République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique

Université Larbi Tébessi - Tébessa
Faculté des Sciences Exactes et des Sciences de la Nature et de la vie

Département : Mathématiques et informatique

MEMOIRE DE MASTER

Domaine : Mathématiques et informatique

Filière : Informatique

Option : Système d'information

Thème

Stéganographie : Technique d'insertion robuste et imperceptible adaptée aux images numériques

Présenté par

Salmi Ismahane

Devant le jury

Menassel Rafik	MCA	Université de Tébessa	Président
Zeggari Ahmed	MCB	Université de Tébessa	Examinateur
Laimeche Lakhdar	MCA	Université de Tébessa	Encadreur
Meraoumia Abdallah	MCA	Université de Tébessa	Co- Encadreur

Date de soutenance : 2020 - 2021

Note : Mention :

Remerciement

***J**e tiens d'abord à remercier Dieu le tout puissant pour me munir de la volonté, la santé et de la patience pour accomplir ce travail.*

***J**'exprime mes sincères remerciements et toute ma gratitude à mon encadreur Professeur **Laimeche Lakhdar** pour son excellente qualité d'encadrement : sa disponibilité, ses conseils précieux, et pour toutes les notions de base qu'il m'a appris tout au long de ces mois que ce soit dans le domaine informatique, que je les considère comme un baguage utile pour la poursuite dans la recherche scientifique. Un vif merci à mon co-directeur de mémoire Professeur **Meraoumia Abdallah** pour son aide, ses qualités pédagogiques, et scientifiques et humaines, qui ont contribué à l'aboutissement de cette mémoire.*

***J**e remercie vivement les honorables membres du jury qui ont accepté d'évaluer ce travail. Je remercie Professeur Menassel Rafik qui a bien voulu présider le jury. Je remercie également l'examinateur : Professeur Zeggari Ahmed.*

***J**'adresse mes sincères remerciements et mon profond respect aux Professeurs : Kamel Akrout , Salima Bourougaa, Menassel.R, Haouam.Y, Amroune, Gattal.A, Laoauar.M, Bendjenna.H, Hamidane.F, Djeddi Chaouki et Hafdallah Abd-El-Kader pour ses conseils, ses encouragements. Ses bonnes humeurs m'ont donné la force pour donner plus aux moments difficiles.*

***J**e voudrais souligner l'appui reçu de mon mari qui m'a soutenu et m'a encouragé tout au long de mes années d'études.*

***E**n terminant, **J**e remercie tous ceux qui m'ont aidé de près ou de loin à terminer ce mémoire*

Dédicaces

À *l'esprit de* ***ma mère****, qui me poussait à la réussite et à emmener avec moi le chemin des difficultés avec fermeté et détermination. C'est une réussite incomplète sans toi.*

À *la personne la plus gentille que j'ai connue dans ce monde qui n'a jamais cessé de me soutenir par tout ce qu'il a, qui m'a appris toutes les valeurs nobles de la vie.*

Mon mari

À ***mon père****, qui grâce à ses prières, j'ai pu résister et continuer*

À *ma chose la plus chère au monde, mes filles :*

Alaa, Aridj et Assil

À *mon petit ange, mon fils :*

Ayoub

À *toutes mes amies , sœurs et frères*

A *toute personne qui a contribué de loin ou du pré dans l'aboutissement de ce travail*

J*e dédié ce travail.*

Résumé

Dans notre vie moderne, les personnes et les institutions choisissent toujours l'Internet comme le moyen de communication le plus rapide. Comme ces entités adoptent un moyen de communication plus rapide et efficace, des techniques de sécurité de l'information comme la stéganographie et la cryptographie deviennent des outils puissants et nécessaires pour mener des communications sécurisées et confidentielles. Actuellement, plusieurs techniques de stéganographie ont été développées, l'insertion dans les bits de poids faibles (LSB) est l'une de ces techniques stéganographique le plus populaire dans le domaine spatial. En effet, comme toute autre technique existante, la sélection des positions pour l'insertion de données dans un support de couverture dépend principalement d'un générateur de nombres pseudo-aléatoires sans considérer la relation entre les LSBs du support de couverture et les données insérées. Dans ce travail, pour avoir les meilleures positions des pixels dans lesquelles la distorsion visuelle de stego image soit minimum, ainsi que le taux de changements devient optimum, nous proposons deux nouveaux schémas stéganographique basées sur le schéma d'insertion LSB. Nos nouveaux travaux visent à améliorer l'efficacité d'insertion, c'est-à-dire sélectionner les valeurs de pixels de l'image de couverture appropriées qui optimisent le taux des changements et la distorsion visuelle.

Mots clés : Sécurité de l'information, Stéganographie, Remplacement 1LSB, Remplacement 2LSB.

Abstract

In our modern life, persons and institutions alike are rapidly embracing the shift toward communication via the Internet. As these entities adopt a faster and efficient communication protocol, information security techniques such as steganography and cryptography become powerful and necessary tools for conducting secure and secrecy communications. Currently, several steganography techniques have been developed, and the least significant bit (LSB) is one of these techniques which are a popular type of steganographic algorithms in the spatial domain. Indeed, as any other existing techniques, the selection of positions for data embedding within a cover signal mainly depends on a pseudorandom number generator without considering the relationship between the LSBs of the cover signal and the embedded data. In this thesis and for best pixels' positions adjustment, in which the visual distortion of the stego-image, as well as the embedding changes, becomes optimum, we propose two new position selection schemes of LSBs-based steganography. Our new works are proposed to improve the embedding efficiency, that is to say, select the suitable cover image pixels' values that optimize the expected number of modifications per pixel and the visual distortion.

Keywords words: Information security, Steganography, 1LSB replacement, 2LSB replacement.

ملخـص

في حياتنا الحديثة، يتبنى الأشخاص والمؤسسات على حد سواء التحول بسرعة نحو الاتصال عن طريق الإنترنت. في مثل هذه الحالات، تقنيات أمن المعلومات مثل إخفاء المعلومات والتشفير تصبح أدوات قوية وضرورية لإجراء اتصالات آمنة وسرية.

حاليا، تم تطوير العديد من تقنيات إخفاء المعلومات خصوصا منها التي تعتمد على تقنية البت الأقل أهمية (LSB) في المجال المكاني والتي تعتبر من أكثر التقنيات الشائعة في عالم إخفاء المعلومات. في الواقع، مثل أي تقنيات أخرى موجودة، اختيار المواضع الخاصة بإخفاء المعلومات داخل الصور تعتمد بشكل أساسي على مولد رقمي شبه عشوائي دون النظر إلى العلاقة بين قيم البت الأقل أهمية LSBs وقيم المعلومة المراد إخفائها.

في هذه المذكرة من اجل اختيار أفضل لمواقع الإخفاء والتي من خلالها تصبح الصورة الحاملة للمعلومة قليلة التشويه وتكون نسبة التغييرات على النحو الأمثل، نقترح سيناريوهين جديدين لاختيار المواقع المناسبة لإخفاء المعلومات.

كلمات مفتاحية : أمن المعلومات، إخفاء المعلومات، استبدال 1LSB , استبدال 2LSB

Table des matières

Chapitre 1 : Confidentialité des communications et la stéganographie

Chapitre 3 : Méthode proposée & Résultats expérimentaux

Liste des figures

Liste des Tableaux

Abréviations

La signification d'une abréviation ou d'un acronyme n'est souvent indiqué que lorsqu'elle apparaît pour la première fois dans le texte. Dans la plupart des cas, il existe une abréviation en français et une abréviation en anglais. Les deux sont indiqués en premier, puis l'abréviation la plus usuelle est utilisée, qui est le plus souvent l'abréviation en anglais.

Acronymes & Abréviations :

BMP Bit Map

DCT Discrete Cosine Transform

DWT Discrete Wavelet Transform

JPEG Joint Photographie Expert Group

LSB Least Significant Bit

RVB Red, Green, Blue / Rouge, Vert, Bleu

TIFF Tagged Image File Format

Introduction Générale

La stéganographie a trouvé des vastes applications dans les communications secrètes, ce qui en fait une technologie attrayante pour compléter les processus cryptographiques dans le domaine de la sécurité de l'information en intégrant des données secrètes dans les supports de couvertures [3]. Pour sa part, la stéganalyse vise à révéler la présence de messages cachés dans un support donné et, si possible, à récupérer des messages secrets. Il s'agit d'une question importante utilisée par les autorités pour détecter les faits de stéganographie par les criminels et les terroristes. Il peut également être utilisé pour mesurer la performance de sécurité des techniques de stéganographie [4]. Une méthodologie de stéganographie doit être robuste et ne pas altérer les statistiques pour remplir les conditions nécessaires à une excellente protection contre la stéganalyse. Cette condition peut être mieux vérifiée si le message secret est placé dans des parties significatives du support de couverture pour minimiser la distorsion dans laquelle l'existence d'un message caché est difficile à détecter.

En effet, la distorsion du signal, qui représente la capacité d'éviter la détection par l'œil humain, peut être mesurée par des mesures subjectives ou objectives. Pour les images, la mesure subjective la plus couramment utilisée pour comparer les images de couverture et les images stéganographiées est le système visuel humain (HVS), qui vise à identifier la distorsion apparente à l'œil nu des stégo images [5]. En général, en utilisant cette mesure, la plupart des méthodes de stéganographie fournissent des stégo images qui ne peuvent pas être distinguées des images de couverture. Contrairement à la mesure subjective, la mesure objective utilise la différence entre les images de couverture et les stégo images pour calculer le degré de similitude entre eux. Sur la base de cette similitude, de nombreuses mesures peuvent être calculées pour évaluer la distorsion dans les stégo images. En règle générale, la mesure de distorsion la plus répandue est le rapport signal/bruit (PSNR) [6]. Une technique de stéganographie est considérée comme adéquate lorsqu'elle donne des stégo images avec des valeurs PSNR plus élevées (haute qualité). En particulier dans les méthodes de stéganographie, une autre mesure, le nombre de modifications de LSBs (EC pour Embedding change) [7], peut être utilisé.

Cette métrique calcule le nombre de bits modifiés dans l'image de couverture pendant la phase d'insertion du message secret. Dans ce cas, une technique de stéganographie est considérée comme adéquate lorsqu'elle donne un taux de changement plus petit.

Dans la littérature, différentes techniques de stéganographie ont été proposées. La méthode la plus utilisée et la plus simple est la technique des bits de poids faible (LSB pour Least Significant Bit) [8]. Le principe de cette technique consiste à insérer des données dans une image de couverture en remplaçant les bits de poids faibles de l'image de couverture par des bits de message secrets. Pour atteindre une capacité de dissimulation plus élevée et une sécurité accrue, de nombreuses méthodes de stéganographie ont été proposées connues par MLSB ($M \geq 2$, où M est le nombre de bits de poids faibles dans lesquels le message secret est inséré). Dans ces techniques, la phase de sélection des positions de pixels dans lesquels les données sont cachées dépend principalement d'un générateur de nombres pseudo aléatoire (PRNG), ce qui signifie que les pixels modifiés seront toujours sélectionnés indépendamment des messages secrets [9]. Il est observé dans [10] que les zones homogènes dans les images sont inévitablement modifiées après la dissimulation des données.

Dans ce manuscrit et pour remédier les faiblesses des techniques basées sur le schéma d'insertion LSB, nous proposons de nouveaux schémas pour sélectionner les positions appropriées pour cacher un message secret. Les scénarios proposés visent à améliorer la qualité de stégo image (plus grande PSNR) avec la possibilité d'augmenter la capacité d'insertion autant que possible en réduisant le taux de changement dans les bits de poids faibles (plus petit EC). Dans nos schémas, nous essayons de diviser les pixels sélectionnés pour l'insertion à des groupe dont les bits de poids faibles corresponds aux bits de flux de données.

Nous allons essayer d'atteindre notre objectif à travers trois chapitres :

Dans le premier chapitre, nous allons présenter les concepts généraux sur la stéganographie à savoir la stéganographie dans l'histoire et d'aujourd'hui, l'architecture générale d'un système stéganographique, et les différentes contraintes pour son développement. Les différentes technologies de protection de l'information ainsi qu'une comparaison entre la stéganographie et ces technologies sont présentés.

Dans le deuxième chapitre, nous allons présenter le principe des schémas d'insertion dans les bits de poids faibles (LSB) dans le domaine spatial. Ensuite, un état de l'art sur les différentes techniques de stéganographie basées sur le schéma d'insertion LSB est présenté.

Dans le dernier chapitre, nous présentons deux schémas d'insertion dans le domaine spatial et fréquentiel. Dans une première étape, les deux schémas proposés sont détaillés. Ensuite, les performances de ces schémas d'insertion sont présentées.

L'originalité de nos schémas stéganographiques réside dans l'amélioration la qualité de stégo image (plus grande PSNR) avec la possibilité d'augmenter la capacité d'insertion autant que possible en réduisant le taux de changement dans les bits de poids faibles (plus petit EC).

Chapitre 1

Confidentialité des communications et la stéganographie

1.1. Introduction

Les progrès technologiques dans les technologies de l'information et des télécommunications ont contribué à soulever une multitude de problèmes liés à la protection (sécurité) de l'information, permettant ainsi un développement scientifique et technique approfondi en réponse aux défis soulevés. Parmi les questions posées, nous citons : les virus informatiques, l'autorisation d'accès, la protection des droits d'auteur et la vérification de l'intégrité des données. A cela, il est possible d'ajouter des problèmes tels que l'authentification, l'accès conditionnel, le tatouage numérique, la signature numérique, la communication secrète et la stéganographie. La stéganographie peut être définie comme l'art et la science de cacher des informations. Ainsi, contrairement à la cryptographie, dont le but est de masquer le contenu d'un message, la stéganographie tente de masquer la présence même de ce message.

Dans ce chapitre nous allons présenter les notions de base de la stéganographie, la stéganographie dans l'histoire ainsi qu'aujourd'hui. Ensuite, nous allons présenter l'architecture d'un système stéganographique ainsi que les différentes phases de son fonctionnement. Nous terminerons ce chapitre par une comparaison entre la stéganographie et les différentes techniques de dissimulation de l'information en l'occurrence du tatouage numérique, le filigrane et la cryptographie.

1.2. Terminologie

Dans la suite de ce mémoire, nous conservons la terminologie définit si dessous, afin de distinguer les différents éléments qui interviennent en stéganographie [1].

- **Cover-médium** : ou bien le medium de couverture, il s'agit d'un support numérique dans lequel seront dissimulées les informations. Il peut s'agir d'un texte, d'une image, d'un son, d'un vidéo, etc.
- **Stégo-médium :** une fois les informations dissimulées, le cover-medium devient un stégo-medium.
- **Données :** ce sont les informations qui vont être cachées dans le médium de couverture. Il peut s'agir d'un message, une marque ou une empreinte.
- **Stégo-clé :** c'est une information secrète additive, mais essentielle dans tout le processus de stéganographie.

1.3. Définition de la stéganographie

La stéganographie (en anglais : stéganographie ou masquage de données) est encore une technique peu connue du grand public : pour preuve, aucun dictionnaire ne lui consacre une entrée (notez d'ailleurs qu'il ne faut pas confondre sténographie et stéganographie). En fait, le mot stéganographie (en anglais : steganography ou data hiding) provient d'une étymologie grecque: stéganos qui signifie cachée, couvert et graphos qui signifie écriture, dessin. Nous pouvons donc en déduire que la stéganographie est l'art de cacher des messages secrets dans des messages plus anodins [2].

1.4. Objectifs de la stéganographie

Le but de la stéganographie est de cacher un message sans attirer l'attention humaine, avec la stéganographie informatisée, vous devez également faire attention à ne pas attirer l'attention des logiciels d'analyse. Car si l'on soupçonne qu'une image contient un message stéganographié, on peut toujours la soumettre à un logiciel en charge de traquer tout bruit de fond excessivement organisé et statistiquement non aléatoire : on peut donc facilement identifier un message stéganographié et réaliser une stéganalyse (tentative de récupération du message). Le message à masquer doit donc être comparable en tous points à une suite de bits aléatoires : pour cette raison, il n'y a qu'une seule solution : le message doit d'abord être chiffré.

Le but de la stéganographie est de cacher l'existence même du message secret en le réalisant pas détectable. Plus la capacité d'insertion est élevée, plus le risque de détectabilité est grand. En stéganographie d'image, nous essaierons donc de maintenir un certain compromis entre « capacité d'insertion » et « indétectable », afin de construire un schéma de stéganographie ε-sûr avec un ε suffisamment petit. De plus, en stéganographie de garde passive, on considère que si le message secret est altéré lors de la transmission, il sera retransmis. L'objectif est donc de transmettre le plus d'informations secrètes possible sans éveiller les soupçons.

1.5. Stéganographie dans l'histoire

La stéganographie à une très longue histoire qui remonte à la Grèce Antique. Herodotus, auteur grec, raconte les communications secrètes entre deux chefs de guerre qui utilisaient des esclaves pour transmettre un message afin d'organiser une révolte contre les Perses. Afin d'assurer le transfert des messages secrets ou plans de batailles sans aucune suspicion des adversaires, les cheveux d'un esclave de confiance ont étaient rasés pour tatouer le message sur son crâne. Une fois que ses cheveux avaient repoussés le message devenait invisible et l'esclave pouvait être envoyé avec l'ordre de se faire raser le crâne une fois arrivé à destination [1].

Une autre technique était utilisée afin de prévenir les Grecs d'une invasion du roi Xerxès de Perse en envoyant un message gravé dans le bois d'une tablette d'écriture recouverte de cire, d'apparence vierge (voir figure 1.1). Les Grecs vont mettre en place plusieurs mécanismes dédiés à la stéganographie. Des trous sur un disque représentant des lettres, des fils de couleurs différentes, permettaient de lire un message secret [2].

Fig.1.1 : Tablette contenant un message caché gravé sur le bois sous la cire [2].

Une méthode de stéganographie fut inventée par Gaspar Schott (1608-1666). Le principe est de coder un message secret selon des notes de musique. Autrement dit, associer une lettre à une note musicale (voir figure 1.2). L'avantage de ce procédé est que le message apparaissait comme une partition musicale, et donc passait totalement inaperçu [3].

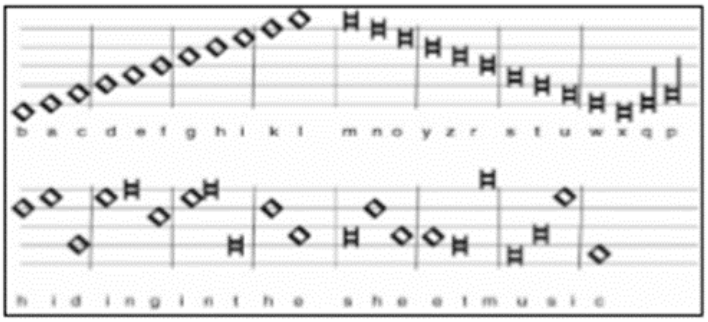

Fig.1.2 : Correspondance entre les lettres de l'alphabet et notes musicales [3].

Au 17ème siècle, Sir John Trevanion fut arrêté et emprisonné dans un château. Il reçut une lettre, que les gardiens avaient jugée sans danger. Lorsque John lut celle-ci, il détecta la présence suspecte de certaines virgules étrangement placées. Il repéra également qu'en prenant la troisième lettre de chaque mot suivant ces virgules, il pouvait former la phrase « Panel at East of Chapel slides » ce qui signifiait « Le panneau à l'extrémité Est de la chapelle peut glisser ». C'est ainsi qu'il demanda un instant de recueillement dans la chapelle et s'évada [3].

Une autre forme stéganographique était connue par le sémagramme qui consiste à transmettre les messages secrètes dans les initiales de chaque vers de poème, mot placé dans des vers ou utilisation de la ponctuation (points, hauteur de lettres et virgules). Alfred de Musset est l'utilisateur le plus connu de ce procédé puisqu'il a entretenu une relation secrète avec Georges Sand (entre 1833 et 1834) au travers de poème qu'il lui envoyait.

Dans les années 1940, la stéganographie a été très souvent employée et s'est ouverte à un grand nombre de formes. Durant la seconde guerre mondiale, plusieurs techniques de stéganographie ont été utilisées. L'encre invisible est la technique stéganographique la plus connue avec laquelle les messages secrets sont écrits sur un papier et qui apparaissent lorsque le papier est approché d'une source de chaleur (voir figure 1.3) [3].

Avec le développement des produits chimiques, par la suite des encres invisibles ont été développé pour communiquer des messages en toute sécurité comme le chlorate de soude ; l'écriture apparaît en passant sur l'encre sèche une petite éponge trempée dans une solution de vitriol de cuivre.

Fig.1.3 : Stéganographie par l'encre invisible [3].

Pendant la seconde guerre mondiale, un procédé de stéganographie a été réalisé par les agents allemands en Angleterre qui envoyaient des pulls en Allemagne contenant des nœuds dans la laine. Les tricots étaient démaillés à leur arrivée. Sur un mur sur lequel se trouvait l'alphabet sous la forme d'une règle, ils posaient l'extrémité du fil à un point et regardait la position du nœud. Grâce à l'emplacement du nœud sur la règle, ils retrouvaient petit à petit le message caché.

Dans les années 1980, Margaret Thatcher, premier ministre britannique a demandé de faire modifier le logiciel de traitement de texte utilisé par les membres du gouvernement afin de dissimuler dans les espaces séparant les mots l'identité de la personne utilisant le traitement de texte [2].

Dans les années 1990, les fabricants d'imprimantes HP et Xerox ont utilisé la stéganographie afin de tracer la falsification de dollar américain. Pour ce faire, de petits points jaunes sont ajoutés au cours de la phase d'impression dans chaque page (voir figure 1.4). Ces points qui sont visible sous la lumière bleue ou avec une loupe peuvent servir à identifier l'imprimante qui a été utilisée (le numéro de série, l'heure d'impression, la marque et le modèle de l'imprimante) (https://w2.eff.org/Privacy/printers/docucolor/).

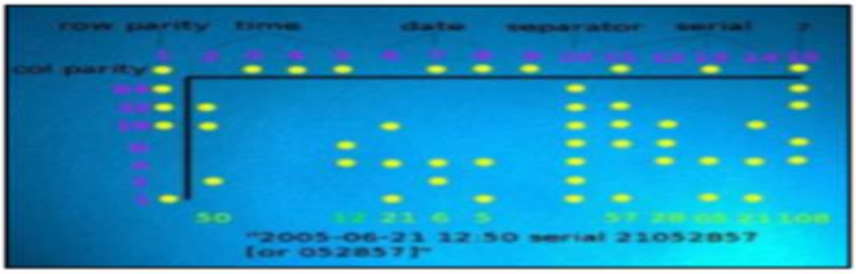

Fig.1.4 : Ajoute des points jaunes par les imprimantes HP.

En 1997, une technique de stéganographie connue par les micros points a été utilisée afin de tracer la falsification des billets suisse.

Cette technique consiste à réduire un texte ou une image en un point d'un millimètre ou moins. Celui-ci est ensuite disposé dans un texte ou une image normale (voir figure 1.5) [3].

Fig.1.5 : Stéganographie dans les billets suisses par la méthode des micros points [3].

De nombreux spécialistes relayés par les médias avancent l'hypothèse selon laquelle Ben Laden aurait coordonné les attentats du 11 septembre 2001 en utilisant des messages cachés dans des images de sites à caractères mauvais.

La stéganographie a été aussi utilisé dans les petites annonces des journaux pour transmettre des messages. On peut citer par exemple, en 2004 un mystérieux groupe terroriste, appelé AZF, qui menaçait de faire sauter des voies ferrées si une rançon ne leur était pas payée. Pour dialoguer avec les autorités, ce groupe exigeait l'utilisation de la rubrique "Messages personnels" de Libération, Cinq messages à « AZF » ont été passés par la police dans Libération [4].

1.6. Stéganographie aujourd'hui

La stéganographie de nos jours Contrairement à la stéganographie ancienne, la stéganographie moderne, ou numérique, est une science jeune, qui date seulement d'une quinzaine d'années. La stéganographie moderne passe par l'utilisation des supports numériques pour la transmission de données secrètes. L'essor d'Internet, et le développement des échanges électroniques via les réseaux sociaux a rendu très simple la dissimulation de messages secrets dans des supports comme : les fichiers audio le texte, les images, les vidéos, les programmes, les sites internet. Les fichiers multimédias représentent des supports privilégiés pour l'échange de données.

La stéganographie numérique constitue un excellent moyen pour la communication secrète. Elle est, en effet, très adaptée pour la dissimulation de données confidentielles. Dans certains pays non démocratiques où la liberté d'expression est réprimée, la stéganographie représente un excellent moyen pour communiquer librement dans des conditions de censure ou de surveillance. Aujourd'hui les messages secrets se transmettent de manière numérique avec des méthodologies plus rigoureuses. De nombreuses méthodes d'insertion sont apparues, ainsi qu'une meilleure formalisation de la stéganographie [5].

La stéganographie moderne est potentiellement applicable à différents supports numériques : fichiers audio, vidéos, textes, ...etc. Parmi les fichiers qui sont très adaptés pour la dissimulation d'information, on retrouve également les images numériques. Ce type de fichier étant très couramment échangé sur Internet, une grande majorité des travaux de recherches lui sont consacrés. Dans le cas d'une image en niveaux de gris, les échantillons sont des pixels, avec I = {0, ...,255}, et forment une matrice de taille n = n1 ×n2. Dans le cas d'une image en couleur,
nous avons I = {0, ...,255} ^{3} codé généralement avec trois canaux de couleurs : rouge, vert et bleu. Les travaux présentés dans ce document considèrent uniquement les images numériques en niveau de gris, c'est à dire celles codées uniquement sur un seul canal [6].

1.7. Type des supports utilisés dans la stéganographie

La stéganographie technique regroupe toutes les techniques qui ne jouent pas sur les mots. La stéganographie technique est intéressante car elle permet de dissimuler des données dans plusieurs types de médias.

1.7.1. Fichier image

Ce support de stéganographie est le plus populaire en ces dernières années par rapport à d'autres types de support de stéganographie, à cause de l'inondation des informations d'images électroniques disponibles avec l'avènement de l'appareil photo numérique et la distribution d'Internet en haute vitesse. Ça peut impliquer la dissimulation d'informations dans le bruit produit naturellement dans l'image. La plupart des types d'informations contiennent ce genre de bruit. Le bruit fait référence aux imperfections inhérentes au processus de rendu d'une image analogique en tant qu'image numérique. Dans la stéganographie de l'image, nous pouvons cacher le message en pixels d'une image [7].

1.7.2. Fichier audio

La stéganographie dans un fichier audio, consiste à dissimuler des messages dans le bruit (audio), ou dans les fréquences que les être humain ne peuvent pas entendre, c'est un autre domaine de dissimulation de données et d'informations qui repose sur l'utilisation d'une source existante comme un espace dans lequel cacher l'information. La stéganographie audio peut être problématique et peut être utile pour transmettre des données secrètes dans un signal audio de couverture inoffensif [8].

Afin de transmettre de l'information de manière cachée dans du son, différentes techniques existent et se basent sur le fait qu'un son affecte la perception d'un autre :

- Un son plus fort peut en cacher un autre,
- Un son peut être caché temporairement lorsqu'il est moins fort et qu'il est placé avant ou après un son plus fort.

Il est également possible de cacher des données en utilisant la représentation des notes. Prenons comme exemple un livre de Gaspar Schott, Schola Steganographica, où l'auteur explique que des messages ont été cachés dans de la musique, de sorte qu'une note correspondante à une lettre. J.S Bach, lui, utilisait le nombre d'occurrences de notes qui apparaissait. John Wilkin a même démontré que deux musiciens discutaient au travers de leur musique comme si leurs instruments parlaient.

1.7.3. Fichier vidéo

Les techniques sont équivalentes à celles utilisées dans les images. Cependant les vidéos sont souvent plus bruitées ce qui facilite l'imperceptibilité des données dissimulées mais les rend aussi moins robustes [8].

1.7.4. Fichier HTML

Certains logiciels de stéganographie proposent de cacher des messages dans des pages HTML : ils ne font que toucher la source pour camoufler le fichier secret en insérant des espaces entre balises, variant minuscules et majuscules dans les balises, ... Astucieux mais cela peut toutefois se détecter par analyse statistique et même par un coup d'œil à la source dont l'indentation exotique pourra attirer l'attention [8].

1.7.5. Systèmes de fichiers

Pour stocker un fichier, le système découpe ce dernier en un nombre de morceaux pour que chaque morceau puisse être logé dans un bloc. Comme la taille d'un fichier a rarement une taille multiple de la taille des blocs, généralement le dernier bloc ne sera pas rempli. Pour cacher des données, il suffit de les stocker dans ce dernier bloc ; si la taille de ces données dépasse l'espace du bloc non rempli, il faut les découper et les stockées sur autant de blocs nécessaires, garder la trace des blocs utilisés et l'ordre pour la récupération. Le problème de cette technique vient du fait que les fichiers peuvent être modifiés, supprimés, déplacés, etc. [8].

1.7.6. Fichier exécutable

Les fichiers exécutables peuvent être utilisés pour transmettre un message d'une façon secrète. Lors de la compilation d'un programme, le code source est transformé en un ensemble d'instructions qui sont facile à comprendre par la machine, pout l'exécution, le système d'exploitation lit les sections dont il a besoin. Donc il est possible de bénéficier les parties du code non exécuté [8].

1.8. Classification des schémas stéganographique

Il existe trois schémas de stéganographie :

1.8.1. La stéganographie pure

est un système dans lequel les données secrètes à dissimulées ne se trouvent que dans l'algorithme utilisé. La découverte de cet algorithme détruit la dissimulation de la communication. Ceci revient à mettre en place de la « sécurité par l'obscurité ».

1.8.2. La stéganographie à clé secrète

L'échange de données confidentielles nécessite tout d'abord l'échange d'une clé secrète que nous ne partagerons qu'avec notre interlocuteur. Il est donc nécessaire de disposer d'un canal sécurisé, ou de rencontrer notre interlocuteur en personne, pour être sûr que ce dernier n'est pas compromis. Cette clé affectera la façon de « cacher » les informations.

1.8.3. Stéganographie à clé publique

La personne qui souhaite transmettre des données à un autre destinataire, sans éveiller les soupçons, utilisera la clé publique de ce dernier. La clé publique étant connue a priori de tous, un échange préalable "sécurisé" ne sera pas nécessaire. Le destinataire sera le seul à pouvoir extraire le contenu à l'aide de sa clé privée [5].

1.9. Fonctionnement d'un système stéganographique

La mise en œuvre d'un schéma de stéganographie s'effectue en deux phases distinctes : phase d'insertion et phase d'extraction [2].

1.9.1. Phase d'insertion

C'est l'étape dans laquelle les messages sont cachés, elle requiert trois paramètres en entrée :

- Une image dans laquelle des données sont insérées,
- Une information à transmettre, une marque ou une empreinte digitale,
- Un algorithme d'insertion qui sélectionne dans l'image les sous-parties favorables à la dissimulation à l'aide d'une clé de stéganographie générer aléatoirement.

1.9.2. Phase d'extraction

Elle prend en entrée l'image stéganographiée et la clé secrète utilisée dans la phase d'insertion. Cette clé est alors utilisée par la suite pour déterminer les positions contenant l'information cachée.

1.10. Contraintes d'un système stéganographique

Trois critères permettent de classer les algorithmes stéganographiques : La capacité, l'invisibilité et la robustesse [2].

1.10.1. Capacité d'insertion

Correspond à la taille de données pouvant être incorporées dans l'objet de couverture, relativement à la taille de celui-ci, c'est-à-dire La capacité d'insertion d'un système de stéganographie est définie par la taille en bits du message secret qui peut être intégré dans un média de taille donnée. La capacité d'insertion relative est le rapport entre la taille du message secret à dissimuler et la taille du médium utilisé.

1.10.2. Imperceptibilité

L'imperceptibilité ou la transparence ou l'invisibilité qui dépend directement de la distorsion introduite par le processus de dissimulation lors de l'insertion des données ; le biais est simplement le nombre de modifications ou de changements dans l'objet de couverture ; Autrement dit, les chances que le support stego soit détecté "non-stego" par un attaquant.

1.10.3. Robustesse

Signifie la résistance de notre stégo-objet, c'est à dire rester normale même s'il subit des transformations (filtrage, compression, etc.…).

Le compromis entre ces trois contraintes est traditionnellement représenté par le triangle représenté dans la figure 1.6. En stéganographie, la capacité et l'imperceptibilité ont beaucoup d'importance, tandis que le tatouage ou l'empreinte privilégient la robustesse. Ces trois critères ne peuvent pas être maximisés simultanément. Chacun d'entre eux aura une influence sur l'autre.

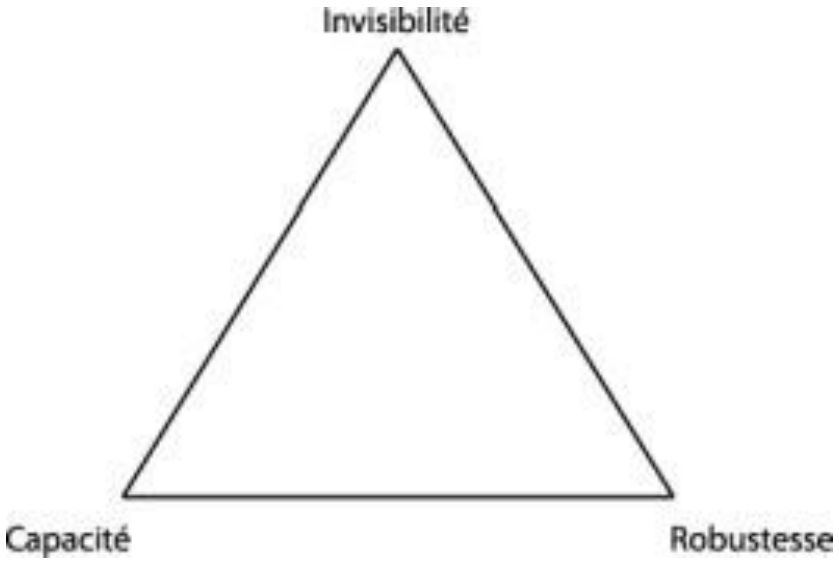

Fig.1.6 : Compromis entre capacité, invisibilité et robustesse

1.11. Evaluation d'un schéma stéganographique

Il est difficile d'évaluer un schéma de stéganographie vu les multiples critères qui rentrent en jeu dans la conception des algorithmes stéganographiques [9]. Il est néanmoins possible d'identifier deux critères d'évaluation : indétectabilité statistique et la quantification visuelle. Dans cette section, nous focalisons seulement sur la quantification perceptuelle ou visuelle.

Quantification perceptuelle

La définition même de la stéganographie indique que les modifications apportées au médium de couverture doivent rester imperceptibles. Afin de respecter cette condition, ou de pouvoir mesurer de façon efficace la distorsion introduite par un algorithme de stéganographie, il est nécessaire d'utiliser des techniques développées sous forme d'algorithme de mesure objective de qualité d'images.

☞ **Rapport signal sur bruit**

La mesure habituellement utilisée pour quantifier la distorsion entre une image originale et une image modifiée est le PSNR (Peak Signal to Noise Ration). Elle est basée sur l'erreur quadratique moyenne (Mean Square Error, MSE), définie par :

$$MSE = \frac{1}{N}\sum_{p\in P}(x_p - \grave{x_p})^2 \qquad (1.1)$$

Où P est l'ensemble de N pixels de l'image, x_p et $\grave{x_p}$ sont les niveaux de gris des images à comparer. Plus le MSE est grand, plus le niveau de dégradation est élevé.

Quant au PSNR, il est calculé par :

$$PSNR = 10log_{10}\frac{x_{max}^2}{MSE} \qquad (1.2)$$

Où x_{max} est la luminance maximale et MSE définit l'erreur quadratique moyenne calculéeentre les pixels de deux images à comparer. Une valeur de *PSNR* égale à l'infini (∞) correspond à deux images parfaitement identiques. Elle décroît en fonction de la distorsion et relie donc l'erreur quadratique moyenne à l'énergie maximale de l'image.

☞ **PSNR pondéré**

Le *wPSNR* (Weighted Peak Signal to Noise Ration, PSNR) est une variante du PSNR, qui prend en compte le voisinage de chaque pixel. Cette métrique est basée sur la sensibilité de l'œil humain aux changements des textures et des homogénéités des régions. Une nouvelle définition de l'erreur quadratique moyenne (ωMSE) donnée par :

$$\omega MSE = \frac{1}{N^2}\sum_{i,j=1}^{N}\left(\frac{x_i - y_i}{1+var(i,j)}\right)^2 \quad (1.3)$$

Où $var(i,j)$ est la variance locale de l'image dans une fenêtre centrée sur le pixel de coordonnées *(i, j).*

Donc le PSNR pondéré est donné par :

$$\omega PSNR = 10log_{10}\frac{x_{max}^2}{\omega MSE} \quad (1.4)$$

La valeur de $\omega PSNR$ augmente quand la variance est grande et décroît dans le cas contraire.

1.12. Liens avec d'autres techniques de dissimulation d'information

La figure 1.7, résume les différentes techniques de sécurité de l'information. Selon la figure 1.5, trois méthodes principales concernent la sécurité de l'information : la cryptographie, le tatouage numérique et le filigrane numérique.

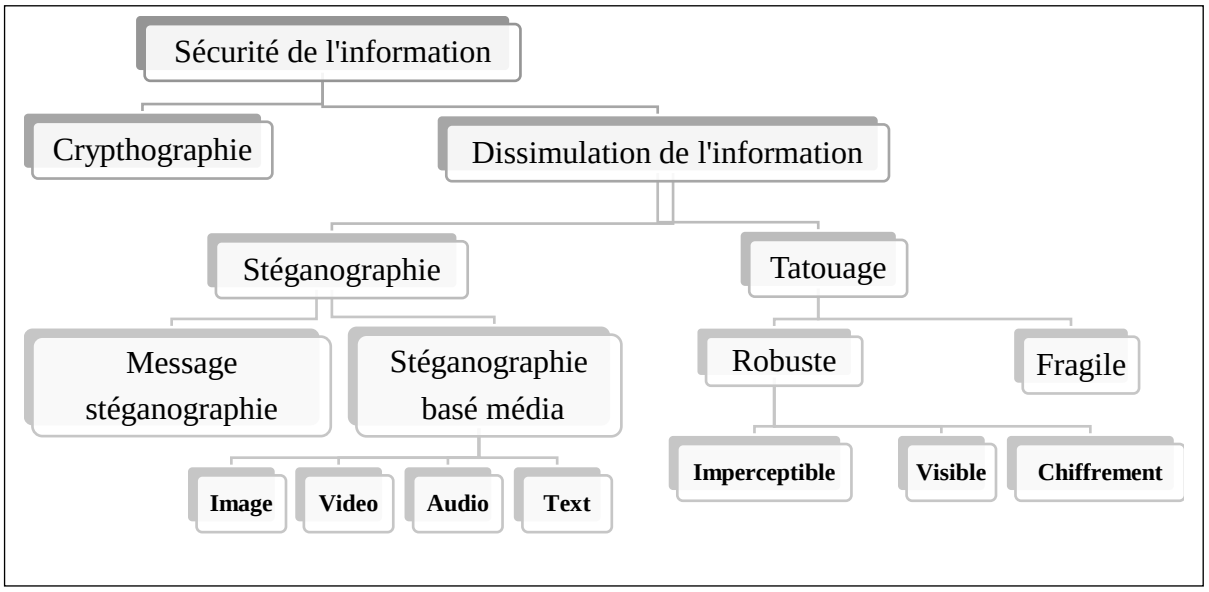

Fig.1.7 : Techniques de la sécurité de l'information

Nous rappelons ci-dessous les différents concepts utilisés dans les différentes techniques relatives à la sécurité de l'information.

1.12.1. Tatouage numérique

Le tatouage tente de répondre au problème de la protection du droit d'auteur. Il essaie de fournir une solution pour prouver qu'une entité est bien le véritable propriétaire d'un médium. En fait, il s'agit de cacher des informations puisque, pour y parvenir, on insère un tatouage (ou marque, ou filigrane) dans le support spécifique du propriétaire. Comme cela veut protéger son support et pas une version trop déformée, l'insertion doit minimiser les changements subis par le support pour être imperceptible. Ainsi, chaque exemplaire du stego-medium contient la même marque, celle du propriétaire légal. La dissimulation n'a pas ici la même signification que la stéganographie : un attaquant sait qu'un tatouage est présent dans le stego-medium, mais cette connaissance ne devrait pas lui permettre de le retirer [10].

1.12.2. Cryptographie

C'est la science d'écriture d'un message en code secret afin de préserver sa sécurité et sa confidentialité. Le but est donc de brouiller un message afin de le rendre incompréhensible pour les personnes non autorisées. Le message initial est appelé message en clair et, après chiffrement, message chiffré ou cryptogramme. Le chiffrement et le déchiffrement sont réalisés principalement à partir d'algorithmes, en utilisant des clés secrètes ou publiques [11].

1.12.3. Filigrane

Aussi appelé simplement filigrane, un motif de bits insérés dans le fichier de couverture qui identifie le les informations de copyright du fichier (auteur, droits, etc.). Le nom provient des filigranes à peine visibles imprimés sur papeterie qui identifie le fabricant de la papeterie. Le but des filigranes numériques est de fournir des droits d'auteur protection de la propriété intellectuelle au format numérique [8].

1.12.4. Comparaison entre les techniques de dissimulation d'information

La différence entre la cryptographie et la stéganographie peut être résumée comme suit : l'une est une écriture secrète mais nue, tandis que l'autre est une écriture discrète : elle nécessite une couverture, un contenu.

En d'autres termes, avec la cryptographie, la sécurité repose sur le fait que le message est incompréhensible, pour la stéganographie, la sécurité repose sur la remise en cause de l'existence même du message. Mais rien ne vous empêche de cacher un message préalablement chiffré. Les deux disciplines n'ont jamais été en compétition, mais elles sont assez complémentaires.

La définition du tatouage le rapproche en fait beaucoup plus de la stéganographie que de la cryptographie. Cependant, il faut garder à l'esprit les différences essentielles entre les deux. Alors que le but de la stéganographie est de rendre la communication furtive, la technique du tatouage repose sur la robustesse des données cachées. L'application "tatouage" est parfois considérée comme une descendante de la stéganographie. Cependant, la contrainte d'imperceptibilité y est beaucoup moins forte. C'est pourquoi, dans la plupart des cas, cette notion de tatouage est placée au même niveau que la stéganographie et les deux sont considérées comme des cas particuliers de dissimulation d'informations. Dans le cas du tatouage, le moyen n'est pas anodin, il a une valeur (marchande, médicale, ...) qu'il faut protéger. En général, des mesures sont prises pour garantir que le tatouage n'interfère pas avec l'utilisation normale du document. De plus, tous les utilisateurs qui accèdent au document auront la même version.

Le tableau 1.1 résume les points communs et les différences entre le triptyque qui cache l'information.

	Données	**Médium**	**Imperceptibilité**	**Robustesse**	**Capacité**
Stéganographie	Message à transmettre	Sans importance	Importante	Important	Autant que possible
Tatouage	Marque dépendant du médium ou du propriétaire	Dont les droits sont A protéger	Importante sauf pour les marques visibles	Importante sauf pour l'intégrité	Très peu
Fingerprinting	Empreinte dépendant du médium/ou propriétaire	Dont on souhaite prévenir la diffusion	Importante	Importante	Autant que possible

Tableau 1.1 : Récapitulatif des caractéristiques et contraintes de dissimulation d'information

1.13. Conclusion

La stéganographie est devenue le moyen de sécurité des communications la plus utilisée grâce au non suspicion des conteneurs numériques de l'information à cacher. Dans ce chapitre, nous avons présenté de manière plus ou moins approfondie les concepts de base de la stéganographie ainsi que la structure générale d'un système stéganographique et le fonctionnement de chaque phase. Finalement, nous avons présenté une comparaison entre la stéganographie et les différentes techniques de sécurité en l'occurrence le tatouage numérique, le filigrane et la cryptographie.

Chapitre 2

Principes des schémas d'insertion LSB et travaux connexes

2.1. Introduction

Il existe de nombreuses études sur la stéganographie adaptées aux images dans le domaine spatial et de nombreuses méthodes sont proposées. L'intérêt de la stéganographie dans le domaine spatial s'explique par sa simplicité de mise en œuvre et sa grande capacité d'insertion des messages secrets. Les méthodes proposées dans ce domaine sont regroupées dans quatre classes de méthodes [8] :

1. Ajout du message à la fin du fichier.
2. Ajout du message dans les espaces inutilisés du conteneur.
3. Ajout du message dans les données de l'image de manière séquentielle.
4. Ajout du message dans les données de l'image en utilisant une séquence pseudo aléatoire.

Les deux dernières classes de méthode de stéganographie peuvent être regroupées dans deux catégories de méthodes suivant le domaine de représentation de l'image : domaine **spatial** ou **fréquentiel**. Dans ce chapitre, nous nous limiterons à la présentation de principe de stéganographie dans le domaine spatial et fréquentiel et les travaux connexes correspondent.

2.2. Principe du schéma d'insertion LSB

Plusieurs techniques de stéganographie, dans le domaine spatial et/ou fréquentiel, ont été développés dont le principe principal d'insertion est le même : la modification des bits de poids faible (**L**east **S**ignificant **B**its **: LSB**) de chaque pixel ou coefficients.

2.2.1. Schémas d'insertion dans le domaine spatial

2.2.1.1. Définition : domaine spatial

Le domaine spatial est le domaine classique où chaque valeur (x, y) dans l'image correspond à la valeur des pixels, nous pouvons alors la visualiser dans un espace a 3 dimensions ou les axes X et Y représentent deux dimensions de l'image, et l'axe Z représente la valeur des pixels.

Les images fixes appartiennent au domaine spatial apparaissent dans de nombreux formats, notamment BMP, Raw, XPixmap, etc. Chaque format correspond à une structure particulière de représentation et de stockage des informations relatives à l'image (données, taille, nombre de bits par donnée . . .).

2.2.1.2. Principe d'insertion dans le domaine spatial

Le domaine spatial concerne les images numériques fixes telles que BMP et PGM. Une image fixe est une image non compressée représentée par un tableau ou une suite de pixels. Notons $In = (x1, \dots xn)T$ le vecteur représentant la suite de*n* pixels d'une image.

Cette image peut être en noire et blanc avec $x_i = \{0,1\}$, en niveaux de gris avec $x_i = \{0, \dots,255\}$, ou en couleur avec $x_i = \{0, \dots,255\}^3$. Chaque pixel est représenté numériquement par un entier positif codé sur *b* bits dont sa représentation binaire est donnée par :

$$X_n = \sum_{i=0}^{b-1} b_{n,i} 2^i \qquad (2.1)$$

Où $b_{n,i} \in \{0,1\}$ représente l'i-ème bit codant le n-ième pixel.

Les bits n'ont pas tous la même importance dans le codage de la valeur X_n ; en effet le premier bit $b_{n,0}$ est pondéré par $2^0=1$ alors que le dernier bit $b_{n,b-1}$ est pondéré par 2^{b-1} en partant du bit de poids fort (MSB pour Most Significant Bit) jusqu'au bit de poids faible (LSB pour Least Significant Bit) (voir figure 2.1).

Numérotation des bits	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
	MSB						LSB	
Valeur des bits	1	1	0	0	0	1	1	1

Fig.2.1 : Exemple représentant un octet et son MSB et LSB

Les bits de même pondération dans une image représentent un plan de bit ou une image binaire. La figure 2.2 présente les différents plans de bits de l'image 'Barbara.BMP' en niveau de gris, en partant du bit de poids faible (LSB pour Least Significant Bit) jusqu'au bit de poids fort (MSB pour Most Significant Bit).

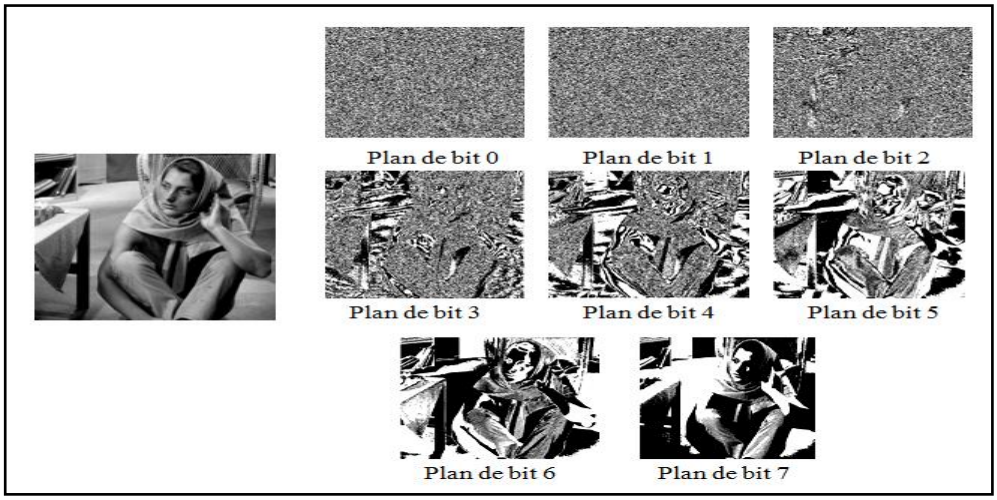

Fig.2.2 : Décomposition en plans de bits de l'image 'Brabara.BMP' en niveaux de gris [3].

On constate que les plans des bits de poids faibles sont nettement moins structurés que ceux de poids plus forts c'est pourquoi les changements des bits de poids faible de 0 à 1 ou de 1 à 0 sont totalement imperceptibles par l'œil humain. De ce fait, la stéganographie dans le domaine spatial regroupe les techniques basées sur la modification des bits de poids faible des pixels par les bits de message que l'on voudrait insérer dans l'image.

L'exemple ci-dessous illustre l'insertion et l'extraction de la lettre *A* dans trois pixels d'une image 24-bits au format Bmp.

1. Soit le code binaire de 3 pixels suivant :

00100111	**11101001**	**11001000**
00100111	11001000	11101001
11001000	00100111	11101001

2. La valeur binaire de la lettre A est : 10000011.

3. Soit une clé secrète *K* calculer par un générateur de nombres aléatoires :

5	13	23	28	39	46	53	71

En insérant la lettre A dans les trois pixels on obtiendrait :

00100101	**11101001**	**11001000**
00100111	**11001000**	**11101000**
11001000	**00100111**	**11101001**

L'extraction de message secret, la lettre A, à partir de stégo-image se fait alors simplement, on extrait les LSBs des pixels de stégo-image dont les emplacements définis dans la clé secrète *K*. Le message est recomposé en concaténant les LSBs des pixels parcourus. Steganos est l'un des outils de stéganographie qui repose sur le schéma d'insertion par remplacement des bits de poids faible (http://steganography.com).

2.2.1.3. Schémas d'insertion LSB

Une grande gamme de techniques de stéganographie ont été proposées dans le domaine spatial, plus de 836 outils de stéganographie sont développés dont 70% utilisaient l'insertion dans les bits de poids faible [9]. Ces techniques peuvent être classées dans deux classes de stéganographie en fonction de la manière d'insertion des bits des messages secrets: insertion par remplacement de LSBs et insertion par correspondance de.

2.2.1.4. Insertion par remplacement de LSBs

Historiquement, la technique de remplacement des bits de poids faible (LSB remplacement) est la première méthode de stéganographie dans la littérature [12-14]. Elle reste encore aujourd'hui la méthode la plus utilisée, sans doute pour sa simplicité d'implémentation. Cette technique consiste à remplacer les bits de poids faibles (les LSB) des pixels par les bits de message à insérer. Autrement dit, pour insérer un message M = (m_1, ..., m_n), le dernier bit de poids faible, de chaque pixel est remplacé par un bit du message à dissimuler. Le sens de parcours des pixels est usuellement choisi par un parcours pseudo-aléatoire. Pour ce faire, l'émetteur et le récepteur doivent préalablement échanger une clé k, utilisée comme graine d'un générateur de nombre pseudo-aléatoire. La figure 2.3, présente les différentes transitions des LSBs lors du processus d'insertion.

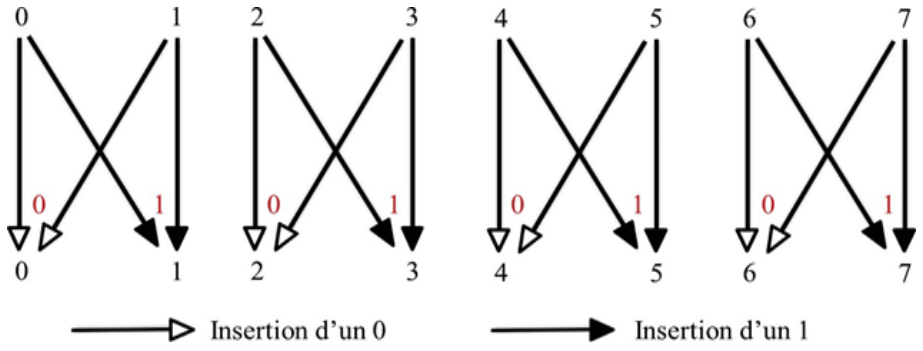

Fig.2.3 : Transitions des LSB des pixels par la technique de remplacement

La stéganographie par remplacement des LSB est une technique très simple dans son implémentation alors elle est facilement détectable (attaque de Qui-Deux). En plus, elle altère considérablement la distribution statistique des pixels du support stéganographié.

2.2.1.5. Insertion par correspondance de LSBs

La stéganographie par correspondance des LSB, également appelée LSB Matching ou ±1embedding, est l'amélioration la plus courante de la stéganographie par remplacement des LSBs [13,15]. Cet algorithme d'insertion, qui est très proche de la technique par remplacement des LSBs, insère également le message $m \in \{0, 1\}^m$ dans les LSBs des pixels, mais en incrémentant ou décrémentant aléatoirement la valeur du pixel. Là encore, le sens de parcours des pixels est habituellement choisi aléatoirement.

La Figure 2.4 illustre un exemple de modification des bits de poids faible des pixels, par la technique de correspondance.

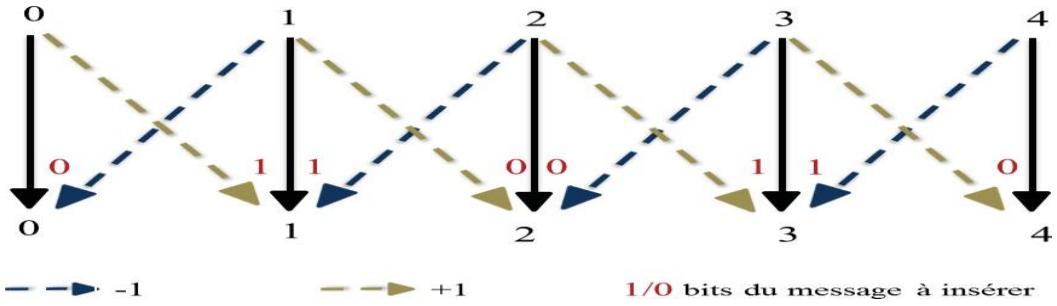

Fig.2.4 : Exemple de modification des LSB des pixels par la technique de correspondance.

Le but de cette technique d'insertion est de fournir une solution au problème des artefacts statistiques de la stéganographie par LSB substitution. En effet, contrairement à la stéganographie par remplacement des LSBs, la méthode de stéganographie par correspondance des LSBs ne modifie pas la distribution statistique du premier ordre du support hôte. Ainsi, toutes les attaques ciblées, spécifiquement dédiées à la détection de la stéganographie par remplacement des LSBs et n'utilisant qu'une statistique de1^{er} ordre, sont inefficaces pour détecter la méthode d'insertion par correspondance des LSB.

2.2.1.6. Travaux connexes

La première variante d'insertion 2LSB ou encore TLSB (Two Least Significant Bit) consiste à remplacer tout simplement les deux bits de poids faible de chaque pixel par deux bits de message secret [16]. Chaque modification entraine quatre valeurs basées sur le fait que deux insertions LSB modifient ces quatre valeurs l'une dans l'autre. Il existe une autre variante du schéma d'insertion 2LSB connue par I2LSB (Independent Two Least Significant Bits). En tant que schéma alternatif de 2LSB, les bits de message peuvent être insérés dans l'image de couverture en sélectionnant des pixels et en ne remplaçant que le deuxième LSB de chaque pixel puis en répétant par une nouvelle sélection de pixels dont le premier LSB est utilisé. Par conséquent, des changements se produisent dans le premier et deuxième LSB indépendamment.

Khalid et al. [17] ont proposés une méthode de stéganographie connue par SM2LSB (Single Mismatch 2LSB) basée sur la similarité et le non similarité entre les deux bits de message que l'on veut insérer et les deux premiers LSBs. L'objectif essentiel de cette méthode consiste à réduire les changements des pixels affectés par l'insertion LSB $\pm k$, ainsi de diminuer la probabilité de détection en comparaison avec les deux schémas d'insertion: LSB par remplacement et LSB par correspondance.

Le travail présenté dans [18], propos une méthode de sténographie LSB pour masquer les informations sensibles dans les images numériques. Cette méthode satisfait la condition d'imperceptibilité des informations cachées, requises dans les systèmes de sténographie et améliore la capacité d'insertion qui peut représenter jusqu'à 37% de la taille de l'image de couverture.

Le principe de base de cette méthode est basé sur l'utilisation de trois générateurs de bruit chaotique basés sur la carte chaotique de tente asymétrique afin de minimiser les altérations statistiques. Cette méthode est évaluée selon deux critères : l'affectation de l'image de couverture et la robustesse contre les attaques de stéganalyse. Pour évaluer l'affectation de l'image de couverture, des métriques de texture, de qualité et de qualité perceptive sont considérés. Pour évaluer la robustesse contre les attaques, l'outil StegExpose est aussi utilisé, afin d'analyser les images obtenues à partir de la méthode proposée, et les principales méthodes de stéganalyse telles que les paires d'échantillons, l'analyse RS, l'attaque du chi carré et l'analyse des ensembles primaires sont considérés.

Dans un autre travail [19], une technique de stéganographie de très haute capacité utilisant des mécanismes de différenciation et de substitution. Il divise l'image en blocs de 3 × 3 pixels non superposés. Pour chaque pixel d'un bloc, la substitution de bit de poids faible (LSB) est appliquée sur deux LSB et la différence de valeur de quotient (QVD) est appliquée sur les six bits restants. Ainsi, il existe deux niveaux d'insertion : (i) substitution de LSB aux plans de bits inférieurs et (ii) QVD aux plans de bits supérieurs. Si un bloc après d'insertion indique que les niveaux des pixels voisins dans l'histogramme de différence de pixels sont égaux, alors ce bloc est annulé et une substitution LSB à 4 bits modifiée est appliquée. Expérimentalement, il est prouvé que la capacité d'insertion est améliorée dans une plus grande mesure.

Afin de pallier les faiblesses de la célèbre méthode de stéganographie PVD [20], une méthode de stéganographie est proposée dans [27]. Dans cette méthode, l'histogramme d'algorithme de gradient orienté (HOG) est utilisé pour trouver la direction de bord dominante pour chaque bloc 2 × 2 d'images de couverture. Les blocs d'intérêt (BOI) sont déterminés de manière adaptative en fonction de l'amplitude du gradient et de l'angle de l'image de couverture.

Ensuite, l'algorithme PVD est utilisé pour masquer les données secrètes dans la direction du bord dominant, tandis que la substitution LSB est utilisée dans les deux autres pixels restants. Des expériences approfondies révèlent que le schéma proposé offre une capacité d'insertion élevée et une meilleure qualité visuelle par rapport à plusieurs autres méthodes basées sur PVD et LSB.

Pour augmenter la capacité d'insertion, la méthode proposée dans [12] présente une technique de stéganographique adaptée aux images numériques dans le domaine spatial. Le schéma proposé prend le bit de message et effectue une opération XOR avec le 7ème bit de chaque composant RVB et, après cela, la sortie produite est insérée dans le 8ème bit de chaque composant de RVB. La procédure d'insertion est effectuée de manière à ce qu'il n'y ait aucun signe de message original à l'intérieur de l'image de couverture. Les résultats expérimentaux montrent un très bon rapport signal / bruit (PSNR) (55,90 dB pour 65536 bits de message dans une image de couverture de 256x256 pixels) et une valeur d'erreur quadratique moyenne (MSE) qui indique moins d'imperceptibilité et plus de sécurité.

La méthode proposée dans [21] présente un schéma de sécurité des messages à trois couches et à haute capacité. Les deux premières couches sont de nature cryptographique, tandis que la troisième couche est de nature stéganographique. Dans la première couche, le cryptage AES-128 est effectué sur le message secret. Dans la seconde couche, un cryptage de carte chaotique logistique est appliqué sur la sortie de la première couche sécurisée pour augmenter la sécurité du schéma. Dans la troisième couche de sécurité, une technique de stéganographie adaptée aux images a développé où le bit de poids faible (LSB) est modifié selon un motif en zigzag dans chacun des trois plans de couleur de l'image de couverture (c'est-à-dire RVB).

Ce schéma stéganographique permet d'obtenir des valeurs plus élevées du rapport signal / bruit (PPSNR), de l'erreur quadratique moyenne (MSE), de la métrique d'indice de similarité structurale (SSIM), de la corrélation croisée normale (NCC) et de la fidélité d'image (IF) par rapport à ses homologues de la littérature.

Dans et al. [22], proposent un nouvel algorithme stéganographique dans le domaine spatial utilisant le concept de modulation de pixels qui diminue les changements qui se produisent dans l'image stéganographiée générée à partir de l'image de couverture. Les résultats expérimentaux montrent l'efficacité de l'algorithme proposé. Différentes métriques telles que l'erreur quadratique moyenne (MSE), le rapport pic / signal (PSNR), l'analyse du plan binaire et l'analyse de l'histogramme ont été utilisées pour montrer les meilleurs résultats de l'algorithme proposé par rapport à ceux existants.

La méthode proposée dans [23] a présenté une nouvelle stratégie pour trouver une solution quasi optimale pour le schéma d'insertion dans les bits de poids faible par paire (LSB).

Il implique le changement de deux pixels de couverture et de deux bits de données secrètes au même moment et change également l'ordre de correspondance entre les bits secrets et les pixels de couverture pour diminuer la distorsion de l'image de couverture. Ce schéma stéganographique permet de réduire la distorsion de stego image, diminue la probabilité de détection et améliore en même temps la qualité visuelle.

2.2.2. Stéganographie dans le domaine fréquentiel

2.2.2.1. Définition : domaine fréquentiel

Le domaine fréquentiel désigne tout simplement la transformation d'une image de domaine spatial dans un autre domaine que l'on pourrait appelé fréquentiel ; plus précisément la transformation appliquée à une image convertit l'ensemble des pixels en un ensemble de coefficients. Les transformations les plus utilisées en traitement de signal et d'images ont la transformation de Fourier, la Transformation en Cosinus Discrète (TCD) et la Transformation en Ondelette. En stéganographie, les algorithmes d'insertion dans le domaine transformé de l'image sont très couramment utilisés, car les images échangées sur Internet sont le plus souvent les images compressées au format JPEG et TIFF.

2.2.2.2. Principe d'insertion dans le domaine fréquentiel

Comme nous avons indiqué dans la section précédente que les schémas d'insertion sont basés sur la modification des bits de poids faible, le principe d'insertion dans le domaine fréquentiel est basé sur la modification des coefficients obtenus (DCT, DWT). Dans ces deux cas de figure, l'insertion de données est réalisée dans les coefficients de la transformée dans l'étape de quantification soit par :

- La modification des bits de poids faible de ces coefficients (eg. Algorithme **Jsteg [**24]).
- La décrémentation de la valeur absolue des coefficients DCT (eg. Algorithme **F5** [25])**.**

La quantification est l'étape dans laquelle on perd réellement des informations. Elle consiste à diviser la matrice retournée par la DCT, par une autre, appelée matrice de quantification, et qui contient 8x8 coefficients. Le but de cette opération est d'atténuer les hautes fréquences, c'est-à-dire celles auxquelles l'œil humain est très peu sensible.

L'insertion dans cette étape est justifiée par le fait que la quantification ramène beaucoup de coefficients à 0 (surtout en bas à droite dans la matrice, là où sont les hautes fréquences). Seules quelques informations essentielles (coin en haut à gauche) sont gardées pour représenter le bloc. Par exemple, dans la matrice de quantification (figure 2.5), on utilise les composantes ayant la même valeur afin de dissimuler les données.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	**22**	29	51	87	80	62
18	**22**	37	56	68	109	103	77
24	35	55	64	81	104	113	81
49	68	74	87	101	121	120	101
72	92	95	112	112	100	103	33

Fig.2.5 : Matrice de quantification

Par exemple on peut prendre les composantes (5,2) et (4,3) valant 22. Après la division scalaire des deux matrices (DCT, Quantification), on obtient une matrice B. Si l'on veut coder un 1, alors on mettra la donnée dans la composante ayant la valeur la plus élevée, si l'on veut coder un 0, c'est le contraire.

2.2.2.3. Travaux connexes

La plupart des méthodes de stéganographie adaptées aux images JPEG, sont des variantes des méthodes stéganographiques spatiales, qui sont décrites auparavant. À titre d'exemple, les algorithmes de stéganographie, classiquement utilisés pour les images JPEG, tels que F5 [25], Jsteg [24] ou Outguess [26], reposent principalement sur la méthode d'insertion par remplacement des LSB. Pour ces algorithmes, la méthode de modification utilisée est appliquée aux coefficients DCT quantifiés et non plus directement aux valeurs des pixels. La Figure 2.6 illustre un exemple de modification des coefficients DCT, pour les algorithmes F5 et Jsteg.

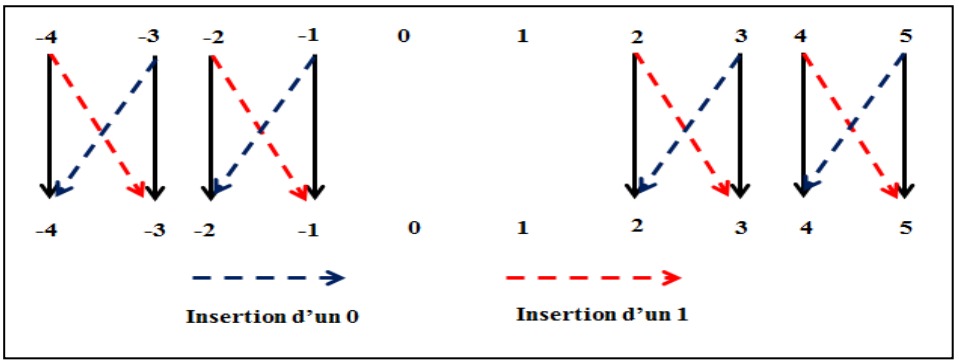

Fig.2.6 (a) : Modification des coefficients DCT pour l'algorithme Jsteg

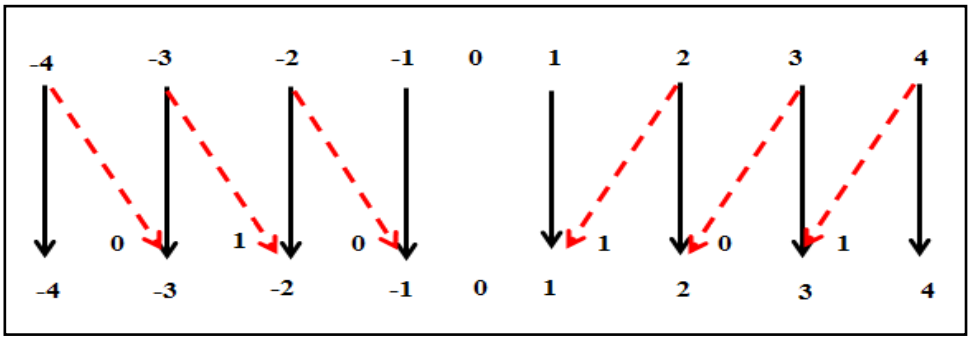

Fig.2.6 (b) : Modification des coefficients DCT pour l'algorithme F5

Fig.2.6 : Exemples de modification des coefficients DCT pour les algorithmes Jsteg et F5.

Dans [27] Junlan et al. introduit une nouvelle technique combinant la détection de LSB et de bord pour améliorer l'invisibilité. La couverture l'image I de l'algorithme est convertie en LSB en effaçant cinq LSB de chaque pixel pour effectuer la détection des contours. Chaque pixel sera soit une zone périphérique, soit une zone non périphérique. Le pixel qui appartenir à la zone de bord est utilisé pour incorporer des données secrètes.

Dans [28], les auteurs ont proposé un algorithme de stéganographie dans le domaine spatial basé sur une logique réversible. Ils utilisent la porte Feynman pour obtenir la réversibilité de l'image avec un simple LSB technique. Un circuit de nano-communication pour l'image la stéganographie est représentée à l'aide du codeur / décodeur proposé. L'algorithme montre une amélioration de 28,33% en termes de la surface sur un métal-oxyde-semi-conducteur complémentaire circuit.

Dans [29], l'auteur applique l'algorithme de stéganographie sur l'ECG images pour sécuriser les informations du patient. Edward et Ramu utilisent transformation curvelet sur les images pour convertir des images ECG 1D dans des images 2D. Une approche de quantification est utilisée pour remplacer autour de zéro coefficient avec des données sécurisées. Auteur utiliser PSNR et BER pour évaluer l'algorithme à l'aide de la base de données MIT-BIH.

2.3. Conclusion

Au cours du présent chapitre, nous avons présenté le principe d'insertion dans le schéma d'insertion LSB dans le domaine spatial et fréquentiel ainsi que les différentes connexes les plus récents. Parmi les méthodes de stéganographie présentées, nous nous sommes intéressés, plus particulièrement, aux schémas d'insertion par remplacement, ceux qui reposent notre méthode proposée.

Chapitre 3

Méthode proposée et résultats expérimentaux

3.1. Introduction

L'objectif de notre travail est de proposer deux schémas de stéganographie dans le domaine spatial et fréquentiel afin d'améliorer les schémas d'insertion LSBs. Pour ce faire, dans ce chapitre, le principe des deux schémas proposés sont détaillés. Nous conclurons le présent chapitre par une analyse et discussion des résultats expérimentaux obtenus.

3.2. Prérequis théoriques

Généralement, tous les problèmes liés à la conception d'une méthode stéganographique sont généralement liés à la sélection des postions de pixels capables à l'insertion d'un message secret. Dans cette section, nous essayons de donner les prérequis théoriques concernant le générateur des séquences pseudos aléatoires (Registre a décalage à rétroaction linéaire) sur lequel est basé les schémas stéganographiques proposés.

Registre a décalage à rétroaction linéaire

Les générateurs pseudos aléatoires ont, à travers le temps, acquis une grande importance pour la sécurité des applications dans divers domaines, allant de la simulation stochastique, confidentialité des échanges sur les réseaux sans fils, sécurisation des applications web, et système de chiffrement.

☞ **Définition**

Un registre à décalage à rétroaction linéaire ou **LFSR** (pour linear feedback shift register en anglais) est un système générant des bits à partir d'un registre et d'une fonction de rétroaction. Après plusieurs itérations, le registre revient à un état antérieur déjà connu et repart en boucle dont le nombre d'itération est appelé sa période.

En pratique, ce genre de registre **LFSR** est utile en cryptographie car il permet la génération de nombres pseudo-aléatoires lorsque la période est suffisamment longue.

☞ **Comment utiliser un LFSR ?**

A partir d'un état actuel du registre, une sélection de bits est choisie pour leurs appliquée une opération XOR (voir figure 3.1). Le résultat est alors concaténé au début du registre (à gauche) tandis que la valeur finale (à droite) est supprimée du registre et affichée en sortie.

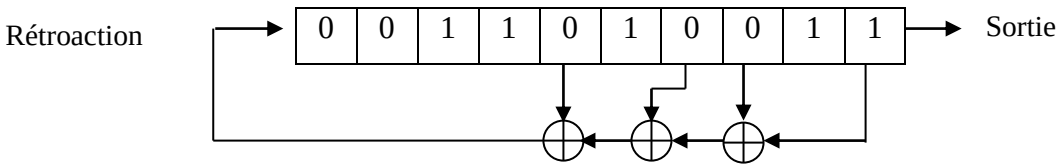

Fig.3.1. Principe de fonctionnement d'un registre à décalage à rétroaction linéaire

3.3. Méthode proposée

Cette section se concentre sur la conception de deux schémas de stéganographie, dans le domaine spatial et fréquentiel, pour la transmission de données secrètes dans lesquelles les images numériques sont sélectionnées comme support de couverture. Dans le premier schéma d'insertion, une technique de sélection des coordonnées de pixels appropriées pour la dissimulation de données est proposée. Dans le deuxième schéma, réalisé dans domaine fréquentiel, la matrice bleue est utilisée pour la dissimulation d'information.

3.3.1. Stéganographie basée sur le schéma LSB dans le domaine spatial

La mise en œuvre de schéma stéganographique proposée s'effectue en deux étapes distinctes :

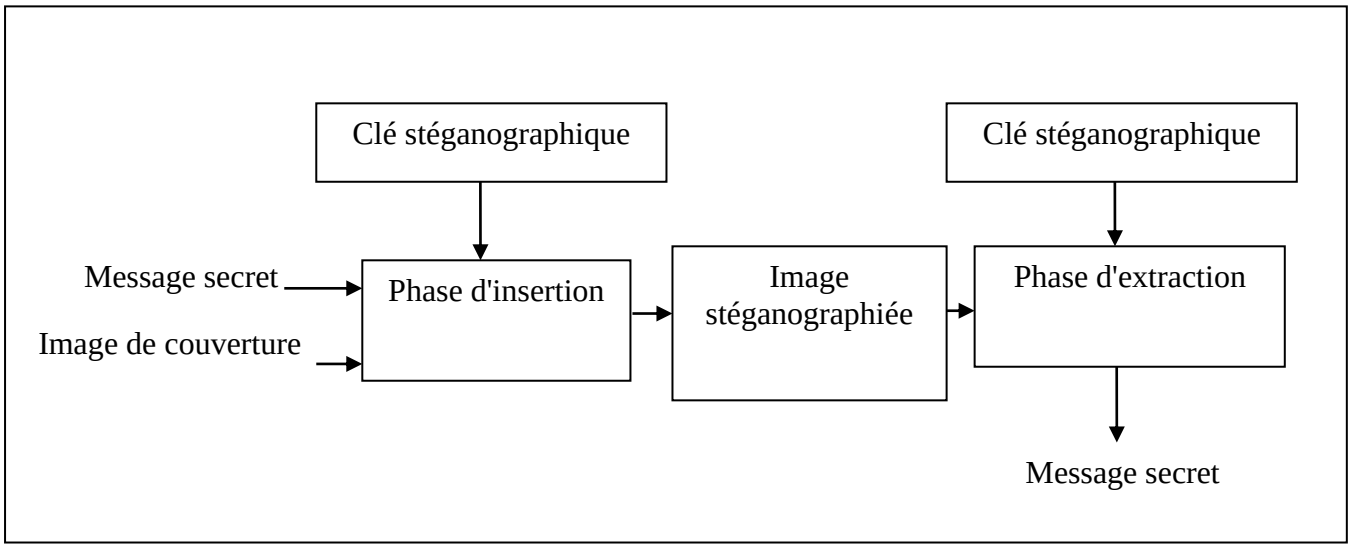

Fig 3.2 : Schéma d'insertion

3.3.1.1. Phase d'insertion

Les principales étapes de la phase d'insertion du notre schéma proposé sont illustrés dans la figure 3.2. Dans la phase d'insertion, nous effectuons les étapes suivantes :

1. Convertissez tout d'abord le message secret en binaire afin d'obtenir un flux binaire ;
2. Divisez le flux binaire obtenu en un ensemble de *n* groupes avec *m* bits ($m \leq 4$) de même valeur de bit ;
3. Un ensemble de pixels de l'image de couverture est sélectionné en fonction de la clé d'insertion du message secret ; il est à noter que le nombre de pixels sélectionnés à cette étape est calculé en fonction de la longueur du message secret.

$$Nombre\ de\ pixels = L/m \tag{3.1}$$

Sachant que : L désigne la longueur du message binaire et *n* est le nombre de LSBs utilisé.

4. Divisez les pixels de l'image de couverture sélectionnés en un ensemble de *n* groupes en fonction de *m* LSBs utilisés ($m \leq 4$).
5. Calculer la différence entre chaque groupe : flux binaire et groupe de pixels.

6. Remplacer le reste des *n* bits de chaque groupe du flux binaire par les bits de poids faibles du reste des pixels dans chaque groupe de pixels.

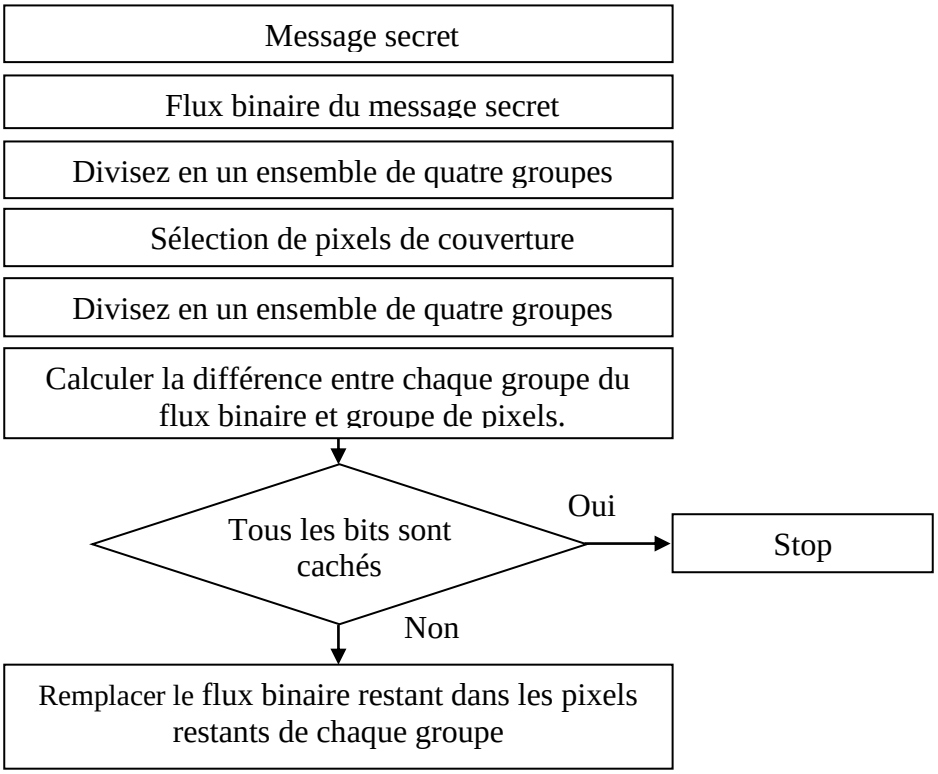

Fig 3.3 : Phase d'insertion

3.3.1.2. Phase d'extraction

Les principales étapes de la phase d'extraction du schéma sont illustrées à la figure 3.3. Dans la phase d'extraction, il suffit d'utiliser l'image stéganographiée et la clé de stéganographie.
Dans la phase d'extraction, nous effectuons les étapes suivantes :

1. Nous extrayons d'abord les pixels de l'image de couverture en fonction de la clé stéganographique utilisés dans la phase d'insertion ;

2. Nous divisons ensuite les pixels en un ensemble de *n* groupes avec *m* pixels dans chaque groupe ;

3. On extrait le message secret selon les *m* LSBs utilisés ;

4. Nous ajoutons les *m* LSBs les uns aux autres et ainsi nous obtenons un flux binaire de messages secrets comme résultat de cette étape.

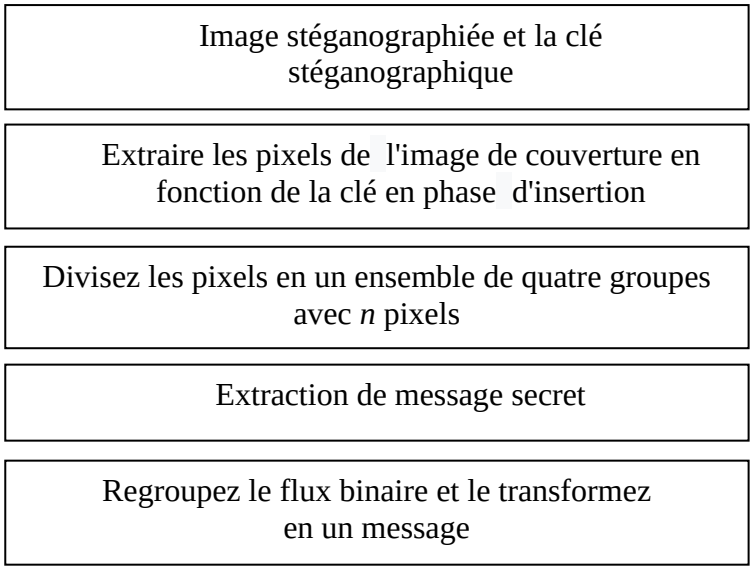

Fig 3.4 : Phase d'extraction

3.3.2. Stéganographie basée sur le schéma d'insertion LSB dans les coefficients DCT

Nous proposons dans cette section un nouveau schéma de stéganographie basé sur la modification des LSBs des coefficients DCT. Dans ce schéma, nous avons appliqué la transformée DCT sur la matrice bleue de l'image originale. L'utilisation de la matrice bleue est justifiée par le fait que la teinte bleue du pixel ne soit visuellement altérée.

3.3.2.1. Phase d'insertion

Les principales étapes de la phase d'insertion de la méthode proposée sont :

1. Extraction de la matrice bleue de l'image de couverture ;
2. Application de la transformée DCT sur la matrice bleue ;
3. Effectuer l'opération de quantification dans chaque block DCT obtenus à l'étape précédente en divisant chaque valeur du block *K* avec la valeur correspondante dans la matrice de quantification Q présentée dans la figure ci-dessous.

Cela aboutissent à la matrice P, qui a les coefficients DCT quantifiés.

$$P(i,j) = K(i,j)/Q(i,j) \qquad (3.2)$$

$$Q = \begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Fig. 3.5 : Matrice de quantification

4. Un parcours en zigzag est effectué sur chaque block DCT quantifié donnant un tableau unidimensionnel A ; les valeurs de ce tableau seront dans l'ordre croissant, ce qui signifie que les coefficients de basse fréquence sont au début.
5. Insertion du message caché dans les premiers 19 coefficients de chaque block DCT ;
6. Le parcours zigzag inverse est appliqué sur le tableau A pour le reconvertir en une matrice 8 × 8. Ensuite, ce block est déquantifié en multipliant chaque valeur du block K avec la valeur correspondante dans la matrice de quantification Q ;
7. La transformée inverse (IDCT) est appliquée pour la transformer l'image bleu en une image représentée dans le domaine spatial.

3.3.2.2. Phase d'extraction

L'extraction du message caché comprend les étapes suivantes :

1. Représentation de la matrice bleue de l'image stéganographiée dans la transformée DCT ;
2. Quantification de chaque block DCT 8 × 8 ;
3. Effectuez un balayage en zigzag et extrayez les données.
4. Concaténation de *n* LSBs les uns aux autres afin d'obtenir le flux binaire de messages secrets qui sera par la suite transformé en message.

3.4. Résultats et discussions

L'objectif principal de notre étude se concentre sur l'amélioration des techniques de stéganographie basées le schéma LSB lorsque les images numériques sont utilisées comme supports de couverture. Dans cette section, nous évaluons les performances de nos schémas d'insertion proposés en fonction de deux métriques importantes, PSNR et EC.

3.4.1. Protocole de tests

L'évaluation de performance d'un système stéganographique peut être décrite par deux métriques essentielles, à savoir le PSNR et EC (voir chapitre I). Ces mesures sont les plus courantes et les plus utilisées pour l'évaluation des images stéganographiées. Le PSNR est utilisé dans de nombreuses applications de traitement d'images et considéré comme une métrique de référence pour évaluer la qualité de l'image traitée. La métrique EC calcule le nombre prévu de bits de message insérer sur le nombre de modification.

3.4.2. Evaluation des performances

Dans nos expériences et afin de garantir la crédibilité des résultats obtenus, nous utilisons des images standard au niveau de gris et couleurs avec des tailles de 256× 256 comme supports de couverture, tels que les images Lena, Baboon, Hat, etc. En outre, l'ensemble des expériences réalisées est divisé en trois parties. Au cours de la première et la deuxième partie, nous avons mené plusieurs expériences pour évaluer les performances de chaque méthode proposée basée en se basant sur le nombre de LSB utilisés.

Tandis que la troisième partie présente une comparaison entre les deux schémas proposés ainsi que les deux schémas standard Un-LSB et Deux-LSB.

Il est important de noter que, dans ces parties, les images stéganographiées sont générées avec différents taux d'insertion allant de 20 à 80% avec une étape de 20% de la taille de l'image de couverture.

3.4.2.1. Evaluation de la méthode de stéganographie basée sur le schéma LSB dans le domaine spatial

Le but de cette partie est d'évaluer les performances de premier schéma proposé lorsque nous utilisons un message secret de différentes tailles. Par conséquent, pour obtenir les spécificités de performance, le message secret est inséré dans l'image de couverture et une mesure subjective et/ou objective est examinée. Il convient de noter que la technique de stéganalyse, comme une forme d'attaque, devient plus facile si le message secret est inséré dans des pixels séquentiels dans lesquels le message secret sera toujours trouvé dans les mêmes endroits.

Pour surmonter cette faiblesse, les positions des pixels (emplacements) doivent être sélectionnées au hasard (par exemple, un générateur de positions basé sur un décalage à droite). Bien sûr, les paramètres du générateur cryptographique sont utilisés comme une clé secrète pour insérer / extraire le message secret. Dans cette section, nous avons mené plusieurs expériences pour évaluer les performances du schéma proposé en fonction de nombre LSBs utilisés.

La figure 3.6 montre les deux images 'Peppers' et 'Nature' et les images stéganographiées associées utilisons les schémas d'insertion Un-LSB et Deux-LSB avec un taux d'insertion de 50%.

Image de couverture
(a)

Un-LSB $\begin{cases} PSNR = 37.43 \\ EC = 52.54\% \end{cases}$
(c)

Deux-LSBs $\begin{cases} PSNR = 41.49 \\ EC = 55.63\% \end{cases}$
(e)

Image de couverture
(b)

Un-LSB $\begin{cases} PSNR = 39.19\ \% \\ EC = 56.14\% \end{cases}$
(d)

Deux-LSBs $\begin{cases} PSNR = 39.53 \\ EC = 68.22\% \end{cases}$
(f)

Fig. 3.6 : Comparaison visuelle des images 'Peppers' et Nature, et ses images stéganographiées avec un taux d'insertion de 50% (a-b) images de couverture, (c-d) images stéganographiées avec le schéma Un-LSB et (e-f) images stéganographiées avec le schéma Deux-LSB dans le domaine spatial.

À partir de ce taux d'insertion, nous pouvons trouver trois remarques importantes :

- ☞ Premièrement, l'inspection visuelle a montré qu'il n'y avait pas de dégradation de la qualité des images stéganographiées pour les deux schémas d'insertion (Un-LSB et Deux-LSB), dans lesquelles les images stéganographiées et l'image de couverture sont visiblement identiques sans aucune indication de messages cachés.
- ☞ Deuxièmement, un PSNR égal à **37.43 %** et **39.19 %** peut être atteint par le schéma d'insertion Un-LSB respectivement (voir fig. 3.6(c), 3.6(d)), ce qui indique clairement que la distorsion visuelle dépend des emplacements sélectionnés.
- ☞ Finalement, du point de vue du taux de changements des LSBs, les résultats obtenus indique que le taux de changement dépend des pixels sélectionnés. Le schéma d'insertion Un-LSB donne un EC égal à **52.54%** pour l'image 'Peppers' en comparaison de l'image 'Nature' avec un taux de changement égal à **56.14%**. Alors, le schéma d'insertion Deux-LSB qui a changé plus de bits dans les deux images de couverture (EC égale à **55.63% et 68.22%**).

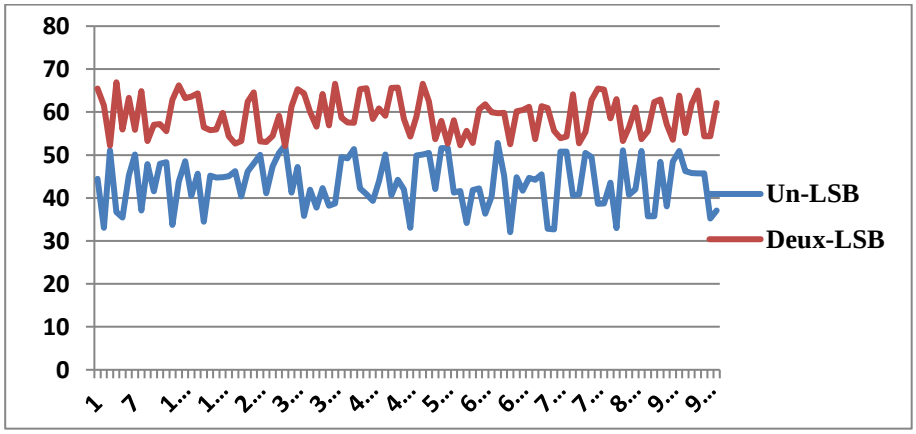

Fig. 3.7 : Comparaison des taux de distorsion du Un-LSB et Deux-LSB

En analysant la courbe de la fig.3.7, on peut voir que, en général, les performances du premier schéma Un-LSB proposé est plus efficace que le schéma Deux-LSB proposé. Par rapport à ce dernier schéma, un taux de changement moyen égal à **59.06%** peut être obtenu avec la technique Deux-LSB pour tous les taux d'insertion.

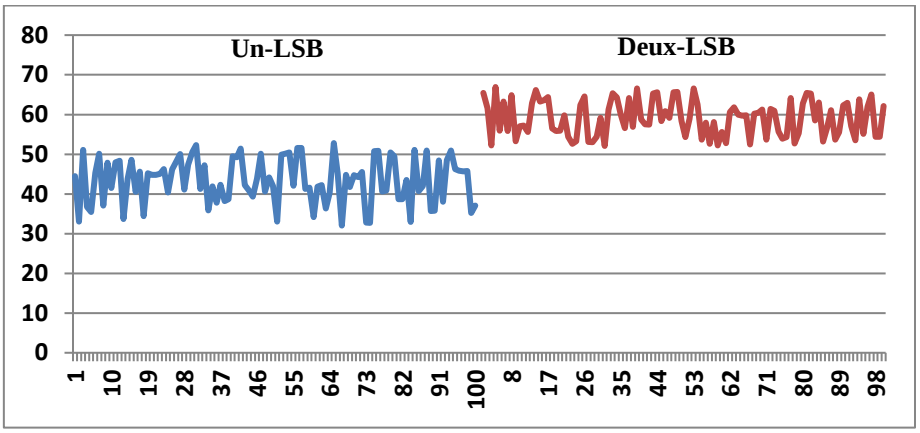

Fig.3.8 : Comparaison des taux de changement du Un-LSB et Deux-LSB

Le deuxième test, présenté dans la fig. 3.8, vise à montrer le taux de changement du LSBs des deux schémas proposés. Cette métrique montre que la technique Un-LSB a la capacité d'améliorer la métrique EC avec une valeur moyenne de **13.60%** par rapport au Deux-LSB.

3.4.2.2.Evaluation de la méthode de stéganographie basée sur le schéma LSB dans le domaine DCT

Dans la deuxième partie, une série d'expériences ont également été menées pour évaluer l'efficacité du schéma d'insertion basée sur la transformé DCT et les résultats sont présentés dans la figure 3.9.

Selon la figure 3.9, il est clair que le schéma d'insertion basé sur la transformé DCT donne de meilleurs résultats en termes de PSNR et Ec pour le schéma d'insertion Un-LSB. Dans ce cas, la distorsion (PSNR) des images stéganographiées 'Peppers' et 'Nature' peut atteindre des PSNR de **46.38%** et **39.19%**.

Alors que la méthode stéganographiée basés sur la modification de deux bits fonctionne avec des PSNR de **25.47 %** et de **19.85 %** pour les images ‘Peppers’ et ‘Nature’, respectivement.

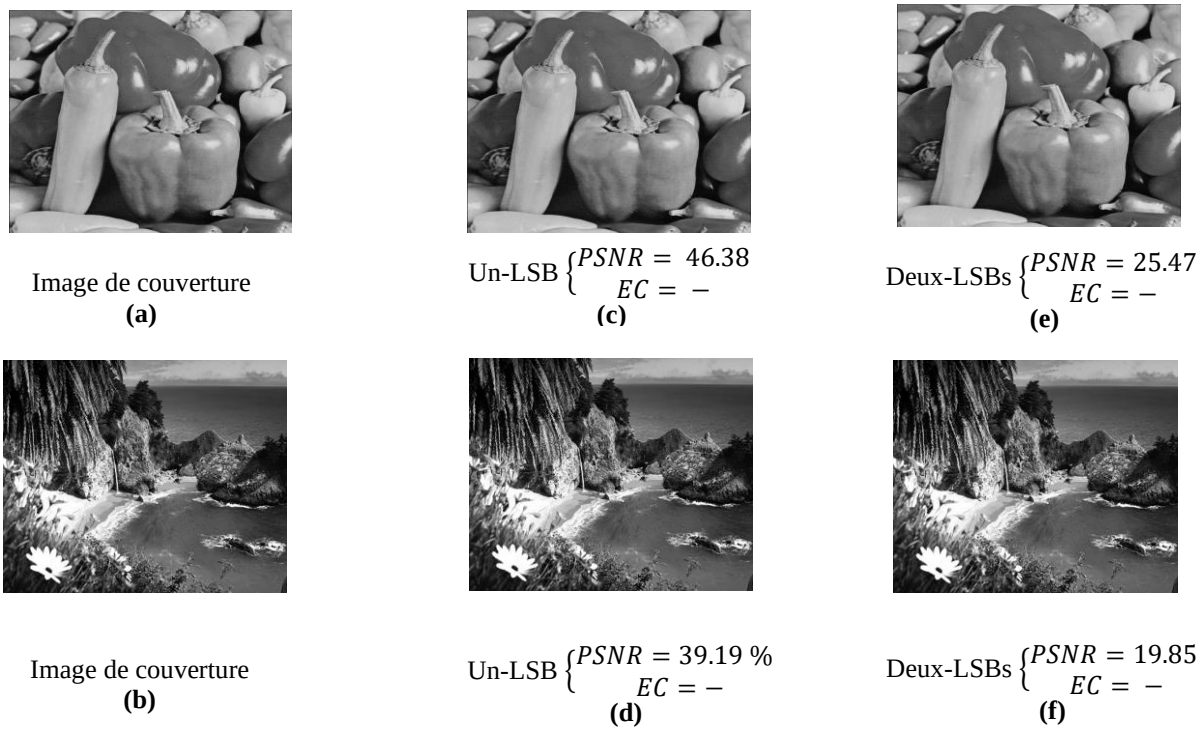

Fig.3.9 : Comparaison visuelle des images ‘Peppers' et Nature, et ses images stéganographiées avec un taux d’insertion de 50% (a-b) images de couverture, (c-d) images stéganographiées avec le schéma Un-LSB et (e-f) images stéganographiées avec le schéma Deux-LSB basée sur la transformée DCT.

3.4.3. Etude comparative

Dans cette section, les schémas stéganographique proposés sont comparés aux schémas stéganographique standard à savoir les techniques 1LSB et 2LSB. Ainsi, le tableau 3.1 montre les performances obtenues pour les deux schémas en termes de PSNR obtenus sur 100 images de taille 256×256 de type Bmp. De ce tableau, on peut lire que les résultats obtenus des deux schémas proposés sont très satisfaisants pour tous les taux d’insertion.

L'inconvénient majeur des schémas proposés est qu'ils dépendent des emplacements sélectionnés pour l'insertion. Pratiquement, une technique parfaite devrait fournir peu de distorsion dans l'image stéganographiée (augmentation de PSNR) et avec très peu de changeant de LSBs dans l'image de couverture (diminution d'EC) qui est le but de notre travail.

	Taux d'insertion (%)		20%	40%	60%	80%
Schémas Standard	1LSB	PSNR	54.23	47.89	39.87	24.68
	2LSB		42.45	37.30	28.85	22.72
Schémas proposés	Un-LSB		66.54	54.24	44.86	32.35
	Deux-LSB		48.54	39.87	35.66	24 .64

Table 3.1 : Comparaison entre les deux méthodes de stéganographie proposées

3.5. Conclusion

Afin d'avoir les meilleures positions des pixels dans lesquelles le message secret est inséré, nous avons proposé dans le présent chapitre deux nouveaux schémas stéganographique basés sur répartition des pixels en *n* groupes. Nos nouveaux travaux visent à améliorer l'efficacité d'insertion, c'est-à-dire, sélectionner les valeurs de pixels de l'image de couverture appropriées qui optimisent le taux des changements et la distorsion visuelle.

Les deux schémas proposés sont appliqués aux deux schémas stéganographique standard à savoir la technique 1LSB et 2LSB. Les résultats expérimentaux montrent les performances obtenues pour les deux schémas, en tenant compte l'optimisation de la distorsion entre les images de couverture et stéganographiée (PSNR) et l'optimisation du taux de changement (EC). Nous notons que les deux scénarios proposés peuvent être appliqués aux schémas d'insertion LSB dans le domaine spatial afin d'améliorer leurs performances.

Conclusion Générale

Dans ce manuscrit, deux nouveaux schémas d'insertion dans les images, dans le domaine spatial et fréquentiel, sont proposées. Comme il est indiqué dans ce manuscrit, dans la plupart des schémas stéganographiques proposés, l'étape de sélection des positions de pixels utilisée pour l'insertion de données est principalement déterminée par un pseudo générateur des nombres aléatoire (PRNG) sans tenir compte de la relation entre le contenu de l'image et le message secret à insérer, ce qui signifie que les régions uniformes peuvent être utilisées par une telle sélection aléatoire. Afin de minimiser le taux des changements affecté par l'insertion et la distorsion visuel dans les images de couverture, nous avons proposé deux schémas de sélection des positions de pixels pour la dissimulation de données, qui peuvent insérer efficacement les données dans les meilleures régions selon les critères d'évaluation des méthodes stéganographiques à savoir le PSNR et EC. Les résultats expérimentaux obtenus à l'aide de 100 images montrent que la distorsion visuelle et le taux des changements dans les images de couverture sont considérablement améliorés par rapport aux schémas d'insertion standard LSB et 2LSB. En outre, nos schémas proposés peuvent être appliqués à d'autres méthodes stéganographiques, telles que la stéganographie dans les fichiers audio et vidéo dans les deux domaines spatial et fréquentiel.

Pour plus d'amélioration, nous prévoyons dans notre futur travail d'utiliser d'abord des systèmes chaotiques tels que la carte de tente, l'attracteur Lorenz et l'attracteur de Rösler et l'utilisation d'autres techniques d'optimisation telles que l'optimisation des colonies de fourmis (ACO).

Bibliographie

1. Barbier J., Analyse de Canaux de Communication dans un Contexte non Coopératif, Thèse pour obtenir le grade de docteur, ESAT - Laboratoire de Virologie et Cryptologie, B.P. 18, 35 998 Rennes Cedex, (2007).

2. **Laimeche L.**, Stéganalyse universelle basée sue les statistiques d'ordre supérieur, Thèse pour obtenir le grade de docteur, LAMIS - Laboratoire de Mathématiques, Informatique et Systèmes, (2018).

3. F.A.P Peticolas, R.J. Anderson and M.G. Kuhn, Information Hiding – A Survey, in proceeding of IEEE, pp. 1062-1078, (1999).

4. Dentand J. D., Daehne P., (2005), stéganographie, Thèse pour obtenir le grade de docteur, Haute École de Gestion de Genève (HEG-GE).

5. Fridrich, J., (2009), Steganography in Digital Media : Principles, Algorithms, and Applications, Cambridge University Press, New York, NY, USA, pp: 2, 13, 16,17, 20, 21, 27 et 60.

6. Chan C.K. and Cheng L.M., (2004), Hiding Data in Images by Simple LSB Substitution. Pattern Recognition, 37 (3) : 469-474.

7. Ljupce Nikolov, Stéganographie : Détection de messages cachés, Haute Ecole Spécialisé de Suisse occidentale (HES.SO), 2008.

8. Frédéric Raynal, Etude d'Outils pour la Dissimulation d'Information, Thèse de doctorat, Université paris XI, 2002.

9. Fridrich J. and Kodovsky J., (2013), Steganalysis of LSB replacement using parity-aware features. In Information Hiding, pp: 31-45, Springer.

10. Christian Rey, Tatouage d'Image : Gain en Robustesse et Intégrité des Images, Thèse pour obtenir le grade de docteur, Université d'Avignon, 2003.

11. Jean-Pierre CLUTIER, Cryptographie et certification, Travail de diplôme, Conservatoire National Des Arts et Métiers (CNAM) ,2002.

12. Gou H. and Wu M., (2007), Improving Embedding Payload in Binary Images with Super-Pixels. ICIP, 3 (1): 277–280.

13. Ker, A. D., (2005), Resampling and the detection of LSB matching in color bitmaps, International journal of Electronic Imaging.

14. Zhang X., Zhang W., and Wang S, (2007), Efficient Double-Layered Steganographic Embedding, Electronics Letter, 43 (8) : 482–483.

15. Holub, V. and Fridrich, J., (2013), *Digital Image Steganography Using Universal Distortion*. In Proceedings of the first ACM workshop on Information hiding and multimedia security, IH & MMSec '13, 59-68, Montpellier, France.

16. Ker, A. D. "Steganalysis of Embedding in Two Least-Significant Bits". IEEE Transactions on Information Forensics and Security, vol. 2, N° 1, pp. 46-54, 2007.

17. Khalid O., Aziz B. "Single-mismatch 2LSB embedding steganography". IEEE international symposium on signal processing and information technology (ISSPIT), pp. 283-286.

18. Fridrich J., Goljan M., and Soukal D. : "Efficient Wet Paper Codes". In Proc. Information Hiding Workshop, Springer LNCS, pp. 204–218, 2005.

19. Fridrich J., Goljan M., Lisonek P. and Soukal D., "Writing on wet paper", IEEE Trans. Signal Processing., vol. 53, N°. 10, pp. 3923–3935, 2005.

20. Fridrich J., Goljan M., and Soukal D. : "Wet Paper Codes with Improved Embedding Efficiency". IEEE Translation. Information Forensics and Security, vol. 1, N° 1, pp. 102–110, 2006.

21. Jung K.H. and Yoo K.Y. (2015), *High-capacity index based data hiding method*, Multimedia Tools and Applications, 74 (6): 2179–2193.

22. Kodovsky J. and Fridrich J., (2008), *Influence of embedding strategies on security of steganographic methods in the JPEG domain*. In Proceedings SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 6819: 21–23, San Jose, CA, January 27–31.

23. **Laimeche L.**, Merouani H.F. (2012), *A novel Technique of Steganalysis in Uncompressed Image through Zipf's Law*, In International Journal of Computer Applications, 40 (6): 0975-8887.

24. Upham D., (1992), *Jpeg-Jsteg*, ftp://ftp.funet.fi/pub/crypt/steganography, 1992.

25. Westfeld A. and Pfitzmann A., (2001), *F5-A Steganographic Algorithm*, Information Hiding : pp. 289-302.

26. Provos N., (1998), Universal steganography Outguess, http: //wwww.outguess.org/.

27. J. Bai, C.-C. Chang, T.-S. Nguyen, C. Zhu, et Y. Liu, « Un algorithme stéganographique à charge utile élevée basé sur le bord détection », affiche, vol. 46, p. 42-51, janvier 2017.

28. B. Debnath, J. C. Das et D. De, « Reversiblelogic-based image stéganographie utilisant des automates cellulaires à points quantiques pour sécuriser nano communication, ”IET Circuits Devices Syst., vol. 11, non. 1, pp. 58 à 67, 2017.

29. S. E. Jero et P. Ramu, « Stéganographie ECG basée sur les curvelets pour les données sécurité », Electron. Lett., Vol. 52, non. 4, pp. 283-285, 2016.