République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Mustapha Ben Boulaid
Batna 2

Faculté de mathématiques et d'informatique

Thèse

En vue de l'obtention du diplôme de

Doctorat en Informatique

Méthodes pour la dissimulation d'information dans une image

Présentée Par

Delenda Sabah

Soutenue le : .....

Membres du jury :

Président :	Seghir Rachid	MCA	Université de Batna 2
Rapporteur :	Noui Lemnouar	Professeur	Université de Batna 2
Examinateurs :	Merah ElKamel	MCA	Université de Khenchela
	Melkemi Lamine	Professeur	Université de Batna 1
	Titouna Faiza	M CA	Université de Batna2

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mustapha Ben Boulaid
Batna2
Faculté des Mathématiques et d'informatique

Thèse

En vue de l'obtention du diplôme de
Doctorat en Informatique

Méthodes pour la dissimulation d'information dans une image

Présentée Par
Delenda Sabah

Membres du jury :

Président :	Seghir rachid	MCA	Université de Batna 2
Rapporteur :	Noui Lemnouar	Professeur	Université de Batna 2
Examinateurs :	Merah ElKamel	MCA	Université de Khenchela
	Melkemi Lamine	Professeur	Université de Batna 1
	Titouna Faiza	MCA	Université de Batna 2

À mes chers parents…
À mes soeurs et frères…
À tous ceux qui comptent pour moi…

Remerciement

Grand merci à Allah, miséricordieux, le tout puissant qui m'a donnée la force, la persévérance et la patience d'accomplir mon travail.

Ma gratitude, mes vifs remerciements et mes respects à mon encadreur Pr. Lemnouar Noui pour tous ses judicieux conseils, son temps qu'il m'a consacré et pour m'avoir toujours orientée vers un esprit purement scientifique.

Je tiens aussi à remercier les membres de jury : Dr. Seghir Rachid, Pr. Merah El Kamel, Pr. Melkemi Lamine, Dr. Titouna Faiza pour l'intérêt qu'ils ont porté à mon travail.

J'exprime également mes remerciements à mes chers parents qui n'ont jamais cessé de m'encourager à bien mener mes travaux. Et à tous ceux qui m'ont encouragée et soutenue moralement et intellectuellement.

Résumé

L'image numérique est l'un des moyens le plus utilisé dans le domaine de communication universelle, C'est aussi le moyen le plus efficace et simple pour communiquer. Ainsi, elle est exploitée par des utilisateurs (médecine, commerce,militaire, ...). Les technologies de communication soulèvent un nombre important de problèmes : la distribution illégale, la falsification et l'authentification. Pour cela, le développement des technologies de multimédia distribuées sur les réseaux d'internet fait apparaître de nombreux et de nouveaux mécanismes de dissimulation qui contribuent à l'amélioration continue de la qualité des schémas de sécurité. Dans ce travail, nous avons présenté deux contributions différentes afin de sécuriser la transmission d'images à travers un support média. La première proposition consiste en un algorithme de tatouage des images couleur (RGB) basé sur l'insertion dans le domaine transformé en utilisant la décomposition polaire, ce système est aveugle (la détection de watermark ne nécessite pas l'image originale). Tandis que la deuxième proposition présente un schéma de stéganographie qui permet de cacher une image en niveau de gris dans une image en couleur, ce schéma est aussi basé sur l'insertion dans le domaine transformé. A notre connaissance la décomposition polaire est utilisée pour la première fois dans ce domaine. Des comparaisons avec des schémas de dissimulation récemment proposés ont été réalisées, elles montrent que les algorithmes proposés offrent des performances très convenables et efficaces.

Mots clés : Décomposition polaire, sécurité d'image, décomposition en valeurs singulièress (SVD)

Abstract

Digital image is one of the most important means used in global communications, but it is also the most effective and simple way to communicate. Thus, it is also exploited by users (medicine, trade, military, ...). Communication technologies raise a number of problems: illicit distribution, counterfeiting and authentication. Therefore, the development of multimedia distributed technologies over internet reveals many and new mechanisms of hiding data that contribute to the continuous improvement of the quality of security schemes. In this work, we presented two different contributions to secure the transmission of images through the cover media. The first proposal is an algorithm of watermarking color images based on insertion in the transform domain using polar decomposition, and this system is blind (the watermark detection does not require the original image). While the second proposal represents a steganography scheme that embed a gray image into color image. This diagram is also based on insertion in the transform domain. In our knowledge polar decomposition is used for the first time in this domain Comparisons have been realized with the recently proposed schemes of hiding data showing that the proposed algorithms provide very appropriate and effective performance.

key words: Polar decomposition, image security, Singular value decomposition (SVD).

ملخص

صورة الرقمية هي واحدة من أهم الوسائل المستخدمة في مجال الاتصالات العالمية، بل هي أيضا الطريقة الأكثر فعالية و البسيطة للتواصل. وبالتالي، يتم استغلالها أيضا من قبل مستخدمين (الطب، التجارة، العسكرية،. . .). وتثير تكنولوجيات الاتصال عددا من المشاكل: التوزيع غير المشروع، والتزوير، والتوثيق. و لذلك، فإن تطوير تكنولوجيات الوسائط المتعددة الموزعة على الشبكات الانترنت يكشف عن آليات عديدة وجديدة للإخفاء التي تساهم في التحسين المستمر لنوعية المخططات الأمنية. في هذا العمل، درسنا مساهمتين مختلفتين لتأمين نقل الصور من خلال وسائط الإعلام. الاقتراح الأول هو خوارزمية وشم الصور الملونة، تعتمد على الإدراج في المجال المحول باستخدام التحليل القطبي، وهذا النظام هو أعمى (كشف العلامة لا يتطلب الصورة الأصلية). في حين أن الاقتراح الثاني يمثل مخطط إخفاء المعلومات الذي يسمح بإخفاء صورة رمادية في صورة ملونة، ويستند هذا المخطط أيضا على الإدراج في المجال المحول. و كما استخدم التحليل القطبي لأول مرة في هذا المجال. وقد أجريت مقارنات مع مخططات الإخفاء المقترحة مؤخرا، وهي تبين أن الخوارزميات المقترحة تقدم أداء مناسبا وفعالا.

الكلمات المفتاحية: التحليل القطبي، أمن الصورة، تحليل القيمة المفردة

Contents

List of Figures

List of Tables

Publications

1. Sabah. Delenda and Lemnouar. Noui, “A new steganography algorithm using polar decomposition,” Information Security Journal: A Global Perspective, vol. 27, no. 3, pp. 133–144, 2018.
2. Sabah Delenda , Lemnouar Noui, ‘A new algorithm for watermarking color images using polar decomposition ’, International conference on coding and cryptography (ICCC 2015). De 2 au 5 November 2015, Algérie, USTHB.

Introduction générale

De nos jours; plusieurs sortes d'informations se transfèrent (images, document, sons ...) à travers l'Internet. Ces données sont devenues des éléments essentiels dans la société moderne, et surtout pour le stockage et pour la communication. Dans les dernières années, les technologies de l'information et de la communication ont connu un vaste développement, et surtout avec le développement de l'internet et l'augmentation des utilisateurs illégaux des médias. Donc la transmission et la distribution de plusieurs informations numériques exigent la protection et la sécurité. Certainement, la tâche la plus importante est celle de rendre les informations confidentielles et intelligibles pour tout autre que le destinataire légitime.
Pour protéger les informations sensibles quand elles sont transmises contre tout accès non autorisé, la dissimulation s'avère être la principale solution conçue pour assurer cette fonctionnalité. Plusieurs techniques de dissimulation ont été proposées par les chercheurs pour répondre au problème de risque d'intrusion des utilisateurs illégaux, et de rendre les informations confidentielles et invisible à tout autre personne que le destinataire légitime. La dissimulation d'information c'est l'art de cacher des informations comme texte, image, audio,..., dans une autre donnée numérique: texte, image, vidéo, audio, http..., pour cela des différentes techniques ont été proposées pour assurer la protection de ces données, et effectuer une transmution plus sécurisée. Les algorithmes et les techniques de dissimulation d'information se distinguent les uns des autres selon l'objectif et l'application utilisée. Plusieurs techniques de dissimulation d'information ont été proposées. Les techniques les plus connues sont la stéganographie et le tatouage. Pour transmettre des messages ou n'importe quelle donnée numérique, on applique des algorithmes de cryptage, ou des algorithmes de stéganographie qui laissent la communication non chiffrée, mais elle ne peut

pas être détectée par une tierce personne. Le tatouage est un autre algorithme de dissimulation d'information qui permet de protéger les droits d'auteurs, le commerce électronique, la médecine et la communication internet.
Au cours des dernières années, les images numériques représentent un énorme type d'information impliquée dans les communications modernes, et comme la vision humaine est très faible sur de petits changements de couleur, la steganographie s'avère être la principale solution conçue pour assurer la confidentialité du transfert des données sous la forme imperceptible, les chercheurs ont construit plusieurs méthodes de dissimulation des informations secrètes dans une image en utilisant une variété de techniques.

Contribution

En parallèle à l'énorme développement des techniques de cacher des informations dans des images numériques, ces dernières années, les chercheurs ont accordé plus d'attention à l'étude de ces techniques en termes d'analyse de sécurité. Ils ont constaté que plusieurs systèmes de dissimulation souffrent d'un ou plusieurs problèmes tel que la faible sensibilité aux attaques [2][3][4][5][6][7][8] , la capacité d'insertion [5][8][9][10][11][12] et l'invisibilité (ou l'imperceptible) d'insertion [13][14][15][16][17].
Afin de sécuriser encore la transmission de données secrètes à travers l'internet et d'obtenir de meilleures performances, nous allons présenter dans cette thèse deux méthodes, elles sont développées spécialement pour assurer la protection des droits d'auteurs et sécuriser la transmission des données dans le réseau internet et camoufler l'information secrète.

La première méthode:

Notre contribution se place dans le cadre de proposer des nouveaux schémas de tatouage d'images couleurs RGB. Nous avons travaillé sur différents critères : robustesse, l'invisibilité, et le domaine transformé, Notre contribution est caractérisée par les points suivants :

- L'algorithme est aveugle (la détection du watermark ne nécessite pas l'image originale).

- Le watermark est inséré dans le domaine fréquentiel, en utilisant la décomposition polaire.
- L'algorithme maintient une haute qualité d'image tatouée.
- L'algorithme du tatouage est robuste.
- Le watermark inséré est une image binaire.
- L'algorithme de tatouage est publique, la sécurité dépend d'une clé secrète.

Cependant, l'algorithme proposé n'est pas probabiliste. Sur la base des résultats obtenus, nous pouvons affirmer que le schéma proposé est adapté pour les applications qui demandent une sécurité moyenne.

La deuxième méthode :

Nous avons proposé un algorithme de stéganographie qui est un autre schéma de dissimulation des informations dans une image [18]et cette fois-ci pour assurer une communication secrète , c'est-à-dire protéger la transmission des informations secrètes. Ce schéma propose de cacher une image en niveau de gris dans une autre image en couleur. Notre méthode est caractérisée par les points suivants

- L'algorithme est aveugle (l'extraction de donnée secrète ne nécessite pas l'image de couverture).
- Les données secrètes sont des images en niveau de gris.
- Des performances satisfaisantes de sécurité ont été obtenues en utilisant l'insertion dans le domaine fréquentiel, en utilisant la décomposition polaire.
- l'algorithme est robuste (résiste aux attaques conventionnels comme les attaques géométriques (rotation, Scaling (modification des dimension), cropping,...), et les attaques d'effacement (Débruitage, Compression JPEG,...).

Cette nouvelle méthode est testée, les résultats des performances obtenues confirment l'efficacité et la sécurité de notre schéma en utilisant les différentes mesures de sécurité.

Organisation de la thèse Notre manuscrit est réparti en deux parties, la première partie présente le contexte de notre travail, alors que la seconde partie expose notre contribution. La première partie est organisée comme suit:

- Le premier chapitre décrit les outils, les principaux aspects et les terminologies liés aux évolutions des technologies de dissimulation, les techniques d'insertion, et particulièrement les caractéristiques de dissimulation. Ensuite on exposera une idée générale sur le domaine des images numériques, Plus précisément, nous présentons une introduction aux images numériques, quelques terminologies et quelques notions pertinentes.
- Le deuxième chapitre donne une présentation des notions de base en mathématique nécessaires à la thèse.
- Le troisième chapitre met le point sur les différentes techniques de dissimulation des données dans une image.

La deuxième partie est composée de deux chapitres présentant les deux contributions

- La première concerne le tatouage d'images couleurs RGB.
- L'objectif de la deuxième est de cacher des images de niveau de gris dans une autre image en couleur RGB.

Dans les deux derniers chapitres , nous présentons des exemples et des résultats expérimentaux afin d'évaluer l'efficacité des méthodes proposées. Le manuscrit s'achève par une conclusion générale et quelques perspectives concernant l'amélioration du système dans le futur.

Part I

Introduction sur le domaine de recherche

Chapter 1

Etat de l’art

1.1 Introduction

la transmission et la protection des données numériques sont des grands défis pour les utilisateurs d'ordinateur pour cela, des différents techniques de dissimulation des informations ont été proposé pour assurer la protection de ces données. [19]. Ces techniques sont variés selon leurs applications et l'objectif de la protection utilisée.
La dissimulation d'information plus particulièrement l'insertion de données cachées peut être une réponse au problème de protection des documents. La stéganographie et le tatouage sont deux techniques reposant sur le data hiding (la dissimulation d'information) mais leurs objectifs sont différents, ainsi que les motifs d'attaques et le but de dissimilation, Pour la stéganographie, le but est de dissimuler un message secret dans le médium de couverture, Pour le tatouage, on cherche juste à marquer une image. Il y'a deux grands domaines de dissimulation d'une information, le domaine spatial et le domaine fréquentiel. L'image est l'un des moyens les plus importants dans le domaine de communication universelle, C'est aussi le moyen le plus efficace pour communiquer, particulièrement dans le domaine de communication militaire, dans la médecine et la communication internet. Le traitement d'images est un système basé sur l'informatique et des applications mathématiques qui étudie les images numériques et leurs transformations dans le but d'améliorer leur qualité ou d'en extraire de l'information.
Dans ce chapitre, nous montrons comment on va sécuriser des données numériques en donnant brièvement les concepts de bases de cryptographie et la Dissimulation d'information (data hiding). Nous abordons, par la suite la définition d'une image et leur résolution, et comment on stocke l'image dans un ordinateur et on termine par les attaques sur les images et la stéganalyse.

1.2 Sécurité de documents numériques

Pour la protection des informations numériques on utilise des techniques de sécurité qui concerne principalement les aspects suivants:

- La confidentialité;
- L'intégrité;

- L'authentification;
- La non répudiation.

Ces dernières exigent des méthodes principales et des concepts mathématiques comme l'art de chiffrer comme la cryptographie, la stéganographie et le tatouage.

1.2.1 La confidentialité

«La confidentialité» ou masquage des données, garantit que le contenu d'une communication ou d'un fichier n'est pas accessible aux tiers personne, c'est à dire seules les personnes autorisées peuvent prendre connaissance des données échangées. Les mécanismes qui permettent d'obtenir ce service sont la cryptographie et la steganographie.

1.2.2 L'intégrité

L'intégrité garantit qu'un message ou un document électronique n'a pas été trafiqué c'est-à-dire n'a pas été modifié de façon malveillante pendant son transfert sur le canal de communication.

1.2.3 L'authentification

Il s'agit de garantir l'identité d'une entité donnée ou l'origine d'une communication ou d'un document. c'est à dire authentification de l'origine des données: elle sert à prouver que les données reçues ont bien été émises par l'émetteur déclaré. Dans ce cas l'authentification désigne souvent la combinaission de deux services: authentification et intégrité en mode non connecté. Ces deux services n'ont en effet pas de sens séparément et sont souvent fournis conjointement .

1.2.4 La non-répudiation

Il s'agit de se protéger contre la contestation d'envoi ou de réception d'un message ou d'un document électronique lors d'une transaction. En d'autres termes, il s'agit

de garantir que l'expéditeur d'un message ne peut pas plus tard nier l'envoyé du message et que le destinataire ne peut pas nier la réception du message. Le service de non-répudiation est réalisé par une signature numérique, qui a une valeur juridique en France depuis la loi du 20 mars 2000 [20].

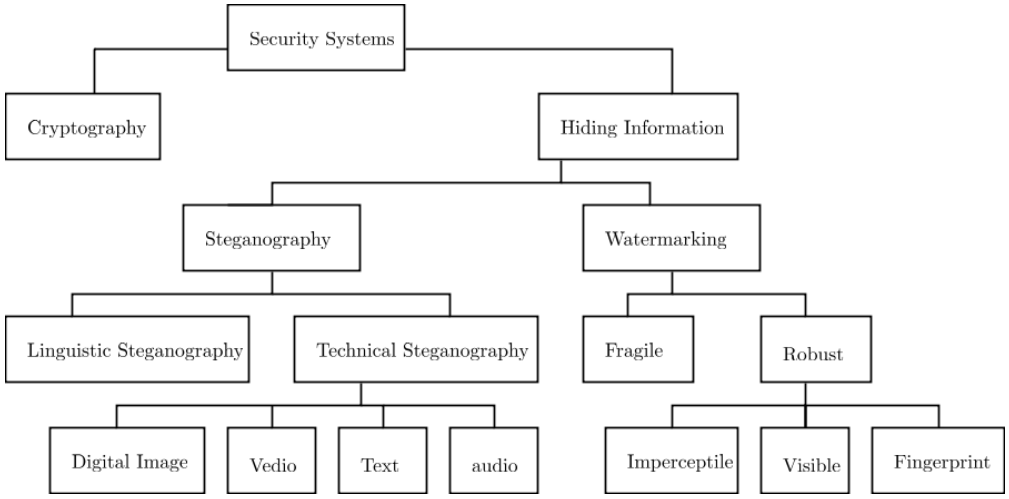

Figure 1.1: Sécurité des documents

1.3 La cryptographie et la stéganographie

Deux pratiques qui sont toujours retrouvées en concurrence pour établir une communication numérique sécurisée: la cryptographie (écriture secrète) et la stéganographie (écriture couverte).
La cryptographie et la stéganographie sont souvent très proches mais ne visent pas le même objectif:

- La cryptographie: il s'agit d'établir une liaison sécurisée entre deux personnes A et B en chiffrant la communication ce qui la rend incompréhensible pour une tierce personne T.

- La steganographie (Chiffrement à l'imperceptibilité):
  Dans la stéganographie la communication n'est pas chiffrée. l'objectif c'est de rendre la comunication invisible entre deux personnes et elle ne peut pas être

détectée par une tierce personne T. T ne se doute pas que A et B échangent des messages.

1.4 Dissimulation d'information (data hiding)

La data hiding consiste à dissimuler des informations dans un document formé de données numériques. En dehors du domaine numérique, ces pratiques sont très anciennes et ne sont plus utilisés de nos jours.
Dans la dissimulation d'information, le problème classique pour la communication avec des données cachées a été proposé premièrement par Simmons [21][22], on a deux principes d'insertion des informations. La steganographie c'est la communication couverte, cette action permet de garantir la confidentialité des données transmises. L'autre principe c'est le tatouage permet d'insérer une information dans un document et permet de l'authentifier et de garantir son intégrité.

1.4.1 Les différentes techniques de dissimulation d'information

Les algorithmes de dissimulation d'information se distinguent les uns des autres par les quatre points suivants [23] :

1. La manière de sélectionner les points ou les blocs dans le document de couverture (le couver objet) qui porteront l'information à cacher;
2. Le choix d'un espace de travail pour réaliser l'opération d'insertion (domaine spatial, domaine transformé comme DCT, DWT, fourier Mellin, ...);
3. Le principe utilisé pour mettre en forme l'information à cacher avant l'insertion (redondance, codes correcteurs, ...);
4. La manière d'insérer l'information dans le support de couverture (le couver objet)

Les schémas de dissimulation d'information portent des noms différents, on en distingue trois principaux[23]:

- La stéganographie (Data Hiding) [24][25] cherche à cacher un message secrett, dans un support de sorte que personne ne puisse distinguer un support original d'un stégo-support. La nature de l'information dissimulée ne revêt pas d'importance: il peut être un texte en clair ou un texte chiffré. Ce message n'a a priori aucun lien avec le stégo-support qui le transporte[26].

- Le tatouage cherche à répondre au problème de la protection des droits d'auteur [27][28][29]. Un client essaye de détecter la présence d'une marque dans un support, puis s'il existe, il vérifie si l'utilisateur a bien acheté une licence. Il s'agit bien de dissimulation d'information puisque, pour y parvenir, on insère un tatouage (ou marque, ou filigrane) dans le support spécifique au propriétaire. Comme celui-ci souhaite protéger son document et non une version trop déformée, l'insertion doit minimiser les modifications subies par le document afin d'être imperceptible. Ensuite, chaque copie du document tatoué contient la même marque, celle du propriétaire légal. Ici, la dissimulation ne signifie pas la même chose qu'en stéganographie : un attaquant sait qu'un tatouage est présent dans le document tatoué, mais cette connaissance ne doit cependant pas lui permettre de le retirer.

- Le fingerprinting assure la détection des copies illégales d'un document tatoué. Chaque utilisateur authentifié reçoit sa propre copie de document qui contient une empreinte l'identifiant. Ainsi, lorsqu'une copie illégale est découverte, la lecture de l'empreinte indique la source de la fuite. A la différence du tatouage où l'origine du document importe, le fingerprinting se préoccupe plutôt de l'utilisateur final. Chaque copie de document contient une information différente, relative à son utilisateur, rendant alors chaque document tatoué différent.

1.4.2 Le schéma de dissimulation :

Le processus complet de dissimulation d'information repose sur deux opérations:

  – L'insertion: qui consiste à insérer l'information dans le support (le document originale dans le tatouage ou le support de couverture dans la

steganographie);

- L'extraction, qui récupère cette information;

- Le mot détection est également utilisé lorsqu'il s'agit de vérifier la présence d'une information dans le support tatoué, sans pour autant vouloir l'extraire.

1.4.3 Les caractéristiques de dissimulation d'information:

Les applications de dissimulation sont triées en fonction de trois critères:

L'imperceptibilité (l'invisibilité) : Les données ne doivent pas être visibles dans le stégo-support. Pour le tatouage, l'objectif est de ne pas détériorer le document protégé c'est à dire la marque doit être invisible à l'oeil humain.
Pour mesurer le degré de l'imperceptibilité ou l'invisibilité, le $PSNR$ est communément utilisé.

La capacité: La capacité d'un système de dissimulation c'est le rapport de nombre de données à dissimuler sur taille de support (le support de couvertur), par exemple. Ou la capacité est la quantité de bits significatifs dissimulés dans le support de couverture. De façon générale, plus la capacité est faible, plus la robustesse et l'imperceptibilité sont fortes, si on insère une marque de grande taille, l'image tatoué risque d'être bien dégradée et le tatouge perd son invisibilité

La robustesse : c'est la résistance de support aux différentes dégradations ou attaques par exemple: la résistance de système de dissimulation dans une image face à des transformations de l'image de couverture. Ces attaques sont dénommées «attaques aveugles», car le pirate agit sans réellement savoir ce qu'il fait. Il espère ainsi laver l'image.

La fragilité est le contraire de la robustesse; une marque W est fragile si sa détection échoue lors de la modification d'un seul pixel de l'image.

La sécurité: caractérise la façon dont la marque va résister à des attaques «malicieuses». par exemple, le pirate essaie à laver l'image de façon intelligente. Il est sensé connaître l'algorithme et va chercher la clé qui lit le tatouage.

1.5 Le tatouage numérique (watermark)

Le tatouage numérique (en anglais digital watermark) [30]est une technique permettant d'ajouter des informations à un fichier ou signal audio, vidéo, une image ou un autre document numérique. généralement , Le message inclus dans le document hôte, appelé la marque (en anglais wetermark) ou bien simplement message, ce message est un ensemble de bits, dont le contenu dépend de l'application. La marque peut être le nom ou un identifiant, du propriétaire, de l'acheteur ou encore une forme de signature décrivant le document hôte.

1.5.1 Types de tatouages

Généralement, le tatouage peut être classé en deux classes: visibles et invisibles

Le tatouage visible Les tatouages visibles altèrent le signal ou le fichier (par exemple ajout d'une image pour en marquer une autre). Il est fréquent que les agences de photos ajoutent un tatouage visible en forme de copyright de leurs photos.

Le tatouage invisible Le tatouage invisible modifie le document d'une manière imperceptible par des autres utilisateurs (par exemple en ne modifiant que le bit le moins significatif de chaque octet). Le tatouage numérique invisible peut être considéré comme une forme de stéganographie, puisque les autre utilisateurs ignorent la présence du tatouage.

Figure 1.2: Exemple de tatouage visible: (a) l'image sans marque, (b) l'image avec marque

Figure 1.3: Exemple de tatouage invisible: (a) l'image originale, (b) la marque, (c) l'image tatouée.

– Il existe aussi le tatouage fragile[31]: c'est un tatouage invisible, qu-est utilisé pour détecter toute modification du document.

1.5.2 Le schéma de tatouage

Le schéma classique de tatouage se décompose en trois phases [32]: la phase d'insertion, la phase de transmission et la phase de détection.

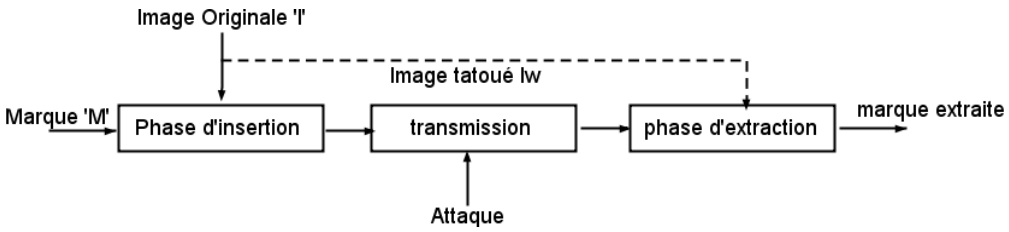

Figure 1.4: Schéma général du tatouage numérique

La phase d'insertion

Cette phase comprend deux étapes principales: la génération et l'insertion de la marque, Par exemple, pour l'objectif d'inserer une marque dans l'image originale notée I,on prend une marque W qui peut être une séquence pseudo aléatoire possédant certaines propriétés ou bien une donnée binaire -1, +1 ou bien une petite image ou un message M crypté par une clé spécifique C_w, permet d'assurer un certain niveau de sécurité, le résultat de tatouage est une image tatoué notée I_w, le processus d'insertion peut se faire dans un espace d'insertion T(I) qui peut être le domaine spatial ou bien le résultat d'une transformation réversible qui facilite l'insertion comme la Transformée en Cosinus Discrète (TCD), la Transformée de Fourier Discrète (TFD) ou encore une Transformation par Ondelettes (TOD) [33] ....

La phase de transmission

Cette phase peut être représentée comme la transmission des données par un support physique comme la publication des images dans le net où la plupart des attaques se produisent.

La phase d'extraction

La détection ou l'extraction de la marque W (ou le message M) incorporé dans un document hote ont pour rôle d'attester si la signature est présente ou non dans l'image. Si la signature est présente, le message qui lui est associé peut ensuite être extrait .
L'image originale et la clé secrète peuvent être ou non nécessaires lors de la détection ou l'extraction, selon les différents algorithmes d'extraction.
les différents algorithmes d'extraction sont:

- **Les schémas non-aveugles:** La détection est dite "non-aveugle" si l'image originale et la clé secrète (privée) sont nécessaires;

- **Les schémas semi-aveugles:** Une détection "semi-aveugle" n'utilise pas l'image originale, mais elle se base sur quelques caractéristiques de cette dernière;

- **Les schémas aveugles :** c'est le cas lorsque l'image originale n'est pas disponible pendant le processus d'extraction, si la clé privée est aussi absente la détection est dite à clé publique;

- **Les schémas asymétriques :** la détection par algorithmes asymétriques peut être schématisée comme une détection aveugle, ces algorithmes utilisent des clés différentes pour insérer et détecter la marque;

1.6 La steganographie

Le mot stéganographie: vient du grec "'steganos"' (caché ou secret) et "'graphy"' (écriture ou dessin) et signifie, littéralement, "'écriture cachée"'. La stéganographie a pour fonction de permettre la transmission sécurisée de messages (ou image au vidéo ...) secret dans des circonstances où la cryptographie ne peut être mise en œuvre.
La stéganographie est un procédé de cacher des donnés, c'est à dire c'est l'art et

la science de dissimuler un message ou une image ou autre document caché dans un autre message quelconque qui peut être une image ou une vidéo . . . .

1.6.1 Le Schéma de stéganographie

La mise en œuvre d'un schéma de stéganographie. Soient Alice et Bob deux personnes partagent un secret commun et désirant communiquer ensemble de façon <sécurisée>.

Insertion: Pour envoyer un message à Bob, Alice effectue les opérations suivantes:

1. Elle compresse un message secret ou presente le secret chifré pour l'insertion,
2. Elle génère un support de couverture,
3. L'algorithme de stéganographie sélectionne les sous parties du support favorables à la dissimulation,
4. Il insert ensuite aléatoirement, à l'aide de la clé stéganographique, le message secret dans les parties favorables,
5. Alice envoie le stégo-médium (ou stégo-support) par un canal classique.

Extraction: Pour lire le message d'Alice, Bob effectue les opérations suivantes:

1. Bob reçoit le stégo-médium par le canal classique,
2. L'algorithme de stéganographie sélectionne les sous parties du support favorables à la dissimulation,

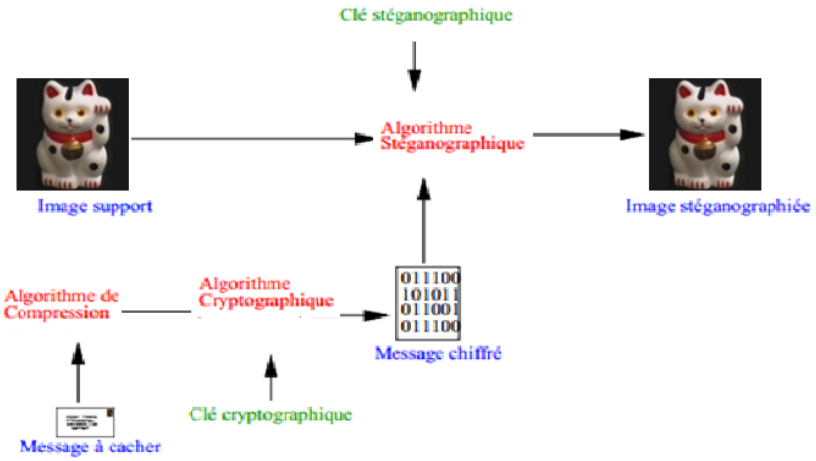

Figure 1.5: Etape de dissimuler une information

3. Il retrouve la position du message secret dans les parties favorables, à l'aide de la clé stéganographique,

4. Il extrait le message secret.

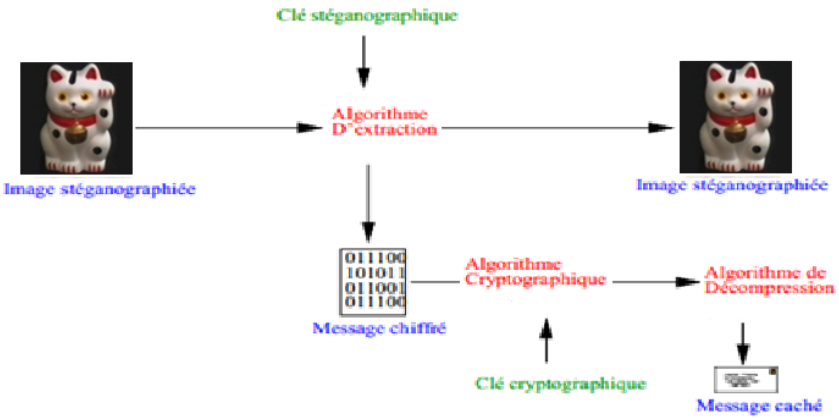

Figure 1.6: Etape d'extraction d'une information

1.6.2 Classification des schémas de steganographie

Le contexte dans lequel se situe un schema de steganographie permet de le classer dans une des catégories suivantes [34] :

- Stéganographie pure: aucune entente préalable, autre que le choix de l'algorithme, n'est nécessaire, Alice et Bob utilisent le canal pour échanger des informations;
- Stéganographie à clé secrète: Alice et bob conviennent au préalable d'une clé qui leur sert à insérer puis extraire le message du stego-medium;
- Stéganographie à clé publique: tout comme en cryptographie, Alice utilise le clé publique de Bob lorsqu'elle souhaite lui envoyer un message. Bob, pour sa part, l'extrait à l'aide de sa clé privée.

1.6.3 Les différentes techniques d'insertion

Le domaine spatial

En réalité, c'est le domaine de donnée de l'image ou ensemble de pixels d'image. L'algorithme va traiter directement avec les valeurs de pixels et les changer afin de cacher une marque. La plupart d'algorithmes utilisent le LSB.
On cite quelque exemples:

L'insertion dans les bits de poids faibles Le bit de poids faible (en anglais least significant bit, ou LSB[35]) c'est pour un nombre binaire le bit ayant dans une représentation donnée la moindre valeur.
Exemple: pour un simple nombre en représentation binaire conventionnelle, le LSB est le bit le plus à droite: 101110. c'est 0), à l'opposé, on a le bit de poids fort (MSB). Les caractéristiques de cette méthode sont:

- L'imperceptibilité: la méthode ne tient compte quasiment d'aucun modèle de la vision humaine. L'insertion a lieu dans n'importe quelle région de l'image.
- La robustesse: Celle-ci est très faible. En effet, la methode ne résiste à aucune transformation. si la moindre compression va changer les bits de

poids faibles ceci permet complètement laver l'image. Il en est de même pour tous les filtres.

– La capacité: Celle-ci est excellente, nous pouvons mettre 1 bit de tatouage pour 8 bits de données.

Spread spectrum (ou spectre large) Il s'agit là de la technique de marquage la plus connue et la plus employée en ce moment. Au moment de l'insertion du tatouage, on peut tenir compte d'un modèle HVS, pour modifier localement l'amplitude du tatouage et ainsi rendre le marquage moins visible. On effectue la détection du marquage en faisant la corrélation du signal watermarké et du signal de marquage [20].

Le domaine fréquentiel

Domaine transformé ou domaine fréquentiel est obtenu de domaine spatial par une transformation. Par exemple, pour inserer des données dans une image, on va changer les coefficients pour implémenter le procédé d'insértion. En suite, une transformation inverse s'applique afin d'acquérir l'image dans la forme originale.
La transformation peut se réaliser en toute l'image ou en des blocs qu'on les obtient par une division d'image en blocs. La deuxième approche permet de réduire le temps d'exécution.

La transformation en cosinus discrète La transformation en cosinus discrète bidimensionnelle DCT-2D ou DCT[36] est une méthode consistant à transformer l'image du domaine spatial au domaine fréquentiel en la décomposant sur une base de fonctions cosinus. La DCT est un mécanisme de base pour décorréler les pixels de l'image et regrouper l'énergie du signal image sur quelques coefficients DC et AC (voir la Figure 1.7). En général, les coefficients de basse fréquence ont des amplitudes non-nulles alors que plusieurs coefficients AC de haute fréquence ont des amplitudes faibles. Les méthodes de compression telles que JPEG prennent avantage de cette propriété pour couper l'information

au niveau des hautes fréquences alors que les basses fréquences sont préservées. Rappelons que la perte d'information s'effectue par quantification des coefficients DCT ou leur mise à zéro. L'image sera reconstruite en appliquant la transformation inverse DCT-1[37]

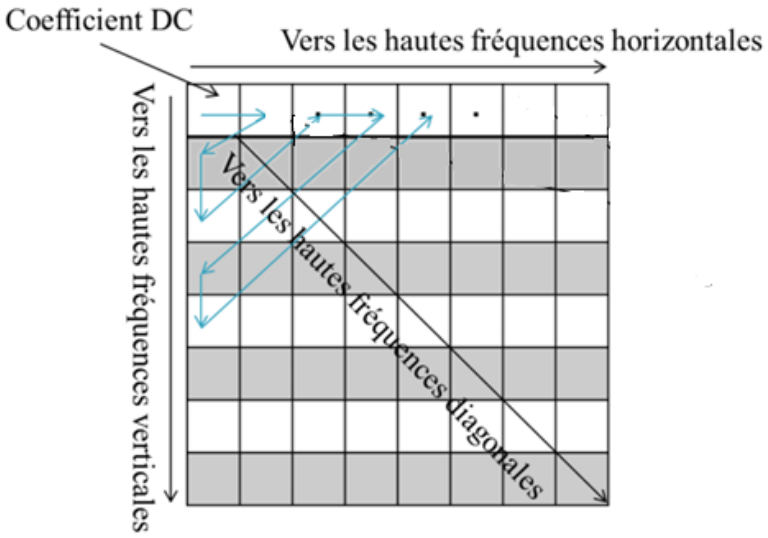

Figure 1.7: Les coefficients de la DCT

Figure 1.8: La transformation en cosinus discrète

La transformation en ondelettes DWT La transformation en ondelettes DWT[36] est une méthode consistant à transformer l'image du domaine spatial au do-

maine spatio-fréquentiel. La DWT se base sur des opérations de filtrage passe-haut et passe-bas et d'échantillonnage appliquées selon un algorithme arborescent et récursif. Le filtrage consiste à décomposer l'image en sous-bandes et l'échantillonnage vise à réduire la résolution de chaque sous-bande au minimum requis. Pour une décomposition à un seul niveau de résolution, la DWT représente l'image sous forme de quatre sous-bandes de résolution inférieure, une représente l'image d'approximation et les trois autres montrent les détails de l'image à orientations horizontales, verticales, et diagonales. La transformée en ondelettes inverse DWT permet une reconstruction parfaite de l'image à partir de ses sous-bandes ondelettes[37].

Figure 1.9: La transformation en ondelettes

1.6.4 Quelques applications classiques de la stéganographie

Une image peut en cacher une autre [38] La stéganographie appliquée aux images numériques s'agit d'« encapsuler » un fichier secret dans un document hôte qu'il est une image. De la sorte, sans conséquence sur l'apparence (l'image pourra être visionnée sans problème), l'image contiendra en fait un message caché.

Les méthodes pour dissimulier un message secret (image, texte) dans une image numérique sont multiples. la plus part de ces méthodes consiste à manipuler les bits de poids faibles des pixels. En l'occurrence, il s'agit de « rogner » sur les bits de chaque pixel d'une image et d'y ajouter le code binaire du fichier

numérique secret[39].
Les pixels d'une image représenter en RGB (ou RVB) sont souvent codés sur trois octets (soit 24 bits), c'est à dire il y a 16,8 millions de couleurs, on comprend qu'une telle dégradation de l'image soit indiscernable à l'œil nu.

Dissimuler un message dans un texte [39] Quoique très anciennes et simples à mettre en œuvre, les techniques stéganographiques consistant à dissimuler un message dans du texte restent toujours d'actualité [23]. Ceci d'autant plus que la quantité de courriels échangés ne cesse de prendre un essor croissant.
Comme nous allons le voir, la dissimulation d'information dans le texte n'a pas grand-chose à voir avec l'image. En effet, alors que la dégradation de l'image pouvait passer inaperçue (l'oeil devant détecter 16,8 millions de couleurs), l'altération d'un texte sera aisément discernable: soit le texte est identique à l'original, soit il ne l'est pas. Dès lors, toutes les méthodes que nous allons présenter vont avoir pour objectif de tendre vers un endommagement minimal du texte original[39].

Son [40][41] De petites variations d'oreille non imperceptible, à basses fréquences ou ce que l'on appelle le bruit de fond peuvent contenir une grande quantité d'informations. par des technique et un petit génie peut cacher les secrets. Ce bruit est préférable d'être transmis numériquement, sinon les pertes de transmission réelles peuvent effacer complètement le message caché.

1.6.5 La différence entre le watermak (le tatouage) et la steganographie

La stéganographie et le watermark (ou le tatouage) sont deux techniques reposant sur le data hiding (la dissimulation d'une information) mais leurs objectifs sont différents, ainsi que les motifs d'attaques. Pour la stéganographie, le but est de dissimuler un message secret dans le support de couverture n'ayant rien à voir avec lui de façon à ce qu'un attaquant ne puisse pas savoir si des

informations sont dissimulées dans le support. Pour le tatouge (ou marquage), on cherche juste à tatouer une image. Le but est de dissimuler une information qui a pour but de démontrer l'intégrité du document ou encore de protéger les droits d'auteurs [42].
Une autre différence entre stéganographie et tatouage réside dans l'étape de l'extraction, Dans le cas de la stéganographie il s'agit d'extraire les données dissimulées dans le support de couverture alors que dans le tatouage il peut aussi s'agir de simplement détecter la présence du marque.
La différence entre la stéganographie et le tatouage, est que dans le tatouage seul le message doit rester caché mais son existence peut être connue, pour la stéganographie, l'existence d'un message caché doit rester secrète[33].

1.7 Définition de L'image

L'image est une représentation d'une personne ou un objet par la peinture, le dessin, la photographie, etc..., les images numériques, destinées à être visualisées sur les écrans d'ordinateur, se divisent en 2 grandes classes: les images matricielles et les images vectorielles [43]. Une image numérique est une fonction à support et borné, et à valeurs discrètes. Le support est multidimensionnel, en général 2d ou 3d. les valeurs peuvent être scalaires (images en niveaux de gris [44]), ou bien vectorielles (imagerie multi composante, imagerie couleur [45].

1.8 Types d'images

Il y'a deux types de présentation d'image

1.8.1 Image vectorielle

L'image vectorielle [46][45] est adaptée au travail sur des objets dont on connaît les paramètres de traçage, elle est décrite en termes de formes élémentaires: (lignes, cercles, rectangles, Les formes sont décrites par des attributs géométriques et par des attributs d'épaisseur, de couleur, de type,...). Une

opération d'affichage ou d'impression nécessite une conversion en mode point (calculs) à cause des périphériques qui sont généralement en mode point.

Les avantage de l'image vectoriel est:

- La taille d'une image vectorielle n'est fonction que de sa complexité; une image très complexe est de l'ordre de 1 à 2 Mo.
- Les modifications spatiales de l'image sont relativement souples car elles consistent en opérations géométriques ne conduisant pas à la perte d'information.

Les inconvénients de l'image vectoriel est:

- La difficulté de stocker des images complexes comme des photographies.
- L'affichage d'une image vectorielle peut prendre plus de temps que l'affichage d'une image bitmap (matricielle) de complexité égale.

– Le format vectoriel (ai, eps).

Figure 1.10: Image vectorielle

1.8.2 Image matricielle

L'image matricielle ou image bitmap, se représente sous forme d'une matrice de points (image binaire, image couleur). Ces points codés sont rangés en lignes et en colonnes avec la correspondance simple suivante: un élément de la matrice (point codé) correspond à un point de l'écran de l'ordinateur, L'image matricielle contient un nombre fixe de points appelé résolution.

Les avantages de l'image matricielle sont:

- Les images bitmaps peuvent facilement être créées et stockées dans un tableau de pixels représentant l'image.
- Les images bitmaps peuvent facilement être affichées sur un écran ou être imprimées.

Les inconvénients de l'image matricielle sont:

- Les fichiers peuvent être très gros (nécessité de compression).
- Les dimensions de l'image doivent être prévues pour la résolution de l'interface de sortie (écran, imprimante).

Le format matriciel est (jpg, tiff, png,...).
Les images numériques sont faciles à stocker dans un matrice pour analyser et bien traiter.

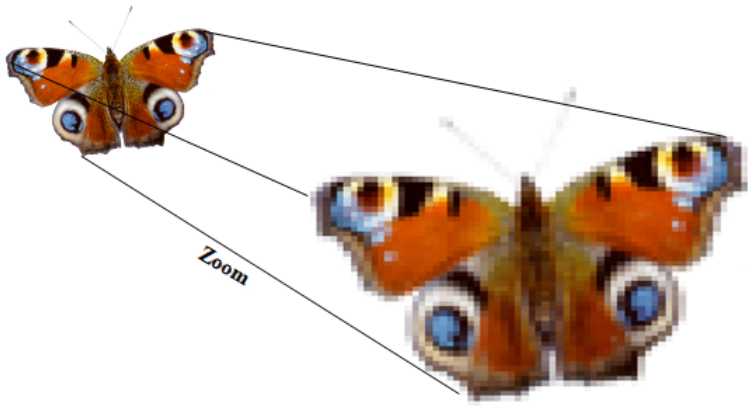

Figure 1.11: Image matricielle

1.9 Images numériques (image bitmap)

Les images matricielles sont également définies par leur définition et leur résolution.

1.9.1 Définition

L'image est définie par le nombre de points le composant. En image numérique, cela correspond au nombre de pixels qui compose l'image en hauteur (axe vertical) et en largeur (axe horizontal): 256 pixels par 512 pixels par exemple, abrégé en « 256 × 512» .
Comme représente la figure 1.12

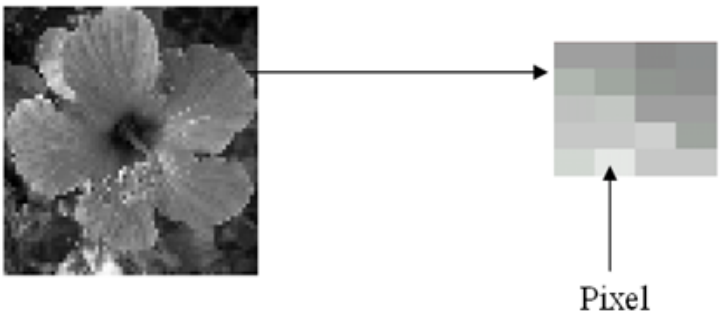

Figure 1.12: Représentation d'image par des pixels

1.10 La résolution d'une image

"La résolution c'est le nombre de pixels par unité de longueur, c'est aussi la densité de pixel de l'image."Elle s'exprime en dpi (dot per inch = point d'encre par pouce) pour une imprimante, ou en ppp (pixel par pouce 1 pouce (ou inch) = 2,54 cm.) pour un fichier image. Évidemment plus la résolution de l'image est élevée (beaucoup de pixels pour un pouce), plus la qualité théorique est importante. Nous parlons de qualité théorique car la notion de qualité est plus fonction de l'oeil humain que de chiffres étalés en vrac.
La figure 1.13 explique la notion de résolutions dans deux images de même taille (1 pouce sur 1 pouce), ou l'image droite est deux fois moindre que l'image

gauche.

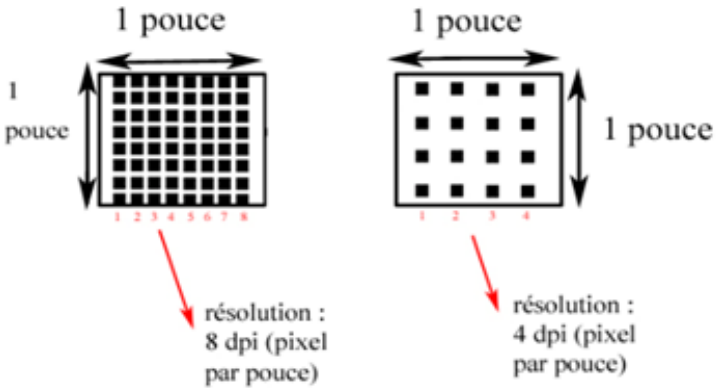

Figure 1.13: Résolution d'une image (8ppp,4ppp)

– Il y a une relation entre Résolution et Définition.

Les trois caractéristiques d'une image: taille en pixels (Définition), Dimension réelle (en cm ou en pouces) et la résolution sont liées par la formule suivante

$$Résolution en pixels par pouce = \frac{nombre de pixels}{taille réelle en cm/2.54}$$

1.11 Représentation des couleurs

La couleur d'un objet dépend de sa géométrie, de l'environnement et de la source de lumière qui l'éclaire, du système visuel humain. on définit deux niveaux de représentation de couleur:

1.11.1 Niveaux de gris

L'image est caractérisée par une quantité de lumière affectée à chaque point et correspondant à un niveau de gris mesuré par une intensité. Il est commode

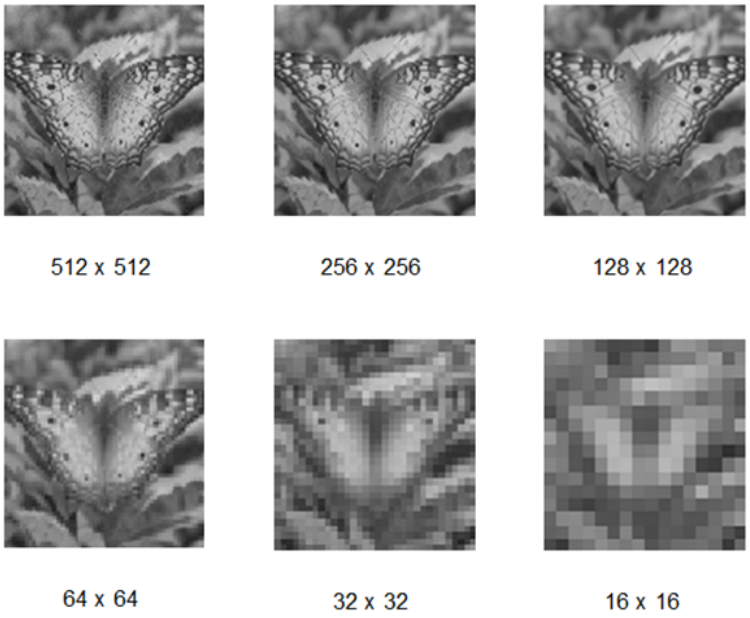

Figure 1.14: Résolution d'une image

d'associer une échelle quantitative aux niveaux d'intensité: 0 pour le noir (intensité lumineuse nulle), 255 pour le blanc (intensité lumineuse maximale), entre les deux il y a les gris [47].

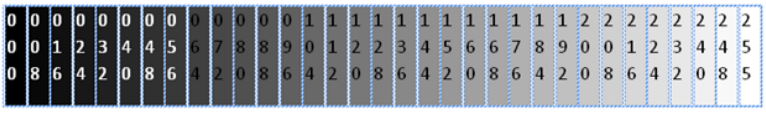

Figure 1.15: Les niveaux de gris (0, 255)

1.11.2 Couleurs

Il existe plusieurs modes de codage informatique des couleurs, le plus utilisé pour le maniement des images est l'espace colorimétrique rouge, vert, bleu (RVB ou RGB). Si le mélange des trois composantes R, V, et B à leur valeur maximum donne du blanc, à l'instar de la lumière. Le mélange de ces trois couleurs à des proportions diverses permet de reproduire à l'écran une part importante du spectre visible, sans avoir à spécifier une multitude de fréquences lumineuses

Une base est un ensemble fini d'éléments qui ont les propriétés suivantes:

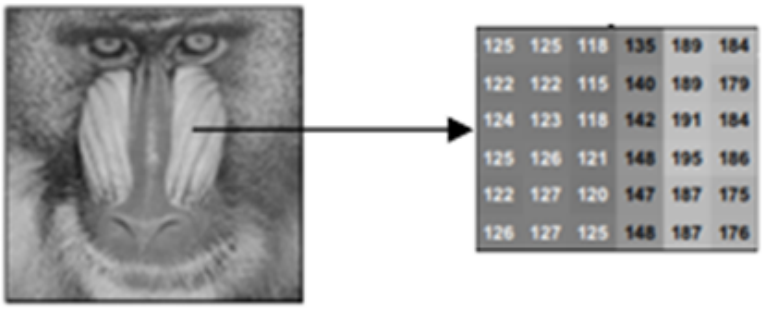

Figure 1.16: La représentation d'une image au niveau de gris

R (Rouge, Red)	V (G) (vert, green)	B (Bleu, Blue)	Couleur
0	0	0	Noir
0	0	1	Nuance de noir
255	0	0	Rouge
0	255	0	Vert
0	0	255	Bleu
128	128	128	Gris
255	255	255	Blanc

Figure 1.17: Rouge, Vert et Bleu constituent une base

- Toutes les couleurs sont obtenues par combinaison des éléments de la base.
- Aucun élément de la base ne peut être une combinaison des autres éléments de la base (indépendance).

Le codage de la couleur est réalisé sur trois octets, chaque octet représentant la valeur d'une composante couleur par un entier de 0 à 255. Ces trois valeurs codent généralement la couleur dans l'espace RVB. Le nombre de couleurs différentes pouvant être ainsi représenté est de 256×256×256 possibilités, soit près de 16 millions de couleurs. Comme la différence de nuance entre deux couleurs très proches mais différentes dans ce mode de représentation est quasiment imperceptible pour l'œil humain, on considère commodément que ce système permet une restitution exacte des couleurs Les images bitmap basées sur cette représentation peuvent rapidement occuper un espace de stockage considérable, chaque pixel nécessitant trois octets pour coder sa couleur (RGB).

1.11.3 Convertir une image couleur en niveau de gris

Pour convertir une image couleur en niveau de gris il faut remplacer, pour chaque pixel les trois valeurs représentant les niveaux de rouge, de vert et de bleu, en une seule valeur représentant la luminosité

$$Luminance = 0,2989 \cdot R + 0,5870 \cdot V + 0,1140 \cdot B. \quad (1)$$

1.12 Différent modèles de représentation de couleur

Pour désigner les couleurs en informatique graphique [48], on peut utiliser plusieurs modèles.

1.12.1 RGB

Le modèle RVB ou RGB (Rouge, Vert, Bleu) Les trois axes correspondent aux couleurs primaires Rouge, Vert, Bleu. La diagonale principale représente les

Figure 1.18: Convertir une image couleur en niveau de gris

niveaux de gris. Ce modèle prend toute son importance au niveau de télévision et des écrans à balayage; en effet, c'est par superposition de rouge, de vert et de bleu que l'affichage couleur est réalisé.

Figure 1.19: L'espace de présentation RGB (les trois plans (Rouge, Vert (gris) et bleu)

1.12.2 YIQ

Le modèle YIQ Il s'agit d'un recodage de RGB par NTSC (National Television Standards Committee) Y luminance et I chrominance Q color component:

$$Y = 0.30 \cdot R + 0.59 \cdot G + 0.11 \cdot B. I = 0.60 \cdot R + -0.27 \cdot G + -0.32 \cdot B. Q = 0.21 \cdot R + -0.52 \cdot G + 0.31 \cdot B. \quad (2)$$

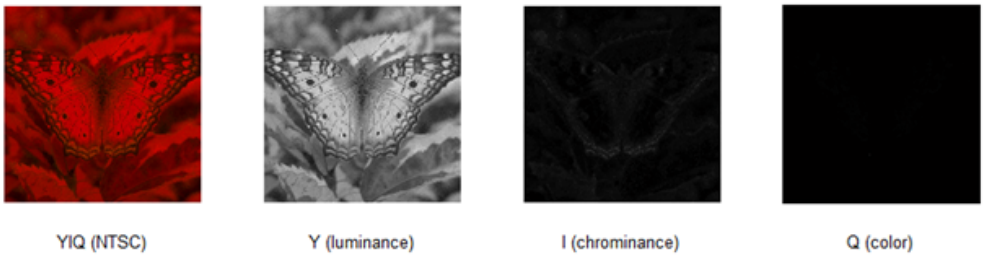

Figure 1.20: L'espace de présentation YIQ(NTSC)

1.12.3 TSL ou (HSV)

Le modèle TSL (Teinte, Saturation, Luminance) ou HSV (Hue, Saturation, Value) Plus proche de la perception de la couleur, ce modèle utilise un espace en forme d'hexagone dont l'axe est celui de la luminance L .Pour L = 1, on a les couleurs d'intensité maximale. La teinte T est donnée par l'angle entre l'axe rouge et un point de l'hexagone. La saturation S est donnée par la distance entre l'axe de la luminance et un point de l'hexagone Le TSL (Teinte, Saturation, Luminosité) modèle de couleur définit un espace de couleur en fonction de trois éléments constitutifs :

1. La teinte: le type de couleur (comme le rouge, bleu ou jaune). Varie de 0 à 360° dans la plupart des applications. (Chaque valeur correspond à une couleur: 0 est rouge, 45 est une nuance d'orange et 55 est une nuance de jaune).
2. Saturation: l'intensité de la couleur. Varie de 0 à 100 % (0 signifie pas de couleur, qui est une nuance de gris entre le noir et le blanc; 100 % signifie une couleurintense).
3. Luminosité (ou la valeur): la luminosité de la couleur. Est compris entre 0 et100% (0 est toujours noir; en fonction de la saturation, 100% peut être blanc ou une couleur plus oumoins saturé).

1.12.4 LAB

Lab est un espace de couleur très grand, capable de coder des couleurs qui n'existent pas.

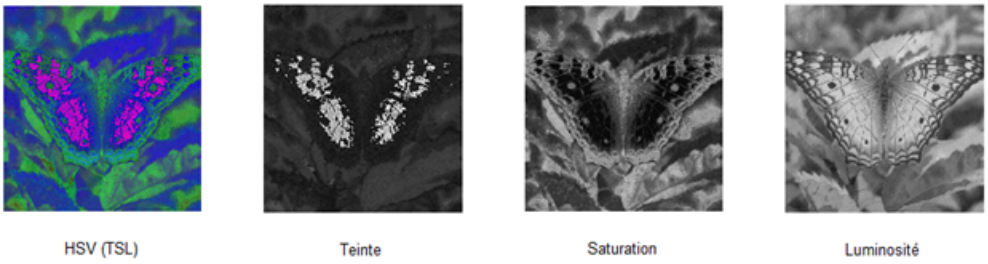

Figure 1.21: L'espace de présentation HSV (TSL)

Une image en couleur Lab est composée de 3 couches:

1. L: la couche luminosité. Les pixels de cette couche prennent une valeur de 0 à 100. 0 étant très sombre, et 100 très lumineux.
2. a: La couche qui représente un axe Vert / Magenta
3. b: qui représente l'axe bleu / jaune.

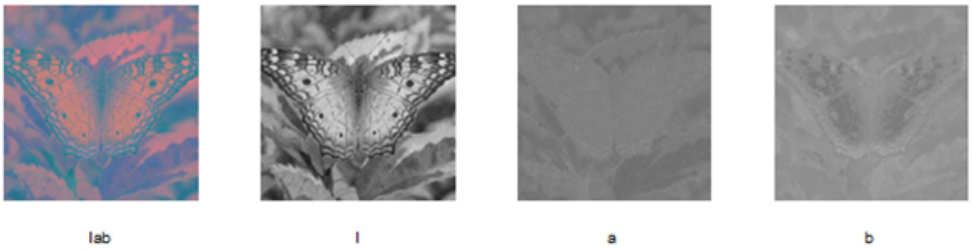

Figure 1.22: L'espace de présentation Lab

1.13 Le pixel

Une image est dite numérique (ou digitale) s'elle est échantillonnée et quantifiée selon une forme qui peut être lue par un ordinateur. Elle est simplement transformée en une longue suite de signaux «0/1 ». L'élément digital équivalent est le pixel (« pix » vient de picture et « el » d'element). Digitaliser une image c'est comme superposer une grille très fine sur une scène en analysant la couleur et la luminosité à travers les mailles puis de noter les valeurs dans une grande liste avec un certain ordre.

1.14 Codage en bit des niveaux de gris

Un BIT Un bit est la plus petite donnée qu'un ordinateur (ou une image) peut utiliser. Si nous décidons d'utiliser un bit pour décrire notre image, nous pouvons utiliser cet état allumé (1) ou éteint (0) pour représenter le noir ou le blanc sans avoir d'état intermédiaire possible (pas de gris).

Deux BIT Si nous utilisons désormais deux bits pour décrire notre image, nous avons désormais quatre états possibles: noir, gris foncé, gris clair, blanc.

n BIT utilisent 3 grands formats: le Jpeg, le Tiff ou un format spécifique à leur appareil photo et qui entre dans la famille des Raw. Vos clients vous demanderont peut-être également de leur communiquer des fichiers dans des formats propriétaires d'Adobe tels que .EPS ou .PSD.

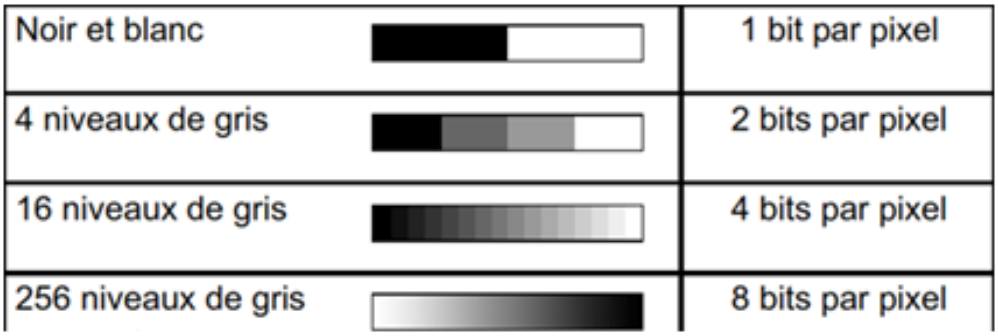

Figure 1.23: Codage en bit (1bit,2,4,8)des niveaux de gris

1.15 Format de l'image numérique (image bitmap)

Un format d'image comprend en général un en-tête qui contient des données sur l'image par exemple la taille de l'image en pixels. La structuration des données est différente pour chaque format d'image. Les différentes Format d'image numérique sont :

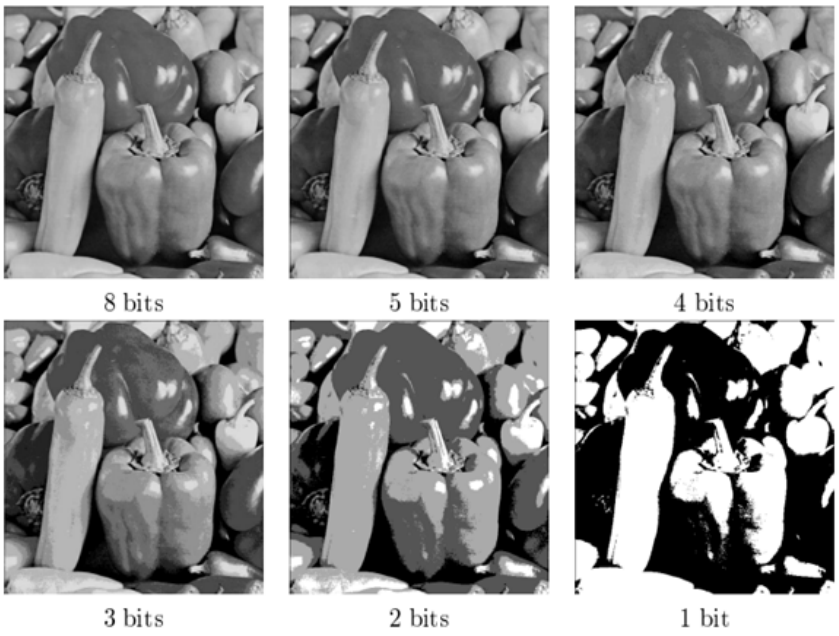

Figure 1.24: Présentation en bit des niveaux de gris d'une image

1.15.1 Le format JPEG

Ce format JPEG [49](Joint Photographic Experts Group[1]) est la représentation d'une norme ISO, et aussi est un format compressé. C'est à dire que pour réduire l'encombrement du fichier, le nombre de données à mémoriser a été réduit en donnant la même valeur à des points très proches de l'image.

- Avantage du « Jpeg »: format compact et universel.
- Inconvénient: la qualité.

1.15.2 Le format Tiff (Tagged Image File Format)

Le format TIFF [50] est principalement utilisé dans le traitement d'image numérique et le rendu des clients exigeants tels que les imprimantes. Sa principale préoccupation dans Gbig est qu'il peut stocker des données sur 8, 16 ou 32 bits et que peu importe le nombre de sauvegardes consécutives, il n'y aura pas de perte d'informations. Il est possible d'enregistrer dans « tiff » compressé sans perte. Comme Jpeg, il est reconnu par tous les logiciels de traitement, d'indexation, etc. ou presque d'images. Certaines caméras offrent d'enregistrer des photos

dans le "Tif" à côté de "JPEG" ou "Raw". C'est un format pour le traitement des images, leur sauvegarde et la livraison aux clients.

- Avantage du « Tiff»: sa qualité et son universalité.
- Inconvénient: le poids des fichiers.

1.15.3 Le format Gif (Graphics Interchange Format)

Le format «.gif» prend en charge un maximum de 256 couleurs. Ce format convient tout à fait à des images simples qui n'utilisent que quelques couleurs (une police de caractères simple, par exemple).

- Avantage du «gif»: Les fichiers occupent très peu de place. Ce format de fichier figure ainsi souvent aux côtés de «.jpg» pour le web.
- Inconvénient: Au format «.gif», les dégradés de couleurs fins et les photos contenant un grand nombre de teintes sont tramés. Ce format d'image ne convient pas à la reproduction de photos.

1.15.4 Le format PNG (Portable Network Graphics)

Le format PNG [51] est le plus couramment utilisé pour une utilisation en ligne et sur les sites en raison de leur faible résolution. Les fichiers PNG sont des images bitmap qui emploient la compression sans perte de données, et comme les fichiers GIF, PNG peuvent être créées avec un fond transparent. C'est une alternative au format GIF. La compression proposée par ce format est une compression sans perte d'une qualité 5 à 25% meilleure que la compression GIF.

1.16 Formation de l'image vectorielle

Les différents Formats d'image vectorielle sont:

1.16.1 Le format EPS (Encapsulated Postscript)

Les fichiers EPS [52] sont généralement utilisés pour transférer une image ou un graphique, généralement à partir d'un fichier vectoriel vers une autre application. En base, les fichiers vectoriels EPS s'adaptent à toutes les tailles. Les

fichiers Eps peuvent être ouverts avec Adobe Illustrator, Freihand ou Adobe Photoshop.

1.16.2 AI (Adobe Illustrator)

Fichier Adobe Illustrator (AI [53]) est un format de fichier développé par Adobe pour représenter les dessins vectoriels en EPS ou PDF. le .ai est l'extension de fichier utilisée par Adobe Illustrator. Les fichiers AI sont des fichiers vectoriels utilisés par les graphistes et les imprimeurs pour générer des dispositifs de communication de différents formats. Les fichiers AI peuvent uniquement être ouverts avec Adobe Illustrator. L'avantage est de pouvoir redimensionner l'image à volonté sans aucun effet d'escalier ou pixellisation.

1.16.3 SVG (Scalable Vector Graphics)

Le Scalable Vector Graphics [54] (en français « graphique vectoriel adaptable»), ou SVG est un format de données conçu pour décrire des groupes de graphiques vectoriels utilisés uniquement avec des navigateurs, car ils sont basés sur un langage XML. Il a été développé en 1998

1.17 Conclusion

Dans ce chapitre, nous avons présenté les images numériques d'une manière générale. Comme nous venons de voir la qualité des images dépend de plusieurs éléments: résolution, la taille d'image, et le taux de compression qui dépend du format d'image elle-même, où chaque format a ses avantages et ses inconvénient, mais ce sont des formats qu'il faut absolument bien connaitre pour arriver à ne pas perdre de vue que sur internet l'importance n'est pas le choix de l'un des formats principaux mais de pouvoir afficher son image de la meilleur qualité visuelle.

Tout cela, afin de pouvoir implémenter des différentes méthodes de dissimulation d'une information dans une image qui sera le contenu du prochain chapitre.

Chapter 2

Outils mathématiques

2.1 Intorduction

Comme l'image est plus en plus utilisée dans la communication sur un réseau externe, La sécurité d'image numérique est devenue plus considérable avec le progrès rapide de l'internet donc il est nécessaire de développer des outils de protection efficace contre les intrusions. Dans le chapitre précédent, nous présentons les caractéristiques de la sécurité d'une image, et les exigences principale de dissimulation d'information numérique ensuite on va citer quelques techniques de dissimulation d'une information dans une image.
Dans ce chapitre, on va presenter les notions de base nécessaires pour comprendre le reste de notre thèse. Tout d'abord, on va présenter: les groupes et les applications bijectives pour construire les matrices de permutation. Ensuite, on va décrire brièvement: les matrices particulières, les opérations sur les matrices, Le produit matriciel et l'inversion des matrices. Finalement,on va examiner les valeurs propres, les vecteurs propres, La décomposition en valeurs singulières et la décomposition polaire.

2.2 Groupe

Definition : Soit $\mathbb{G}$ un ensemble non vide muni d'une loi de composition interne, un couple $(\mathbb{G},\cdot)$ constitué d'un ensemble $\mathbb{G}$ et d'une loi de composition interne sur $\mathbb{G}$ est un groupe si:

- La loi est associative : $\forall a,b,c \in \mathbb{G}\ \ a\cdot(b\cdot c)=(a\cdot b)\cdot c$.
- La loi possède un élément neutre e : $\forall a \in \mathbb{G}\ \ e\cdot a = a\cdot e = a$.
- Tout élément de $\mathbb{G}$ possède un inverse : $\forall a \in \mathbb{G}$, $\exists a^{-1} \in \mathbb{G}$: $a\cdot a^{-1} = a^{-1}\cdot a = e$.

- Si de plus la loi $(\cdot)$ est commutatif $a\cdot b = b\cdot a$ on dit que $(\mathbb{G},\cdot)$ est un groupe commutatif (abélien).
- Si $\mathbb{G}$ est fini on appelle ordre de $\mathbb{G}$ et note $o(\mathbb{G})$ le cardinal de $\mathbb{G}$.

Exemple :

- $(\mathbb{Z}, +)$ est un groupe commutative.
- Pour chaque entier $n \geq 2$ l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des entiers modulos n muni de l'addition (modulo n) est un groupe commutative fini.

2.3 Application bijective

Definition :
Soit f une application de $\mathbb{E}$ dans $\mathbb{F}$. f est bijective si et seulement si tout élément de l'ensemble d'arrivée $\mathbb{F}$ a exactement un antécédent par f dans l'ensemble de départ E, c'est-à-dire :

$$\forall y \in F, \exists! x \in E \text{ tq: } f(x) = y.$$

2.4 Quelques définitions et opérations sur les matrices

Definition :
Une matrice (réelle) A est un tableau rectangulaire de nombres (réels).Elle est dite de taille m × n si le tableau posséde m lignes et n colonnes. Les nombres du tableau sont appelés les éléments de A. L'élément situé à la i-ème ligne et à la j-ème colonne est noté a_{ij}.
La matrice A est également notée

$$A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$$

Ou simplement :

$$A = (a_{ij})_{ij}$$

Si $n = m$, la matrice est dit carrée

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Matrice carrée n × n

Dans le cas d'une matrice carrée, les éléments $a_{11}, a_{22}, \ldots, a_{nn}$ sont appelés les éléments diagonaux.

$$\begin{pmatrix} a_{11} & \cdots & & \\ \vdots & a_{22} & \cdots & \\ & \vdots & \ddots & \\ & & & a_{nn} \end{pmatrix}$$

Deux matrices sont égales lorsqu'elles ont la même taille et que les éléments correspondants sont égaux.

Definition :
(Somme de deux matrices). On peut définir la somme de deux matrices si elles sont de même taille. Soient A et B deux matrices de taille m × n. On définit leur somme $C = A + B$, de taille m × n, par

$$c_{ij} = a_{ij} + b_{ij}. \tag{1}$$

En d'autres termes, on somme composante par composante.

Definition :
(Produit d'une matrice par un scalaire). Le produit d'une matrice A par un scalaire k est formé en multipliant chaque élément de A par k. Il est noté kA.

2.5 Le produit matriciel

Le produit $A \cdot B$ de deux matrices A et B est défini seulement si le nombre de colonnes de A est égal au nombre de lignes de B.

Definition :
(Produit de deux matrices). Soit $A = (a_{ij})$ une matrice m × n et $B = (b_{ij})$ une matrice n × p. Alors le produit $C = A \cdot B$ est une matrice m × p dont les éléments c_{ij} sont définis par :

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{im}b_{mj} = \sum_{k=1}^{n} a_{ik}b_{kj}$$

$$A.B = C, \qquad \begin{pmatrix} b_{11} & \cdots & \cdots & \cdots \\ b_{21} & \cdots & \cdots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & \cdots & \cdots & \ddots \end{pmatrix}$$

$$\begin{pmatrix} \cdots & \cdots & \cdots & \cdots \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \cdots & \cdots & \cdots & \ddots \end{pmatrix} = \begin{pmatrix} \cdots & \cdots & \cdots & \cdots \\ c_{21} & & \cdots & \\ \vdots & \vdots & \ddots & \vdots \\ \cdots & & \cdots & \ddots \end{pmatrix}$$

$$c_{21} = a_{21}b_{11} + a_{22}b_{21} + \ldots + a_{2m}b_{m1}$$

Exemple :

$$\begin{pmatrix} 1 & -7 & 2 & 0 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -1 \\ 3 \\ 8 \end{pmatrix} = (2 + 7 + 6 + 0) = 15$$

1×4 $\qquad$ 4×1 $\qquad$ 1×1

Remarque :

– Le produit des matrices n'est pas nécessairement commutatif.
On peut avoir:

$$A \cdot B \neq B \cdot A$$

– Il peut arriver que le produit de deux matrices non nulles soit nul. En d'autres termes, on peut avoir:

$$A,\ B \neq 0 \ \ et \ \ A \cdot B = 0.$$

2.6 Matrice identité

Definition :
La matrice carrée n × n

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

s'appelle la matrice identité. Ses éléments diagonaux sont égaux à 1 et tous ses autres éléments sont égaux à 0. Dans le calcul matriciel, la matrice identité joue un réle analogue à celui du nombre 1 dans l'arithmétique des scalaires. C'est l'élément neutre pour la multiplication. En d'autres termes, si A une matrice m × n, alors:

$$I_m \cdot A = A \ \ \ et \ \ \ A \cdot I_m = A$$

2.7 L'inversion des matrices

Definition :
(Matrice inverse) Soit A une matrice carrée de taille n × n. S'il existe une matrice carrée B de taille n × n telle que

$$A \cdot B = I \ \ \ et \ \ \ B \cdot A = I$$

on dit que A est inversible et on appelle B un inverse de A.

2.8 La transposition

Soit A la matrice de taille m × n

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

Definition :
On appelle matrice transposée de A, la matrice A^T de taille n × m définie par :

$$\begin{pmatrix} a_{11} & a_{21} & \cdots & a_{n1} \\ a_{12} & a_{22} & \cdots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \cdots & a_{nn} \end{pmatrix}$$

Autrement dit, la i-ème colonne de A^T est la i-ème ligne de A, ou encore

$$a^T = a_{ji}.$$

Theorem 1 *[55]*
L'opération de transposition obéit aux règles suivantes :

1. $(A+B)^T = A^T + B^T$
2. $(k \cdot A)^T = k \cdot A^T$.
3. $(A \cdot B)^T = B^T \cdot A^T$
4. $(A^T)^T = A$.
5. *Si A est inversible, alors* A^T *l'est aussi et on a* $(A^T)^{-1} = (A^{-1})^T$ *qui sera notée* A^{-T}.

2.9 La trace

Soit A la matrice n × n

$$\begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{nn} \end{pmatrix}$$

Definition :
On appelle trace de A, et on note $trace(A)$, le nombre obtenu en additionnant les éléments diagonaux de A c'est-à-dire :

$$trace(A) = a_{11} + \ldots + a_{nn}$$

Exemple : Soient

$$A = \begin{pmatrix} 4 & 7 \\ 1 & 8 \end{pmatrix} \quad et \quad B = \begin{pmatrix} -5 & 2 & 5 \\ 3 & 1 & 1 \\ 2 & 8 & 0 \end{pmatrix}$$

$$trace(A) = (4+8) = 12, \quad trace(B) = (-5+1+0) = -4$$

Theorem 2 *[55]*
Soient A et B deux matrices $n \times n$. Alors

1. $trace(A+B) = trace(A) + trace(B)$;
2. $(trace(\lambda \cdot A) = \lambda \cdot trace(A)$ *pour tout* $\lambda \in \mathbb{G}$;
3. $trace(A^T) = trace(A)$;
4. $trace(A \cdot B) = trace(B \cdot A)$.

2.10 Permutation d'un ensemble

Definition :
L'ensemble S_n des bijections de 1×n dans lui même est un groupe pour la loi de

Figure 2.1: Permutation d'un ensemble de cardinale 12

composition des applications :

$$|S_n| = n! \tag{2}$$

Soit $X = \{x_1, x_2, \ldots, x_n\}$ un ensemble de cardinal n. L'ensemble $B_{ij}(X)$ des bijections de X dans lui même est aussi un groupe pour la loi de composition des applications qui est appelé groupe des permutations de X. Ce groupe $B_{ij}(X)$ est isomorphe au groupe symétrique S_n.
Soit $p \in S_n$, on note $p(x)$ l'image de $x \in \{1, \ldots, n\}$. Une permutation p est entièrement déterminée par la donnée des $p(x)$ pour tout $x \in \{1, \ldots, n\}$, On présente souvent une permutation sous la notation suivante :

$$P = \begin{bmatrix} 1 & 2 & \ldots & n \\ p(1) & p(2) & \ldots & p(n) \end{bmatrix}$$

Le groupe S_n est non commutatif dès que $n \geq 3$.

– On note l'ensemble des indices par $E = \{1, 2, \ldots, n\}$, un ensemble fini.

2.11 Construire une matrice de permutation

Pour construire une matrice de permutation Π , en se basant sur la permutation d'un ensemble fini E, puis on permute les colonnes de la matrice identité.

Exemple : Soit l'ensemble des indices $E = \{1, 2, 3, 4\}$, de cardinal $|E| = 4, p$ est la bijection de l'ensemble, et elle est définie de la façon suivante :

$$P(E) = \begin{bmatrix} 1 & 2 & 3 & 4 \\ p(1) = 3 & p(2) = 1 & p(3) = 4 & p(4) = 2 \end{bmatrix}$$

c'est-à-dire:

$$I_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \rightarrow \Pi = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Soit $X = \{x_1, x_2, x_3, x_4\}$ un ensemble de cardinal 4. L'ensemble $P(X)$ c'est la permutation de X par la bijection p, donc $P(X) = X \cdot \Pi$:

$$X = x_1, x_2, x_3, x_4 \rightarrow p(X) = x_2, x_4, x_1, x_3$$

On note Π^{-1}l'inverse de la matrice Π,

$$\Pi = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

La matrice Π^{-1}c'est la transpose de Π , aussi c'est la permutation des lignes de la matrice identité par la même permutation p.

2.12 Matrices symétriques

Definition :
Une matrice A de taille n × n est dite symétrique si elle est égale à sa transposée, c'est-à-dire si

$$A = A^T$$

ou encore si $a_{ij} = a_{ji}$ pour tout $i, j = 1, \ldots, n$.

Theorem 3 *[55]*
Pour une matrice B quelconque, les matrices $B \cdot B^T$ et $B^T \cdot B$ sont symétriques.

$$(B \cdot B^T)^T = (B^T)^T \cdot B^T = B \cdot B^T.$$

$$(B^T \cdot B)^T = B^T \cdot (B^T)^T = B^T \cdot B.$$

2.13 Matrices antisymétriques

Definition :

Une matrice A de taille n × n est dite antisymétrique si:

$$A^T = -A$$

c'est-à-dire si: $a_{ij} = -a_{ji}$ pour tout $i, j = 1, \ldots, n$.

2.14 Produit scalaire

Definition :

(Produit scalaire canonique de K^n) Soit $x = (x_1, \ldots, x_n)^T$,et $y = (y_1, \ldots, y_n)^T$ deux vecteurs de K_n, alors on définitle produit scalaire de x avec y par:

$$\langle x|y\rangle_{K_n} = \sum_{i=1}^{n} x_i \cdot y_i \tag{3}$$

2.15 Orthogonalité

Definition :

- Deux vecteurs x, y de K^n sont dits orthogonaux si $\langle x|y\rangle_{K_n} = 0$.
- Deux s.e.v. E et$F$ de K^n sont dits orthogonaux si

$$\forall x \in E, \forall y \in F, \langle x|y\rangle_{K_n} = 0$$

.

Remarque :

- Le vecteur 0_{K^n} est orthogonal à tous les vecteurs de K^n.
- Dans $\mathbb{R}^2$,la notion d'orthogonalité décrite dans la Définition coïncide avec la notion d'orthogonalité géométrique usuelle.

2.16 Matrices orthogonales, unitaires

Definition :

1. Une matrice $O \in M_n(\mathbb{R})$ est dite orthogonale si $O^T = O^{-1}$. On note $O_n(\mathbb{R})$ l'ensemble des matrices orthogonales de $M_n(\mathbb{R})$.
2. Une matrice $U \in M_n(\mathbb{C})$ est dite unitaire si $U^* = U^{-1}$. On note $U_n(R)$ l'ensemble des matrices unitaires de $M_n(\mathbb{C})$.

Proposition 1 *Si O est unitaire (resp. orthogonale dans le cas réel), alors O^{-1} l'est aussi.*

Proposition 2 *Soient O, P deux matrices orthogonales (resp. unitaires) de $M_n(R)$ (resp.$M_n(\mathbb{C})$), alors $O \cdot P$ est orthogonale (resp. unitaire).*

2.17 Valeurs propres, vecteurs propres

Definition :
Soenit E un espace vectoriel et φ un endomorphisme de E (c'est-a-dire une application linéaire de E dans lui mème).

Definition :
Si il existe un scalaire $\lambda \in \mathbb{R}$ (resp. $\mathbb{C}$)et un vecteur non nul $v \in E$ tels que:

$$\varphi(v) = \lambda v$$

on dit que λ est une valeur propre de u. Si λ est une valeur propre et un vecteur propre de φ, associé λ est un vecteur v tel que $\varphi(v) = \lambda v$.

Proposition 3 *Soit λ une valeur propre de φ, le sous ensemble des vecteurs propres de φ associè à λ est un sous-espace vectoriel appelé sous-espace propre de φ associé à λ et noté E_λ.*

L'ensemble des valeurs propres d'un endomorphisme φ est appelé le spectre de φ et est noté $Spec(\varphi)$.

2.18 détermination des valeurs propres, polynôme caractéristique

Definition :
un endomorphisme est une application linéaire de E dans lui-même.
Soient E un espace vectoriel et φ un endomorphisme de E et $\lambda \in \mathbb{R}(resp.\mathbb{C})$.

Definition :
Pour calculer $det(A - XI_n)$ on obtient un polynôme en X degré n de coefficient dominant $(-1)^n$. Ce polynôme est appelé le polynôme caractéristique de φ ou le polynôme caractéristique de la matrice A. On le notera $c_\varphi(X)$ ou $c_A(X)$. Sa valeur pour $X = 0$est $det(A)$. Il s'écrit donc :

$$c_A(X) = (-1)^n \cdot X^n + \ldots + det(A)$$

Proposition 4 *Le coefficient du terme de degré* $n-1$ *est* $(-1)^{n-1} trace(A)$.
Donc:

$$c_A(X) = (-1)^n \cdot X^n + (-1)^{(n-1)} \cdot trace(A) \cdot X^{(n-1)} + \ldots + det(A)$$

Exemple : Le polynôme caractéristique d'une matrice

$$\begin{pmatrix} 5 & -3 \\ 3 & 1 \end{pmatrix} \in M_2\mathbb{R}$$

est

$$c_A(X) = \begin{vmatrix} 5-X & -3 \\ 3 & 1-X \end{vmatrix} = X^2 - trace(A) \cdot X + det(A)$$

Remarque : On appellera valeur propre d'une matrice A de taille n × n, les racines du polynôme caractéristique $c^A(X)$. Ce sont les valeurs propres de l'endomorphisme dont la matrice est A dans la base standard de $\mathbb{R}^n$(resp. $\mathbb{C}^n$).

2.19 Calcul des vecteurs propres

Soit A une matrice carrée et λ une valeur propre de A. Les vecteurs propres de A correspondant à la valeur propre λ sont les vecteurs $x \neq 0$ qui satisfont l'équation $Ax = \lambda x$. De façon équivalente, ces vecteurs sont les vecteurs non nuls de l'espace des solutions de:

$$(\lambda I - A)x = 0$$

L'ensemble de ces vecteurs propres est appelé l'espace propre de A correspondant à la valeur propre λ et est noté E_λ.

Exemple : On considère la matrice

$$\begin{pmatrix} 1 & 0 & 1 \\ -1 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

Le polynôme caracatéristique est $(1-X)\cdot(2-X)^2$ dont les racines sont 2 (double) et 1 (simple). Les valeurs propres de A sont donc λ_1 la première racine et λ_2 la deuxième racine.
Il y a donc deux espaces propres. Pour calculer E_2 (l'espace propre associé à la valeur propre 2), il faut trouver le noyau de $2I - A$ et Pour $\lambda = 1$(Pour calculer E_2), on calcule le noyau de $I - A$. On obtient les vecteurs propres en résolvant les systèmes suivants:

$$\begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

et

$$\begin{pmatrix} 0 & 0 & 1 \\ -1 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

les vecteurs forment une base de l'espace des solutions (espace propre E_2) est donnée par:

$$\begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}$$

les vecteurs forment une base de l'espace des solutions (espace propre E_1) est donnée par:

$$\begin{pmatrix}1\\1\\0\end{pmatrix}$$

2.20 Diagonalisation

Soit E un espace vectoriel et φ un endomorphisme.

Definition :
On dit que φ est diagonalisable s'il existe une base de E dans laquelle la matrice de φ est diagonale.
Autrement dit φ est diagonalisable si et seulement si on peut trouver une base de E dans laquelle la matrice de φ est de la forme:

$$\begin{pmatrix}\lambda_1 & 0 & & & \\ 0 & \lambda_1 & 0 & & \\ & & \cdots & \cdots & \\ & \cdots & & & \\ & & & 0 & \lambda_r\end{pmatrix}$$

où $\lambda_1,\ldots,\lambda_r$ désignent les valeurs propres de φ.

Definition :
Soit A une matrice carrée. On dit que A est diagonalisable s'il existe une matrice

inversible P telle que $P^{-1} \cdot A \cdot P$ soit une matrice diagonale

2.20.1 Méthode pour diagonaliser une matrice

1. Trouver n vecteurs propres linéairement indépendants, $p_1, p_2, \ldots, p_n$.
2. Construire la matrice P ayant $p_1, p_2, , p_n$ comme vecteurs colonne.
3. La matrice $P^{-1} \cdot A \cdot P$ est diagonale. Les éléments diagonaux sont les valeurs propres $\lambda 1, \lambda 2, \ldots, \lambda n$, correspondant respectivement aux vecteurs propres $p_1, p_2, \ldots, p_n$.

Exemple : Diagonalisons la matrice

$$A = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 2 & 1 \\ 1 & 0 & 3 \end{pmatrix}$$

le polynôme caracatéristique de A est

$$(\lambda - 1) \cdot (\lambda - 2)^2 = 0$$

les valeurs propres sont alors $\lambda = 1$ et $\lambda = 2$.
Une base de E_2 est donnée par:

$$p_1 = \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Une base de E_1 est donnée par le vecteur:

$$p_3 = \begin{pmatrix} -2 \\ 1 \\ 1 \end{pmatrix}$$

Ces 3 vecteurs propres étant linéairement indépendants, la matrice A est diagonalisable. On pose alors:

$$P = \begin{pmatrix} -1 & 0 & -2 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

et on a:

$$P^{-1} \cdot A \cdot P = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

2.21 La décomposition en valeurs singulières

On a vu que pour certaines matrices carrées, on pouvait faire une décomposition en valeurs propres:

$$A = X \cdot D \cdot X^{-1}$$

L'idée de la décomposition en valeurs singulière est similaire à la décomposition en valeurs propres, mais fonctionne pour n'importe quelle matrice A de taille m×n: on factorise A en produit de trois matrices.

Theorem 4 *[56]*
soit $A \in \mathbb{R}^{m \cdot n}$. Il existe deux matrices orthogonales $U \in \mathbb{R}^{m \cdot m}$ et $V \in \mathbb{R}^{n \cdot n}$ tels que:

$$A = U \cdot \sum \cdot V^T \tag{4}$$

avec $\sum = diag(\sigma_1, \ldots, \sigma_p) \in \mathbb{R}^{m \cdot n}$ avec $p = min(m, n)$ et $\sigma_1 \geq \ldots \geq \sigma_p \geq 0$.

les σ_i sont les valeurs singulières de A

Theorem 5 *[56]*
existence et unicité de la SVD. Toute matrice $A \in C\ n \times n$ possède une SVD. Les valeurs singulières σ_i sont déterminées de façon unique. Si A est carrée $(m = n)$

et les valeurs singulières σ_j sont distinctes, les vecteurs d'entrée et de sorties v_j et u_j sont déterminés de façon unique à un facteur complexe unité près.

Theorem 6 *[56]*
Les valeurs singulières d'une matrice A sont les racines carrées des valeurs propres non-nulles de $A^T \cdot A$ et $A \cdot A^T$

Theorem 7 *[56] Les colonnes de U sont les vecteurs propres orthogonaux de $A \cdot A^t$ et les colonnes de V sont les vecteurs propres orthogonaux de $A^T \cdot A$ à unité complexe près.*

2.22 Décomposition polaire

Theorem 8 *[57]*
Soit $A \in M_n(\mathbb{C})$. A admis une decomposition polaire

$$A = Q \cdot P \tag{5}$$

telles que $Q \in Q_n(\mathbb{R})$ une matrice orthogonale et $P \in P_n^+(\mathbb{R})$ une matrice symétrique définie positive[58].

Remarque : (Matrice inversible)
Soit $A \in GL_n(\mathbb{R})$ alors A s'écrit de façon unique $A = P \cdot Q$ avec P symétrique positive et Q orthogonale.
En effet $A^T \cdot A$ est une matrice symétrique définie positive elle admet une racine carrée P qui est définie positive donc inversible.
Posons $Q = P^{-1}A$ alors

$$Q^T \cdot Q = A^T \cdot P^{-T} \cdot P^{-1} \cdot A = A^T \cdot (P^2)^{-1} \cdot A = A^T (A \cdot A^T)^{-1} \cdot A = I_n$$

Unicité: Si $P \cdot Q = P' \cdot Q'$avec les P, P'symétriques définies positives et Q et Q' orthogonales. Alors on a $P^2 = P'^2 = A \cdot A^T$, donc par unicité de la racines carrée d'une matrice symétrique positive on a $P = P'$ et par suite $Q = Q'$.

Remarque : Si A est non inversible, on a existence de P et Q. Mais on n'a pas l'unicité.

2.22.1 SVD et la Décomposition polaire

Pour obtenir la décomposition polaire d'une matrice carrée A, Nous suivons les étapes suivantes:

1. On décompose A en la décompositon SVD:

$$A = U \cdot S \cdot V^T$$

2. On prend $P = U \cdot S \cdot V^T$ et $Q = U \cdot V^T$.

ona donc $A = U \cdot S \cdot V^T = (U \cdot S \cdot U^T) \cdot (U \cdot V^T) = P \cdot Q$.

Exemple : Soit Aune matrice de 2×2:

$$A = \begin{pmatrix} 4 & 10 \\ 13 & 3 \end{pmatrix}$$

A est inversible.
On a donc:

$$P = \begin{pmatrix} 10.1643 & 3.5619 \\ 3.5619 & 12.8574 \end{pmatrix}$$

et

$$Q = \begin{pmatrix} 0.0434 & 0.9991 \\ 0.9991 & -0.0434 \end{pmatrix}$$

La matrice P est une matrice symétrique définie positive et Q orthogonale.
on peut vérifier que:

$$A = \begin{pmatrix} 10.1643 & 3.5619 \\ 3.5619 & 12.8574 \end{pmatrix} \cdot \begin{pmatrix} 0.0434 & 0.9991 \\ 0.9991 & -0.0434 \end{pmatrix} = \begin{pmatrix} 4 & 10 \\ 13 & 3 \end{pmatrix}$$

2.23 Conclusion

Dans ce chapitre, nous avons examiné le bagage mathématique utilisé pour bien comprendre la decomposition SVD et aussi la decomposition polare, nous avons présenté les notions et les oulils mathématiques nécessaires. nous avons présenté: les matrices, les opérations sur les matrices, Le produit matriciel, les valeurs propres, les vecteurs propres, La décomposition en valeurs singulières et la décomposition polaire.

La décomposition polaire est très liée à la décomposition SVD, son avantage réside dans l'unicité. Cette décomposition sera utilisée par la suite dans les deux techniques de dissimulation proposées.

Chapter 3

Les techniques de dissimulation

3.1 Introduction

Aujourd'hui, La sécurité des images numériques est devenue plus importante à l'évolution rapide de l'Internet dans le monde numérique, en particulier avec l'énorme croissance des réseaux et des technologies de communication, et surtout avec l'utilisation intensive et la généralisation des Smartphones. Afin de protéger les informations sensibles contre tout accès non autorisé, quand elles sont sauvegardées ou transmises à travers un réseau non sûr, les chercheurs ont construit plusieurs principes, pour assurer cette fonctionnalité.
La dissimulation d'information est l'un de ces principes, plus particulièrement l'insertion de données secrètes peut être une réponse à ce problème. En effet, l'insertion d'une marque dans un document permet de l'authentifier et de garantir son intégrité [59]. La sécurité des images numériques a attiré plus d'attention récemment, et différentes méthodes de cacher la présence des images secrètes ont été proposées de rehausser la sécurité de ces images.
Dans ce contexte, plusieurs techniques de dissimulation d'information ont été proposées. Les techniques les plus connues sont la stéganographie et le tatouage. La stéganographie numérique est une technique récente qui a émergé comme une source importante pour la sécurité des données. Elle consiste à envoyer secrètement des informations et non pas seulement à masquer leur présence. Les fichiers médias numériques, tels que l'image, le son et la vidéo, sont utilisés comme support pour cacher des informations secrètes d'une façon invisible. L'objectif principal des algorithmes de stéganographie consiste à fournir des données sécurisées, indétectables et imperceptibles. La stéganographie est utilisée sous l'hypothèse qu'elle ne sera pas détectée. Les techniques récentes de stéganographie ont été employées dans diverses applications. La majorité de ces applications ont pour objectif d'assurer la confidentialité des données. L'utilisation de la stéganographie à des fins criminelles, d'espionnage ou de piraterie.
Dans ce chapitre, nous allons voir les outils élémentaires d'analyse statique d'une image,les caractéristiques de la sécurité d'une image, et les exigences principale de dissimulation d'information numérique, ensuite on va citer quelques techniques de dissimulation d'une information dans une image.

3.2 Outils élémentaires d'analyse statique d'une image

Les différentes techniques d'analyse qui permettent de comparer deux images, sont: l'histogramme, corrélation, PSNR, SSIM et VIF....

3.2.1 Histogramme

Soit une image comportant n lignes et p colonnes, donc n × p pixels. Chacun de ces pixels est codé sur q bits (si $q = 8$, on a 256 niveaux). On peut effectuer une statistique sur les niveaux en comptant, pour chaque niveau, combien de pixels possèdent ce niveau. La représentation graphique de cette statistique est un histogramme par niveau [31]. L'histogramme d'une image comporte de niveaux 256, à tendance à se présenter sous forme d'une courbe, par exemple si on prend l'image au niveau de gris, de type (512 × 512). Où les pixels sont représentés sur 8 bit (des valeurs entre (0,1,...,255))

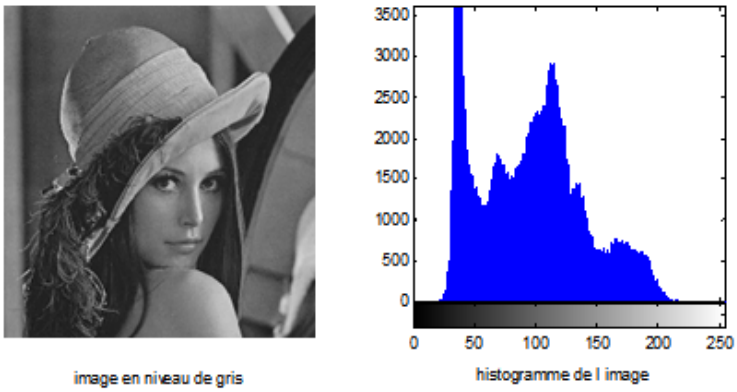

Figure 3.1: L'histogramme d'une image en niveau de gris de type (512 × 512)

Nous allons utiliser l'histogramme pour comparer l'image avant le traitement et après, pour voir s'il y a un changement sur l'intensité des pixels ou non.

3.2.2 Corrélations

La corrélation est le lien possible entre deux variables statistiques, Le coefficient de corrélation entre 2 variables numériques revient à chercher la liaison qui

existe entre ces deux variables, donc la corrélation est une technique qui permet d'étudier la relation qui pourrait exister entre deux variables quantitatives X et Y:

- Corrélation positive, c'est-à-dire à toute augmentation au niveau de X correspond une augmentation au niveau de Y. Les deux variables varient dans le même sens et avec une intensité similaire.
- Corrélation négative, c'est-à-dire à toute augmentation au niveau de X correspond une diminution au niveau de Y. Les deux variables varient dans deux sens opposés et avec une intensité similaire.

Ce coefficient varie entre -1 et +1; l'intensité de la relation linéaire sera donc d'autant plus forte que la valeur du coefficient est proche de +1 ou de -1, et d'autant plus faible qu'elle est proche de 0.

- Une valeur proche de +1 montre une forte liaison entre les deux caractères. La relation linéaire est ici croissante (c'est-à-dire que les variables varient dans le même sens);
- Une valeur proche de -1 montre également une forte liaison mais la relation linéaire entre les deux caractères est décroissante (les variables varient dans le sens contraire);
- Une valeur proche de 0 montre une absence de relation linéaire entre les deux caractères.

La corrélation d'images est une technique qui compare deux images pour estimer les déplacements des pixels d'une image par rapport à une autre image. Les algorithmes de corrélation utilisent les images sous forme de matrices de niveaux de gris donc si l'image utilise des niveaux de couleur il faut calculer la corrélation dans chaque plan, il y a plusieurs formules pour calculer la corrélation.

- Pour calculer la corrélation entre deux images de niveau de gris, on utilise la formule suivante

$$corr = \frac{\sum_{i=1}^{i=N}\sum_{j=1}^{j=N}(W_{ij}-\overline{W})\cdot(W'_{ij}-\overline{W'})}{\sqrt{(\sum_{i=1}^{i=N}\sum_{j=1}^{j=N}(W_{ij}-\overline{W})^2)\cdot(\sum_{j=1}^{i=N}\sum_{j=1}^{j=N}(W'_{ij}-\overline{W'})^2)}} \quad (1)$$

Où W la matrice de la première image (au niveau de gris), et $\overline{W}$ la matrice moyenne de W. Ensuite W' la matrice de la deuxième image, ($\overline{W'}$) sa matrice moyenne. La valeur de $corr \in [0,1]$, Si $corr = 1$ donc $W = W'$, c'est la même image. Si $corr = 0$ alors les deux images sont différentes.

– Pour calculer la corrélation entre deux images binaires

$$NC = \frac{1}{MN} \sum_{i=1}^{i=M} \sum_{j=1}^{j=N} W'_{ij} \oplus W_{ij} \tag{2}$$

Où W la matrice de première image (en binaire) avec type M × N, et W' la matrice de deuxième image, et $\oplus$ dénoter le (ou exclusive).

3.2.3 PSNR

$PSNR$ (sigle de Peak Signal to Noise Ratio) est une mesure de distorsion utilisée en image numérique, tout particulièrement en compression d'image. Il s'agit de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale. Il est défini par:

$$\text{PSNR} = 10\log_{10} \frac{255^2}{MSE}(dB) \tag{3}$$

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^{i=M} \sum_{j=1}^{j=N} \left(H_{ij} - HA_{ij}\right)^2 \tag{4}$$

Où H est l'image avant l'insertion (ou le support de couverture), HA l'image après l'insertion (l'image tatoué), M le nombre de lignes, N le nombre de colonnes. L'unité du $PSNR$ est le décibel (db) (dB est la valeur maximale du pixel codé sur un octet).

3.2.4 SSIM

L'indice de similarité structurelle proposé par Wang et al. [60] est basé sur l'hypothèse que le système visuel humain est fortement influencé par les structures présentes dans une scène. Le SSIM (Strucutal SIMilarity index) mesure

ainsi la dégradation des structures entre deux image A et B:

$$\text{SSIM} = [I(A,B)^{\alpha}] \cdot [C(A,B)^{\beta}] \cdot [S(A,B)^{\gamma}]. \tag{5}$$

où

$$I(A,B) = \frac{2\mu_A\mu_B + C_1}{\mu_A^2 + \mu_B^2 + C_1} \tag{6}$$

et

$$C(A,B) = \frac{2\sigma_A\sigma_B + C_2}{\sigma_A^2 + \sigma_B^2 + C_2} \tag{7}$$

et

$$S(A,B) = \frac{2\sigma_{AB} + C_3}{\sigma_A\sigma_B + C_3} \tag{8}$$

où μ_A (resp. μ_B) est l'intensité moyenne de A (resp. B), σ_A (resp. σ_B) est l'écart-type des intensités de A (resp. B) et σ_{AB} est la covariance entre les intensités de A et B et $C_1 = (k_1 d)^2$, $C_2 = (k_2 d)^2$ sont deux petites constantes positives nécessaires pour stabiliser la division. d est l'étendue des intensités et $k_1 = 0.01$, $k_2 = 0.03$ par défaut.
Si $\alpha = \beta = \gamma = 1$ (la valeur par défaut pour les exposants) et $C_3 = C_2/2$ par défaut.
Le SSIM (Strucutal Similarity index) simplifie par:

$$\text{SSIM} = \frac{(2\mu_A\mu_B + C_1) \cdot (2\sigma_{AB} + C_2)}{(\mu_A^2 + \mu_B^2 + C_1)(\sigma_{AB} + \sigma_B^2 + C_2)} \tag{9}$$

3.2.5 VIF

Fidélité de l'information Visuel utilise une modélisation probabilistique des coefficients du filtre temporel suivi d'une mesure de fidélité de l'information (VIF).

3.3 Les caractéristiques de la sécurité d'une image

La sécurité de l'image exige des caractéristiques suivantes:

- Le processus d'insertion et d'extraction doit être assez rapide.
- Les algorithmes d'insertion doit être facile à implémenter par l'utilisateur dans un ordinateur personnel.
- Le mécanisme de la sécurité doit être sûr le plus largement possible.

3.4 Exigences principales de dissimulation d'information numérique

Il existe plusieurs techniques et des différents protocoles qui nous permettent de dissimuler des images numériques dans un autre. Cependant, tous ces protocoles et ces techniques doivent satisfaire un certain nombre de conditions pour que la stéganographie peut être appliquée correctement [32]. Les exigences principales de dissimulation d'information sont:

- L'intégrité de l'information cachée après l'insertion dans le stego-objet doit être correcte.
- Le stego-objet doit rester inchangé ou presque inchangé à l'œil humain.
- Enfin, nous supposons toujours que l'attaquant sait qu'il ya des informations cachées à l'intérieur du stego-objet.

3.5 Quelques nouvelles méthodes de dissimulation d'une information dans une image

La stéganographie dans le domaine spatial regroupe les modifications sur les LSB (Least Significant Bit). Les différents algorithmes modernes de dissimulation d'une information dans une image sont basés sur l'insertion dans le domaine fréquentiel.
On va présenter quelque nouvelles algorithmes de la dissimulation d'un message secret dans des images numériques:

3.5.1 Dans le domaine spatial

LSB

L'insertion dans les bits les moins significatifs (LSB) est une approche simple pour intégrer des informations dans le fichier image. Lorsque on cache les bits de message dans l'image en utilisant des algorithmes LSB, les bits du message intègrent directement dans les bits les moins significatif de l'image couverture. L'insertion dans le bit le moins significatif ne provoque pas de différence perceptible par l'humain, car l'amplitude de la variation est faible. Considérons quatre pixels d'une image ainsi que leur format binaire :

$$123 = 01111011, 101 = 01100101, 120 = 01111000, 99 = 01011010$$

En supposant que le numéro 14 c'est le message secret, où la représentation binaire est 1110, est intégré dans les bits les moins significatifs. Le résultat d'insertion est comme suivant :

$$123 = 01111011, 101 = 01100101, 120 = 01111001, 99 = 01011010$$

Pallavi Das et al. [61] ont proposé une méthode qui permet d'insérer plusieurs images secrètes en une image couleur (de 24 bits), (une seule image couleur peut cacher plusieurs images), utilisant LSB substitution basée sur l'image stéganographie. Chaque image secrète est d'abord chiffrée en utilisant Arnold Transform. Ensuite, les trois premiers bits MSB de la première image secrète chiffrée sont intégrés au hasard dans les trois derniers bits LSB des pixels rouges de l'image de couverture. Le remaniement des bits au cours du processus d'intégration agit comme une couche supplémentaire de protection contre les attaques. De même, les trois premiers bits MSB de la deuxième et troisième image secrète cryptée sont intégrés au hasard dans les trois derniers bits LSB des pixels verts et bleus de l'image de couverture, respectivement. Ces pixels modifiés sont ensuite combinés pour créer l'image stego.
Chang et Cheng [62, 63], ont proposé LSB substitution avec un réglage de pixel optimal pour cacher l'information d'une manière simple.

PVD

Da-Chun Wu et al [54], ont suggéré une nouvelle et efficace méthode de stéganographie pour cacher des données dans des images en niveau de gris. En utilisant les différences des valeurs grises dans deux blocs de l'image de couverture comme des caractéristiques pour regrouper ces blocs dans un certain nombre de catégories de lissage et des propriétés contrastées. Les données secrètes peuvent être intégrées dans les différentes catégories en fonction du degré de lissage ou le contraste. Cette méthode fournit un moyen facile de produire des résultats plus imperceptibles que ceux produits par des méthodes de remplacement simples (LSB). La méthode proposée a été conçu de telle manière qu'il n'y a pas besoin d'utiliser l'image originale pour récupérer le message secret.
La méthode de modification de valeur de pixel(PVM) [63] proposé par V.Nagara1 j et al a été basée sur l'insertion dans des images couleurs, dans cette méthode l'image de couverture est divisée en trois plans (rouge, vert et bleu), les trois composants ont été utilisés pour intégrer des données . Tout d'abord, la méthode est basée sur l'intégration des bits dans le premier pixel de la matrice du composant rouge, puis dans le premier pixel de la matrice de composante verte et enfin, dans la composante bleue.
Weiqi Luo et al [11] ont proposé un nouveau schéma de stéganographie pour améliorer la sécurité, ainsi que la qualité visuelle des images stego, une image de couverture est d'abord divisée en petits carrés. Chaque carré est ensuite mis en rotation par un degré aléatoire de $0, 90, 180$ ou 270. L'image résultante est ensuite divisée en des unités d'insertion avec trois pixels consécutifs dans chaque unité, l'insertion est faite dans le pixel central. Le nombre de bits intégré dépend des différences entre les trois pixels.

3.5.2 Dans le domaine fréquentiel

DCT

A.Nag, S et al [64] ont proposé une nouvelle technique de stéganographie appliquée à l'image basée sur le bloc-DCT, où DCT est utilisé pour transformer les blocs de l'image d'origine (image de couverture) du domaine spatial au domaine fréquentiel. Tout d'abord une image en niveaux de gris de taille M × N est divisé

en 8 × 8 blocs et (2-d DCT) est effectuée sur chacun des blocs. Ensuite, le codage de Huffman est également effectué sur les messages secrets avant l'insertion, chaque bit de code de Huffman du message secret est intégré en modifiant le bit de poids faible (LSB) de chacun des coefficients DCT de blocs d'images de couverture.
J.R.Krenn [64] a proposé une méthode pour insérer un message secret dans LSB des coefficients DC d'une image de couverture. Il a proposé un algorithme pseudo-code simple pour cacher un message dans une image JPEG.
KokSheik Wong et al [65, 64] ont proposé la méthode de stéganographie Mod 4 dans le domaine de transformée en cosinus discrète (DCT). Mod4 est capable d'intégrer des informations à la fois dans l'image non compressé et l'image compressé en JPEG.
Tseng et changement dans [66, 64] ont proposé une nouvelle méthode de stéganographie basé sur JPEG. Dans cette méthode le DCT pour chaque bloc de 8 × 8 pixels a été appliquée afin d'améliorer la capacité et de contrôler le taux de compression.

DWT (IWT)

Della Baby et al [67] ont suggéré une technique de sécurisation des données qui est utilisée pour cacher plusieurs images en couleurs dans une image en couleur unique à l'aide de la transformée en ondelette discrète DWT. L'image de couverture est divisée en trois plans R, G et B. Les images secrètes sont intégrées dans ces plans. Une décomposition du N niveau de l'image de couverture et les images secrètes sont faites, ensuite certaines composantes de même fréquence sont combinées. Ici, le steg-image obtenu a une évolution moins perceptible par rapport à l'image originale avec la sécurité globale élevée.
Dans [8], une nouvelle technique de stégnographie qui basée sur Différence modulation dans la transformée en ondelette discrète (DWTDM) est présentée par S. Bhattacharyya et al, lorsque les données secrètes sont intégrées dans les différences coefficients de DWT adjacents. Medisetty Nagendra Kumar et al [14] ont proposé une nouvelle technique de stéganographie appliquée à l'image qui permet de récupérer les données cachées dans l'image couleur sans dégradation significative de la qualité de l'image en couleur. Dans la méthodologie de cette

technique l'insertion est faite dans les bits les moins significatifs des trois canaux (rouge, vert, bleu) dans une image couleur donnée, le processus d'insertion du message secret est basé sur l'intégration dans le domaine fréquentiel DWT, Génétique Algorithme et le processus d'ajustement de Pixel Optimal (OPAP).
S. Hemalatha et al [17] ont proposé une technique de stéganographie appliquée à l'image pour cacher plusieurs images secrètes et les clés d'insertion dans une image de couleur à l'aide de la transformée en ondelette discrète (DWT). Il n'y a pas de différence visuelle entre le stego image et l'image de couverture. Les images secrètes extraites sont également semblables à des images originales.
M. F. Tolba et al [68] ont proposé un algorithme qui intègre les bits de message secret dans les LSB des coefficients entiers ondelettes d'une image couleur. L'algorithme applique également une étape de prétraitement sur l'image de couverture pour régler les composants de pixels afin de récupérer le message intégré sans perte.

S.Uma Maheswari et al [69] ont présentés une nouvelle technique de dissimulation d'une information en utilisant la transformée en ondelettes entier(IWT) par système d'élévation qui vise à atteindre une haute qualité de stego image. Cette méthode cache le message secret dans le détail des coefficients (CH, CV, CD) de transformée en ondelettes entier(IWT). Cette méthode est très simple et efficace.

SVD

Dans [70], Une nouvelle approche pour l'insertion des données dans des images numériques est proposée par Vladimir I. Gorodetski et al. Cette méthode fournit un taux élevé de données intégrées et est robuste à certaines attaques. L'approche proposée est basée sur l'intégration d'un bit de données par modifications légères des valeurs singulières d'un petit bloc des couvertures. Bergman et Davidson ont proposé une technique de stéganographie qui divise l'image de couverture dans des blocs, puis calcule le SVD des ces blocs et intègre le message secret dans les vecteurs singuliers gauches [2, 71]. Leur algorithme est robuste à certaines des attaques statistiques stéganalytiques, qui a analysé directement la valeur de pixel.

Chung et al ont développé un système de dissimulation dans une image numérique basée sur le SVD et la quantification vectorielle (VQ) [72, 71]. Leur algorithme fournit un bon taux de compression et une qualité d'image faible.
Raja et al ont proposé une technique de stéganographie de haute capacité et robuste en utilisant SVD (RHISSVD), cette méthode est basée sur l'insertion des bits de messages secret dans des valeurs singulières de l'image de couverture [73, 71].

Hybride DWT et DCT et SVD, autre méthodes

Dans [74] un algorithme de tatouage d'image basé sur DWT, DCT et SVD a été proposé par Manie Kansal eyt al. La transformée de Arnold a été appliquée à l'image tatouer afin d'assurer la robustesse de l'algorithme.
Mansi S. Subhedar et al [75] ont proposé une nouvelle technique qui permet d'intégrer des informations secrètes dans une image de couverture basée sur la transformée en ondelettes discrète (DWT) et la décomposition en valeurs singulières (SVD). L'algorithme est basé sur la modification des valeurs singulières de la bande HH de l'image de couverture par celle de l'image secrète.
Qingtang Su et al [76] ont présenté une nouvelle technique de tatouage d'image aveugle qui permet d'intégrer une image de couleur (la marque) dans une image de couleur (l'image originale), cette algorithme est différent de certains algorithmes existants en utilisant l'image de niveau de gris ou l'image binaire comme une marque. Tout d'abord, l'image couleur utilisée comme l'image originale est divisé en 4×4 blocs de pixels. Ensuite, chaque bloc de pixels sélectionné est décomposé par la décomposition QR et l'élément de la première ligne et la quatrième colonne dans la matrice R est quantifiée pour intégrer les informations de la marque. Dans la procédure d'extraction, la marque peut être extraite de l'image tatouée sans l'exigence de l'image origine ou la marque.
Dans [77] une technique de dissimulation d'une information dans une image basée sur la déviation minimale de fidélité (STMDF) a été proposée par J. K. Mandal et al, où deux bits par octet ont été remplacés en choisissant la position aléatoire entre LSB et la quatrième bit MSB. Cette technique a également optimisé la valeur d'intensité de pixel après l'insertion en la comparant avec la valeur de pixel originale.

Yuan-Hui Yu et al [78] ont proposé une nouvelle méthode de stéganographie pour intégrer une image de couleur ou une image en niveaux de gris dans une image de couleur, tout en offrant une capacité de dissimulation élevée et en conservant une haute qualité d'image. dans la méthode proposée il existe trois types d'insertion: l'insertion d'une image de couleur dans une image de couleurs, dissimulant une palette basée sur image secrète de 256 couleur dans une image de couleur, et de cacher une image en niveaux de gris dans une image de couleur. Le deuxième type d'insertion peut extraire directement la palette et les indices des données à partir d'une image secrète de 256 couleur et intégrer ces données dans une image de couverture.
Jeebananda Panda et al [79] ont proposé un nouveau système hybride basé sur IWT, SVD, Norm Quantification, l'approche de Modulo 2 et le chiffrement de la marque. Après avoir appliqué IWT à l'image de couverture nous appliquons SVD et norme matricielle quantification à trois sous-bandes de haute fréquence dans le premier niveau. Ensuite, les valeurs quantifiées sont modifiées en fonction des bits du filigrane. Dans le deuxième niveau l'approche du modulo 2 est utilisée pour intégrer la marque.

3.6 Attaques et stéganalyse

Le but d'un ennemi actif (ou attaquant, hacker) est de désactiver le support de l'hôte (support de tatouage) de manière à rendre toute détection de marque impossible. Cela peut être possible sans connaître la présence de la marque. L'attaque consiste seulement de rendre la marque inutilisable dans le cas où elle existe.
Pour un stiganographe, une attaque efficace est simplement lorsqu'elle détecte un message inséré dans le support[80].
Lorsqu'un attaquant tente uniquement de détecter si un message transite dans un médium sur le canal de communication, on dit de lui qu'il est passif. La plupart des solutions de stéganographie ne considèrent que ce type d'attaquant, au contraire dans le tatouage où il est actif: l'attaquant sait alors que le médium tatoué contient une marque et il tente de la modifier ou de la retirer.
Il existe deux grands types d'attaques:

– Les attaques liées à l'image (ou au signal de watermark), dont le but est clairement une suppression simple d'un donnée masqué dans l'image, en ignorant son contenu. Cela se résume à des transformations plus ou moins violentes. Ces transformations ont pour but de rendre illisible le marquage. Il est intéressant de remarquer néanmoins que ces attaques ne sont pas forcément volontaires. En effet, sans le savoir l'image peut être dégradée suffisamment pour que le tatouage soit effacé. Un algorithme de marquage robuste est sensé résister de manière efficace à ces types de transformation, ou du moins tant que l'image reste utilisable.

– Les attaques plus "malicieuses˘a" ont pour but est retrouver le marquage. Pour cela il suffit de récupérer par différents moyens la "clé" à utiliser au tatouage de I image originale. Nous pourrons alors modifier cette image, le lire, le supprimer...

3.6.1 Les attaques Basiques Involontaires

Commençons par une liste, non exhaustive, des types de transformations pouvant potentiellement altérer le tatouage :

Figure 3.2: Transformation symétrie horizontale

Les transformations géométriques

Symétrie horizontale Le fait simplement d'inverser horizontalement une image est très souvent fatal a une grande partie de watermark. Cette transformation peux sembler aux premier abord bien trop brutale pour conserver le sens d'une image, mais il peux passer inaperçu pour un paysage, ou même pour

un film ou aucune scène d'écriture n'intervient (sous-titrage à proscrire). Un exemple est illustré sur la figure.3.2

Figure 3.3: Rotaion de 10°

Recadrement Ces types des attaques peuvent être très efficace. Ces transformations concernent surtout la mise en page des différentes images. Cela peut être un découpage brutal d'une partie de l'image, ou bien une simple rotation de quelque degrés.

Les transformations frequentielles

Ces transformations modifient essentiellement les coefficients de la DCT. Bruitage et Filtrage.

Le bruit Le bruit est une altération de l'image: toute l'information pertinente dans l'image n'est pas simplement accessible. Des exemples de bruit artificiel peuvent être:

- le bruit gaussien qui consiste à un ajout successif de valeurs générées aléatoirement à chaque pixel d'une image (figure3.4)
- ou encore le bruit "sel et poivre" qui transforme aléatoirement des pixels de l'image en pixel noir ou blanc (figure3.5).
- Filtres passe-bas: Faisant partie de la catégorie des filtrages linéaires. On utilise ici la transformée de Fourier pour travailler dans l'espace des

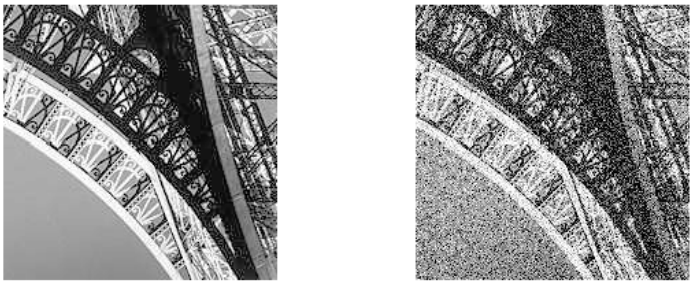

Figure 3.4: Le bruit gaussien

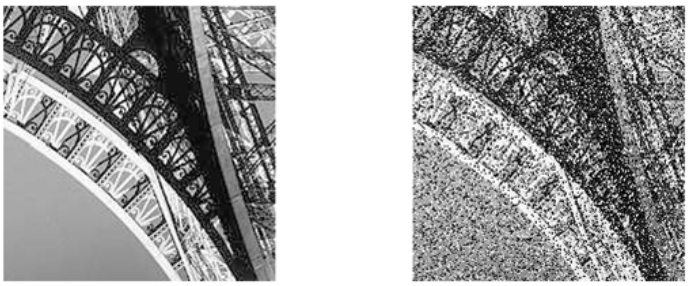

Figure 3.5: Sel et poivre

fréquences de l'image et dans lequel on ne laisse alors passer que les basses fréquences. En fait, il ne s'agit ni plus ni moins que d'un produit de convolution du signal avec une fonction passe bas (figure 3.6).

– Filtre passe-haut: Toujours dans les filtrages linéaires, et souvent appelé "Sharpen" du au fait qu'il a pour but d'accentuer des contours. Il s'agit simplement de l'inverse du filtre passe-bas, car il ne conserve que les hautes fréquences. Cette attaque est certainement la moins efficace des transformations car elle conserve le bruit, et que c'est souvent à ce niveau la que se situe le tatouage. figure3.6.

– Filtre median : Ce filtre, non linéaire, remplace la valeur d'un pixel par la médiane des valeur de ces voisin. Il est plus robuste que le precedent pour differents types de bruits artificiels, donc plus éfficace en tant qu'attaque (figure 3.6).

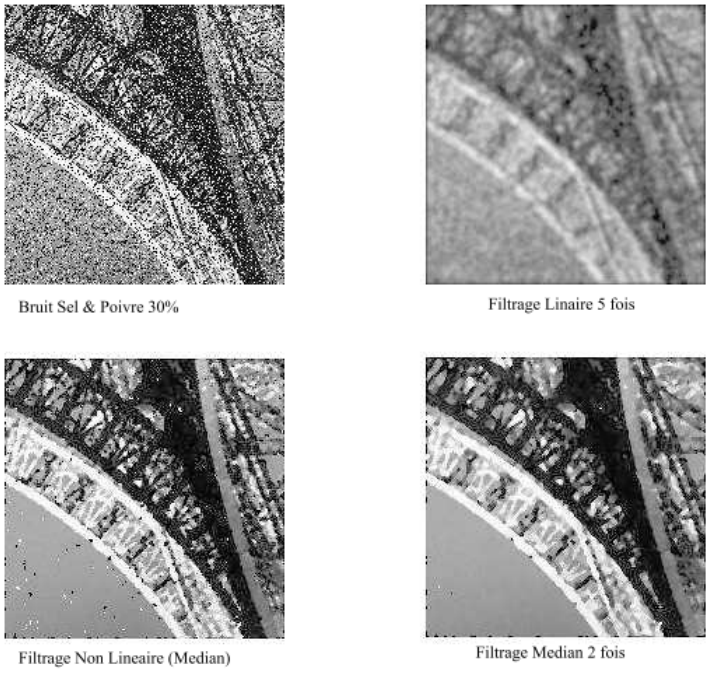

Figure 3.6: Filtrage

3.7 Les Compressions

Les compressions à pertes sont souvent une succession des différentes transformation vu précédemment, ce qui en font des attaques involontaires et souvent très efficace. Un exemple peut être la compression Jpeg (figure 3.7).

Figure 3.7: Compressions

Ce type d'attaque s'applique aussi à tout ce qui est conversion de format, par exemple du jpeg vers du gif.

Gamma correction (Le gamma est une déformation de la luminosité). En mathématique est une courbe (une fonction) qui permet de connaître le lien - la corrélation - qu'il y a entre un signal émis (la lumière perçue) et la réponse d'un capteur, (par exemple notre œil). Cette fonction s'écrit sous la forme:

$$Signaldesortie = Signald'entrée^{gamma} \tag{10}$$

La correction gamma est un procédé qui permet de gestion des couleurs, notamment au moment du calibrage de l'écran. En d'autres termes, si une tension de 1 volt donne le blanc, c'est à dire la luminance maximum de 100 %, une tension moyenne de 0,5 volt ne donnera pas une luminance de 50 % comme on pourrait l'esperer mais plutôt une luminance bien plus faible de 20 % seulement. Et cet écart s'amplifie de plus en plus en s'approchant des valeurs proches du noir.

3.8 Discussion

Assurer la sécurité des images numérique distribuées dans un réseau non sur est fortement lié à l'algorithme de dissimulation d'images utilisé.Cependant, en raison de sa caractéristique de grandes quantités de données et ca inportance

Plusieurs algorithmes de dissimulassions ont été proposé en se basant sur différentes techniques et stratégies. Néanmoins, la plupart de ces algorithmes souffrent d'une ou plusieurs problèmes tels que la faible sensibilité à différentes types d'attaques Un problème qui nous préoccupe concerne la robustesse des algorithmes surtout contre les attaques géométriques dans les techniques de tatouage, par contre dans les technique de steganographie nous préoccupe l'insertion une quantité important d'information et bien sur de prend en compte la robustesse et l'invisibilité de l'algorithme.

Afin de résoudre ces problèmes, des recherches proposent différentes solution pour surmonter les limitations précédentes. Presque toutes les limitations ont été résolues, néanmoins, le grand problème est dans la résistance à l'attaque géométrique dans les algorithmes de tatouage proposé. Nous réfléchissons à la structure à donner à notre outil pour limiter les risques liés à ces attaques. et d'assurer l'invisibilité des données qu'est ont insert

3.9 Conclusion

Dans ce chapitre, nous avons présenté les Outils élémentaires d'analyse statique d'une image, les caractéristiques de la sécurité d'une image, les exigences principales de dissimulation d'information numérique, ensuite nous avons essayé de mettre le point sur quelques techniques de dissimulation d'une information dans une image. Nous nous sommes intéressés aux techniques qui sont basées sur l'insertion dans le domaine fréquentiel.
La dissimulation d'une information dans une image est un domaine qui a vu un développement important pour réaliser un processus symétrique de transmission fiable d'image secrète Les techniques de steganographie peuvent être regroupées en deux catégories: les technique travaillant dans le domaine spatial et les technique travaillant dans le domaine fréquentiel.
Dans le prochain chapitre, nous présenterons notre première contribution

qu'est un schémas de tatouage des images couleurs RGB. Le nouveau schéma de tatouege aveugle proposé est basé sur l'insertion dans le domaine fréquentiel. Nous avons travaillé sur différents critères: robustesse, l'invisibilité...

Part II

Contributions

Chapter 4

Un nouvel algorithme de tatouage des images couleurs basé sur l'utilisation de la décomposition polaire

4.1 Introduction

Dans le chapitre précédent, nous avons présenté un état de l'art sur les algorithmes de dissimilation d'une information dans une image qui sont basées sur différentes techniques. Les techniques les plus connues sont la stéganographie et le tatouage. La recherche dans ces domaines a été très généreuse ces dernières années, elle est ouverte pour de nouvelles idées afin de sécuriser encore les protocoles existants pour obtenir de meilleures performances.

La protection de transmission et de distribution des données devient de plus en plus importante.
Le tatouage numérique a été proposé comme l'une des techniques possibles pour traiter ce problème et pour assurer la sécurité des informations. Notre contribution est le tatouage des images couleurs basé sur un outil algébrique linéaire qui est la décomposition polaire, où un composant de l'image couleur (R, G or B) est sélectionné et divisé en blocs de taille 4×4, le watermark est intégré dans des blocs appropriés. Nous nous sommes intéressés à la proposition d'un algorithme aveugle, cela permet de ne pas diffuser les données originales qui peuvent être détruites après tatouage, l'algorithme de détection est aveugle, i.e. seulement l'image tatouée et la clé sont utilisées pour détecter le watermark. Dans ce chapitre, nous expliquerons l'implémentation de notre méthode. Nous commençons d'abord par l'algorithme d'insertion et ensuite l'algorithme de détection, puis nous discutons les résultats expérimentaux de notre contribution.

4.2 Méthode proposée

Le principe de notre méthode de tatouage [34] est reposé sur deux opérations, le processus d'insertion et le processus d'extraction ou détection de watermark.

4.2.1 Algorithme d'insertion

Dans cette section, nous présentons l'algorithme d'insertion, qui permet d'insérer un watermark dans une image couleur RGB.
L'algorithme d'insertion comprend:

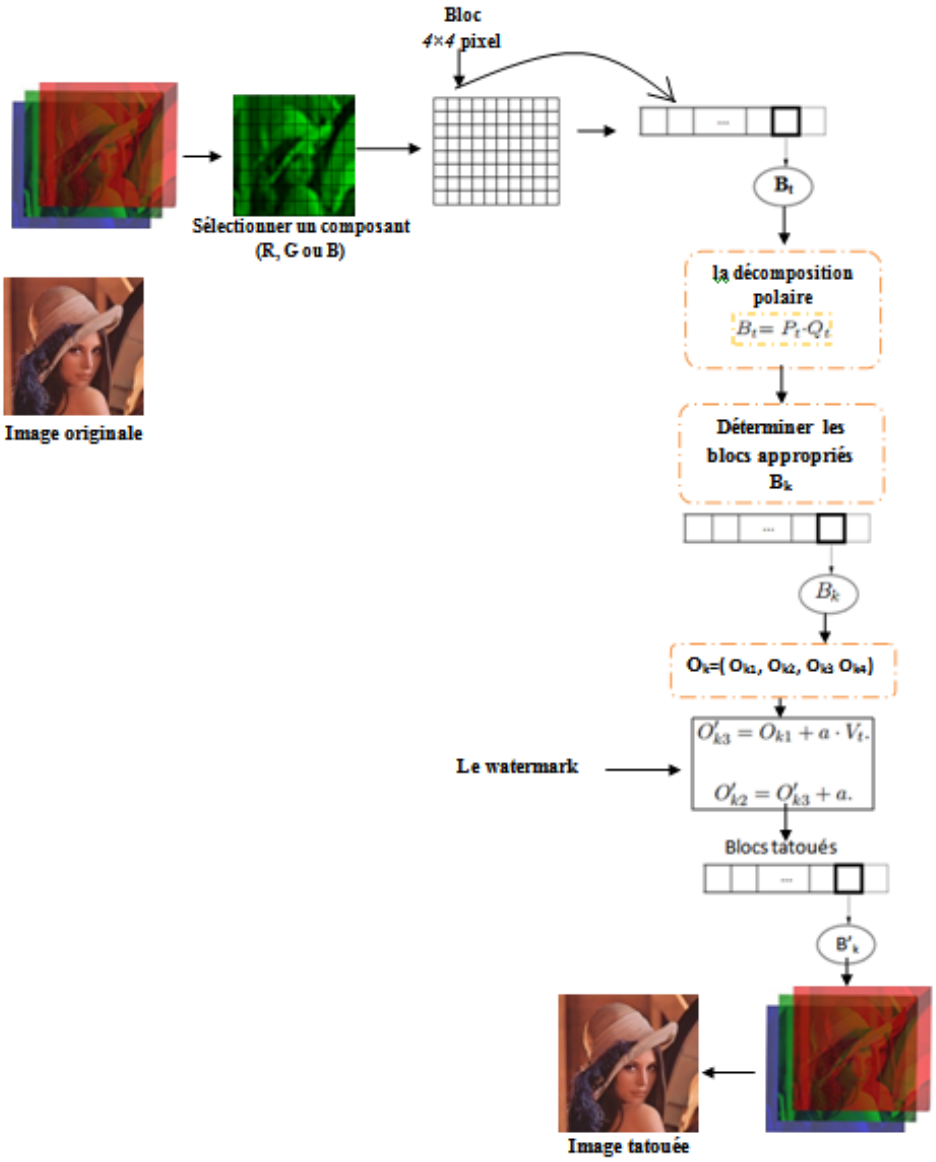

Figure 4.1: Le schéma d'insertion

– En entrée un watermark représente en binaire logo W de taille n × n, une image originale I.

– En sortie une image tatouée I', la clé générée par des blocs sélectionnés.

Les étapes détaillées de cette phase sont présentées comme suit:

– **Étape 1:** Sélectionner un composant de l'image couleur I $(I_R, I_G or I_B)$, puis diviser-le en blocs B_t de taille 4×4, où $t = 0, 1, \ldots, (N \cdot N/16) - 1$.

– **Étape 2:** Appliquer la décomposition polaire B$t_= P_t \cdot Q_t$, trier les blocs dans un ordre décroissant en fonction de la variance V_t calculée dans l'équation (1).

$$V_t = \frac{1}{4} \sum_{i=1}^{i=4} (P_{tii} - M_t)^2 \tag{1}$$

Où P_{tii} représente les composants de la diagonale de la matrice P, et M_t calculé par:

$$M_t = \frac{1}{4} \sum_{i=1}^{i=4} P_{tii} \tag{2}$$

M_t c'est la moyenne des valeurs diagonales.

– **Étape 3:** Soit $k = 0, 1, \ldots, (N \cdot N/16) - 1$, l'adresse des blocs ordonnés. Mettre le vecteur $O_k = (P_{k11}, P_{k22}, P_{k33}, P_{k44})$.

– **Étape 4:** Si: $(M_k \prec V_k)$: alors passer au bloc suivant $k = k + 1$, et revenez à l'étape précédant.
Sinon: Passer à l'étape suivante.

- **Étape 5:** trier dans l'ordre décroissant le vecteur O_k, c'est-à-dire $O_k = (P_{k11}, P_{k22}, P_{k33}, P_{k44}) \cdot \Pi = (O_{k1}, O_{k2}, O_{k3}, O_{k4})$, avec Π est une matrice de permutation.

- **Étape 6:** Si: $O_k 1$ est égal au P_{k11} Passer à l'étape suivante.
  Sinon: faites $k = k + 1$ et revenir à l'étape 3.

- **Étape 7:** Si: $W(i, j) = 0$ alors:

$$O'_{k3} = O_{k1} + \alpha \cdot V_k. \tag{3}$$

$$O'_{k2} = O'_{k3} + \alpha. \tag{4}$$

  où α est le facteur d'inclusion du système de tatouage, $\alpha \in [0,2]$, et $i; j = 0, 1, \ldots, n-1$
  Alors: $O'_k = (O_{k1}, O'_{k2}, O'_{k3}, O_{k4})$.

- Si: $W(i, j) \neq 0$ on ne change pas l'ordre des valeurs diagonales, donc le but de cette méthode est de changer l'order des éléments diagonales si le bit est 0.
- **Étape 8:** Mettre $O"_k = O'_k \cdot \Pi$,puis $B'_k = P'_k \cdot Q_k$, où P'_k est obtenu à partir de P_k en remplaçant les éléments diagonaux par $O"_k$.

L'adresse des blocs où le watermark a été inseré détermine la clé d'extraction $K1$.

4.2.2 Algorithme d'extraction

Dans ce schéma, le watermark peut etre extrait sans l'utilisation de l'image originale, donc ce systheme est aveugle. La procédure d'extraction est présentée comme suit:

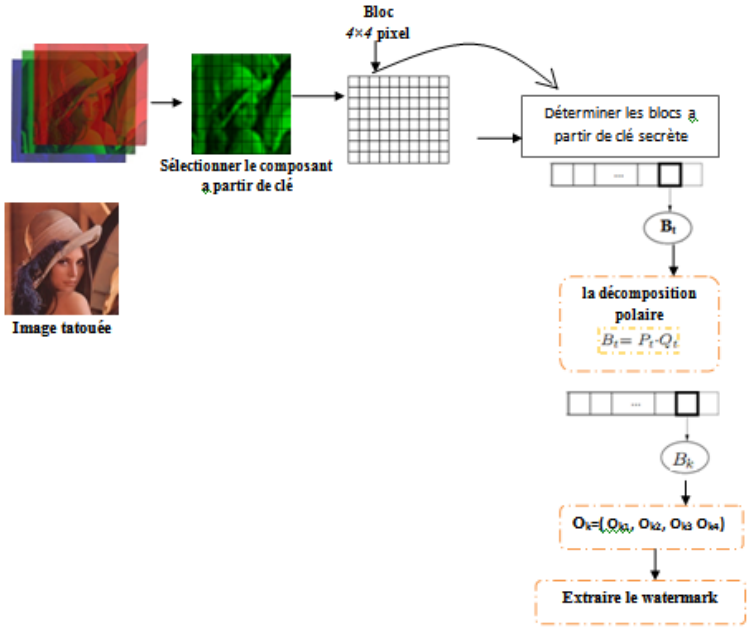

Figure 4.2: Le schéma d'extraction

L'algorithme comprend:

- En entrée: l'image tatouée I' et la clé $K1$.
- En sortie: Le watermark extrait.
- **Étape 1:** Sélectionner le composant où le watermark a été inseré, puis déterminer les blocs à l'aide de la clé K1.
- **Étape 2:** Appliquer la décomposition polaire $B'_k = P'_k \cdot Q'_k$.
- **Étape 3:** Soit le vecteur $O'_k = (P'_{k11}, P'_{k22}, P'_{k33}, P'_{k44})$.trier dans l'ordre décroissant le vecteur O'_k, c'est-à-dire $O'_k = (O'_{k1}, O'_{k2}, O'_{k3}, O'_{k4}) = (P'_{k11}, P'_{k22}, P'_{k33}, P'_{k44}) \cdot \Pi$, avec Π est une matrice de permutation.

– **Étape 4:** Extraire le watermark

$$\begin{aligned} W'(i,j) &= 1, si O'_{k1} = P'_{k11} \\ W'(i,j) &= 0, si O'_{k1} \neq P'_{k11} \end{aligned} \tag{5}$$

– Si la position du plus grand élément dans le diagonale est changée donc la valeur du secret est 0 sinon on a 1

4.3 Les resultats expérimentaux

Dans cette section, en utilisant Matlab des performances de notre méthode en termes d'imperceptibilité et robustesse ont été réalisée. Ces résultats expérimentaux sont séparés en deux parties: la premire est consacrée au test de la propriété d'imperceptibilité (invisibilité) alors que la deuxième est consacrée à l'analyse de la robustesse contre quelques types d'attaques standards.

4.3.1 Analyse d'imperceptibilité

Pour étudier l'imperceptibilité du système de tatouage proposé, on utilise le PSNR pour estimer la distorsion des images tatouées. Plusieurs images couleurs RGB de taille 512 × 512 sont tatouées avec un logo de taille 64 × 64.

Figure 4.3: Images originales en couleurs I

Les images originales en couleurs et en niveau de gris sont présentées respectivement dans figure 4.3 et figure 4.4, leurs images tatouées sont présentées

Figure 4.4: Images originale de niveau de gris I

respectivement dans la Figure.4.5 et Figure.4.6.

Figure 4.5: Images tatouées I' en couleurs

A partir de ces figures, on peut voir qu'il est difficile de différencier entre les images originales et leurs images tatouées.

Les résultats de cette évaluation d'après l'insertion en utilisant des images originales en couleur de taille 512×512 et du NC entre W et W', sont illustrés dans la table 4.1

Figure 4.6: Images tatouées I' de niveau de gris

L'image originale	PSNR	NC entre W et W'
Lena	54.26	1
Girl1	54.88	1
Afghan	55.12	1
Pepper	55.62	1
Goldhil	54.62	1
Barbara	54.71	1
Girl2	53.88	1
Girl3	54.18	1
House	54.25	1
Sailboat	55.02	1
Cat	54.72	1
sails	54.82	1

Table 4.1: Les valeurs du PSNR et du NC entre W et W'

Autre évaluation de notre système de tatouage a été réalisé en utilisent des images hôtes de niveaux de gris de taille 512×512
Les images originales et leurs images tatouées sont présentées respectivement dans figure 4.5 et la Figure.4.6.

Les résultats de cette évaluation d'après l'insertion en utilisant des images originales de niveau de gris de taille 512×512 et du NC entre W et W', sont illustrés dans la table 4.2.

L'image originale	PSNR	NC entre W et W'
boa	50.26	1
Man	50.88	1
Airplan	50.02	1
elaine	50.62	1
Girl	50.62	1
einstein	50.71	1

Table 4.2: Les valeurs du PSNR et du NC entre W et W'

4.4 Analyse de robustesse

Nous avons choisi de faire subir à chaque image tatouée un ensemble d'attaques et de vérifier la robustesse de l'algorithme proposé contre toute modification et transformation dans l'image tatouée. La table 4.3 montre la *NC* entre le watermark W et le watermark extrait après quelques manipulations d'images communes pour les images tatouées telles que: Sel et Peppers (0,04), le bruit Impulse (0,02), Recadrage 25%,Compression (10%), Rotation (0.2°). Tous les résultats montrent que l'algorithme proposé peut résister à de nombreux types d'attaques.

L'image tatouée	attaque				
	1	2	3	4	5
Lena	0.95	0.97	0.80	0.98	0.80
Girl1	0.95	0.97	0.98	0.98	0.80
Afghan	0.95	0.97	0.98	0.98	0.80
Pepper	0.95	0.97	0.96	0.98	0.80
Goldhil	0.95	0.97	0.97	0.98	0.80
Barbara	0.95	0.97	0.98	0.98	0.80
Girl2	0.95	0.97	0.96	0.98	0.80
Girl3	0.95	0.97	0.98	0.94	0.80
House	0.93	0.99	0.96	0.85	0.83
Sailboat	0.94	0.99	0.97	0.81	0.84
Cat	0.95	0.99	0.98	0.85	0.79
sails	0.95	0.97	0.94	0.98	0.81

Table 4.3: Les valeurs de NC entre W et W'

4.5 Conclusion et perspectives

Ce chapitre présente notre première proposition ; qui est un nouveau schéma de tatouage sécurisé et efficace qui permet d'assurer la protection de transmission des images couleur. L'algorithme de tatouage d'image basé sur un outil algébrique linéaire qui est la décomposition polaire. Dans le processus

d'extraction, le watermark peut être extrait de l'image tatouée sans l'exigence de l'image originale. Des simulations pour l'analyse de la sécurité ont été effectuées pour assurer l'efficacité du système proposé contre les attaques d'effacement et les attaques géométriques. Comme perspective nous allons essayer d'améliorez l'aspect progressif du schéma de tatouage pour obtenir un schéma résistant à différents types d'attaques. Nous allons utiliser le schéma hybride pour insère la marque en combinant la transformation DWT et la décomposition polaire. Dans le chapitre qui suit, nous allons introduire notre deuxième contribution, qui consiste en un schéma de steganographie basé sur un le même outil algébrique mais le principe d'insertion est différent.

Chapter 5

Un nouvel algorithme de stéganographie utilisant la décomposition polaire

5.1 Introduction

L'objectif principal des algorithmes de stéganographie consiste à fournir des données sécurisées, indétectables et imperceptibles. Les systèmes de dissimilation d'une information dans une image existants sont classés en deux groups: Les systèmes de dissimilation dans le domaine spatial [81] [24][82][83][84], Les systèmes de dissimilation dans le domaine fréquentiel [85][86][87]. Dans le premier groupe, La plupart d'algorithmes utilisent le LSB [88][89] dans son procédé d'insertion. Cependant, le deuxième groupe est obtenu de premier groupe (le domaine spatial) par une transformation. Pour obtenir les composantes fréquentielles d'une image, l'une des techniques de transformation doivent être utilisés, tels que Transformation de Fourier discrète (DFT) [90], discrète transformation de Fourier à court (DSFT) [89], cosinus discrète Transformation (DCT) [87][76], la transformation en ondelettes discrète (DWT) [87][91][92], et la décomposition en valeurs singulières (SVD)[93][94]. Les différents algorithmes modernes sont basés sur l'insertion dans le domaine fréquentiel pour obtenir de meilleures performances.

Ce chapitre présente une nouvelle approche de dissimulation d'une information dans uns image basée sur la décomposition polaire [18]. Nous montrons l'application de notre méthode sur des images en couleurs en insérant des images en niveau de gris (le message secret). Dans le processus d'insertion, l'image de couverture est divisée en des blocs de dimension 2×2 pixels. Ensuite, une décomposition polaire est appliquée à chaque bloc, les données secrètes sont intégrées dans des blocs appropriés. En outre, l'algorithme proposé est comparé avec autres algorithmes et montre que notre méthode proposée donne une imperceptibilité plus élevée, et un bon niveau de sécurité. Dans le processus d'extraction, l'image originale n'est pas exigée pendant l'extraction du secret, mais la clé peut être disponible, dans ce cas on dit que le schéma proposé est symétrique.

Le reste de ce chapitre comprend les sections suivantes. Dans la section 2, nous présentons L'algorithme proposé en détail. Dans la section 3, nous discutons les performances et les résultats expérimentaux. Enfin, la section 5 tire les conclusions.

5.2 Méthode proposé

Dans l'algorithme proposé, on utiliss une méthode algébrique, qui est la décomposition polaire. Cette décomposition peut être obtenue à partir du SVD, mais il a plus d'avantages que SVD en raison de l'unicité. Toute matrice carrée A a une décomposition polaire A = P.Q, où P est une matrice semi-définie positive et Q est orthogonale. Le système proposé est comparé avec d'autres schéma existants, le message secret ne peut pas être facilement observé par l'oeil humain.

L'objectif principal du schéma de steganographie proposé est d'avoir une bonne imperceptibilité, et aussi fournit un degré élevé de sécurité en utilisant l'un des méthodes d'insertion dans le domaine fréquentiel. Dans le système proposé le choix de l'image de couverture dépend de l'histogramme de l'image secrète et le vecteur M qu'est calculé à partir des blocs de l'image de couverture. La méthode proposée basée sur la décomposition polaire permet de décomposer les blocs de l'image de couverture en deux matrices, ensuite on va insérer les octets de l'image secrète dans la diagonale de la matrice symétrique de la décomposition polaire. Pour extraite l'image secrète il faut utiliser une clé K1: la clé d'extraction permet de connaître les positions des blocs où le message secret a été intégré.

Le schéma de stéganographie comprend actuellement trois phases principales: choisir l'image de couverture, le processus d'insertion, et le processus d'extraction. Les diagrammes d'insertion et d'extraction sont illustrés dans la (figure 5.2) et (figure 5.3), respectivement.

5.2.1 Le choix de l'image de couverture C

Pour intégrer des données secrètes dans une image, nous avons d'abord sélectionné une image de couverture par ces étapes suivantes:
Étape.1: Diviser les composantes C_R, C_G, C_B en blocs B_i de taille 2×2 où $i = 0, 1, \cdots, (N \times N)/4 - 1$.

- Pour chaque bloc B_i faire:

Étape.2: Appliquer la décomposition polaire,

$$B_i = P_i \cdot Q_i. \tag{1}$$

Étape.3: Calculer la moyenne M_i des éléments de la diagonale de P_i par:

$$M_i = \frac{1}{2} \sum_{i=1}^{i=2} P_{ii} \tag{2}$$

Étape.4: Construire le vecteur $M = (M_i)$.
Étape.5: Comparer l'histogramme de la donnée secrète $S = S_t$ (représentée en octet) à l'histogramme de la vecteur $M = (M_i)$. Si l'histogramme de M est supérieur à celle des données secrètes, l'image C peut être utilisée comme une image de couverture.
Dans (Figure.5.1), un exemple représente comment nous pouvons choisir une image de couverture pour la transmission des données secrètes. (Figure 5.1 (a)) représente une donnée secrète comme une image de niveau de gris de taille 130 × 130, et l'image de niveau de gris de taille 512 × 512 qui est illustrée dans (Figure 5.1 (b)) représente une image de couverture, et (figure 5.1 (c)) représente l'histogramme de l'image secrète avec le vecteur M. Les résultats de cet histogramme montre que l'image choisie (figure 5.1 (b)) peut être utilisée comme une image de couverture pour cacher l'image secrète (Figure 5.1(a)).

5.2.2 L'algorithme d'insertion

Dans ce processus, nous sélectionnons une image en niveaux de gris comme des données secrètes et une image en couleur comme une image de couverture
Les étapes de ce procédé sont présentées comme suit: Entrées:
I: l'image de couverture (une image couleur RGB de taille N × N où $N = 2 \cdot n$).
S: le message secret (une image en niveau de gris de taille M × M, où $M = 2 \cdot m$ et $n > m$). Sortie: I' stego-image.

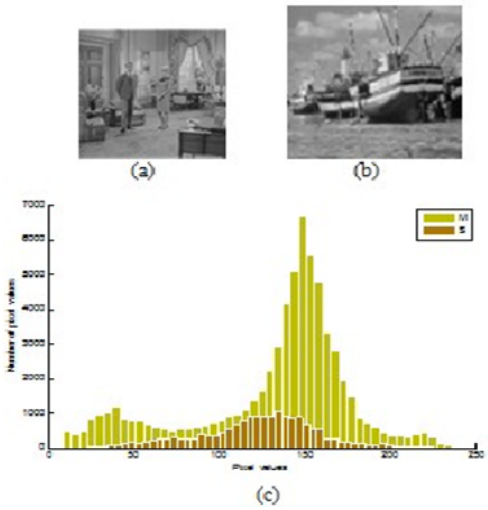

Figure 5.1: L'image Secret(a), l'image de couverture (b), l'histogramme (c)

Pour chaque composante (canal) de couleur $C \in R, G, B$ faire:
Étape.1: Diviser les composants C_R (C_G et C_B) en blocs B_i de taille 2×2 où $i = 0, 1, \ldots, (N \times \mathrm{N})/4 - 1$. Pour chaque bloc B_i faire:
Étape.2: appliquer la décomposition polaire,

$$B_i = P_i \cdot Q_i. \tag{3}$$

Étape.3: Soit le vecteur $O_k = (P_{K11}, P_{K22})$.
Étape.4: ranger dans un ordre décroissant les composants de O_k, c'est à dire:
$O_k = (P_{K11}, P_{K22}) \cdot \Pi = (O_{K1}, O_{K2})$, avec Π la matrice de permutation.
Si: $(|S_t - O_{K1}| \prec \alpha)$ passer à l'étape suivante.
Sinon: $k = k + 1$ et revenir à l'**Étape.3**.
où $\alpha \prec 10$.
Étape.5: Insérer S_t:

$$O'_{k1} = \frac{S_t + O_{k1}}{2}. \tag{4}$$

Étape.6: Mettre $O"_k = O'_k \cdot \Pi$, ensuite calculer le nouveau bloc $B'_k = P'_i \cdot Q_i$ où P'_k

est obtenu à partir de P_k en remplaçant les éléments diagonaux avec $O"_k$.
Étape.7: Répétez les **Étapes 2** à **6** pour intégrer tous les octets des données secrètes.

– Les adresses des blocs où le secret a été intégré déterminent la clé d'extraction $K1$.

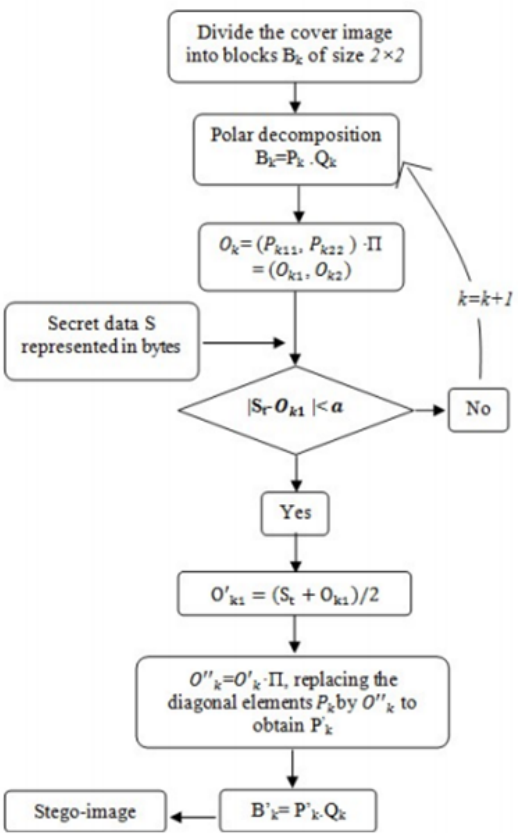

Figure 5.2: Le processus d'insertion

5.2.3 L'algorithme d'extraction

Dans ce schéma, les données secrètes peuvent être extraites de manière aveugle.
Les étapes d'opération d'extraction sont présentées comme suit:
Entrée: Stégo-image I' et la clé d'extraction $K1$.

Sortie: Les données secrètes extraites S'.

Pour chaque composante de couleur $C' \in R, G, B$ faire:

Étape.1: Diviser les composants C'_R (C'_G et C'_B) en blocs B_i de taille 2×2 où $i = 0, 1, \ldots, (\mathrm{N} \times \mathrm{N})/4 - 1$.

Étape.2: Sélectionner les blocs en utilisant la clé $K1$.

Pour chaque bloc Bi faire:

Étape.3: Appliquer la décomposition polaire,$B'_i = P'_i \cdot Q'_i$.

Étape.4: Soit le vecteur $O'_k = (P'_{K11}, P'_{K22})$.

Étape.5: Extraire le secret:

$$S'_t = \left|\mathbf{max}(P'_{k11}, P'_{K22})\right| \tag{5}$$

Où $|X|$ désigne la partie entière de X.

Étape.6: Extraire tous les octets des données secrètes.

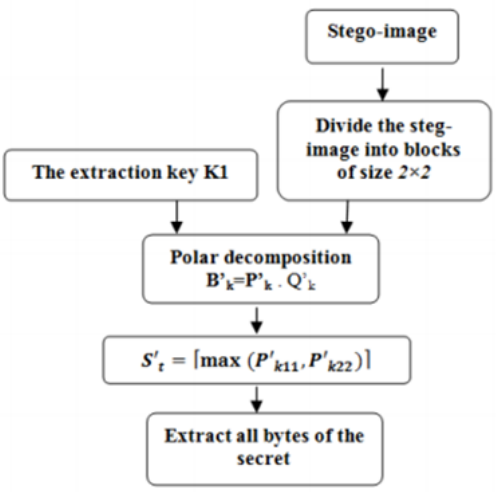

Figure 5.3: Le processus d'extraction

5.3 Analyse de performances

Dans cette section, en utilisant Matlab des simulations numériques ont été effectuées en utilisant différentes mesures pour montrer la sécurité de l'algorithme

proposé.

Nous évaluons les performances de notre méthode en termes d'imperceptibilité et robustesse. Plusieurs images en niveau de gris de différentes tailles sont intégrées dans des images de couleur en utilisant l'algorithme proposé. Les résultats expérimentaux sont classées en trois parties: la première partie est consacrée au test du choix de l'image de couverture, la deuxième consacrée au test de la propriété d'imperceptibilité (invisibilité) et sa capacité, et la troisième est consacrée à l'analyse de la robustesse contre quelques types d'attaques standards.

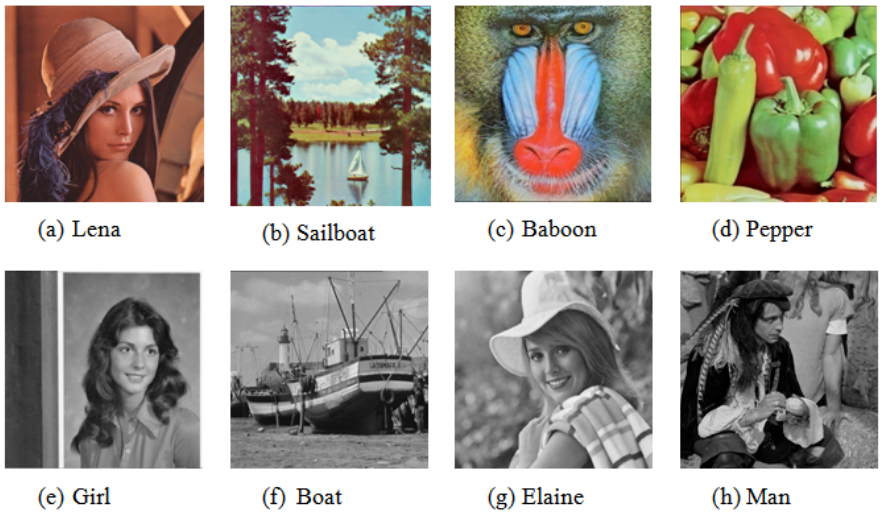

Figure 5.4: Les images de couverture: (a-h) les images couleurs RGB, (i-l) les images en niveau de gris

Les figures 5.4 et 5.5 montrent les images de couverture et les images secrètes qui ont été utilisées pour évaluer les performances de notre méthode respectivement.

5.3.1 Le choix de l'image de couverture

Pour choisir une image de couverture pour la transmission des données secrètes, il faut tester l'histogramme en utilisant la méthode proposée. Dans le Table 5.1. On peut voir comment nous pouvons choisir des images pour l'insertion des

Figure 5.5: Les images secrètes: des images en niveau de gris de différentes tailles.

images secrètes.

L'image secrète	L'image de couverture utilisée
S1, S3, S5	Lena
S2, S3	Baboon
S5	Pepper
S4	Sailboat
S5, S2	Girl
S2, S5	Boat
S3	Elaine
S1, S2, S3, S5	Man

Table 5.1: Le choix de l'image de couverture

5.3.2 Propriété d'imperceptibilité et de capacité

Pour tester la propriété d'imperceptibilité de notre méthode proposée, plusieurs images en niveau de gris des différents tailles sont intégrées dans des images couleurs des tailles 256×256 et 512×512. Les stégo-images et les images secrètes extraites sont présentées respectivement dans les Figures 5.6 et 5.7. Les images obtenues après processus d'insertion sont donnés dans (Figure 5.6), où

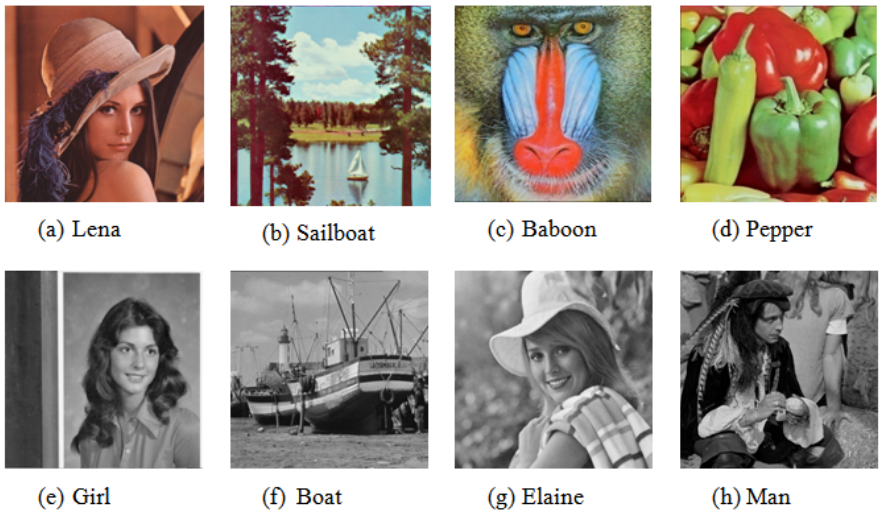

Figure 5.6: Stégo-image

les stego-images ont une bonne valeur de $PSNR$ (avec $PSNR > 53(dB)$), ce qui indique que la présence de l'image secrète ne peut pas être facilement observée par l'oeil. (Figure 5.7), présente l'image secrète extraite avec $NC > 0,998$ et $PSNR > 40$.

Figure 5.7: Les images secrètes extraites

Dans ces figures, on peut voir qu'il est difficile de différencier entre les images de couverture et les stégo-images.

Pour évaluer la qualité de notre méthode de stéganographie, on utilise le $PSNR$ pour estimer la distorsion des stego-images.
Les résultats de cette évaluation d'après l'insertion en utilisant des images de couverture en couleur de taille 256×256 sont illustrés dans la table 5.2, et aussi le PSNR de l'image secrète extraite sans attacque.

les images			PSNR			
L'image de couverture	L'image secrète		stégo-image		secrète extraite	
			a=5	a=7	a=5	a=7
Lena	S1	130*130	53.62	50.31	40.16	37.50
		150*150	52.35	48.98	36.15	37.31
	S3	130*130	53.75	50.40	40.73	37.63
	S5	130*130	53.74	50.83	40.24	36.45
Baboon	S2	130*130	53.69	50.36	41.70	38.70
		150*150	51.54	49.03	41.43	38.59
	S3	130*130	53.92	50.44	42.30	38.91
		150*150	52.58	49.15	42.14	38.84
Pepper	S3	130*130	53.27	50.40	41.12	37.77
	S5	130*130	53.61	50.25	40.83	37.61
		150*150	52.29	48.87	40.67	37.49
	S6	130*130	53.84	50.50	41.16	37.92
		150*150	52.50	49.15	41.03	37.75
Sailboat	S1	130*130	53.71	50.40	41.18	37.99
	S5	130*130	53.63	50.92	41.45	38.13
		150*150	52.34	48.97	36.02	37.97
	S6	130*130	53.93	50.95	41.65	38.20
		150*150	52.70	49.33	41.77	38.33

Table 5.2: Le PSNR de stego image après l'insertion des images secrètes des déférentes taille dans les images en couleurs

Les résultats de cette évaluation d'après l'insertion en utilisant des images de couverture en couleur de taille 512×512 sont illustrés dans la table 5.3, et aussi

le PSNR de l'image secrète extraite sans attaque.

les images			PSNR			
L'image de couverture	L'image secrète		stégo-image		secrète extraite	
			a=5	a=7	a=5	a=7
Girl	S2	130*130	55.17	51.78	39.32	35.65
	S4	130*130	54.85	51.64	38.98	35.49
Beat	S2	130*130	55.13	51.81	39.62	36.26
		150*150	53.85	50.46	39.62	36.16
	S5	130*130	55.23	51.95	39.87	36.82
Elaine	S2	130*130	54.71	51.28	38.57	36.18
		150*150	53.48	49.99	36.79	39.28
	S3	130*130	54.94	51.57	41.04	37.18
		150*150	53.64	50.29	41.00	37.83
Man	S2	130*130	59.88	56.47	39.87	37.03
		150*150	58.62	55.22	39.66	36.64
	S4	130*130	58.84	56.70	40.17	37.28
		150*150	58.66	55.35	40.15	37.23

Table 5.3: Le PSNR de stego image après l'insertion des images secrètes des déférentes tailles dans des image de niveau de gris

L'imperceptibilité et la capacité de notre algorithme proposé sont comparées à la deuxième technique de G.Swain. [4] et aussi avec la méthode de J. K. Mandal et al [77]

G.Swain Swain. [4] Swain a proposé deux valeurs de pixel de différenciation stéganographie technique (PVD) (pixel value differencing steganography using both vertical and horizontal edge). Dans sa première technique proposée, l'image de couverture est divisée en blocs de taille 2×2 pixels et filtrées. Pour chaque bloc, les pixels supérieurs droit et gauche sont ciblés en fonction de leur corrélation avec les deux autres pixels. Les deux de bords verticaux et horizontaux sont utilisés pour insérer des données. Lorsque, dans sa deuxième technique proposée, l'image de couverture est divisée en blocs de taille 3×3 pixels et filtrée. Ensuite, le pixel central est ciblé pour l'intégration de données secrètes. Un des bords verticaux ou horizontaux est utilisé pour insérer des

données au niveau du pixel choisi.

Dans Mandal et al. [77], J. K. Mandal et M.Sengupta ont proposé des techniques d'enrobage des données basée sur la déviation minimale de fidélité (steganographie technique based on the minimum deviation of fidelity ($STMDF$), où deux bits par octet ont été remplacées en choisissant aléatoirement la position entre LSB et le quatrième bit vers MSB.

les images	Méthode proposée						Méthode de Mandal et al		
	150×150			250×250			130×130		
	PSNR	capacité	NC	PSNR	capacité	NC	PSNR	capacité	NC
Elaine	52.64	0.69	0.99	49.85	1.91	0.99	42.66	0.52	0.99
Beat	53.44	0.69	0.99	49.70	1.91	0.99	42.86	0.52	0.99

Table 5.4: La comparison de PSNR, la capacité et le NC de notre méthode avec la méthode de Mandal et al utilisant des image de niveau des gris

Dans la Table 5.4, la comparaison de notre méthode et la méthode de J. K.Mandal et al a été illustrée; dans ces comparaisons, les images en niveaux de gris de taille 512 × 512 ont été utilisées. La capacité d'insertion est 0.52bpp alors les images secrète utilisent dans cette comparaison sont des tailles 150 × 150 pixels (180000 bits) et 250 × 250 pixels (500000 bits), cependant, dans la méthode de Mandal a utilisé l'image secrète de taille 130 × 130 pixels (135000 bits), résultats après l'insertion et l'extraction sont résumés dans la table 5.4. Néanmoins, le tableau 3 et le tableau 4 montrent les mêmes expériences mais en utilisant une image en couleurs de taille 256 × 256 et 512 × 512.

les images	Méthode proposée		Méthode de Mandal et al	
	PSNR	capacité	PSNR	capacité
Lena	49.62	1.17	42.73	0.52
Baboon	48.69	1.17	42.75	0.52
Peppers	49.84	1.17	42.82	0.52

Table 5.5: La comparison de PSNR, la capacité de notre méthode avec la méthode de Mandal et al utilisant des images en couleurs

Dans la Table 5.5, la comparaison de notre méthode et la méthode de J. K.Mandal et al a été illustrée; dans ces comparaisons, les images en couleur de taille 256 × 256 ont été utilisées. La capacité d'insertion est 0.52bpp

les images	Méthode proposée		Méthode de G.Swain		Méthode de Nagaraj[63]	
	PSNR	capacité	PSNR	capacité	PSNR	capacité
Lena	51.92	0.97	50.57	0.15	45.09	0.85
Baboon	52.29	0.97	49.56	0.61	39.06	0.92
Peppers	52.04	0.97	50.27	0.23	43.93	0.83
Sailboat	53.01	0.79	50.20	0.27	-	-

Table 5.6: La comparison de PSNR, la capacité de notre méthode avec la méthode de G.Swian et Nagaraj utilisant des images en couleurs

Dans la Table 5.6, nous avons utilisé des images couleurs de taille 512 × 512 pour comparer notre méthode avec la méthode de G.Swain et la méthode de Nagaraj's[63]. La capacité d'insertion varie entre 0.14 bpp et 0.61 bpp dans la méthode de G.Swain, par contre dans la méthode de Nagaraj's, elle varie entre 0.79 bpp et 0.92 bpp .

La comparaison avec la méthode G.Swain et J. K. Mandal et al montre que le schéma de stéganographie proposé offre de bonnes performances.

5.3.3 L'analyse de la robustesse

Nous avons subi à chaque stego-image un ensemble d'attaques et vérifié la robustesse de l'algorithme proposé contre toute modification et transformation dans la stégo-image.
Les figure 5.7, figure 5.8 et figure 5.9 montrent le *NC* d'image secrète extraite après quelques manipulations d'images communes pour les stego-images telles que: Sel et Peppers (0,02), le bruit Impulse (0,02), Recadrage 15%, correction gamma (2.0), Compression (10%), Tous les résultats montrent que l'algorithme proposé peut résister à ces types d'attaques.

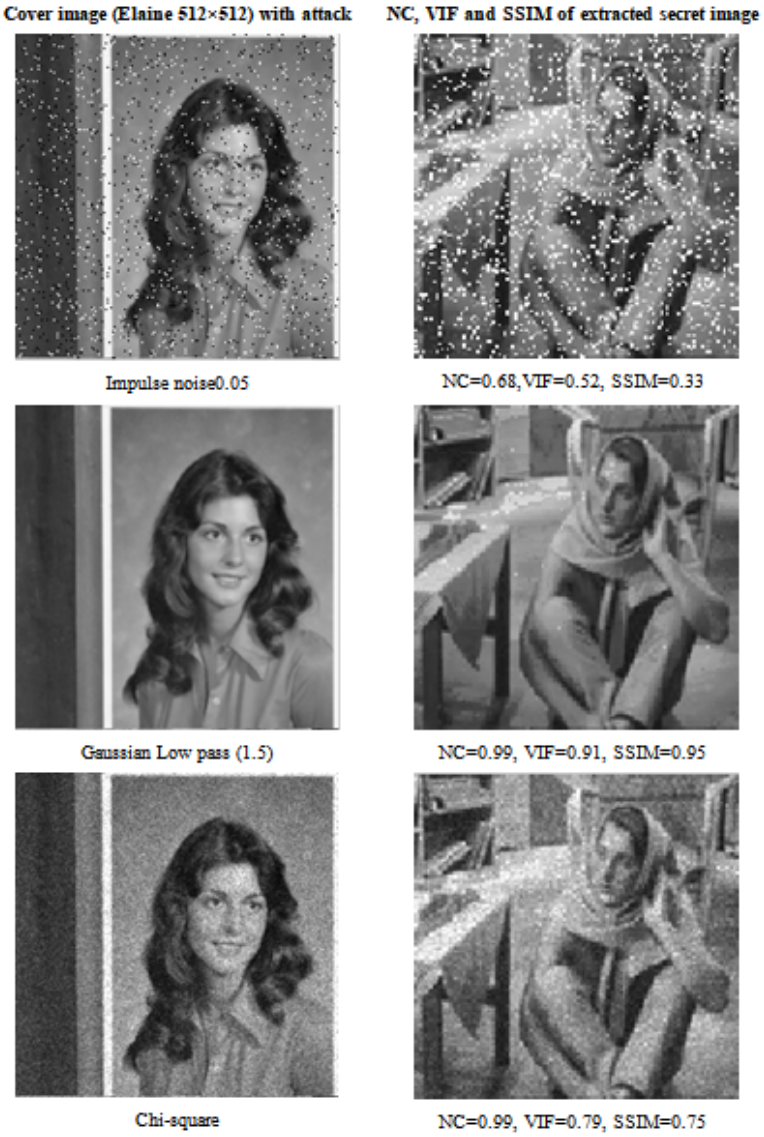

Figure 5.8: NC, VIF et le SSIM

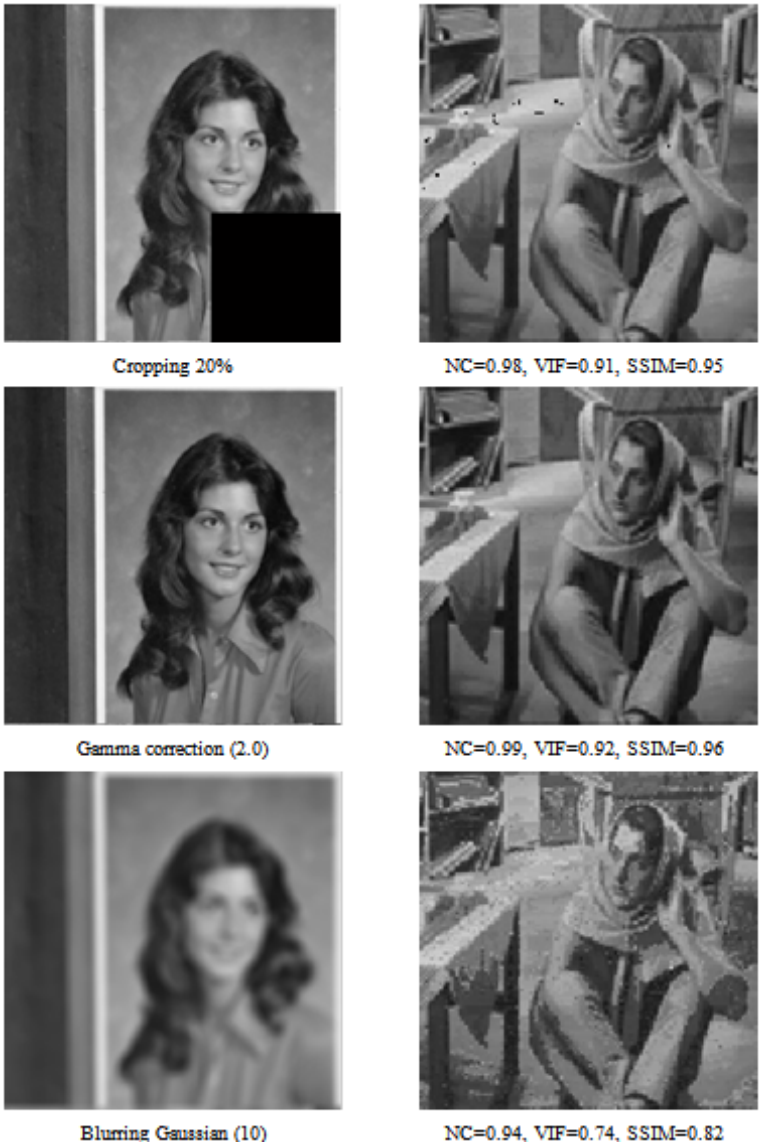

Figure 5.9: NC, VIF et le SSIM

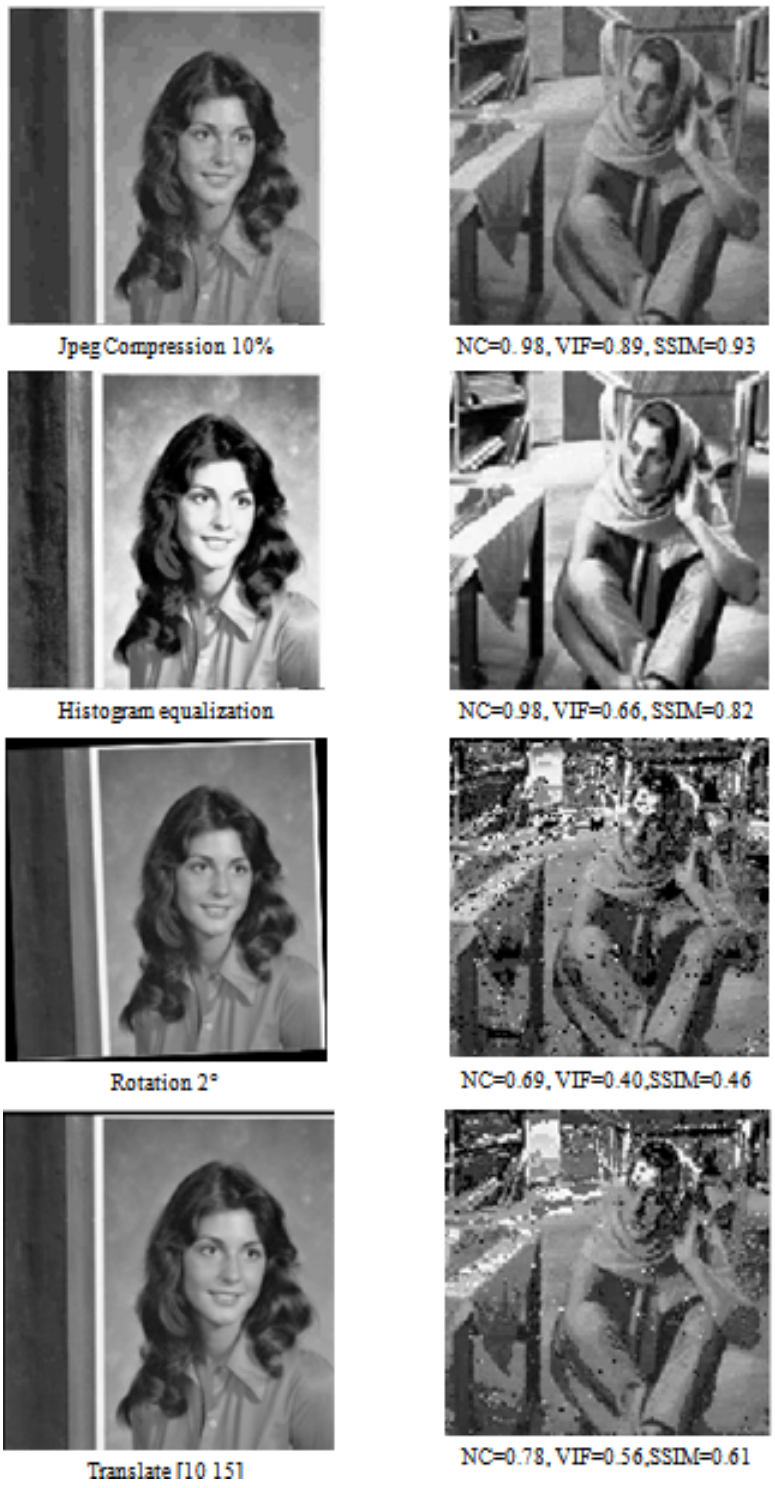

Figure 5.10: NC, VIF et le SSIM

5.4 Conclusion

Dans ce chapitre, nous avons présenté un nouvel algorithme de stéganographie basé sur une méthode algébrique pour sécuriser des informations en particulier les images. Cette méthode est basée sur la décomposition polaire, l'information secrète est insérée dans des blocs de taille 2×2 après d'application de la décomposition polaire.

Des performances de sécurité satisfaisantes sont atteintes en utilisant différents critères. Les résultats expérimentaux ont démontré que l'algorithme proposé n'atteint pas seulement une plus grande capacité de dissimulation, mais atteint également une plus grande invisibilité du schéma de stéganographie, les expériences montrent également la robustesse de notre schéma proposé contre différents types d'attaques.

Conclusion générale

Au cours des dernières années, la confidentialité des services électroniques est très importante, surtout pour traiter les problèmes de la sécurité des informations transmises ou stockées sur des réseaux non sûrs. Les techniques qui ont étés employées pour assurer la protection et la sécurité de ces informations sont: la cryptographie, la stéganographiei et le tatouage. Les recherches portent actuellement autant sur la mise au point de ces algorithmes, particulièrement les algorithmes de dissimulation et de les encadrer afin d'en accroître la sécurité. Dans cette thèse, nous avons abordé la problématique de la sécurité des images numériques, problème qui a pris de plus en plus d'importance depuis le développement d'Internet et de réseaux d'échange des supports multimédia, nous avons étudiés deux problématiques. Le premier problème concerne le tatouage numérique, qu'a été proposé comme une solution pour protéger la propriété des œuvres numériques et les droits d'auteurs. La deuxième méthode concerne la securisation de communication et les informations secrètes à travers un réseau non sécurisé, cette méthode concerne la steganographie, qui consiste à cacher un message dans un médium comme l'image.
Nos contributions dans ce domaine ont été les suivantes:

1. D'une façon précise notre première contribution a porté sur le développement d'une nouvelle technique de tatouage aveugle. Cette méthode est basée sur l'insertion de watermark dans le domaine transformé en utilisant une approche algébrique (la décomposition polaire). Les résultats expérimentaux ont permis de montrer que ce schéma maintient une haute qualité d'images tatouées et une robustesse contre plusieurs types d'attaques standards comme la compression JPEG, le filtrage, cropping, le bruit, . . . etc.

2. Dans la deuxième proposition, nous avons introduit un schéma de steganographie, qui permet de dissimuler une image secrète dans une autre, cette contribution est basée sur une technique algébrique (la décomposition polaire), nous nous sommes intéressés à la capacité d'insertion, l'invisibilité et la robustesse du schémas contre plusieurs types d'attaques conventionnels comme les attaques géométriques et les attaques d'effacement.

Bien que les techniques proposées soient assez efficaces, elles ne sont pas suffisantes pour réaliser une protection optimale. Cependant, Il existe plusieurs points qui peuvent être améliorés et développés ultérieurement. Nous allons essayer d'améliorer l'aspect progressif du schéma de tatouage pour obtenir un schéma résistant à différents types d'attaques. Nous allons utiliser le schéma hybride pour insérer la marque en combinant la transformation DWT et la décomposition polaire. Il reste aussi a étudier les nouvelles éventuelles attaques sur les méthodes proposées.

Bibliography

[1] C. Bergman and J. Davidson, "Unitary embedding for data hiding with the svd," in *Security, Steganography, and Watermarking of Multimedia Contents VII*, vol. 5681, pp. 619–631, International Society for Optics and Photonics, 2005.

[2] Y. J. Chanu, K. M. Singh, and T. Tuithung, "Steganography technique based on svd," *International Journal of Research in Engineering and Technology (IJRET)*, vol. 6, pp. 293–297, 2012.

[3] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges," *Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13541–13556, 2016.

[4] G. Swain and S. K. Lenka, "Steganography using two sided, three sided, and four sided side match methods," *CSI transactions on ICT*, vol. 1, no. 2, pp. 127–133, 2013.

[5] A.-G. T. Al-Tamimi and A. A. Alqobaty, "Image steganography using least significant bits (lsbs): A novel algorithm," *International Journal of Computer Science and Information Security*, vol. 13, no. 1, p. 1, 2015.

[6] O. M. Al-Shatanawi and N. N. El Emam, "A new image steganography algorithm based on mlsb method with random pixels selection," *International Journal of Network Security & Its Applications*, vol. 7, no. 2, p. 37, 2015.

[7] S. Bhattacharyya and G. Sanyal, "A robust image steganography using dwt difference modulation (dwtdm)," *International Journal of Computer Network and Information Security*, vol. 4, no. 7, p. 27, 2012.

[8] H. Sajedi and M. Jamzad, "Using contourlet transform and cover selection for secure steganography," 2001.

[9] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, no. 9-10, pp. 1613–1626, 2003.

[10] W. Luo, F. Huang, and J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme," *Multimedia tools and applications*, vol. 52, no. 2-3, pp. 407–430, 2011.

[11] C.-C. Chang, P.-Y. Pai, C.-M. Yeh, and Y.-K. Chan, "A high payload frequency-based reversible image hiding method," *Information Sciences*, vol. 180, no. 11, pp. 2286–2298, 2010.

[12] E. Ghasemi, J. Shanbehzadeh, and B. ZahirAzami, "A steganographic method based on integer wavelet transform and genetic algorithm," in *Communications and Signal Processing (ICCSP), 2011 International Conference on*, pp. 42–45, IEEE, 2011.

[13] M. N. Kumar and S. Srividya, "Genetic algorithm based color image steganogaphy using integer wavelet transform and optimal pixel adjustment process," *International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN*, vol. 3, pp. 2278–3075, 2013.

[14] R. El Safy, H. Zayed, and A. El Dessouki, "An adaptive steganographic technique based on integer wavelet transform," in *Networking and Media Convergence, 2009. ICNM 2009. International Conference on*, pp. 111–117, IEEE, 2009.

[15] N. Ghoshal and J. Mandal, "A steganographic scheme for colour image authentication (sscia)," in *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*, pp. 826–831, IEEE, 2011.

[16] S. Hemalatha, U. D. Acharya, A. Renuka, and P. R. Kamath, "A secure image steganography technique to hide multiple secret images," in *Computer Networks & Communications (NetCom)*, pp. 613–620, Springer, 2013.

[17] S. Delenda and L. Noui, "A new steganography algorithm using polar decomposition," *Information Security Journal: A Global Perspective*, vol. 27, no. 3, pp. 133–144, 2018.

[18] J. Nath and A. Nath, "Advanced steganography algorithm using encrypted secret message," *International journal of advanced computer science and applications*, vol. 2, no. 3, 2011.

[19] G. Wang, "Generic non-repudiation protocols supporting transparent off-line ttp," *Journal of Computer Security*, vol. 14, no. 5, pp. 441–467, 2006.

[20] J. Barbier, "La stéganographie moderne: d'hérodotea nos jours," *Computer & Electronics Security Application Rendez-vous, CESAR*, 2007.

[21] A. J. Marconi and M. Rodrigues, *Transfert securise d'images par combinaison de techniques de compression et cryptage*. PhD thesis, these de doctorat de l'universite de Montpellier II, 2006.

[22] A. ALI-PACHA, N. HADJ-SAID, A. BELGORAF, and A. M'HAMED, "Stéganographie: Sécurité par dissimulation," *RIST*, vol. 16, no. 1, 2006.

[23] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[24] R. Anderson, *Information Hiding: First International Workshop, Cambridge, UK, May 30-June 1, 1996. Proceedings*, vol. 1. Springer Science & Business Media, 1996.

[25] O. Medeni and M. Bouye, *Application des codes correcteurs d'erreurs en stéganographie*. Université Mohammed V-Agdal, Faculté des Sciences, Rabat, 2012.

[26] M. Barni, F. Bartolini, A. De Rosa, and A. Piva, "Capacity of the watermark channel: How many bits can be hidden within a digital image?," in *Security and Watermarking of Multimedia Contents*, vol. 3657, pp. 437–449, International Society for Optics and Photonics, 1999.

[27] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1079–1107, 1999.

[28] M. Kutter and S. Voloshynovskiy, "Alexander herrigel," *The Watermark Copy Attack: Security and Watermarking of Multimedia Content II*, vol. 3971, 2000.

[29] R. G. Van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark," in *Image Processing, 1994. Proceedings. ICIP-94., IEEE International Conference*, vol. 2, pp. 86–90, IEEE, 1994.

[30] S. Deslandes, "Initiation aux méthodes de traitement numérique des images satellites, sur le système pci inc," *EASUPACE. CARTEL*, 1990.

[31] J. Cummins, P. Diskin, S. Lau, and R. Parlett, "Steganography and digital watermarking," *School of Computer Science, The University of Birmingham*, vol. 14, p. 60, 2004.

[32] H. Bouziri, *Identification de cristaux dans un phoswich par la méthode de mesure de temps au dessus d'un seuil (ToT) pour le scanner LabPET II*. Université de Sherbrooke, 2014.

[33] S. Delenda and L. Noui, "A new algorithm for watermarking color images using the polar decomposition," in *International Conference on Coding and Cryptography ICCC 2015*, pp. 171–178, 2015.

[34] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple lsb substitution," *Pattern recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[35] A. K. Singh, M. Dave, and A. Mohan, "Hybrid technique for robust and imperceptible image watermarking in dwt–dct–svd domain," *National Academy Science Letters*, vol. 37, no. 4, pp. 351–358, 2014.

[36] B. Khaled, *Approche par marquage pour l'évaluation de la qualité d'image dans les applications multimédias*. PhD thesis, Université du Québec en Outaouais, 2012.

[37] S. Bothfeld, "Un trait peut en cacher un autre–gains and losses of individual autonomy in activating welfare reforms," in *Paper prepared ffor the international conference 'Activation policies on the fringes of society: a challenge for European Welfare States*, 2008.

[38] A. Ali-Pacha, N. Hadj-Said, A. Belgoraf, and A. M'HAMED, "Stéganographie: Sécurité par dissimulation," *Revue d'Information Scientifique et Technique*, vol. 16, no. 1, 2006.

[39] C. Baras, *Tatouage informé de signaux audio numériques*. PhD thesis, Télécom ParisTech, 2005.

[40] J. Pinel, L. Girin, and C. Baras, "Une technique de tatouage" haute-capacité" pour signaux musicaux au format cd-audio," in *10ème Congrès Français d'Acoustique*, 2010.

[41] M. Koubaa, *Tatouage robuste de vidéo basé sur la notion de régions d'intérêt*. PhD thesis, Bordeaux 1, 2010.

[42] J.-P. Allouche *et al.*, "Sur la complexité des suites infinies," *Bulletin of the Belgian Mathematical Society-Simon Stevin*, vol. 1, no. 2, pp. 133–143, 1994.

[43] P. Bolon, J.-M. Chassery, J.-P. Cocquerez, D. Demigny, C. Graffigne, A. Montanvert, S. Philipp, R. Zéboudj, J. Zerubia, and H. Maître, *Analyse d'images: filtrage et segmentation*. Masson, 1995.

[44] M. Ciuc, *Traitement d'images multicomposantes: application à l'imagerie couleur et radar*. PhD thesis, Université Savoie Mont Blanc, 2002.

[45] J. Martinet, *Un modèle vectoriel relationnel de recherche d'information adapté aux images*. PhD thesis, Université Joseph Fourier (Grenoble I), 2004.

[46] S. Raman, "Axe" génie des procédés", centre spin," *Ecole des Mines de Saint-Etienne*, pp. 6–7, 2008.

[47] J. Angulo and J. Serra, "2-traitements des images de couleur en représentation luminance/saturation/teinte par norme l1," 2004.

[48] W. F. Good, G. S. Maitz, and D. Gur, "Joint photographic experts group (jpeg) compatible data compression of mammograms," *Journal of digital imaging*, vol. 7, no. 3, p. 123, 1994.

[49] W. F. Good, G. S. Maitz, and D. Gur, "Joint photographic experts group (jpeg) compatible data compression of mammograms," *Journal of Digital Imaging*, vol. 7, no. 3, p. 123, 1994.

[50] R. H. Wiggins, H. C. Davidson, H. R. Harnsberger, J. R. Lauman, and P. A. Goede, "Image file formats: past, present, and future," *Radiographics*, vol. 21, no. 3, pp. 789–798, 2001.

[51] G. Roelofs and R. Koman, *PNG: the definitive guide*. O'Reilly & Associates, Inc., 1999.

[52] J. Müller and K. Müller, "Treegraph: automated drawing of complex tree figures using an extensible tree description format," *Molecular Ecology Notes*, vol. 4, no. 4, pp. 786–788, 2004.

[53] A. C. Team, *Adobe Illustrator CS6 Classroom in a Book*. Adobe Press, 2012.

[54] A. Quint, "Scalable vector graphics," *IEEE MultiMedia*, vol. 10, no. 3, pp. 99–102, 2003.

[55] G. Allaire and S. M. Kaber, *Algebre linéaire numérique*, vol. 512. Ellipses, 2002.

[56] J. Mars, *Traitement du signal pour géologues et géophysiciens*, vol. 3. Editions Technip, 2004.

[57] N. J. Higham and V. Noferini, "An algorithm to compute the polar decomposition of a 3 3 matrix," *Numerical Algorithms*, vol. 73, no. 2, pp. 349–369, 2016.

[58] R. Bhatia, *Positive definite matrices*, vol. 24. Princeton university press, 2009.

[59] C. Rey and J.-L. Dugelay, "A survey of watermarking algorithms for image authentication," *EURASIP Journal on applied signal processing*, vol. 2002, no. 1, pp. 613–621, 2002.

[60] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE transactions on image processing*, vol. 13, no. 4, pp. 600–612, 2004.

[61] P. Das, S. C. Kushwaha, and M. Chakraborty, "Multiple embedding secret key image steganography using lsb substitution and arnold transform," in *Electronics and Communication Systems (ICECS), 2015 2nd International Conference on*, pp. 845–849, IEEE, 2015.

[62] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple lsb substitution," *Pattern recognition*, vol. 37, no. 3, pp. 469–474, 2004.

[63] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color image steganography based on pixel value modification method using modulus function," *IERI Procedia*, vol. 4, pp. 17–24, 2013.

[64] A. Nag, S. Biswas, D. Sarkar, and P. P. Sarkar, "A novel technique for image steganography based on block-dct and huffman encoding," *arXiv preprint arXiv:1006.1186*, 2010.

[65] K. Wong, X. Qi, and K. Tanaka, "A dct-based mod4 steganographic method," *Signal Processing*, vol. 87, no. 6, pp. 1251–1263, 2007.

[66] R. Chu, X. You, X. Kong, and X. Ba, "A dct-based image steganographic method resisting statistical attacks," in *Acoustics, Speech, and Signal Processing, 2004. Proceedings.(ICASSP'04). IEEE International Conference on*, vol. 5, pp. V–953, IEEE, 2004.

[67] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel dwt based image securing method using steganography," *Procedia Computer Science*, vol. 46, pp. 612–618, 2015.

[68] M. Tolba, M. Ghonemy, I. Taha, and A. Khalifa, "Using integer wavelet transforms in colored image steganography," *International Journal on Intelligent Cooperative Information Systems*, vol. 4, no. 2, pp. 230–235, 2004.

[69] S. U. Maheswari and D. J. Hemanth, "Data hiding in gray scale images using integer wavelet transform," in *Information Communication and Embedded Systems (ICICES), 2014 International Conference on*, pp. 1–5, IEEE, 2014.

[70] V. I. Gorodetski, L. J. Popyack, V. Samoilov, and V. A. Skormin, "Svd-based approach to transparent embedding data into digital images," in *International Workshop on Mathematical Methods, Models, and Architectures for Network Security*, pp. 263–274, Springer, 2001.

[71] Y. J. Chanu, K. M. Singh, and T. Tuithung, "A robust steganographic method based on singular value decomposition," *Int. J. Inf. Comput. Technol*, vol. 4, no. 7, pp. 717–726, 2014.

[72] K.-L. Chung, C.-H. Shen, and L.-C. Chang, "A novel svd-and vq-based image hiding scheme," *Pattern Recognition Letters*, vol. 22, no. 9, pp. 1051–1058, 2001.

[73] K. Raja, S. Sindhu, T. Mahalakshmi, S. Akshatha, B. Nithin, M. Sarvajith, K. Venugopal, and L. M. Patnaik, "Robust image adaptive steganography using integer wavelets," in *Communication Systems Software and Middleware and Workshops, 2008. COMSWARE 2008. 3rd International Conference on*, pp. 614–621, IEEE, 2008.

[74] M. Kansal, G. Singh, and B. Kranthi, "Dwt, dct and svd based digital image watermarking," in *Computing Sciences (ICCS), 2012 International Conference on*, pp. 77–81, IEEE, 2012.

[75] M. S. Subhedar and V. H. Mankar, "High capacity image steganography based on discrete wavelet transform and singular value decomposition," in *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies*, p. 63, ACM, 2014.

[76] Q. Su, Y. Niu, G. Wang, S. Jia, and J. Yue, "Color image blind watermarking scheme based on qr decomposition," *Signal Processing*, vol. 94, pp. 219–235, 2014.

[77] J. Mandal and M. Sengupta, "Steganographic technique based on minimum deviation of fidelity (stmdf)," in *Emerging Applications of Information Technology (EAIT), 2011 Second International Conference on*, pp. 298–301, IEEE, 2011.

[78] Y.-H. Yu, C.-C. Chang, and I.-C. Lin, "A new steganographic method for color and grayscale image hiding," *Computer Vision and Image Understanding*, vol. 107, no. 3, pp. 183–194, 2007.

[79] J. Panda, J. Bisht, R. Kapoor, and A. Bhattacharyya, "Digital image watermarking in integer wavelet domain using hybrid technique," in *Advances in Computer Engineering (ACE), 2010 International Conference on*, pp. 163–167, IEEE, 2010.

[80] P. Bas, "Analyse stéganographique d'images numériques: Comparaison de différentes méthodes," *Rapport de stage, Laboratoire des Images et des Signaux, University of Joseph Fourier, 23rd June*, 2003.

[81] M.-S. Hwang, C.-C. Chang, and K.-F. Hwang, "A watermarking technique based on one-way hash functions," *IEEE Transactions on Consumer Electronics*, vol. 45, no. 2, pp. 286–294, 1999.

[82] C.-C. Chang, K.-F. Hwang, and M.-S. Hwang, "Digital watermarking scheme using human visual effects," *Informatica(Ljubljana)*, vol. 24, no. 4, pp. 505–511, 2000.

[83] C. Temi, S. Choomchuay, and A. Lasakul, "A robust image watermarking using multiresolution analysis of wavelet," in *Communications and Information Technology, 2005. ISCIT 2005. IEEE International Symposium on*, vol. 1, pp. 623–626, IEEE, 2005.

[84] Z.-M. Lu and X.-W. Liao, "Counterfeiting attacks on two robust watermarking schemes," *International Journal of Innovative Computing, Information and Control*, vol. 2, no. 4, pp. 841–848, 2006.

[85] P. Meerwald and A. Uhl, "Survey of wavelet-domain watermarking algorithms," in *Security and Watermarking of Multimedia Contents III*, vol. 4314, pp. 505–517, International Society for Optics and Photonics, 2001.

[86] D. Kundur and D. Hatzinakos, "Toward robust logo watermarking using multiresolution image fusion principles," *IEEE Transactions on Multimedia*, vol. 6, no. 1, pp. 185–198, 2004.

[87] G. Bhatnagar and B. Raman, "A new robust reference watermarking scheme based on dwt-svd," *Computer Standards & Interfaces*, vol. 31, no. 5, pp. 1002–1013, 2009.

[88] L. Quan and A. Qingsong, "A combination of dct-based and svd-based watermarking scheme," in *Signal Processing, 2004. Proceedings. ICSP'04. 2004 7th International Conference on*, vol. 1, pp. 873–876, IEEE, 2004.

[89] V. Santhi and A. Thangavelu, "Dwt-svd combined full band robust watermarking technique for color images in yuv color space," *International Journal of Computer Theory and Engineering*, vol. 1, no. 4, p. 424, 2009.

[90] M. Cedillo-Hernández, F. García-Ugalde, M. Nakano-Miyatake, and H. M. Pérez-Meana, "Robust hybrid color image watermarking method based on dft domain and 2d histogram modification," *Signal, Image and Video Processing*, vol. 8, no. 1, pp. 49–63, 2014.

[91] A. K. Singh, B. Kumar, M. Dave, and A. Mohan, "Multiple watermarking on medical images using selective discrete wavelet transform coefficients," *Journal of Medical Imaging and Health Informatics*, vol. 5, no. 3, pp. 607–614, 2015.

[92] S. Atawneh, A. Almomani, H. Al Bazar, P. Sumari, and B. Gupta, "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in dwt domain," *Multimedia tools and applications*, vol. 76, no. 18, pp. 18451–18472, 2017.

[93] M. Ali, C. W. Ahn, and M. Pant, "A robust image watermarking technique using svd and differential evolution in dct domain," *Optik-International Journal for Light and Electron Optics*, vol. 125, no. 1, pp. 428–434, 2014.

[94] M. S. Goli and A. Naghsh, "A comparative study of image-in-image steganography using three methods of least significant bit, discrete wavelet transform and singular value decomposition," *Bulletin de la Société Royale des Sciences de Liège*, vol. 85, pp. 1465–1474, 2016.