1 0 1 0 0 0 1	81	+	0 1 0 1 0 0 0 0	80	+
7-6-5	1 1 1 0 1 0 1 0	234	-	1 1 1 0 1 0 0 1	233	+	1 1 1 0 1 0 0 0	232	+
7-6-4	1 1 1 1 0 0 1 0	242	+	1 1 1 1 0 0 0 1	241	+	1 1 1 1 0 0 0 0	240	+
6-5-4	1 0 1 0 0 0 1 0	162	-	1 0 1 0 0 0 0 1	161	+	1 0 1 0 0 0 0 0	160	+
8-7-6-5	0 1 1 0 1 0 1 0	106	+	0 1 1 0 1 0 0 1	105	-	0 1 1 0 1 0 0 0	104	+
8-7-6-4	0 1 1 1 0 0 1 0	114	-	0 1 1 1 0 0 0 1	113	+	0 1 1 1 0 0 0 0	112	+
8-7-5-4	0 1 0 0 0 0 1 0	66	-	0 1 0 0 0 0 0 1	65	+	0 1 0 0 0 0 0 0	64	+
8-6-5-4	0 0 1 0 0 0 1 0	34	+	0 0 1 0 0 0 0 1	33	+	0 0 1 0 0 0 0 0	32	+
7-6-5-4	1 1 1 0 0 0 1 0	226	-	1 1 1 0 0 0 0 1	225	-	1 1 1 0 0 0 0 0	224	+
8-7-6-5-4	0 1 1 0 0 0 1 0	98	-	0 1 1 0 0 0 0 1	97	+	0 1 1 0 0 0 0 0	96	+

(+) : L'erreur est détecte. (-) : L'erreur n'est pas détecte.

TABLE 6.3: Scénarios des bits altérés et la capacité des méthodes de tatouage à détecter les erreurs.

6.3.2.4 Analyse du temps d'exécution

Nous avons également analysé la complexité temporelle du schéma proposé pour étudier son efficacité de calcul. Dans nos expériences, un ordinateur portable avec un processeur Intel

i3 2.GHZ, 4 Go de RAM, Windows 7 est utilisé comme plate-forme informatique. Les résultats expérimentaux sont donnés dans la table 6.4. Figure 6.19 présente les effets de l'augmentation de la taille de l'image sur le temps d'exécution pour les images *Airplane* et *Lena*.

Temps total = temps d'insertion + temps de vérification, et Temps d'insertion = Temps de génération du watermark + Temps d'insertion du watermark).

À partir de ces résultats, nous pouvons voir que notre méthode proposée offre un calcul plus rapide par rapport à la méthode Durgesh [Durgesh et al., 2013].

		Approche proposée		Approche [Durgesh et al., 2013]	
Image hôte	Taille	Insertion (s)	Vérification (s)	Insertion (s)	Vérification (s)
Air-plane					
	64 × 64	2.83	1.30	61.52	63.044
	128 × 128	7.86	4.37	245.59	246.60
	256 × 256	22.8	14.28	990.89	973.00
Baboon					
	64 × 64	1.89	0.83	73.93	47.86
	128 × 128	6.42	4.25	159.54	243.96
	256 × 256	17.20	41.00	976.73	932.78
Elaine					
	64 × 64	1.71	0.68	57.71	58.89
	128 × 128	7.24	3.50	229.74	231.16
	256 × 256	17.20	41.00	953.47	910.63
Lena					
	64 × 64	2.66	1.23	59.54	57.73
	128 × 128	8.04	3.77	232.46	232.17
	256 × 256	30.61	12.31	928.92	919.69
Man					
	64 × 64	2.36	1.31	57.03	57.06
	128 × 128	8.78	3.50	229.43	228.71
	256 × 256	26.71	20.42	919.18	963.27
Peppers					
	64 × 64	2.70	1.21	64.41	57.79
	128 × 128	7.18	3.84	254.88	241.37
	256 × 256	20.95	11.52	969.69	933.57
Splash					
	64 × 64	1.46	0.54	56.99	57.02
	128 × 128	6.43	4.03	254.43	228.29
	256 × 256	10.76	5.52	971.03	940.86
Tree					
	64 × 64	6.474245	1.932281	56.19	57.19
	128 × 128	8.46	5.521817	242.48	216.83
	256 × 256	23.857	14.00	739.05	755.66

TABLE 6.4: Analyse du temps d'exécution.

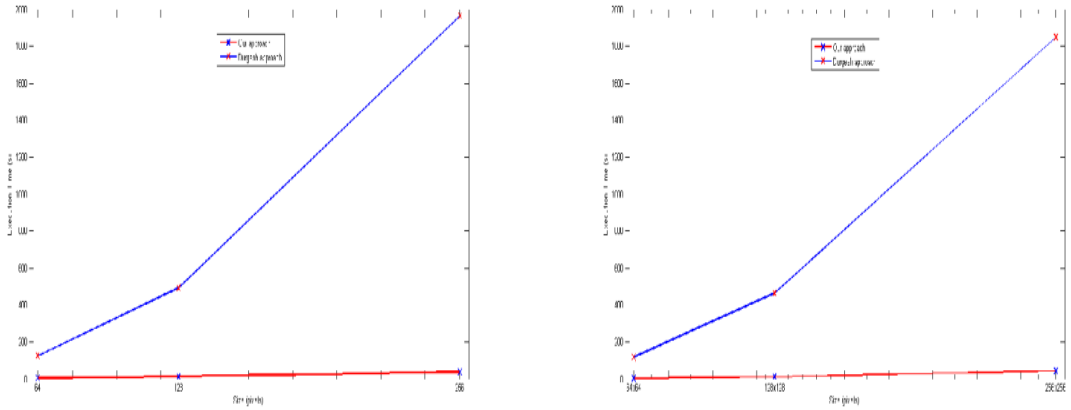
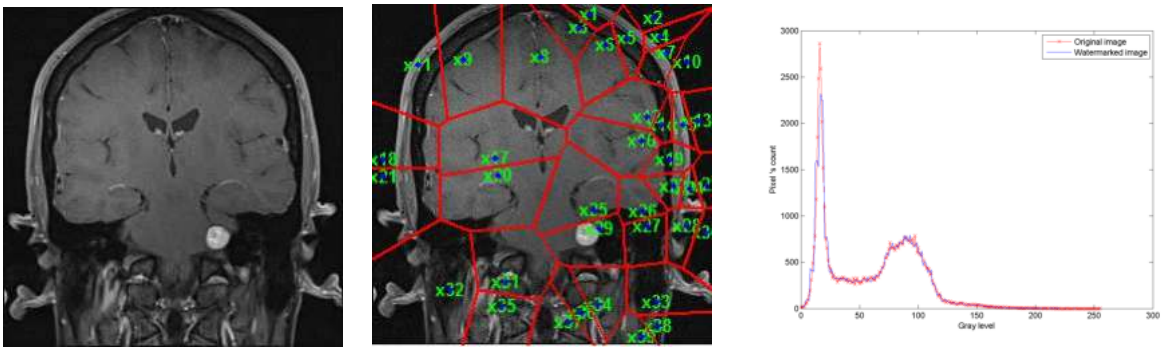


FIGURE 6.19: Impact de l'augmentation de la taille de l'image sur le temps d'exécution pour les image*Airplane* et *Lena*.

6.4 Application à l'imagerie médicale

Dans la littérature, la plupart des techniques de tatouage d'images médicales divisent l'image manuellement ou automatiquement en deux régions : la ROI (région d'intérêt) et la RONI (région de non-intérêt). La ROI est la partie contenant les informations importantes pour le diagnostic. Habituellement, les informations de détection d'altération et de récupération de la ROI sont stockées dans RONI qui accepte une dégradation de la qualité visuelle. Dans certaines situations, le récepteur est impuissant de changer ce partitionnement. Par exemple, lorsqu'il détecte des ROIs dans la RONI. Notre schéma proposé peut être applicable aux images médicales et le récepteur peut spécifier plusieurs ROIs et si elles sont altérées, seuls les paquets altérés dans ces régions sont retransmis par l'expéditeur. La figure 6.20 présente un exemple d'image médicale décomposée avec VD. Si nous supposons que les ROI spécifiés par le récepteur sont X_8 et X_{17}. En effet, dans le cas des altérations, le médecin a envoyé NAK pour retransmettre seulement ces régions.

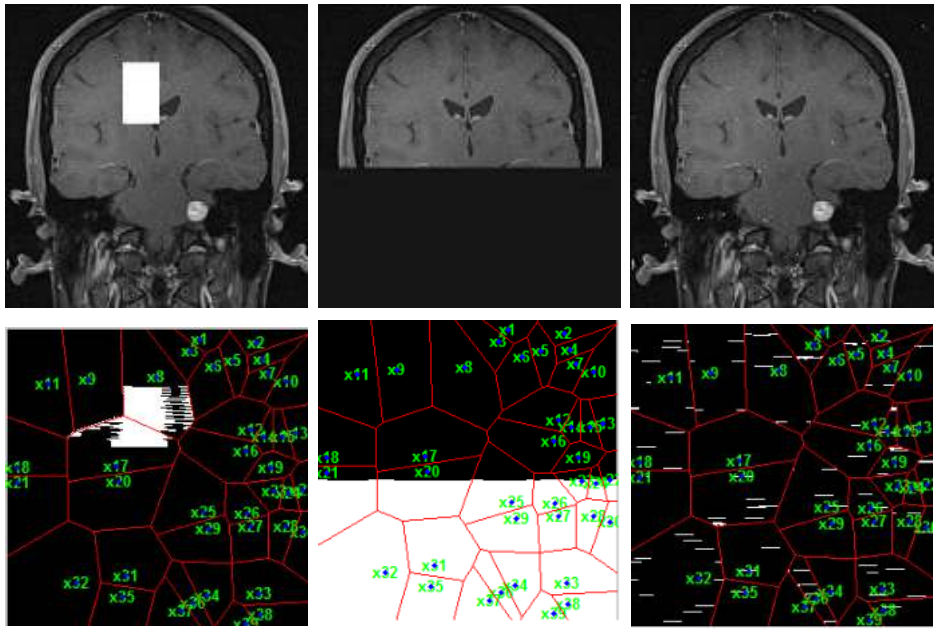


(a) (b) (c)

FIGURE 6.20: Exemple d'application à l'imagerie médicale : (a)Image originale. (b) Image médical décomposée en utilisant VD. (c) Histogrammes de l'image originale et tatouée (PSNR = 47.22, SSIM = 0.9851).

A partir de ces résultats, nous pouvons noter que la méthode proposée donne de bonnes valeurs PSNR et SSIM, qui sont interprétées par une bonne qualité d'images filigranées. Les histogrammes indiquent également la similarité entre les images médicales originales et tatouées.

La figure 6.21 illustre différents scénarios d'images altérées et le TDM qui permet au récepteur de détecter les régions altérées. En fonction du degré d'altération (nombre de paquets altérés) et de l'intérêt de la région, le récepteur renvoie un accusé de réception négatif (NAK) à l'expéditeur, demandant que la région soit retransmise.



(a) (b) (c)

FIGURE 6.21: Différent scénarios d'altération : Scénario (a) : les ROIs X_8 et X_{17} sont altérées. Scénario (b) : ROIs ne sont pas altérées. Scénario (c) : six paquets sont altérés dans X_8 et la ROI X_{17} non altérée.

6.5 Conclusion

Dans le dernier chapitre, nous avons présenté une approche de tatouage fragile de première génération des images couleurs RGB utilisant le code CRC. En utilisant le CRC, les séquences binaires sont traitées comme des polynômes dont les coefficients correspondent à la séquence binaire. Nous ajoutons à la séquence binaire le reste d'une division polynomiale (division par un polynôme générateur). A la réception, le reste de la division reçu et le reste de la division calculé doit être ou alors il y a erreur de transmission. Une phase de génération d'un polynôme générateur (G(x)) de degré ne dépassé pas six est nécessaire. La matrice de G(x) est ensuite crypté en utilisant l'algorithme RSA. En fait, le paramètre le plus important dans la détection d'erreur d'un flux de messages est la sélection du polynôme générateur. Pour pallier le problème de génération d'un polynôme générateur de petit degré, nous proposons une nouvelle l'approche de tatouage de deuxième génération en utilisant le VD et des polynômes standard de degré élevé ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans les régions de l'image après une décomposition en Diagrammes de Voronoi. Les résultats de la simulation montrent que le système proposé fonctionne assez bien lorsqu'il est nécessaire de détecter tout type d'altération, indiquant précisément la région altérée. Une application à l'imagerie médicale est aussi présenté dans ce chapitre.

Conclusion générale

Dans cette thèse, nous avons proposé plusieurs approches de tatouage numérique. La première approche proposée est une nouvelle approche évolutionnaire à base d'AG pour la protection des droits d'auteurs des images couleurs RGB. La méthode proposée a pour objectif d'optimiser les deux exigences contradictoires d'un schéma de tatouage aveugle et robuste : l'imperceptibilité et la robustesse contre les attaques. Nous avons combiné un algorithme de tatouage basé sur la SVD et un algorithme d'optimisation multi-objectif à base d'AG (NSGA-II). La décomposition SVD est employé pour un insérer le watermark et l'algorithme NSGA-II est appliqué par la suite pour optimiser le processus de tatouage.

Dans un premier temps, chaque composante de l'image est décomposée en blocs de taille fixe. Ensuite la SVD est appliquée sur chaque bloc et un pixel de watermark est inséré dans une SV du milieu d'ordre n en utilisant une force d'insertion α. La méthode basée sur la SVD proposée est résumée par les points suivants :

- Appliquer l'algorithme d'insertion en utilisant le couple (n, α) ;
- Évaluer l'imperceptibilité ;
- Appliquer X types d'attaque sur l'image tatouée ;
- Extraire les watermarks à partir des images tatouées et attaquées ;
- Évaluer la robustesse.

Un bloc de taille $T \times T$ peut avoir $\frac{T}{3}$ SVs du milieu qui peuvent révéler une tolérance différente à la modification. Puisque nous n'avons aucune idée sur la sensibilité de l'image à différentes valeurs de (n, α), un algorithme est nécessaire pour obtenir l'optimum (n, α) qui produisent une imperceptibilité et une robustesse maximales. Pour cette raison, nous avons proposé d'utiliser l'algorithme d'optimisation multi-objective NSGA-II. Nous avons défini deux fonctions objectives : la première permet d'évaluer l'imperceptibilité entre l'image originale et l'image tatouée. Tandis que la deuxième permet de juger la robustesse contre différents types d'attaques. Les résultats expérimentaux ont montré que le système de tatouage aveugle basé sur le NSGA-II et la SVD est efficace en termes d'imperceptibilité et robustesse contre les attaques.

Par la suite, nous avons focalisé nos intérêts à la protection des images médicales et nous avons proposé deux nouvelles approches de tatouage numérique utilisant le code CRC et RS. L'approche basée sur le CRC est une technique de tatouage fragile qui permet de détecter les altérations dans la ROI. Dans cette stratégie, l'utilisateur sélectionne tout d'abord la ROI à protéger. Ensuite, cette région est décomposée en paquets et la procédure de codage CRC est exécutée sur chaque paquet pour générer le checksum considéré comme un watermark à insérer dans des LSB de chaque pixel correspondant dans la ROI. A la réception, le récepteur extrait le watermark et exécute le décodage CRC pour détecter les pixels altérés. Les performances de notre méthode dépendent du degré de polynôme générateur. Nous sommes choisis le générateur standard de degré 32 (CRC-32) qui est connu par sa bonne capacité à détecter les erreurs. Les résultats expérimentaux montrent que notre schéma donne un bon compromis entre

l'imperceptibilité et la fragilité. Par contre, l'approche basée sur le RS, est un schéma de tatouage zéro-bit proposé pour la détection et la récupération des altérations dans la ROI. Tout d'abord, l'utilisateur sélectionne la ROI à protéger et stocke les sommets comme clé secrète. Ensuite, cette région est décomposée en paquets et un codage RS est effectué sur chaque paquet pour générer le SS qui est utilisé comme watermark à incorporer dans le domaine fréquentiel de RONI en utilisant la transformée LWT. A la réception, le récepteur décompose l'image en ROI et RONI en appliquant la même clé secrète. Les SS sont extraits de la RONI et combinés avec la MS correspondante. Le codeur RS est exécuté à cette nouvelle séquence. Les résultats expérimentaux montrent que cette approche produit de bonne performance en termes d'imperceptibilité où la valeur de PSNR est dans la gamme de 47 dB et une robustesse importante où elle peut récupérer strictement la ROI après l'insertion de bruit dur.

Dans la dernière contribution, nous avons proposé une approche de tatouage fragile de première génération des images couleurs RGB utilisant le code CRC. En utilisant le CRC, les séquences binaires sont traitées comme des polynômes dont les coefficients correspondent à la séquence binaire. On ajoute à la séquence binaire le reste d'une division polynomiale (division par un polynôme générateur). A la réception, le reste de la division reçu et le reste de la division calculé doit être égaux ou alors il y a erreur de transmission. Une phase de génération d'un polynôme générateur (G(x)) de degré ne dépassé pas six est nécessaire. La matrice de G(x) est ensuite crypte en utilisant l'algorithme RSA. En fait, le paramètre le plus important dans la détection d'erreur d'un flux de messages est la sélection du polynôme générateur. Pour pallier le problème de génération d'un polynôme générateur de petit degré, nous avons proposé une nouvelle approche de deuxième génération en utilisant le VD et des polynômes standard de degré élevée ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans chaque région de l'image après une décomposition en Diagramme de Voronoi. Les résultats de la simulation montrent que le système proposé fonctionne assez bien lorsqu'il est nécessaire de détecter tout type d'altération, indiquant précisément la région altérée.

Dans les travaux futurs, nous nous attendons à apporter les systèmes proposés pour protéger la transmission des images dans des environnement mobile, car les smart phones et les tablettes sont très utilisé pour l'acquisition et la transmission des images numériques.

Nous avons aussi envisagé à appliquer les codes correcteurs des erreurs pour d'autre types d'image tel que les images satellitaires.

Une autre perspective de notre travail est de proposer notre propre code de détection et correction d'erreurs.

Annexe A
Code de contrôle de redondance cyclique CRC

Le code CRC est l'une des techniques de vérification d'erreur les plus cruciales utilisées dans divers systèmes de communication numériques et dispositifs de stockage de données tels qu'un lecteur de disque. Différents polynômes CRC sont utilisés pour la détection d'erreurs. La mise en œuvre du CRC nécessite de choisir un polynôme appelé le *polynôme générateur* de référence souvent nommé $G(x)$ qui est connu de l'émetteur et du récepteur. L'émetteur exécute la *Procédure de codage* sur le flux de messages pour générer un certain nombre de bits de contrôle appelés *la somme de contrôle* en anglais *checksum*. Cette somme de contrôle est ajoutée au message en cours de transmission. A la réception, le destinataire exécute la *Procédure de décodage*, pour vérifier que la somme de contrôle est valide.

Un code CRC avec des symboles du champ de Galois $GF(2)$ (avec deux éléments 0 et 1) est noté $CRC(n, k)$ où :

- n : longueur du mot de code (message + checksum).
- k : longueur du mot (ou message).
- $r = n - k$: longueur du checksum.

La figure A.1 montre une représentation schématique du code $CRC(n, k)$.

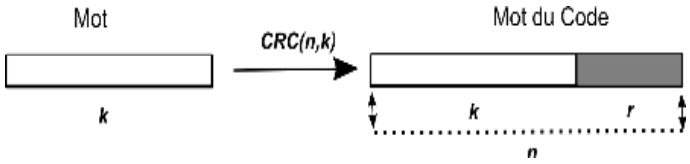


FIGURE A.1: Représentation Schématique du code $CRC(n, k)$.

Le code $CRC(n, k)$ représente le message binaire à transmettre $M = \{m_1, m_2, ..., m_n\}$ par un polynôme $M(x)$ utilisant l'équation suivante :

$$M(x) = \sum_{i=1}^{k} m_i x^{k-i} \tag{A. 1}$$

Par exemple, le message $M = \{1101\}$ est représenté par $M(x) = x^3 + x^2 + 1$. Le transmetteur génère un checksum de taille r en représentant le message M par un polynôme $M(x)$, multipliant $M(x)$ par x^r, et divisant le résultat par $G(x)$ de degré r. Le reste de la division $R(x)$ est le checksum qui est annexée au polynôme $M(x)$ et transmise. A la réception, le polynôme transmis

$(M(x) + R(x))$ est ensuite divisé par le même $G(x)$. Si le résultat de cette division n'a pas de reste, alors il n'y a pas d'erreurs de transmission [Tanenbaum, 2003]. Les algorithmes A.1 et A.2 décrient les procédures de codage et de décodage.

Algorithme A.1 Procédure de codage CRC

Input :
- M : message à transmettre ;
- $G(x)$: polynôme générateur de degré r.

Output :
- M' : message transmis au récepteur (message avec le checksum).

Étapes :
1. Représente le message M par un polynôme $M(x)$, en appliquant l'équation A. 1.
2. Calculer $M(x) \times x^r$. Ceci est équivalent à un décalage de $M(x)$, de r positions vers la gauche.
3. Calculer $\frac{M(x)\times x^r}{G(x)}$
4. Le reste de la division $R(x)$ est le checksum généré.
5. Annexer le reste de la division $R(x)$ à $M(x)$.
6. Le message transmis est $M' = M + R$.

Algorithme A.2 Procédure de décodage CRC

Entrés :
- M'' : message reçu ;
- $G(x)$: polynôme générateur de degré r.

Sorties :
- Reste de la division.

Étapes :
1. Représente le message M'' par un polynôme $M''(x)$.
2. Calculer $\frac{M''(x)\times x^r}{G(x)}$.
3. Si le reste est nul alors le message n'est pas corrompu sinon il est.

La Figure A.2 illustre un an exemple de codage $CRC(7, 4)$. Supposant $M = \{1101\}$ le message à transmettre, et $G(x) = x^3 + 1$, cela est équivalent à 1001. D'abord, M est représenté par un polynôme $M(x) = x^3 + x^2 + 1$. Ensuite, multipliant $M(x)$ par x^3 ceci est équivalent à ajouter trois zéros à la fin de $M(x)$ (décalage vers la gauche) . Ainsi, $M(x) \times x^3$ est 1101000. En fin, on divise 1101000 par 1001 utilisant le modulo-2 arithmétique ce qu'est une simple opération de XOR. A la réception, nous proposons deux scénarios : le premier est sans erreurs et le second est avec des erreurs. Ces scénarios sont illustrés dans la figure A.3.

Les performances du code CRC dépend du choix d'un bon polynôme générateur $G(x)$. Typiquement, dans les applications réelles, le degré r de $G(x)$ est compris entre 8 et 32. La Table A.1 listes certains polynômes générateurs standards prouvés qui ont de nombreuses bonnes propriétés [Ramabadran and Gaitonde, 1988].

Le polynôme CRC-32 utilisé dans la norme de réseau IEEE 802.3 (Ethernet) est connu pour être largement sous-optimal et très efficace pour détecter différents types d'erreurs [Crow et al., 1997, Koopman, 2002]. Depuis, nous avons inspiré l'utilisation de CRC-32 sur les applications Internet pour le tatouage numérique.

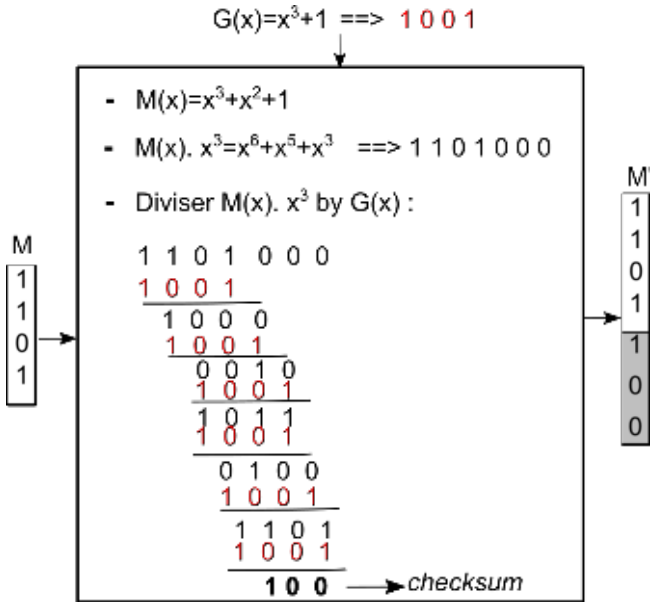


FIGURE A.2: Exemple de codage $CRC(7,4)$ utilisant $G(x) = x^3 + 1$.

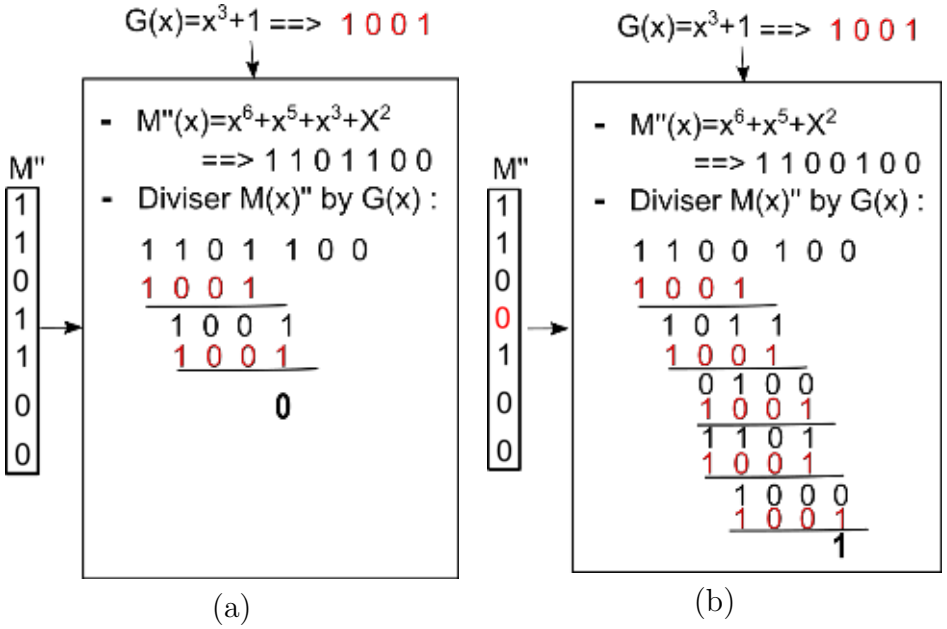


FIGURE A.3: Exemple de décodage $CRC(7,4)$ utilisant le même générateur $G(x) = x^3 + 1$: (a) Scénario sans erreurs, (b) Scénario avec erreurs.

Nom	Degré	Polynôme
LRCC-8	8	$x^8 + 1$
CRC-12	12	$x^{12} + x^{11} + x^3 + x^2 + x + 1$
CRC-16	16	$x^{16} + x^{15} + x^2 + 1$
CRC-CCITT	16	$x^{16} + x^{12} + x^5 + 1$
LRCC-16	16	$x^16 + 1$
CRC-32	32	$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

TABLE A.1: Polynômes générateurs de certains codes CRC standards. [Ramabadran and Gaitonde, 1988].

Annexe B
Code Reed Solomon RS

Reed Solomon, est un code *linéaire*, *non-binaire* et *cyclique*. Un code *t-erreur-correction* avec des symboles de champ de Galois $GF(2^m)$ est noté $RS(n,k)$ avec m-bit symboles($m \geq 2$) où ;

- n : longueur du mot de code (symbole + checksum) $n = 2^m - 1$.
- k : longueur du mot .
- $n - k$: nombre de bits du checksum.
- t : capacité du code de corriger les erreurs, $2t = n - k$.

Le codage RS, créer un mot de code de taille n en ajoutant une redondance de taille $n - k$ à k symboles du mot. Ainsi, le décodeur est capable de corriger jusqu'à t erreurs. L'encodeur et le décodeur utilisent un polynôme $G(x)$ appelé *générateur polynomial* qui est défini comme suit [Wicker and Bhargava, 1999, Clarke, 2002] :

$$G(x) = \prod_{i=1}^{2t}(x + \alpha^i) \tag{B. 1}$$

Où α^i sont les racines de $G(x)$.

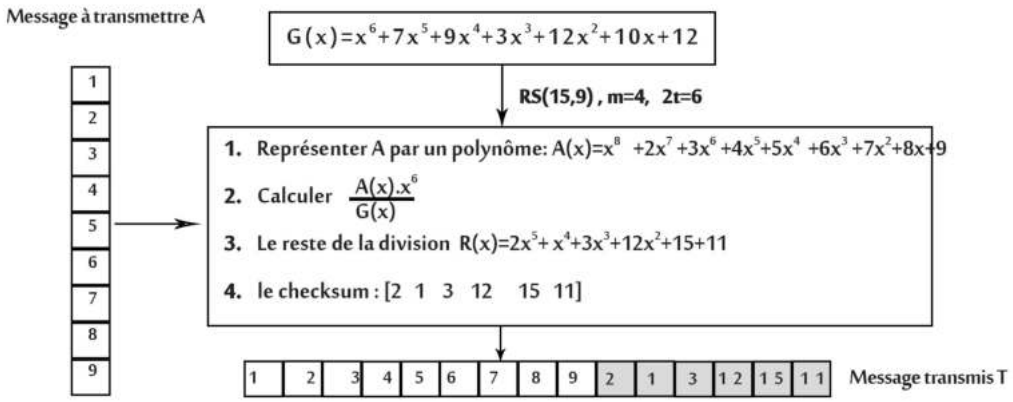


FIGURE B.1: Exemple de codage RS.

Algorithme B.1 Procédure de codage RS

Input :
- A : message à transmettre ;
- n, k : paramètres du code RS.

Output :
- T : message transmis au récepteur (message avec le checksum).

Étapes :
- Le bloc de k symboles est représenté par un polynôme $A(x)$ de degré $k-1$, soit :

$$A(x) = A_0 + A_1 x + A_2 x^2 + ... + A_{k-1} x^{k-1} \tag{B. 2}$$

- Multipliant $A(x)$ par x^{2t} : $M(x) = A(x).x^{2t}$.
- Diviser $M(x)$ par $G(x)$: $\frac{M(x)}{G(x)} = Q(x) + \frac{R(x)}{G(x)}$. Où $Q(x)$ est le quotient et $R(x)$ est le reste de la division.
- Les $2t$ symboles de checksum sont les coefficients R_i du $R(x)$:

$$R(x) = R_0 + R_1 x + ... + R_{2t-1} x^{2t-1} \tag{B. 3}$$

- Le mot de code transmis est créé en combinant le checksum $R(x)$ et $M(x)$:

$$T(x) = A(x).x^{2t} + R(x) \tag{B. 4}$$

En ajoutant le reste $R(x)$ à la fin du message, nous assurons que le mot de code créé sera toujours divisible par $G(x)$ sans reste.

La Figure B.1 présent un exemple du codage d'un message $A = 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9$ utilisant $RS(15, 9)$.

Algorithme B.2 Procédure de décodage RS

Entrés :

- T' : message reçu ;
- n, k : paramètres du code RS.

Sorties :

- Positions des erreurs.
- Message corrigé.

Étapes :

- Soit $T(x)$ la représentation polynomiale du message transmis et $T'(x)$ la représentation polynomiale du message reçu, nous pouvons écrire : $T'(x) = T(x) + E(x)$. Où $E(x)$ est un modèle d'erreurs lié au canal de transmission.
- Diviser le message reçu $T'(x)$ par $G(x)$. Les restes S_i sont appelés syndrome, $i \in \{1, 2, ..., 2t\}$
- En cas d'absence d'erreur, tous les S_i ont des valeurs nulles. Toute valeur non nulle S_i indique la présence d'erreurs.
- Afin de trouver le polynôme d'emplacement (position) d'erreur $L(x)$ et le nombre d'erreurs ν, nous effectuons l'algorithme itératif de *Berlekamp*.
- Étant donné l'emplacement polynomial de l'erreur $L(x)$ et le nombre d'erreurs ν on peut trouver les racines de $L(x)$.
- Ces racines sont utilisées avec les syndromes S_i pour trouver les valeurs d'erreurs (Forney's algorithm).
- Les erreurs sont corrigées en combinant toutes les données précédentes et en estimant le polynôme d'erreur.

Un exemple de décodage d'un message reçu T' utilisant RS $(15, 9)$ est illustré dans la Figure B.2.

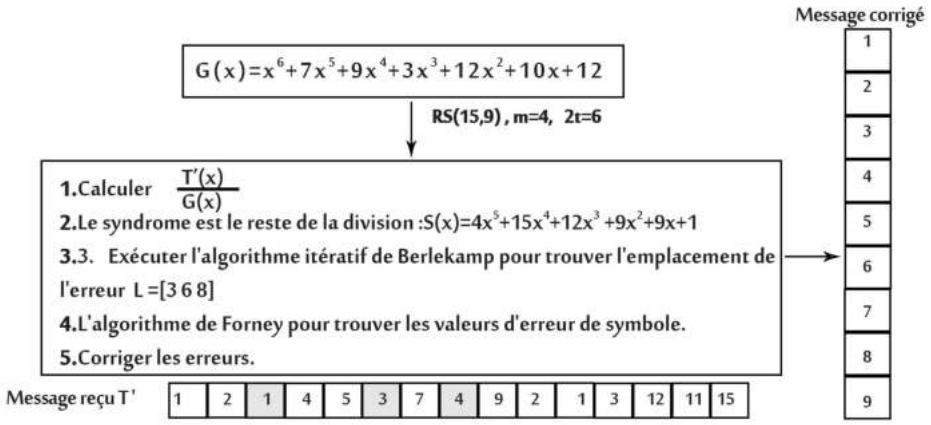


FIGURE B.2: Exemple de décodage RS.

Bibliographie

[Abraham and Jain, 2005] Abraham, A. and Jain, L. (2005). Evolutionary multiobjective optimization. *Evolutionary Multiobjective Optimization*, pages 1–6.

[Acharya et al., 2004] Acharya, R., Niranjan, U., Iyengar, S. S., Kannathal, N., and Min, L. C. (2004). Simultaneous storage of patient information with medical images in the frequency domain. *Computer Methods and Programs in Biomedicine*, 76(1) :13–19.

[Al-Qershi and Khoo, 2009] Al-Qershi, O. M. and Khoo, B. (2009). Authentication and data hiding using a reversible ROI-based watermarking scheme for DICOM images. In *Proceedings of International Conference on Medical Systems Engineering (ICMSE)*, pages 829–834.

[Al-Qershi and Khoo, 2011a] Al-Qershi, O. M. and Khoo, B. E. (2011a). Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images. *Journal of Digital Imaging*, 24(1) :114–125.

[Al-Qershi and Khoo, 2011b] Al-Qershi, O. M. and Khoo, B. E. (2011b). High capacity data hiding schemes for medical images based on difference expansion. *Journal of Systems and Software*, 84(1) :105–112.

[Alba, 2002] Alba, E. (2002). Parallel evolutionary algorithms can achieve super-linear performance. *Information Processing Letters*, 82(1) :7–13.

[Bäck et al., 1997] Bäck, T., Fogel, D., and Michalewicz, Z. (1997). Handbook of evolutionary computation. *Release*, 97(1) :B1.

[Bäck et al., 2000] Bäck, T., Fogel, D. B., and Michalewicz, Z. (2000). *Evolutionary computation 1 : Basic algorithms and operators*, volume 1. CRC press.

[Back et al., 1991] Back, T., Hoffmeister, F., and Schwefel, H.-P. (1991). A survey of evolution strategies. In *Proceedings of the fourth international conference on genetic algorithms*, volume 2. Morgan Kaufmann Publishers, San Mateo.

[Baker, 1985] Baker, J. E. (1985). Adaptive selection methods for genetic algorithms. In *Proceedings of an International Conference on Genetic Algorithms and their applications*, pages 101–111. Hillsdale, New Jersey.

[Beyer and Schwefel, 2002] Beyer, H.-G. and Schwefel, H.-P. (2002). Evolution strategies–a comprehensive introduction. *Natural computing*, 1(1) :3–52.

[Branke et al., 2008] Branke, J., Deb, K., and Miettinen, K. (2008). *Multiobjective optimization : Interactive and evolutionary approaches*, volume 5252. Springer Science & Business Media.

[Burrus et al., 1998] Burrus, C. S., Gopinath, R. A., Guo, H., Odegard, J. E., and Selesnick, I. W. (1998). *Introduction to wavelets and wavelet transforms : a primer*, volume 1. Prentice hall New Jersey.

[Chae and Manjunath, 1997] Chae, J. J. and Manjunath, B. (1997). Robust embedded data from wavelet coefficients. In *Photonics West'98 Electronic Imaging*, pages 308–317. International Society for Optics and Photonics.

[Chang et al., 1999] Chang, C.-C., Hwang, K.-F., and Hwang, M.-S. (1999). A block based digital watermarks for copy protection of images. In *Communications, 1999. APCC/OECC '99. Fifth Asia-Pacific Conference on ... and Fourth Optoelectronics and Communications Conference*, volume 2, pages 977–980 vol.2.

[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.

[Charalampidis, 2005] Charalampidis, D. (2005). Improved robust VQ-based watermarking. *Electronics Letters*, 41(23) :21–22.

[Chemak et al., 2007] Chemak, C., Bouhlel, M.-S., and Lapayre, J.-C. (2007). A new scheme of image watermarking based on 5/3 wavelet decomposition and turbo-code. *WSEAS Transaction on Biology and Biomedicine*, 4(4) :45–52.

[Chun-Shien, 2005] Chun-Shien, L. (2005). *Multimedia Security : Steganography and Digital Watermarking Techniques for Protection of Intellectual Property*. IDEA GROUP PUBLISHING.

[Clarke, 2002] Clarke, C. (2002). R&D white paper. *Reed-Solomon Error Correction," WHP*, 31.

[Coatrieux et al., 2013] Coatrieux, G., Huang, H., Shu, H., Luo, L., and Roux, C. (2013). A watermarking-based medical image integrity control system and an image moment signature for tampering characterization. *IEEE journal of biomedical and health informatics*, 17(6) :1057–1067.

[Coatrieux et al., 2009] Coatrieux, G., Le Guillou, C., Cauvin, J.-M., and Roux, C. (2009). Reversible watermarking for knowledge digest embedding and reliability control in medical images. *IEEE Transactions on Information Technology in Biomedicine*, 13(2) :158–165.

[Coatrieux et al., 2006a] Coatrieux, G., Lecornu, L., Sankur, B., and Roux, C. (2006a). A review of image watermarking applications in healthcare. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*, pages 4691–4694. IEEE.

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

[Coatrieux et al., 2006b] Coatrieux, G., Puentes, J., Roux, C., Lamard, M., and Daccache, W. (2006b). A low distorsion and reversible watermark : application to angiographic images of the retina. In *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pages 2224–2227. IEEE.

[Coello, 2002] Coello, C. A. C. (2002). Theoretical and numerical constraint-handling techniques used with evolutionary algorithms : a survey of the state of the art. *Computer methods in applied mechanics and engineering*, 191(11) :1245–1287.

[Coello and Christiansen, 1998] Coello, C. A. C. and Christiansen, A. D. (1998). Two new ga-based methods for multiobjective optimization. *Civil Engineering Systems*, 15(3) :207–243.

[Coello et al., 1999] Coello, C. A. C. et al. (1999). A comprehensive survey of evolutionary-based multiobjective optimization techniques. *Knowledge and Information systems*, 1(3) :129–156.

[Coello et al., 2007] Coello, C. A. C., Lamont, G. B., Van Veldhuizen, D. A., et al. (2007). *Evolutionary algorithms for solving multi-objective problems*, volume 5. Springer.

[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., 1997] Cox, I. J., Kilian, J., Leighton, F. T., and Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE transactions on image processing*, 6(12) :1673–1687.

[Cox et al., 2000] Cox, I. J., Miller, M. L., and Bloom, J. A. (2000). Watermarking applications and their properties. In *itcc*, pages 6–10.

[Cox et al., 2002] Cox, I. J., Miller, M. L., Bloom, J. A., and Honsinger, C. (2002). *Digital watermarking*, volume 1558607145. Springer.

[Crow et al., 1997] Crow, B. P., Widjaja, I., Kim, J. G., and Sakai, P. T. (1997). IEEE 802.11 wireless local area networks. *IEEE Communications magazine*, 35(9) :116–126.

[Das and Kundu, 2012] Das, S. and Kundu, M. K. (2012). Effective management of medical information through a novel blind watermarking technique. *Journal of medical systems*, 36(5) :3339–3351.

[Deb, 1999] Deb, K. (1999). Solving goal programming problems using multi-objective genetic algorithms. In *Evolutionary Computation, 1999. CEC 99. Proceedings of the 1999 Congress on*, volume 1, pages 77–84. IEEE.

[Deb, 2001a] Deb, K. (2001a). *Multi-objective optimization using evolutionary algorithms*, volume 16. John Wiley & Sons.

[Deb, 2001b] Deb, K. (2001b). Nonlinear goal programming using multi-objective genetic algorithms. *Journal of the Operational Research Society*, pages 291–302.

[Deb et al., 2000] Deb, K., Agrawal, S., Pratap, A., and Meyarivan, T. (2000). A fast elitist non-dominated sorting genetic algorithm for multi-objective optimization : Nsga-ii. In *International Conference on Parallel Problem Solving From Nature*, pages 849–858. Springer.

[Deb and Goldberg, 1989] Deb, K. and Goldberg, D. E. (1989). An investigation of niche and species formation in genetic function optimization. In *Proceedings of the 3rd international conference on genetic algorithms*, pages 42–50. Morgan Kaufmann Publishers Inc.

[Deb et al., 2002] Deb, K., Pratap, A., Agarwal, S., and Meyarivan, T. (2002). A fast and elitist multiobjective genetic algorithm : Nsga-ii. *IEEE transactions on evolutionary computation*, 6(2) :182–197.

[Devi et al., 2009] Devi, P. M., Venkatesan, M., and Duraiswamy, K. (2009). Reversible Image Authentication with Tamper Localization Based on Integer Wavelet Transform. *arXiv preprint arXiv :0912.0607*.

[Diffie and Hellman, 1976] Diffie, W. and Hellman, M. (1976). New directions in cryptography. *IEEE transactions on Information Theory*, 22(6) :644–654.

[Dong et al., 2011] Dong, C., Zhang, H., Li, J., and w. Chen, Y. (2011). Robust zero-watermarking for medical image based on DCT. In *Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on*, pages 900–904.

[Durgesh et al., 2013] Durgesh, S., Shivendra, S., and Suneeta, A. (2013). Self-embedding pixel wise fragile watermarking scheme for image authentication. In *IITM 2013, CCIS 276*, pages 111–122. Springer-Verlag Berlin Heidelberg.

[Edgeworth, 1881] Edgeworth, F. Y. (1881). *Mathematical psychics : An essay on the application of mathematics to the moral sciences*, volume 10. Kegan Paul.

[Eggers et al., 2000] Eggers, J. J., Su, J. K., and Girod, B. (2000). Asymmetric watermarking schemes. *Sicherheit in Netzen und Medienströmen*, pages 124–133.

[Espejo et al., 2010] Espejo, P. G., Ventura, S., and Herrera, F. (2010). A survey on the application of genetic programming to classification. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 40(2) :121–144.

[Eswaraiah and Reddy, 2014] Eswaraiah, R. and Reddy, E. S. (2014). Medical Image Watermarking Technique for Accurate Tamper Detection in ROI and Exact Recovery of ROI. *Int. J. Telemedicine Appl.*, 2014(13) :1–10.

[Fallahpour et al., 2009] Fallahpour, M., Megias, D., and Ghanbari, M. (2009). High capacity, reversible data hiding in medical images. In *Image Processing (ICIP), 2009 16th IEEE International Conference on*, pages 4241–4244. IEEE.

[Faoziyah et al., 2013] Faoziyah, P., Permana, F., Wirayuda, T., Wisesty, U., et al. (2013). Tamper detection and recovery of medical image watermarking using modified LSB and Huffman compression. In *Informatics and Applications (ICIA), 2013 Second International Conference on*, pages 129–132. IEEE.

[Fogel, 1997] Fogel, D. B. (1997). The advantages of evolutionary computation. In *BCEC*, pages 1–11.

[Fogel et al., 1966] Fogel, L. J., Owens, A. J., and Walsh, M. J. (1966). Artificial intelligence through simulated evolution.

[Fonseca et al., 1993] Fonseca, C. M., Fleming, P. J., et al. (1993). Genetic algorithms for multiobjective optimization : Formulation discussion and generalization. In *Icga*, volume 93, pages 416–423.

[Fotopoulos et al., 2008] Fotopoulos, V., Stavrinou, M. L., and Skodras, A. N. (2008). Medical image authentication and self-correction through an adaptive reversible watermarking technique. In *BioInformatics and BioEngineering, 2008. BIBE 2008. 8th IEEE International Conference on*, pages 1–5. IEEE.

[Fourman, 1985] Fourman, M. P. (1985). Compaction of symbolic layout using genetic algorithms. In *Proceedings of the 1st International Conference on Genetic Algorithms*, pages 141–153. L. Erlbaum Associates Inc.

[Fridrich, 1998] Fridrich, J. (1998). Combining low-frequency and spread spectrum watermarking. In *Proc. SPIE Int. Symposium on Optical Science, Engineering, and Instrumentation*, volume 333, page 340.

[Goldberg, 1989] Goldberg, D. E. (1989). Genetic algorithms in search, optimization, and machine learning. *Reading : Addison-Wesley*.

[Goldberg and Deb, 1991] Goldberg, D. E. and Deb, K. (1991). A comparative analysis of selection schemes used in genetic algorithms. *Foundations of genetic algorithms*, 1 :69–93.

[Golea, 2010] Golea, N. E.-H. (2010). Tatouage numérique des images couleurs RGB. In *Mémoire de magister, Université de Batna*.

[Golea, 2012] Golea, N. E.-H. (2012). A fragile watermarking scheme based CRC checksum and public key cryptosystem for RGB color image authentication. In *International Conference on Image and Signal Processing*, pages 316–325. Springer.

[Golea and Melkemi,] Golea, N. E.-H. and Melkemi, K. E. Feature-based Fragile Watermarking for Tamper Detection using Voronoi Diagram Decomposition. *to be submitted*.

[Golea and Melkemi, 2017] Golea, N. E.-H. and Melkemi, K. E. (2017). ROI-based fragile watermarking for medical image tamper detection. *International Journal of High Performance Computing and Networking*.

[Golea et al.,] Golea, N. E.-H., Melkemi, K. E., and Behloul, A. Zero-bit Fragile Watermarking for Medical Image Tamper Detection and Recovery using RS Code and Lifting Wavelet Transform. *to be submitted*.

[Golea et al., 2011] Golea, N. E.-H., Melkemi, K. E., and Melkemi, M. (2011). A novel multi-objective genetic algorithm optimization for blind RGB color image watermarking. In *Signal-Image Technology and Internet-Based Systems (SITIS), 2011 Seventh International Conference on*, pages 306–313. IEEE.

[Golea et al., 2010] Golea, N. E.-H., Seghir, R., and Benzid, R. (2010). A blind RGB color image watermarking based on singular value decomposition. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on*, pages 1–5. IEEE.

[Golpira and Danyali, 2009] Golpira, H. and Danyali, H. (2009). Reversible blind watermarking for medical images based on wavelet histogram shifting. In *Signal Processing and Information Technology (ISSPIT), 2009 IEEE International Symposium on*, pages 31–36. IEEE.

[Gonzalez et al., 1997] Gonzalez, A., Herrera, F., Gonzalez, A., and Herrera, F. (1997). Multi-stage genetic fuzzy systems based on the iterative rule learning approach.

[Hajela and Lin, 1992] Hajela, P. and Lin, C.-Y. (1992). Genetic search strategies in multicriterion optimal design. *Structural optimization*, 4(2) :99–107.

[Hajjaji et al., 2011] Hajjaji, M. A., Mtibaa, A., and Bourennane, E.-B. (2011). A Watermarking of Medical Image : New Approach Based On "Multi-Layer" Method. *International Journal of Computer Science Issues*, 8(2) :33–41.

[Han and Kim, 2000] Han, K.-H. and Kim, J.-H. (2000). Genetic quantum algorithm and its application to combinatorial optimization problem. In *Evolutionary Computation, 2000. Proceedings of the 2000 Congress on*, volume 2, pages 1354–1360. IEEE.

[Hanjalic et al., 2000] Hanjalic, A., Langelaar, G., Van Roosmalen, P., Biemond, J., and Lagendijk, R. (2000). *Image and video databases : restoration, watermarking and retrieval*, volume 8. Elsevier.

[Hartung and Girod, 1997] Hartung, F. and Girod, B. (1997). Fast public-key watermarking of compressed video. In *Image Processing, 1997. Proceedings., International Conference on*, volume 1, pages 528–531. IEEE.

[Holland, 1975] Holland, J. H. (1975). Adaptation in natural and artificial systems : An introductory analysis with application to biology, control, and artificial intelligence. *Ann Arbor, MI : University of Michigan Press*.

[Horn et al., 1994] Horn, J., Nafpliotis, N., and Goldberg, D. E. (1994). A niched pareto genetic algorithm for multiobjective optimization. In *Evolutionary Computation, 1994. IEEE World Congress on Computational Intelligence., Proceedings of the First IEEE Conference on*, pages 82–87. Ieee.

[Huang et al., 2008] Huang, H., Coatrieux, G., Montagner, J., Shu, H., Luo, L., and Roux, C. (2008). Medical image integrity control seeking into the detail of the tampering. In *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE*, pages 414–417. IEEE.

[Huang et al., 2001] Huang, H.-C., Wang, F.-H., Pan, J.-S., et al. (2001). Efficient and robust watermarking algorithm with vector quantisation. *Electronics Letters*, 37(13) :826–828.

[Jian-hu and Jia-xing, 2007] Jian-hu, M. and Jia-xing, H. (2007). A wavelet-based method of zero-watermark. *Journal of Image and Graphics*, 4 :003.

[Kalantari et al., 2009] Kalantari, N. K., Akhaee, M. A., Ahadi, S. M., and Amindavar, H. (2009). Robust multiplicative patchwork method for audio watermarking. *IEEE Transactions on Audio, speech, and language processing*, 17(6) :1133–1141.

[Kamstra and Heijmans, 2005] Kamstra, L. and Heijmans, H. J. (2005). Reversible Data Embedding into Images Using Wavelet Techniques and Sorting. *IEEE transactions on image processing*, 14(12) :2082–2090.

[Kerckhoffs, 1883] Kerckhoffs, A. (1883). La cryptographie militaire. *Dokument dostupnỳ na URL< http ://www. petitcolas. net/fabien/kerckhoffs/>(m áj 2008)*, 3.

[Khayam, 2003] Khayam, S. A. (2003). The discrete cosine transform (DCT) : theory and application. *Michigan State University*, 114.

[Kim and de Weck, 2005] Kim, I. Y. and de Weck, O. L. (2005). Adaptive weighted-sum method for bi-objective optimization : Pareto front generation. *Structural and multidisciplinary optimization*, 29(2) :149–158.

[Kirovski, 2006] Kirovski, D. (2006). *Multimedia watermarking techniques and applications*. CRC Press.

[Koopman, 2002] Koopman, P. (2002). 32-bit cyclic redundancy codes for internet applications. In *Dependable Systems and Networks, 2002. DSN 2002. Proceedings. International Conference on*, pages 459–468. IEEE.

[Koza, 1992] Koza, J. R. (1992). *Genetic programming : on the programming of computers by means of natural selection*, volume 1. MIT press.

[Kuhn,] Kuhn, H. Nonlinear programming. In *Proceedings of 2nd Berkeley Symposium. Berkeley : University of California Press*, pages 481–492.

[Kumar et al., 2015] Kumar, B., Kumar, S. B., and Chauhan, D. S. (2015). Wavelet based imperceptible medical image watermarking using spread-spectrum. In *Telecommunications and Signal Processing (TSP), 2015 38th International Conference on*, pages 1–5.

[Kutter et al., 1999] Kutter, M., Bhattacharjee, S. K., and Ebrahimi, T. (1999). Towards second generation watermarking schemes. In *Image Processing, 1999. ICIP 99. Proceedings. 1999 International Conference on*, volume 1, pages 320–323. IEEE.

[Kwitt et al., 2011] Kwitt, R., Meerwald, P., and Uhl, A. (2011). Lightweight detection of additive watermarking in the DWT-domain. *IEEE transactions on image processing*, 20(2) :474–484.

[Lai., 2011] Lai., C.-C. (2011). A Digital Watermarking Scheme Based on Singular Value Decomposition and Tiny Genetic Algorithm. In *Digital Signal Processing*, pages 522–527.

[Laumanns et al., 2006] Laumanns, M., Thiele, L., and Zitzler, E. (2006). An efficient, adaptive parameter variation scheme for metaheuristics based on the epsilon-constraint method. *European Journal of Operational Research*, 169(3) :932–942.

[Lee and Won, 2000] Lee, J. and Won, C. S. (2000). A watermarking sequence using parities of error control coding for image authentication and correction. *IEEE Transactions on Consumer Electronics*, 46(2) :313–317.

[Li et al., 2011] Li, J., Han, X., Dong, C., and w. Chen, Y. (2011). Robust multiple watermarks for medical image based on DWT and DFT. In *Computer Sciences and Convergence Information Technology (ICCIT), 2011 6th International Conference on*, pages 895–899.

[Li et al., 2012] Li, J., Zhang, H., and Chen, Y.-w. (2012). Robust Zero-Watermarking for Medical Image Based on DCT. In *Photonics and Optoelectronics (SOPO), 2012 Symposium on*, pages 21–23.

[Li et al., 2005] Li, M., Poovendran, R., and Narayanan, S. (2005). Protecting patient privacy against unauthorized release of medical images in a group communication environment. *Computerized Medical Imaging and Graphics*, 29(5) :367–383.

[Lin and Chang, 2000] Lin, C.-Y. and Chang, S.-F. (2000). Semi-fragile watermarking for authenticating JPEG visual content. In *Security and Watermarking of Multimedia Contents*, pages 140–151.

[Lin and Delp, 1999] Lin, E. T. and Delp, E. J. (1999). A review of fragile image watermarks. In *Proceedings of the Multimedia and Security Workshop (ACM Multimedia'99) Multimedia Contents*, volume 1, pages 25–29.

[Lin et al., 2005] Lin, P. L., Hsieh, C.-K., and Huang, P.-W. (2005). A hierarchical digital watermarking method for image tamper detection and recovery. *Pattern recognition*, 38(12) :2519–2529.

[Lin et al., 2004] Lin, P.-L., Huang, P.-W., and Peng, A.-W. (2004). A fragile watermarking scheme for image authentication with localization and recovery. In *Multimedia Software Engineering, 2004. Proceedings. IEEE Sixth International Symposium on*, pages 146–153.

[Liu et al., 2015] Liu, F., Gong, Z., Chen, Y., and Gu, Y. (2015). Segmentation of mass in mammograms by a novel integrated active contour method. *International Journal of Computational Science and Engineering*, 11(2) :207–215.

[Liu and Tan, 2002] Liu, R. and Tan, T. (March 2002). An SVD-Based Watermarking Scheme for Protecting Rightful Ownership. In *IEEE Transactions on Multimedia*, volume 4, pages 121–128.

[Machkour et al., 2009] Machkour, M., Khamlichi, Y. I., and Afdel, K. (2009). Data security in medical information system. In *Multimedia Computing and Systems, 2009. ICMCS'09. International Conference on*, pages 391–394. IEEE.

[Macq and Dewey, 1999] Macq, B. and Dewey, F. (1999). Trusted headers for medical images. In *DFG VIII-D II Watermarking Workshop*, volume 10. Erlangen Germany.

[Mavrotas, 2009] Mavrotas, G. (2009). Effective implementation of the ε-constraint method in multi-objective mathematical programming problems. *Applied mathematics and computation*, 213(2) :455–465.

[MedPix, 2017] MedPix (2017). Department of radiology and radiological sciences, uniformed services university of health sciences (USUHS).

[Memon and Wong, 1998] Memon, N. and Wong, P. W. (1998). Protecting digital media content. *Communications of the ACM*, 41(7) :35–43.

[Memon et al., 2011] Memon, N. A., Chaudhry, A., Ahmad, M., and Keerio, Z. A. (2011). Hybrid Watermarking of Medical Images For ROI Authentication and Recovery. *International Journal of Computer Mathematics*, 88(10) :2057–2071.

[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.

[Menezes et al., 1996] Menezes, A. J., Van Oorschot, P. C., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. CRC press.

[Meyer, 1995] Meyer, Y. (1995). *Wavelets and operators*, volume 1. Cambridge university press.

[Michalewicz, 2013] Michalewicz, Z. (2013). *Genetic algorithms+ data structures= evolution programs*. Springer Science & Business Media.

[Mitchell, 1998] Mitchell, M. (1998). *An introduction to genetic algorithms*. MIT press.

[Mostafa et al., 2010] Mostafa, S. A. K., El-Sheimy, N., Tolba, A. S., Abdelkader, F. M., and Elhindy, H. M. (2010). Wavelet Packets-Based Blind Watermarking for Medical Image Management. *Open Biomedical Engineering Journal*, 4 :93–98.

[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.

[Münch et al., 2004] Münch, H., Engelmann, U., Schröter, A., and Meinzer, H. (2004). The integration of medical images with the electronic patient record and their web-based distribution 1. *Academic radiology*, 11(6) :661–668.

[Navas et al., 2007] Navas, K., Nithya, S., Rakhi, R., and Sasikumar, M. (2007). Lossless watermarking in JPEG2000 for EPR data hiding. *Proc. IEEE-EIT*, 2007 :697–702.

[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.

[Navas et al., 2008] Navas, K., Thampy, S. A., and Sasikumar, M. (2008). EPR hiding in medical images for telemedicine. *International Journal of Biomedical Sciences*, 3(1) :44–47.

[Nayak et al., 2004] Nayak, J., Bhat, P. S., Kumar, M. S., and Acharya, U. R. (2004). Reliable transmission and storage of medical images with patient information using error control codes. In *India Annual Conference, 2004. Proceedings of the IEEE INDICON 2004. First*, pages 147–150.

[Nayak et al., 2009] Nayak, J., Subbanna Bhat, P., Acharya U, R., and Sathish Kumar, M. (2009). Efficient storage and transmission of digital fundus images with patient information using reversible watermarking technique and error control codes. *Journal of Medical Systems*, 33(3) :163–171.

[Nyeem et al., 2013] Nyeem, H., Boles, W., and Boyd, C. (2013). A review of medical image watermarking requirements for teleradiology. *Journal of digital imaging*, 26(2) :326–343.

[Ochi et al., 1998] Ochi, L. S., Vianna, D. S., Drummond, L. M., and Victor, A. (1998). A parallel evolutionary algorithm for the vehicle routing problem with heterogeneous fleet. *Future Generation Computer Systems*, 14(5-6) :285–292.

[O'Ruanaidh et al., 1996] O'Ruanaidh, J. J., Dowling, W., and Boland, F. (1996). Watermarking digital images for copyright protection. *IEE Proceedings-Vision, Image and Signal Processing*, 143(4) :250–256.

[Osyczka, 1985] Osyczka, A. (1985). Multicriteria optimization for engineering design. *Design optimization*, 1 :193–227.

[Osyczka and Kundu, 1995] Osyczka, A. and Kundu, S. (1995). A new method to solve generalized multicriteria optimization problems using the simple genetic algorithm. *Structural and Multidisciplinary Optimization*, 10(2) :94–99.

[Pan et al., 2009] Pan, W., Coatrieux, G., Cuppens-Boulahia, N., Cuppens, F., and Roux, C. (2009). Medical image integrity control combining digital signature and lossless watermarking. In *DPM/SETOP*, pages 153–162. Springer.

[Pan et al., 2010] Pan, W., Coatrieux, G., Cuppens-Boulahia, N., Cuppens, F., and Roux, C. (2010). Medical image integrity control combining digital signature and lossless watermarking. In *Data privacy management and autonomous spontaneous security*, pages 153–162. Springer.

[Pérez-Freire and Pérez-González, 2009] Pérez-Freire, L. and Pérez-González, F. (2009). Spread-spectrum watermarking security. *IEEE Transactions on Information Forensics and Security*, 4(1) :2–24.

[Pianykh, 2009] Pianykh, O. S. (2009). *Digital imaging and communications in medicine (DICOM) : a practical introduction and survival guide*. Springer Science & Business Media.

[Piva et al., 2005] Piva, A., Barni, M., Bartolini, F., and De Rosa, A. (2005). Data hiding technologies for digital radiography. *IEE Proceedings-Vision, Image and Signal Processing*, 152(5) :604–610.

[Podilchuk and Delp, 2001] Podilchuk, C. I. and Delp, E. J. (2001). Digital watermarking : algorithms and applications. *IEEE signal processing Magazine*, 18(4) :33–46.

[Popa, 1998] Popa, R. (1998). An analysis of steganographic techniques. *The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering*.

[Priya and Sadasivam, 2014] Priya, R. L. and Sadasivam, V. (2014). A survey on watermarking techniques, requirements, applications for medical images. *Journal of Theoretical and Applied Information Technology*, 65(1) :103–120.

[Qi and Qi, 2007] Qi, X. and Qi, J. (2007). A robust content-based digital image watermarking scheme. *Signal Processing*, 87(6) :1264 – 1280.

[Rahmat-Samii and Michielssen, 1999] Rahmat-Samii, Y. and Michielssen, E. (1999). Electromagnetic optimization by genetic algorithms. *Microwave Journal*, 42(11) :232–232.

[Ramabadran and Gaitonde, 1988] Ramabadran, T. V. and Gaitonde, S. S. (1988). A tutorial on CRC computations. *IEEE Micro*, 8(4) :62–75.

[Rechenberg, 1973] Rechenberg, I. (1973). Evolution strategy : Optimization of technical systems by means of biological evolution. *Fromman-Holzboog, Stuttgart*, 104.

[Rey and Dugelay, 2002] Rey, C. and Dugelay, J. (2002). A Survey of Watermarking Algorithms for Image Authentication. *EURASIP Journal on Applied Signal Processing*, 4314(6) :613–621.

[Roček et al., 2016] Roček, A., Slavíček, K., Dostál, O., and Javorník, M. (2016). A new approach to fully-reversible watermarking in medical imaging with breakthrough visibility parameters. *Biomedical Signal Processing and Control*, 29(August 2016) :44–52.

[Ruanaidh et al., 1996] Ruanaidh, J., Dowling, W., and Boland, F. M. (1996). Phase watermarking of digital images. In *Image Processing, 1996. Proceedings., International Conference on*, volume 3, pages 239–242. IEEE.

[Sang et al., 2006] Sang, J., Liao, X., and Alam, M. (2006). Neural-network-based zero-watermark scheme for digital images. *Optical engineering*, 45(9) :097006–097006.

[Schaffer, 1985] Schaffer, J. D. (1985). Multiple objective optimization with vector evaluated genetic algorithm. In *Proceeding of the First International Conference of Genetic Algorithms and Their Application*, pages 93–100.

[Schott, 1665] Schott, C. (1665). *Schola steganographia*. Jobus Hertz.

[Seenivasagam and Velumani, 2013] Seenivasagam, V. and Velumani, R. (2013). A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud. *Computational and mathematical methods in medicine*, 2013.

[Shang and Kang, 2013] Shang, Y.-f. and Kang, Y.-n. (2013). Medical images watermarking algorithm based on improved DCT. *Journal of Multimedia*, 8(6) :796–801.

[Shih, 2007] Shih, F. Y. (2007). *Digital Watermarking and Steganography : Fundamentals and Techniques*. CRC Press.

[Shih and Wu, 2005] Shih, F. Y. and Wu, Y.-T. (2005). Robust watermarking and compression for medical images based on genetic algorithms. *Information Sciences*, 175(3) :200–216.

[Simmons, 1984] Simmons, G. J. (1984). The prisoners' problem and the subliminal channel. In *Advances in Cryptology*, pages 51–67. Springer.

[Singh et al., 2016] Singh, A. K., Dave, M., and Mohan, A. (2016). Hybrid technique for robust and imperceptible multiple watermarking using medical images. *Multimedia Tools and Applications*, 75(14) :8381–8401.

[Singh and Chadha, 2013] Singh, P. and Chadha, R. (2013). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9) :165–175.

[Sivanandam and Deepa, 2007] Sivanandam, S. and Deepa, S. (2007). *Introduction to genetic algorithms*. Springer Science & Business Media.

[Srinivas and Deb, 1994] Srinivas, N. and Deb, K. (1994). Muiltiobjective optimization using nondominated sorting in genetic algorithms. *Evolutionary computation*, 2(3) :221–248.

[Stadler, 1988] Stadler, W. (1988). Fundamentals of multicriteria optimization. In *Multicriteria Optimization in Engineering and in the Sciences*, pages 1–25. Springer.

[Stanimirovic et al., 2011] Stanimirovic, I. P., Zlatanovic, M. L., and Petkovic, M. D. (2011). On the linear weighted sum method for multi-objective optimization. *Facta Acta Universitatis*, 26(4).

[Sumathi et al., 2008] Sumathi, S., Hamsapriya, T., and Surekha, P. (2008). *Evolutionary intelligence : an introduction to theory and applications with Matlab*. Springer Science & Business Media.

[Sweldens, 1996] Sweldens, W. (1996). The Lifting Scheme : A Custom-Design Construction of Biorthogonal Wavelets. *Applied and computational harmonic analysis*, 3(2) :186–200.

[Tanenbaum, 2003] Tanenbaum, A. (2003). *Computer Networks*. 4th edn. Pearson Education International, The Netherlands.

[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.

[Terzija and Geisselhardt, 2004] Terzija, N. and Geisselhardt, W. (2004). Digital image watermarking using complex wavelet transform. In *Proceedings of the 2004 Workshop on Multimedia and Security*, pages 193–198, New York, NY, USA. ACM.

[Tian-yu, 2011] Tian-yu, Y. (2011). A Robust Zero-Watermarking Algorithm Using Variance in Singular Value Decomposition Domain [J]. *Acta Photonica Sinica*, 6 :033.

[Ulutas et al., 2011] Ulutas, M., Ulutas, G., and Nabiyev, V. V. (2011). Medical image security and EPR hiding using Shamir's secret sharing scheme. *Journal of Systems and Software*, 84(3) :341–353.

[Van Schyndel et al., 1994] Van Schyndel, R. G., Tirkel, A. Z., and Osborne, C. F. (1994). A digital watermark. In *Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference*, volume 2, pages 86–90. IEEE.

[Vaudenay, 2006] Vaudenay, S. (2006). *A classical introduction to cryptography : Applications for communications security*. Springer Science & Business Media.

[Veldhuizen, 1999] Veldhuizen, D. (1999). Multiobjective evolutionary algorithms : classifications, analyses, and new innovations. *School of Engineering of the Air Force Institute of Technology, Dayton, Ohio*.

[Veysel, 2008] Veysel, A. (2008). A Singular Value Decomposition-based Image Watermarking Using Genetic Algorithm. In *International Journal of Electronics and Communications*, volume 62, pages 386–394.

[Wakatani, 2002] Wakatani, A. (2002). Digital watermarking for ROI medical images by using compressed signature image. In *System Sciences, 2002. HICSS. Proceedings of the 35th Annual Hawaii International Conference on*, pages 2043–2048. IEEE.

[Wang et al., 201] Wang, X., Yang, Y., and Yang, H. (201). Invariant image watermarking using multiscale harris detector and wavelet moments. *Comput. Electr. Eng*, 36(41) :31–44.

[Wicker, 1995] Wicker, S. B. (1995). *Error Control Systems For Digital Communication And Storage*, volume 1. Prentice hall Englewood Cliffs.

[Wicker and Bhargava, 1999] Wicker, S. B. and Bhargava, V. K. (1999). An Introduction to Reed-Solomon Codes. *Reed-Solomon codes and their applications*, pages 1–16.

[Wong, 1998] Wong, P. W. (1998). A public key watermark for image verification and authentication. In *Image Processing, 1998. ICIP 98. Proceedings. 1998 International Conference on*, volume 1, pages 455–459. IEEE.

[Wong and Memon, 2001] Wong, P. W. and Memon, N. (2001). Secret and public key image watermarking schemes for image authentication and ownership verification. *IEEE transactions on image processing*, 10(10) :1593–1601.

[Wong et al., 1995] Wong, S. T., Abundo, M., and Huang, H. (1995). Authenticity techniques for PACS images and records. In *Medical Imaging 1995*, pages 68–79. International Society for Optics and Photonics.

[Yang et al., 2012] Yang, Y., Lei, M., Liu, H., Zhou, Y., and Luo, Q. (2012). A novel robust zero-watermarking scheme based on discrete wavelet transform. *Journal of multimedia*, 7(4) :303–308.

[Yassin, 2015] Yassin, N. I. (2015). Digital watermarking for telemedicine applications : A review. *International Journal of Computer Applications*, 129(17).

[Zain and Fauzi, 2006] Zain, J. M. and Fauzi, A. R. (2006). Medical image watermarking with tamper detection and recovery. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*, pages 3270–3273. IEEE.

[Zhang and Zhang, 2004] Zhang, F. and Zhang, H. (2004). Digital watermarking capacity and reliability. In *e-Commerce Technology, 2004. CEC 2004. Proceedings. IEEE International Conference on*, pages 295–298. IEEE.

[Zhang et al., 2006] Zhang, J., Sun, J., Yang, Y., Liang, C., Yao, Y., Cai, W., Jin, J., Zhang, G., and Sun, K. (2006). Image-based electronic patient records for secured collaborative medical applications. In *Engineering in Medicine and Biology Society, 2005. IEEE-EMBS 2005. 27th Annual International Conference of the*, pages 3218–3220. IEEE.

[Zhao et al., 1998] Zhao, J., Koch, E., and Luo, C. (1998). In business today and tomorrow. *Communications of the ACM*, 41(7) :67–72.

[Zhou et al., 2002] Zhou, W., Rockwood, T., and Sagetong, P. (2002). Non-repudiation oblivious watermarking schema for secure digital video distribution. In *Multimedia Signal Processing, 2002 IEEE Workshop on*, pages 343–346. IEEE.

[Zhou et al., 2004] Zhou, X., Duan, X., and Wang, D. (2004). A semi-fragile watermark scheme for image authentication. In *Multimedia Modelling Conference, 2004. Proceedings. 10th International*, pages 374–377.

[Zinger et al., 2001] Zinger, S., Jin, Z., Maître, H., and Sankur, B. (2001). Optimization of watermarking performances using error correcting codes and repetition. In *Communications and Multimedia Security Issues of the New Century*, pages 229–240. Springer.

[Zitzler, 1999] Zitzler, E. (1999). Evolutionary algorithms for multiobjective optimization : Methods and applications.

[Zitzler and Thiele, 1998] Zitzler, E. and Thiele, L. (1998). An evolutionary algorithm for multiobjective optimization : The strength pareto approach. *TIK-report*, 43.

Thèse de Doctorat en Sciences en Informatique

Approches Evolutionnaires Hybrides pour Le Tatouage Numérique des Images.

Nour El-Houda GOLEA

Résumé

Au cours de ses des dernières années, le passage vers le monde numérique offre aux utilisateurs plusieurs commodités, pour utiliser, traiter, stocker et transmettre leurs données. En outre, l'évolution rapide et sans cesse des systèmes d'acquisition d'images a permis un formidable essor de l'utilisation de l'image numérique. En effet, la numérisation est une épée à double tranchant, elle offre plusieurs bénéfices d'une part et pose des problèmes de sécurité d'autre part. Pour cette raison, il est obligatoire de concevoir des systèmes de protection des images numériques contre toutes manipulations illégales. Dans ces dernières décennies, le tatouage numérique, une technique brillante proposée pour répondre à plusieurs aspects de la sécurité. Le principe de cette technique est d'implanter un signal numérique appelé watermark dans un autre signal numérique appelé signal hôte (texte, image, audio, vidéo, ...). Dans ce cadre, nous proposons dans cette thèse des nouvelles approches de tatouage numérique des images. La première contribution consiste à proposer une nouvelle approche évolutionnaire à base des algorithmes génétiques pour la protection de droit d'auteurs des images couleurs RGB. L'objectif de cette approche est d'optimiser les deux exigences contradictoires du tatouage : l'imperceptibilité et la robustesse. La deuxième et la troisième contributions décrient des nouvelles approches de tatouage appliquées à l'imagerie médicale. Ces deux approches sont inspirées de la transmission en réseau où l'utilisation des codes détecteur et correcteur des erreurs est apparu naturel. Une de ces approches repose sur l'utilisation du code détecteur des erreurs (CRC) afin de garantir l'authentification de la région d'intérêt de l'image médicale. Tandis que, l'autre utilise un code correcteur des erreurs (RS) pour assurer en plus de l'authentification, l'intégrité. Dans la quatrième contribution, nous proposons une nouvelle approche de tatouage de deuxième génération basée sur les Diagrammes de Voronoi (VD) et le code CRC en utilisant des polynômes standard de degré élevée ayant des propriétés mathématiques particulières comme CRC-32, CRC-16 et CRC-8 pour générer le watermark. Ce dernier est inséré dans chaque région de l'image après une décomposition en utilisant VDs.

Mots clés : Approches évolutionnaire, Optimisation multi-objectif, Algorithme génétique, Tatouage numérique, image numérique, Imagerie médicale.