République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieure et de la Recherche Scientifique

Université Ahmed Draia - Adrar

Faculté des Sciences et de la Technologie

Département des Mathématiques et Informatique

Mémoire de fin d'étude, en vue de l'obtention du diplôme de master en informatique

Option : Systèmes intelligents

Thème

Sécurité de l'information par stéganographie

Préparé par :

DAOUALI Somia

OULHADJ Fatima

Encadreur :

Mr. OUAHAB Abdelwhab

Année universitaire : 2019/2020

Dédicace

Je Dédie mon travail a....

A ma maman »mezaouli fatima » qui m'a soutenu et encouragé durant ces années d'études.

Qu'elle trouve ici le témoignage de ma profonde reconnaissance.

A mes frères, mes grands-parents et Ceux qui ont partagé avec moi tous les moments d'émotion lors de la réalisation de ce travail. Ils m'ont chaleureusement supporté et encouragé tout au long de mon parcours.

A ma famille, mes proches et à ceux qui me donnent de l'amour et de la vivacité.

A tous mes amis qui m'ont toujours encouragé, et à qui je souhaite plus de succès.

A tous ceux que j'aime

Daouali Somia

Remerciement

On remercie dieu le tout puissant de nous avoir donné la santé et la volonté d'entamer et de terminer ce mémoire.

Tout d'abord, ce travail ne serait pas aussi riche et n'aurait pas pu avoir le jour sans l'aide et l'encadrement de **Mr. OUAHAB Abdelwhab**, on le

Remercie pour la qualité de son encadrement exceptionnel, pour sa patience, sa rigueur et sa disponibilité durant notre préparation de ce mémoire.

Nous remercions les membres du jury d'avoir pris la peine de lire et de juger ce travail.

Nos remerciements s'adressent également à tous nos professeurs de la spécialité pour leur aide.

Nos profonds remerciements vont également à toutes les personnes qui nous ont aidé et soutenu de prés ou de loin.

Table des matières

Y

Y

Table of Contents

Table de figure

Liste des tableaux

Abréviations

BMP: Bit Map

DCT : Discrète Cosine Transform

JPEG : Joint Photographie Expert Group

LSB: Least Significant Bit

MSB: Most Significant Bit

PGM: Portable GrayMap

PNSR: Peak Signal to Noise Ration

RGB: Rouge, Green, Bleu

TIFF: Tagged Image File Format

Introduction Générale

L'image est un support d'information très important, et comme on dit : une image vaut plus que mille mots. Vu l'importance de l'image, et la grande quantité d'information qu'elle peut contenir, le monde s'intéresse de plus en plus à l'image et tends vers l'universalisation de son utilisation. En effet, l'image a touché plusieurs domaines de notre vie : la médecine, la météo, la télécommunication, la cartographie, la géologie, etc. Avec le développement de l'outil informatique, plusieurs techniques de traitement des images ont vu le jour [1].

De nos jours, avec le développement des supports numériques et des réseaux de communication, ceci a facilité le partage et le transfert de données numériques, introduisant ainsi de nouvelles formes de piratage de documents et de nouveaux défis de sécurité à relever.

De plus, le problème de la protection du contenu d'un support numérique multimédia ne connait pas encore de solutions satisfaisantes. Il est devenu aisé de modifier ou de reproduire un média et même de revendiquer ses droits d'exploitation.

Afin de diminuer la copie des œuvres multimédias et assurer la confidentialité d'une transmission, des nouvelles méthodes ont été développées. Il s'agit des méthodes de dissimulation d'information.

La dissimulation d'information cherche à cacher une information de n'importe qu'elle type dans un autre support qui peut être de type texte, image, audio ou vidéo. Les applications de la dissimulation se distinguent par leurs objectifs. En stéganographie, le but est de cacher un message dans un support numérique pour permettre à des partenaires de communiquer d'une façon secrète, le support n'a aucun lien avec le message à envoyer [2].

La stéganographie possède trois grandes propriétés qui caractérisent son utilisation : la robustesse, la sécurité et la capacité. La robustesse assure que l'information secrète ne peut pas être détruite et sans dégrader fortement l'image. La sécurité vise à ce que l'image stégo ne soit pas perturbée par l'information secrète insérée. La capacité définit la quantité d'information qui peut être intégrée dans le support sans détérioration visible. Ces trois caractéristiques sont en relation étroite et inverse [3].

Il existe des techniques permettant de découvrir le média stéganographie : c'est le cas de la stéganalyse appelée aussi l'analyse stéganographique [2].

Dans notre projet, nous allons présenter une méthode de dissimulation d'information « La stéganographie » pour cacher un message dans une image, et pour cela nous avons utilisé, proposé, testé et comparer trois algorithmes.

L'objectif de notre projet consiste à insérer un image dans une image et que la perception humaine ne peut pas détecter les petites modifications introduites dans l'image qui est destinée à renfermer ce image.

Afin de réaliser ces objectifs, le mémoire est structuré autour de trois chapitres

Le chapitre 1, est réservé à des généralités sur la stéganographie , nous allons Présenter quelques notions de base sur la sécurité d'information ,Certains Propriétés des systèmes de stéganographie, les Domaines de stéganographie et La stéganalyse.

Le chapitre 2, Nous nous concentrons, dans ce chapitre, sur les Méthodes de stéganographie usuelles en passant par le principe de cette méthode.

Le chapitre 3, Dans ce chapitre nous avons présenté l'implémentation de technique LSB et LSB-MOD sur la stéganographie pour les différents algorithmes proposés et à réaliser dans l'environnement MATLAB, et comparé les résultats obtenu par le PSNR. Finalement une conclusion générale est donnée pour synthétiser notre travail, et proposer des perspectives de recherche

Chapitre 1

La sécurité des informations,

La stéganographie et la stéganalyse.

Introduction.

Transmission sécurisée de l'information.

Propriétés des systèmes de stéganographie.

Domaines de stéganographie.

La stéganalyse.

Conclusion.

1 Chapitre 1 : La sécurité des informations, la stéganographie et la stéganalyse.

1.1 Introduction

Les avancées technologiques en informatique et télécommunications ont contribué soulever plusieurs problèmes liés à la sécurité de l'information.

Nous nous focalisons dans nos travaux sur la question de la sécurité de la transmission d'informations confidentielles sous forme numérique, basées principalement sur la stéganographie [3].

La stéganographie est l'art de dissimulation des informations, d'où elle cherche à insérer un message dans un contenu anodin qui peut être une image, une vidéo, ou un son [4], de tel sorte à prendre le processus de dissimulation indétectable. Autrement dit, l'objectif est de rendre difficile ou impossible la distinction entre un document original et un document modifié comportant le message secret [5]. Nous nous intéressons sur les images numériques car ce contenu est majoritairement utilisé lors des échanges numériques [4].

La stéganographie a également comme discipline la stéganalyse. Cette dernière a pour but de détecter la présence d'un message caché (secret). Ainsi, en stéganalyse l'objectif principal n'est pas d'extraire le message caché, mais plutôt de détecter sa présence [5].

Dans ce chapitre, nous allons voir quelques notions sur la sécurité de information, et allons détailler les notions de la stéganographie et stéganalyse.

1.2Transmission sécurisée de l'information

En ce qui concerne le transfert sécurisé d'informations, trois arts peuvent être identifiées: la cryptographie, la stéganographie et le tatouage. La cryptographie consiste en une écriture indéchiffrable d'un message ou d'une information (ainsi rendue secrète), la stéganographie va cacher un message dans un contenu pour qu'il soit, non seulement indéchiffrable, mais imperceptible. Quant au tatouage, La figure 1.1, donné par [6] résume les différentes techniques de la sécurité de l'information.

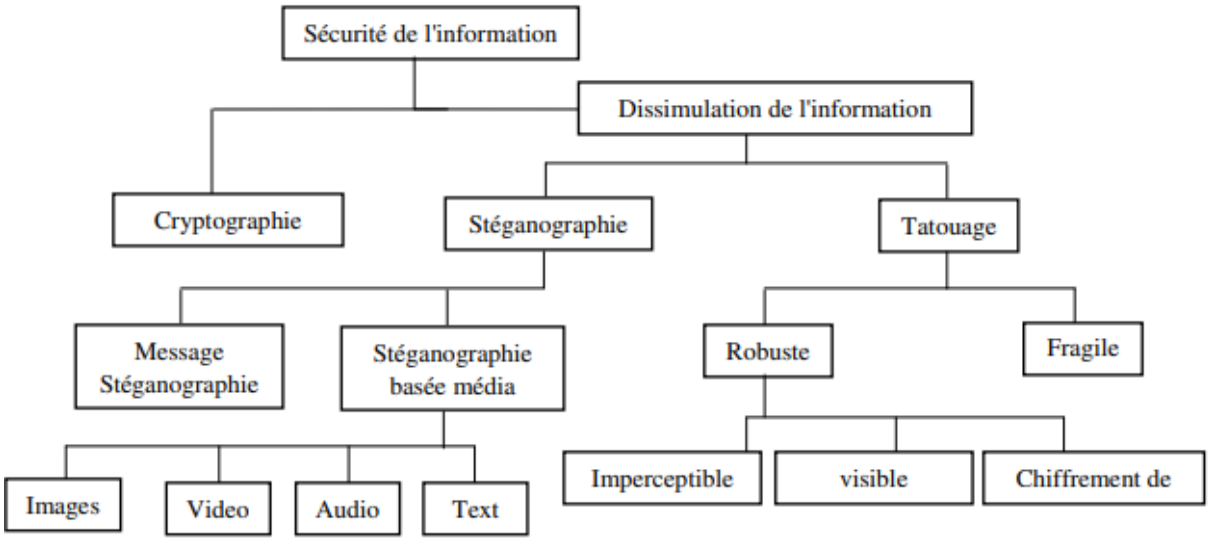


Figure 1.1 : Techniques de la sécurité de l'information

Selon la figure 1.1, trois méthodes principales traitent de la sécurité de l'information : la cryptographie, la stéganographie, et le tatouage numérique. Les deux derniers assurent la dissimulation de l'information. Nous nous rappelons ci-dessous les différentes notions utilisées dans les différentes techniques liées à la sécurité de l'information :

1.2.1 Cryptographie

La science d'écrire un message avec un code secret pour le garder en sécurité fait principalement d'algorithmes utilisant des clés secrètes du public.

1.2.2 Tatouage numérique

Le tatouage comprend deux types : le tatouage fragile et le tatouage robuste.

Le tatouage numérique fragile n'est utilisé que pour prouver l'authenticité des documents et

L'intégrité des données.

Le tatouage robuste est plus dur à contourner et doit résister à diverses attaques.

1.2.3 Stéganographie

La stéganographie est l'art de la communication secrète. Le but est de cacher un message secret dans un support inoffensif (image, vidéo, audio...) afin qu'il ne puisse pas être détecté (visuellement mais aussi statistiquement).

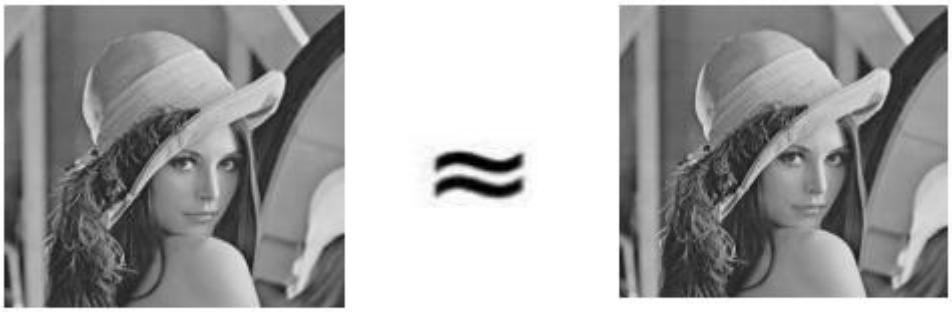


Image Hôte ≈ Image Stego

Figure 1.2

Il existe deux types de stéganographie :

- La sténographie linguistique,
- La stéganographie technique.

1.2.3.1Stéganographie linguistique

Consiste à modifier propriétés linguistiques d'un texte pour cacher l'information, elle est la plus faible par rapport à d'autres médias, Probablement parce qu'il est plus facile à modifier le Média non linguistique dans lequel le message secret ne peut pas être découvert par l'observateur.

Les différentes formes de la stéganographie linguistique sont :

- Sémagramme

La forme la plus connue en stéganographie linguistique est le sémagramme, Il fait que la stéganographie échappe complètement à l'observateur.

- Acrostiche

Ce processus permet aux données d'être transmises à travers les lettres initiales de chaque ligne d'un poème qui sont lues de haut en bas, formant un mot ou une phrase. Il a de nombreuses variantes (mot placé dans des versets ou des chapitres,...).

- Ponctuation

L'utilisation des points, des exposants et des virgules par les prisonniers de guerre Ils sont autorisés à transmettre des messages à leurs familles.

- Nulles

Les symboles subliminaux, également appelés nuls, consistent à marquer certaines lettres du texte d'une certaine marque (en perçant des aiguilles sur ou sous les lettres). Ensuite, il suffit de rassembler les lettres marquées pour former un mot.

- Insertion d'erreurs

Améliorer l'information par des erreurs ou des variations stylistiques dans le texte. Cependant, ces différentes opérations restent difficiles et chronophages à mettre en œuvre et partent rapidement Suspecté de la possibilité d'un message caché. Beaucoup ont été blâmés comme ça Appliquer pour limiter l'utilisation de ces techniques.

1.2.3.2 La stéganographie technique

La stéganographie combine toutes les techniques qui ne manipulent pas les mots. Les Cacher des informations techniques est intéressant car cela permet de cacher des données dans Plusieurs types de médias : audio, images et vidéos.

1.3 Propriétés des systèmes de stéganographie

1.3.1 Capacité

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. Dans le domaine spatial, pour une image numérique, la capacité d'insertion relative peut être exprimée en nombre de bits de message secret insérés par pixel (bpp). Dans le domaine fréquentiel

1.3.2 Sécurité

Toutes les exigences de sécurité pour les systèmes cryptographiques peuvent (doivent) également être considérées pour les systèmes de stéganographie. Cela signifie que la sécurité de l'algorithme de stéganographiene ne doit pas s'appuyer seulement sur l'algorithme, qui devrait être publique, mais sur le caractère secret de la clé. Dans la stéganographie, il ne devrait pas être possible de distinguer une image d'origine d'une image stego si la clé est inconnue. Par ailleurs, les modifications apportées sur l'image originale afin de pouvoir incorporer le message secret ne devrait pas modifier les propriétés statistiques de l'image. La technique qui étudie la sécurité des systèmes de stéganographie est la stéganalyse.

1.3.3 Robustesse

Elle quantifie la résistance du message dissimulé aux diverses attaques (transformations) apportées au médium stégo.

1.4 Domaines de stéganographie

La stéganographie est divisée en deux domaines, spatial et fréquentiel. [7], [8]

1.4.1 Domaine spatial

La stéganographie spatiale consiste à modifier des bits de pixels de l'image pour inclure les bits du message secret. La technique LSB est l'une des techniques la plus simple et la plus répandue.

1.4.2 Domaine fréquentiel

Le message est inséré dans les coefficients transformés de l'image, ce qui a pour offrir plus de durabilité contre les attaques.

La stéganographie fréquentielle est une technique de base pour cacher des informations confidentielles : à l'heure actuelle, la plupart des systèmes de stéganographie fonctionnent dans le domaine fréquentiel.

1.5 La stéganalyse :

Plusieurs études ont été menées pour révéler la présence de données ou Informations cachées à l'aide de l'algorithme de stéganographie [9, 10]. Ce type d'étude Elle constitue ce qu'on appelle la stéganographie ou analyse cryptique [10]. Compatible avec La double discipline de la stéganographie [9], donc l'analyse de la stéganographie représente Moyens mis en œuvre pour détecter l'existence d'une communication secrète [11].

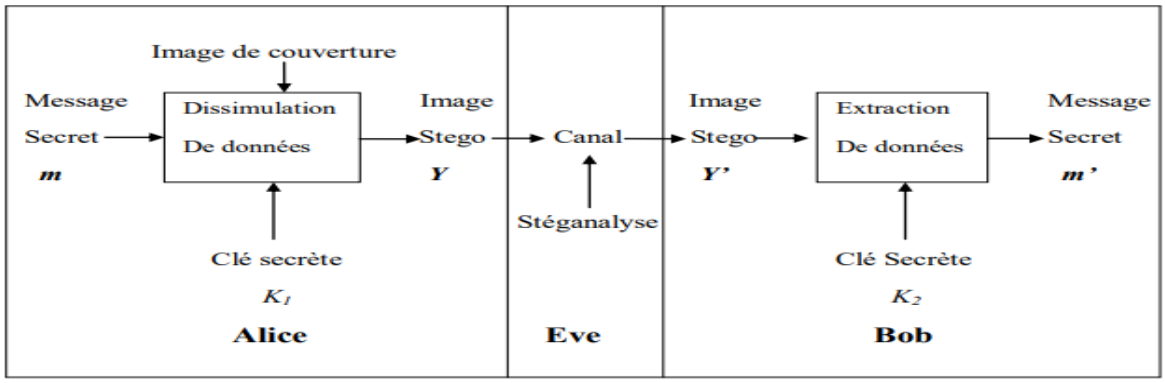


Figure 1.3 : problème des prisonniers [10].

1.6 Conclusion

Le travail présenté dans ce chapitre consiste à expliquer la sécurité d'informations, les Propriétés des systèmes de stéganographie, les Domaines de stéganographie et la stéganalyse.

Chapitre 02

Les différentes méthodes de stéganographie

Introduction.

Définition de stéganographie

Principe

Méthodes de stéganographie usuelles

Conclusion

2 Chapitre 02 : les différentes méthodes de stéganographie

2.1 Introduction

Les progrès technologiques de l'informatique et des télécommunications ont contribué à Il soulève de nombreux problèmes de sécurité de l'information. Nous nous concentrons dans nos travaux sur la question de la sécurité de la transmission des informations confidentielles sous forme numérique, en nous appuyant principalement sur la stéganographie [12].

Dans ce chapitre, nous allons parler sur la stéganographie, son principe et ses méthodes usuelles

2.2 Définition de stéganographie :

La stéganographie vient du mot Grec « stéganos » qui veut dire : « dissimulé » et de mot « graphien » signifiant : « écriture », littéralement on traduit par « écriture dissimulée » elle s'agit de cacher ou de cacher un message dans un autre, afin que le message caché ne soit pas être découvert que par la personne familière avec le processus de dissimulation.

Figure 2.1 : Exemple de stéganographie à l'aide de lait [13].

2.3 Principe :

Le principe de la stéganographie est de cacher un message secret, de taille importante dans une image, audio ou une vidéo, nommée média cover (ou original), d'où le média résultant appelé média stégo, Pas très différent des médias d'origine, du moins à l'œil humain Cela

veut dire que l'existence du message secret dans le média stégo est pratiquement indétectable. Le message secret peut être de texte brut, du texte chiffré ou une image.

La figure suivante 2.2 explique le principe de la stéganographie, dans le cas où le média original est une image et le message secret une image numérique.

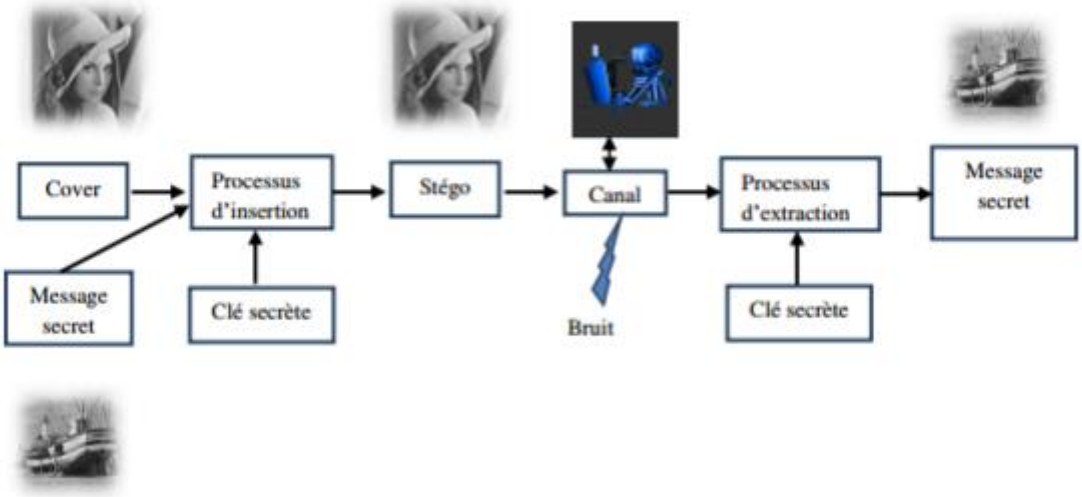


Figure 2.2 : principe de la stéganographie.

2.4 Méthodes de stéganographie usuelles

2.4.1 Insertion dans le domaine spatial

On focalise sur les images fixes non compressées qui peuvent représenter sous formats BMP, RAW, TIFF, PGM ... etc.

On peut définir l'image qui est une succession de n échantillons appelés pixels. Qui peut être noir et blanc L = {0,1}, ou on niveau de gris L = {0,...,255} ou en couleur L = $\{0,...,255\}^3$ Pour chaque canal de couleur, la valeur de chacun des pixels, xi ∈ F2 b = {0,...,2b −1} avec i = {1,..., n}, est représentée numériquement par un entier non-signé (positif ou nul) codé sur b bits, et donnée par :

$$x_i = \sum_{l=0}^{b-1} b_{i,l}\, 2^l,$$

Tel que $b_{i,l} \in \{0,1\}$ représente le l ème bit codant le pixel xi. Cette formulation mathématique met en évidence que le degré informatif des bits, pour le codage d'un pixel xi, est différent d'un plan à un autre. En effet, on peut constater que le premier bit $b_{i,0}$ est pondéré par 2^0, alors que

dernier bit $b_{i,\,b-1}$ est pondéré par 2^{b-1}. Cette propriété est à l'origine des premiers algorithmes stéganographiques de l'état de l'art, qui sont décrits ci-dessous.

La Figure 2.3 illustre les différents plans de bit d'une image en niveau de gris, en partant du bit de poids fort (MSB) jusqu'au bit de poids faible (LSB)

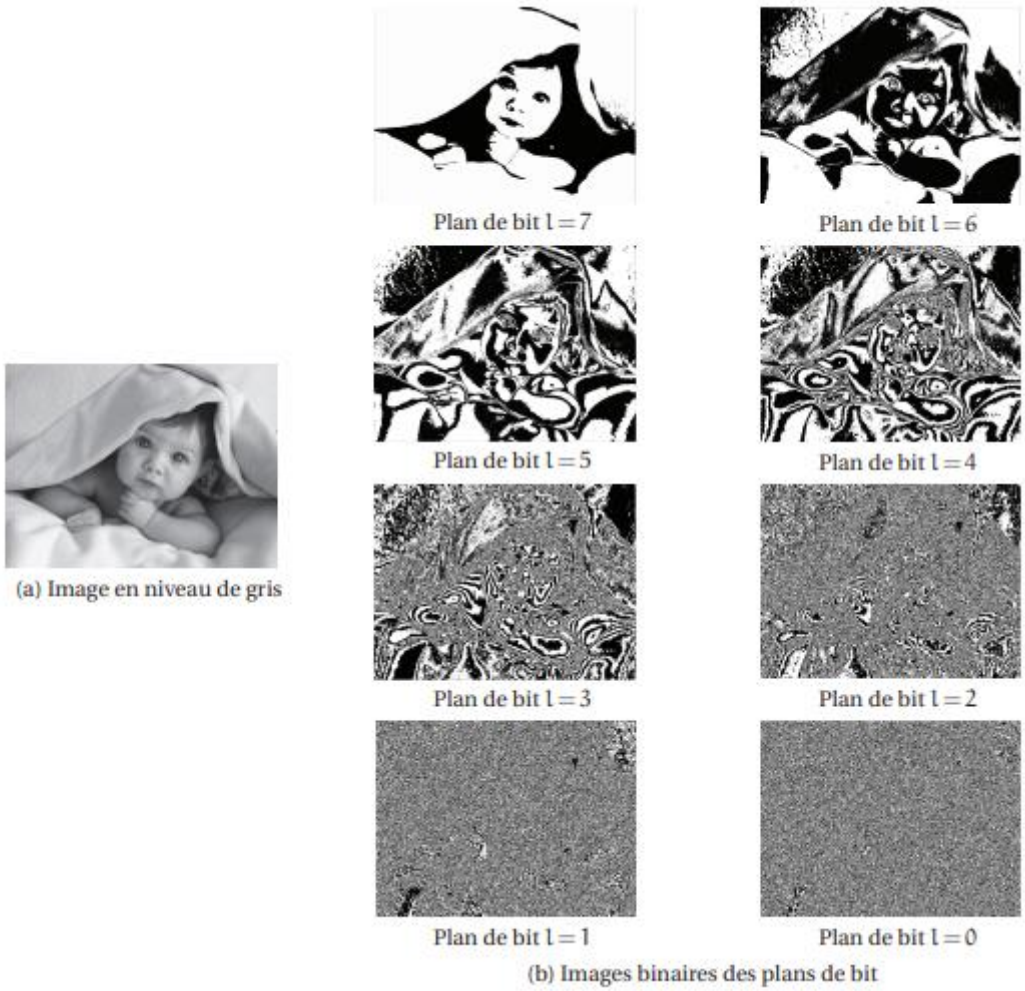


Figure 2.3 : Décomposition en plans de bits d'une image en niveaux de gris.

2.4.1.1 Stéganographie par substitution de LSB (LSB Replacement)

La technique de substitution des bits de poids faible (LSB Substitution) est la plus utilisé méthode de nos jours sur internet grâce à sa simplicité d'implémentation. Elle permet de remplacer les bits de poids faibles (les LSB) des pixels par les bits de message à insérer.

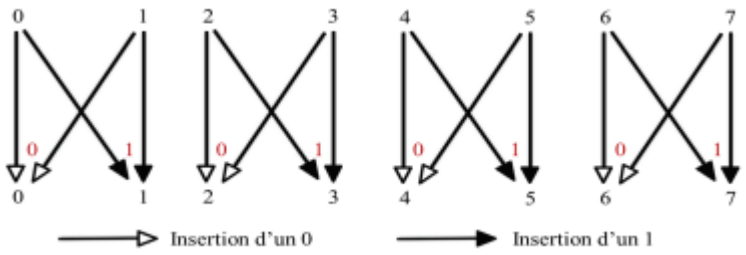


Figure 2.4 : Exemple de modification des LSB des pixels par la technique de substitution Pour rappel, les pixels pairs ont un LSB égal à 0, alors que les pixels impairs ont LSB égal à 1.

On peut observer sur l'exemple de la Figure 2.4, la substitution du LSB, pour un pixel donné, peut entrainer au plus une modification d'amplitude 1. Cette modification est imperceptible à l'œil nu. Par ailleurs, si nous observons les différents plans de bits d'une image en niveaux de gris, comme l'illustre la Figure 2.3, nous remarquons que les plans des bits de poids faibles contiennent moins d'information pertinente. Donc les plans LSB des pixels sont nettement moins structurés que ceux du poids fort (les MSB).

2.4.1.2 Stéganographie par correspondance de LSB (LSB Matching)

La stéganographie par correspondance des LSB, encore appelée LSB Matching ou ±1 embedding, est l'algorithme la très proche de la technique par substitution des LSB, elle permet d'améliorer la stéganographie par substitution des LSB. Cet algorithme d'insertion, qui est, insère également le message m ∈ {0,1}, m dans les LSB des pixels, mais en incrémentant ou décrémentant aléatoirement la valeur du pixel. Ici encore, le sens de parcours des pixels est habituellement choisi aléatoirement. La méthode de stéganographie par correspondance des LSB a été proposée pour la première fois par [14]. Le but de cette technique d'insertion est d'apporter une solution au problème des artefacts statistiques de la stéganographie par LSB substitution. En effet, contrairement à la stéganographie par substitution des LSB, la méthode de stéganographie par correspondance des LSB n'altère pas la distribution statistique du premier ordre du support hôte. Ainsi, toutes les attaques ciblés, spécifiquement dédiées à la détection de la stéganographie par substitution des LSB et n'utilisant qu'une statistique de 1 er-ordre, sont inefficaces pour détecter la méthode d'insertion par correspondance des LSB.

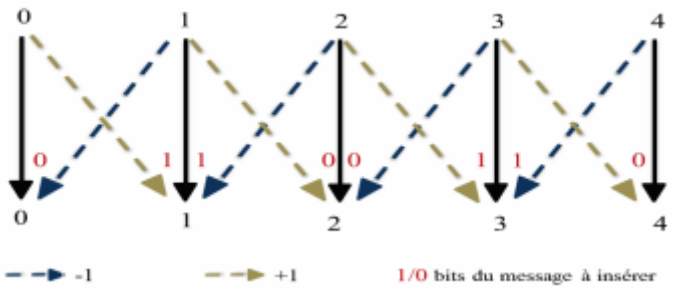


Figure 2.5 Exemple de modification des LSB des pixels par la technique de correspondance.

La Figure 2.5 illustre un exemple de modification des bits de poids faible des pixels, par la technique de correspondance.

2.4.2 Insertion dans le domaine transformé

En stéganographie, la dissimulation d'informations confidentielles dans un domaine transformé de l'image, est très couramment utilisée, car les images échangées sur Internet sont le plus souvent compressées avec pertes au format JPEG ou JFIF. Pour cela, des schémas sténographiques appropriés ont été développées pour ce type de format. Ces formats d'images, qui ils sont basés sur une transformation discrète, et ont des propriétés statistiques spécifiques.

Ne pas en tenir compte peut rendre le système de dissimulation détectable.

À y regarder de plus près, la plupart des méthodes de stéganographie qui opèrent dans un domaine transformé est des variantes des méthodes de stéganographie spatiale, qui ont été décrites précédemment [15]. Les algorithmes de stéganographie, classiquement utilisés pour les images JPEG, tels que F5 [16], Jsteg [17] ou Outguess [18], basé principalement sur la méthode d'insertion par modification des LSB. Pour ces algorithmes, la méthode de modification utilisée est appliquées 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.

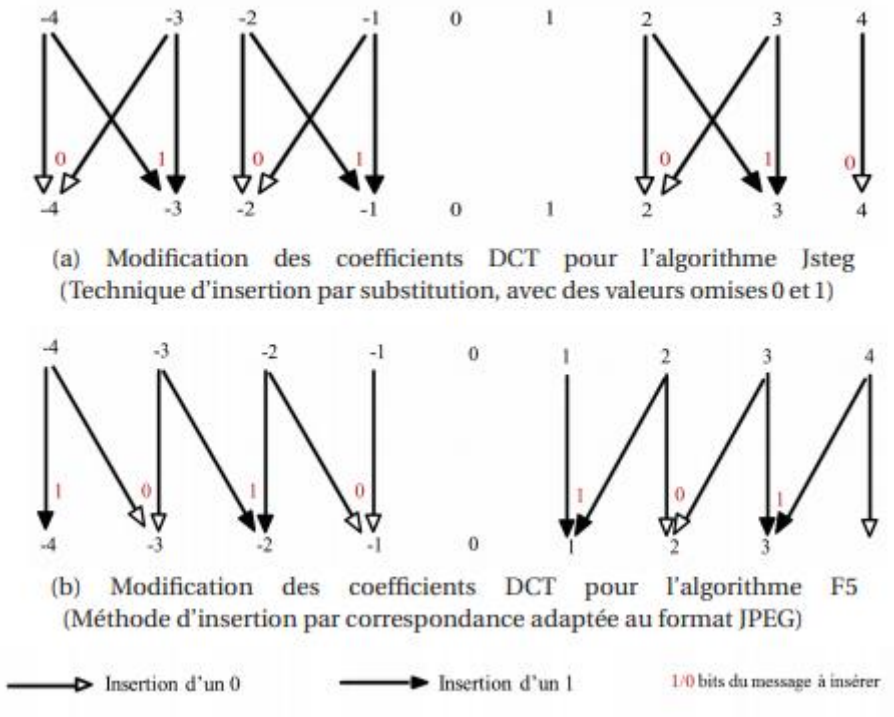


Figure 2.6 – Exemple de modification des coefficients DCT pour les algorithmes Jsteg et F5.

2.5 Conclusion

Dans ce chapitre nous avons expliqué le principe d'une stéganographie, et certaines Méthodes usuelles.

Chapitre 03

L’approche proposée et implémentation

Introduction.

Le choix de langage de programmation.

La Méthode LSB et la Méthode LSB MODULATION.

La méthode LSB.

La méthode LSB basée sur le pixel modulation.

Interfaces et déroulement de l’application principale.

Discussion des résultats trouvés.

Comparaison PSNR.

Conclusion

3 Chapitre 03 :L’approche proposée et implémentation

3.1 Introduction

La stéganographie est l'art de la dissimulation. Elle consiste à cacher un message au sein d'un autre message anodin, de sorte que l'ignore l'existence même du secret.

Dans ce chapitre, on va présenter, tester et comparer les algorithmes de steganographie LSB et LSB MODULISATION.

3.2 Le choix de langage de programmation

- MATLAB est un langage de haut niveau pour le calcul scientifique et technique.
- Environnement bureau pensé pour l'exploration itérative, la conception et la résolution de problèmes
- MATLAB propose un ensemble complet de fonctionnalités de Machine Learning et de statistiques, ainsi que des méthodes avancées telles que l'optimisation non-linéaire, l'identification de système et des milliers d'algorithmes prédéfinis pour le traitement d’image et de vidéo, la modélisation financière, la conception de systèmes de contrôle
- Traitement rapide de grands jeux de données.
- Applications dédiées à l'ajustement de courbes, la classification de données, l'analyse de signaux et bien d'autres tâches spécialisées.
- Boîtes à outils additionnelles conçues pour répondre à de nombreux besoins spécifiques aux ingénieurs et aux scientifiques.
- Outils permettant la création d'applications avec interface utilisateur personnalisée.
- Interfaces vers C, C++, FORTRAN, Java™, COM, et Microsoft® Excel®.
- Options de déploiement libre de droits permettant de partager des programmes MATLAB avec les utilisateurs finaux [59].

Les caractéristiques de la machine utilisée dans la simulation sont résumées dans le tableau suivant :

Hardware	Caractéristiques
Processeur	Intel(R) Core(TM) i3-2328M CPU @ 2.20GHz, 2.20GHz.
Mémoire (RAM)	4.00 Go.
Opération système	Microsoft Windows8.1 Professional 64 bits.

Tableau 3.1 : Caractéristiques matérielles.

3.3La Méthode LSB La Méthode LSB MODULATION

3.3.1Introduction

L'utilisation du signal numérique multimédia est devenue très populaire au cours de la dernière décennie en raison de la propagation du sans fil.

Services basés sur Internet tels que l'introduction des systèmes de communication mobile de quatrième génération, l'utilisateur peut transférer des données jusqu'à 1 Gbps [19]. En raison de la disponibilité d'outils d'édition à faible coût, les données numériques peuvent être facilement copiées, modifiés et retransmis dans le réseau par tout utilisateur. Pour accompagner efficacement la croissance de la multimédia communication, il est essentiel de développer des outils qui protègent et authentifient les informations numériques. Dans cette contribution, nous présentons un nouveau schéma d'intégration basé sur la technique LSB. [20] Si la valeur du pixel d'une image est modifiée par une valeur de «1», il n'affecte pas l'apparence de l'image. Cette idée nous aide à cacher des données dans une image.

3.3.2 La méthode LSB

3.3.2.1 Description de la Méthode LSB, ou méthode de bit de poids faible.

La méthode d'insertion de données sur les bits de poids faible ou LSB est la technique de Stéganographie d'image la plus connue. Son principe est d'utiliser le dernier bit de chaque nombre définissant l'intensité d'une couleur primaire d'un pixel, pour les données à dissimulées (figure 3.1). Ainsi, trois bits peuvent être encodés dans chaque pixel, et la différence de couleur obtenue est imperceptible pour l'œil [21].

Dans le cas d'une image non compressée codée sur 24 bits, chaque pixel est décrit par trois octets.
Pour dissimuler la chaîne de bits, on utilise le bit de poids faible de chaque octet

(00100111 11101001 11001000)		(00100111 11101000 11001000)
(00100111 11001000 11101001)	+ **10000011** =	(00100110 11001000 11101000)
(11001000 00100111 11101001)		(11001000 00100111 11101001)

Figure 3. 1:Insertion dans les bits de poids faible.

Les changements des bits de poids faible (de 0 à 1 ou de 1 à 0) sont totalement imperceptibles pour l'œil puisqu'il n'est modifié que d'un point.

3.3.2.2 Architecture de la méthode LSB

Il y a deux opérations :

- Génération d'une image stéganographie

Ce schéma représente la génération d'une image steganographie à partir de deux images RGB de type quelconque utilisant la méthode LSB qui est basée à la combinaison des bits de poids fort de la première image et les de poids faible de la deuxième dans chaque couche R, G, B .Cette combinaison peut être appliqué après la conversion en binaire de chaque bit -après la combinaison, ces bits doivent convertir en décimale pour avoir l'image résultat qui est l'image stéganographie(voir la figure 3.2)

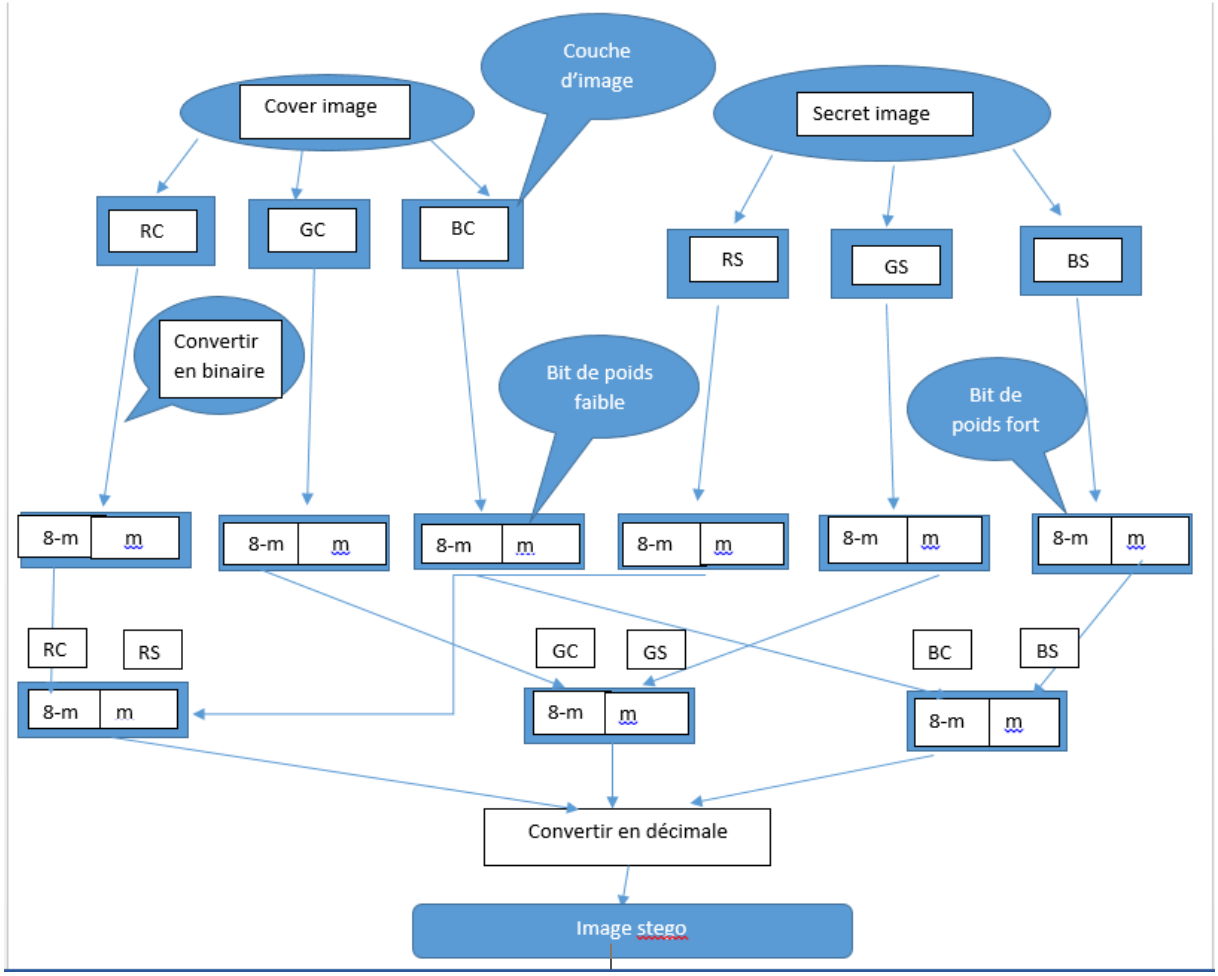


Figure 3. 2:architecture LSB.

- Extraction d'une image secrète

La phase d'extraction d'une image secrètes s'applique après la conversion en binaire. Elle consiste à diviser en deux partiesles bits d'une image stéganographie en bits de poids fort qui appartient à la première image et autre en poids faible qui appartient à la deuxième image.

On remplit le reste de bits par zéros et on convertit les bits résultats en décimale pour formuler l'image secrète et l'image couver.

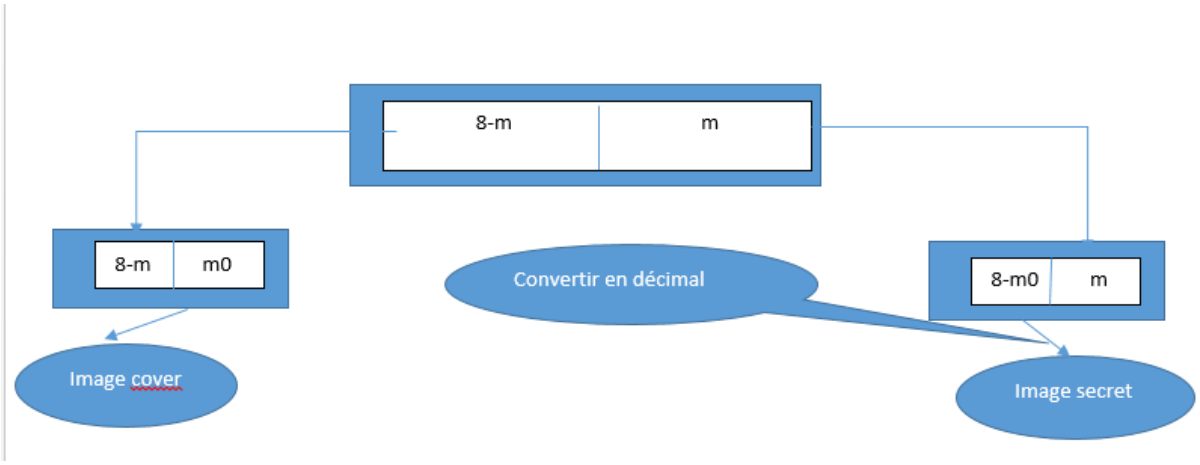


Figure 3. 3:architecture LSB inverse.

3.3.3 La méthode LSB basée sur le pixel modulation

3.3.3.1 Architecture de la méthode LSB Modulation

Il y a deux opérations :

- Génération de l'image steganographie

Ce schéma représente la génération d'une image steganographie à partir de deux images RGB de type quelconque utilisant la méthode LSB Modulation qui est basée sur la combinaison des pixels de poids fort de la première image et les bits de poids faible de la deuxième dans chaque couche R, G, B. Cette combinaison peut être appliqué après la conversion en binaire de chaque pixel -après la combinaison, ces pixels doivent convertir en décimale pour avoir l'image résultat qui est l'image steganographie (voir la figure 3.4).

Avant d'appliquer la conversion de l'image originale en binaire, On divise chaque pixels sur la valeur n pour réduire le nombre de bits demandés pour la représentation en binaire chaque valeur. La valeur est calculée par la formule :

$$n = 2^{8-m}$$

Tel que m représente le nombre de bits demandée pour coder l'image secrètes.

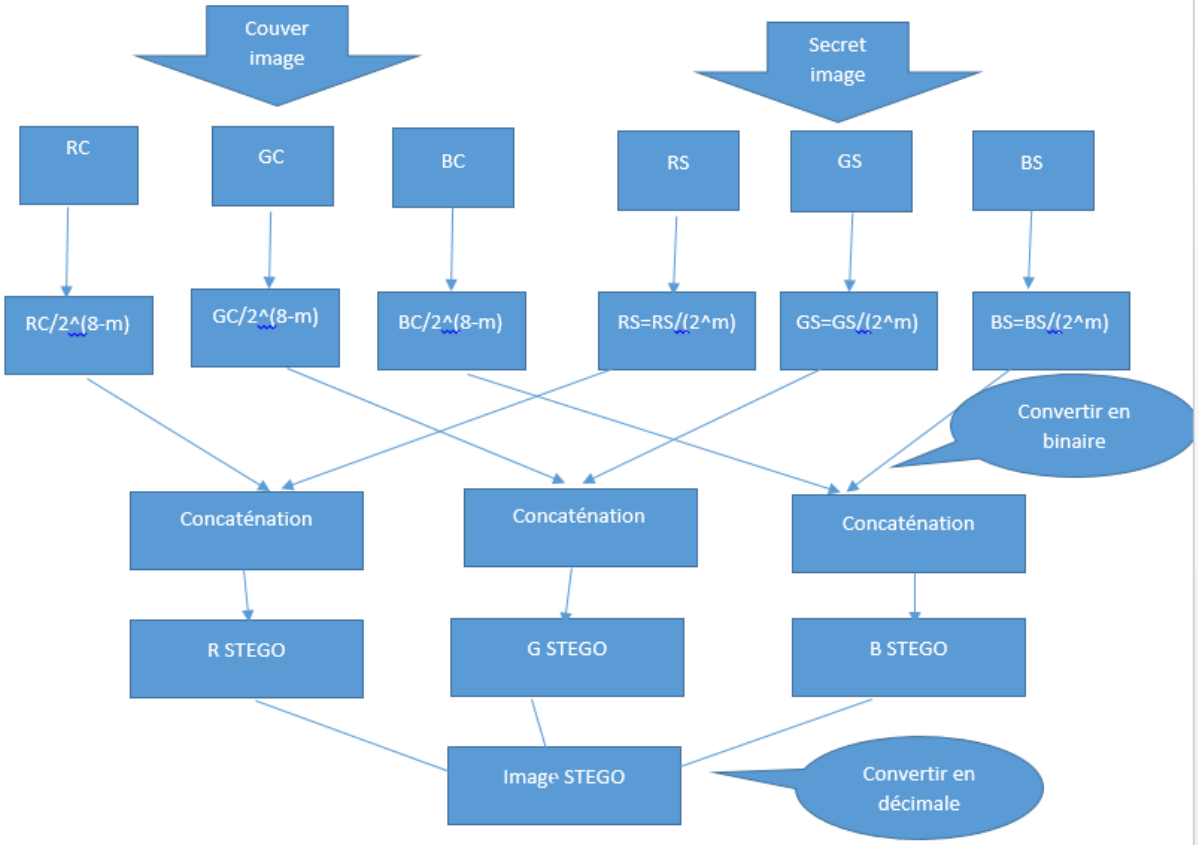


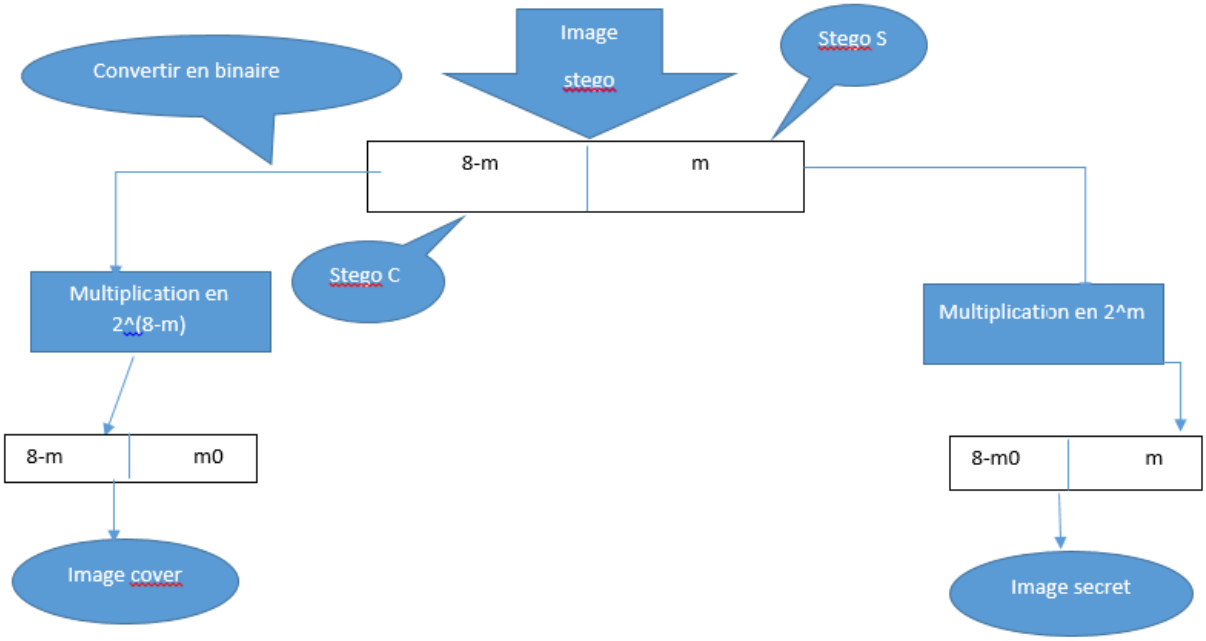
Figure 3. 4 : architecture LSB modulation.

- L'extraction d'une image secrète

La phase d'extraction d'une image secrètes s'applique après la conversion en binaire. Elle consiste à diviser en deux parties les pixels d'une image steganographie en pixels de poids fort qui appartient à la première image et autre en poids faible qui appartient à la deuxième image.

On applique une multiplication en 2^ (8-m) ce qui concerne la première image et en 2^m ce qui concerne la deuxième.

On continue le reste de bitsen zéros et les convertir en décimale pour formuler l'image secret et l'image couver.



.

Figure3.5: architecture LSB-modulation inverse.

Tel que :

m est le nombre de bits d'une message image qui peut cacher dans la couvre image.

3.4Interfaces et déroulement de l'application principale.

3.4.1Interface de Sélection

Cette interface donne le choix de la méthode souhaitée.

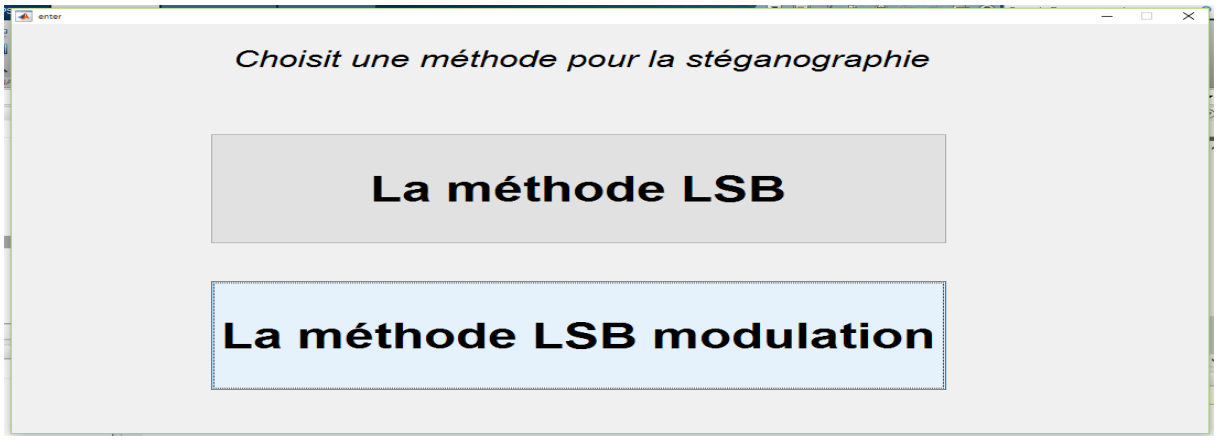


Figure 3. 6:les méthodes souhaitables de stéganographie.

3.4.2 Interface de LSB méthode

Cette interface est utilisée pour appliquer la méthode LSB.

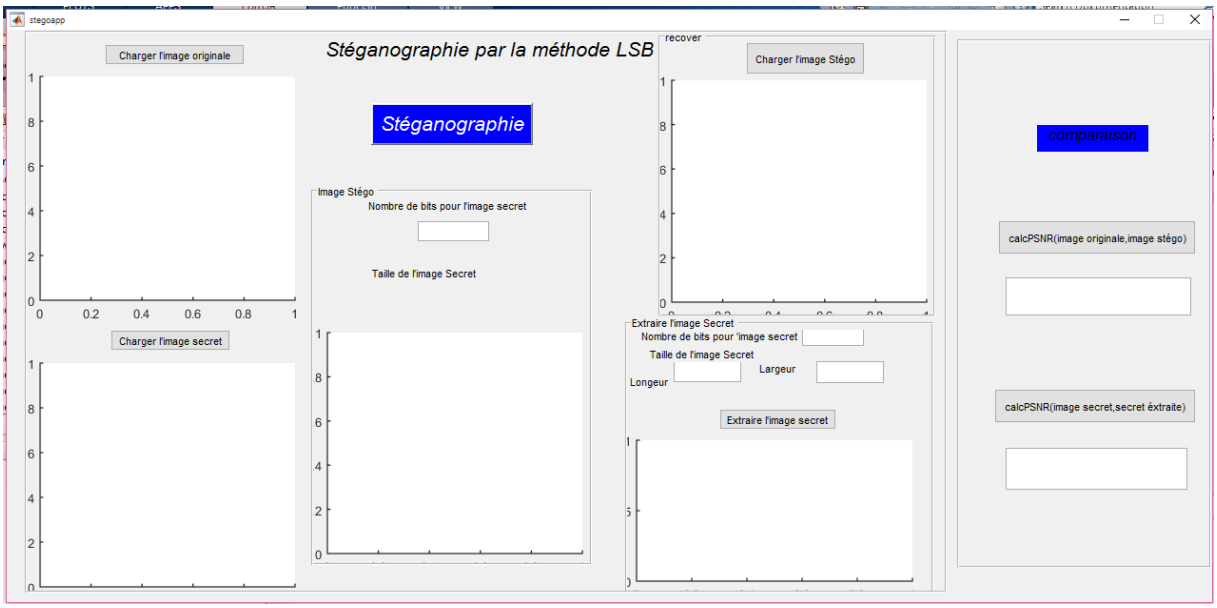


Figure 3.7:Interface de la méthode LSB.

Tel que :

- Bouton charger l'image originale : offre la possibilité de choisir l'image considérée image originale à partir du même fichier d'application.
- Bouton charger l'image secret : offre la possibilité de choisir l'image considérée image secret à partir du même fichier d'application.
- Bouton stéganographie : permet d'appliquer le principe de LSB entre les deux images et donne comme résultat l'image stégo qui sera préservé dans le même fichier d'application

- Bouton charger l'image stégo : permet de charger l'image stégo
- Bouton extraire l'image secret : permet d'extraire l'image secret de l'image stego
- Bouton calcPSNR(image originale,image stego) :donner la valeur de rapport signal sur bruit en crête entre image originale et image stego
- Bouton calcPSNR(image secret,secret extraite) :donner la valeur de rapport signal sur bruit en crête entre image secret et secret extraite

3.4.3 Interface de la LSB MOD méthode

Cette interface consiste à appliquer la méthode LSB MOD entre deux images.

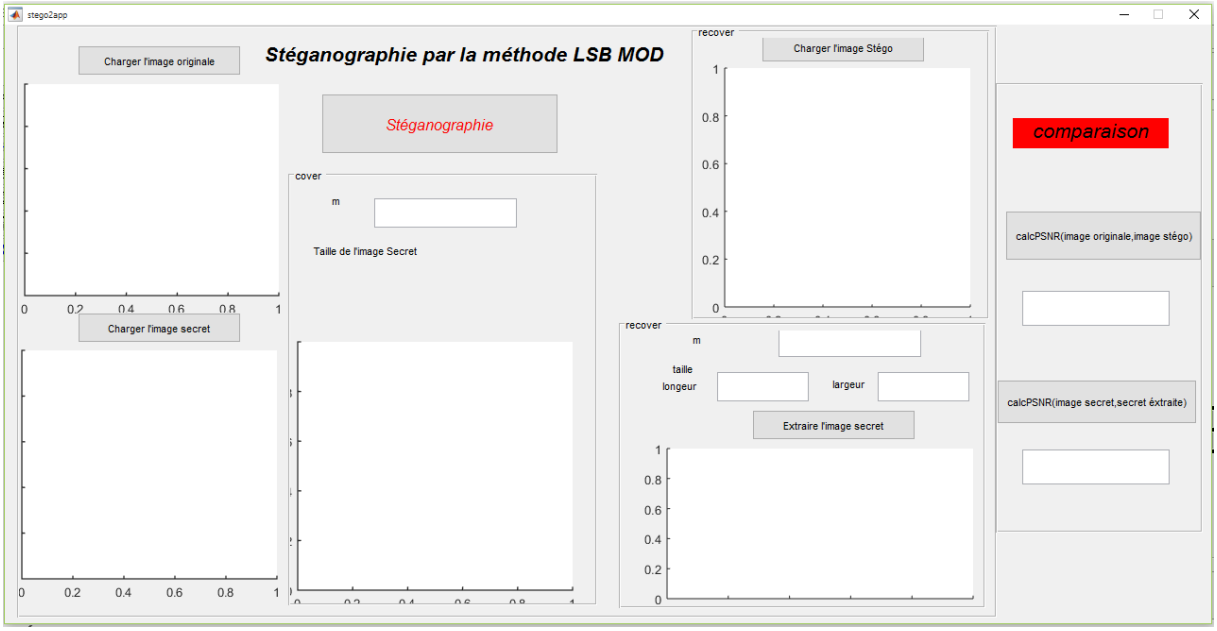


Figure 3. 8:Interface de la méthode LSB MOD.

Tel que :

- Bouton charger l'image originale : offre la possibilité de choisir l'image considérée image originale à partir du même fichier d'application.
- Bouton charger l'image secret : offre la possibilité de choisir l'image considérée image secret à partir du même fichier d'application.
- Bouton stéganographie : permet d'appliquer le principe de LSB MOD entre les deux images et donne comme résultat l'image stégo qui sera préservé dans le même fichier d'application
- Bouton charger l'image stégo : permet de charger l'image stégo
- Bouton extraire l'image secret : permet d'extraire l'image secret de l'image stego

- Bouton calcPSNR(image originale,image stego) :donner la valeur de rapport signal sur bruit en crête entre image originale et image stego
- Bouton calcPSNR(image secret,secret extraite) :donner la valeur de rapport signal sur bruit entre image secrète et une image extraite .3.5 Discussion des résultats trouvés.

3.5.1 Méthode LSB

Après insérer les deux images originales et les images secrètes et appliquer la méthode LSB sur les deux images, on a comme résultat l’image steganographie et l’image secrète extraite. On peut observer que l’image originale et l’image stéganographie sont presque le même mais l’image secrète et l’image secrète extraite sont diffèrentes en terme de couleur.

Figure 3. 9:Image originale de la méthode LSB.

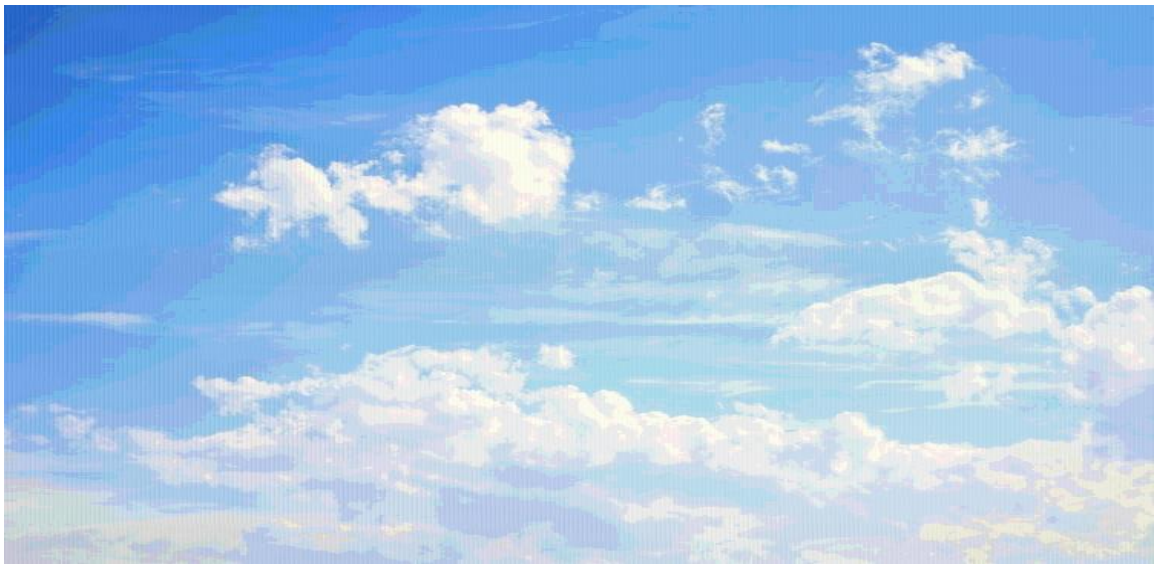


Figure 3.10:Image stego de la méthode LSB.

Figure 3.11:Image secret de la méthode LSB.

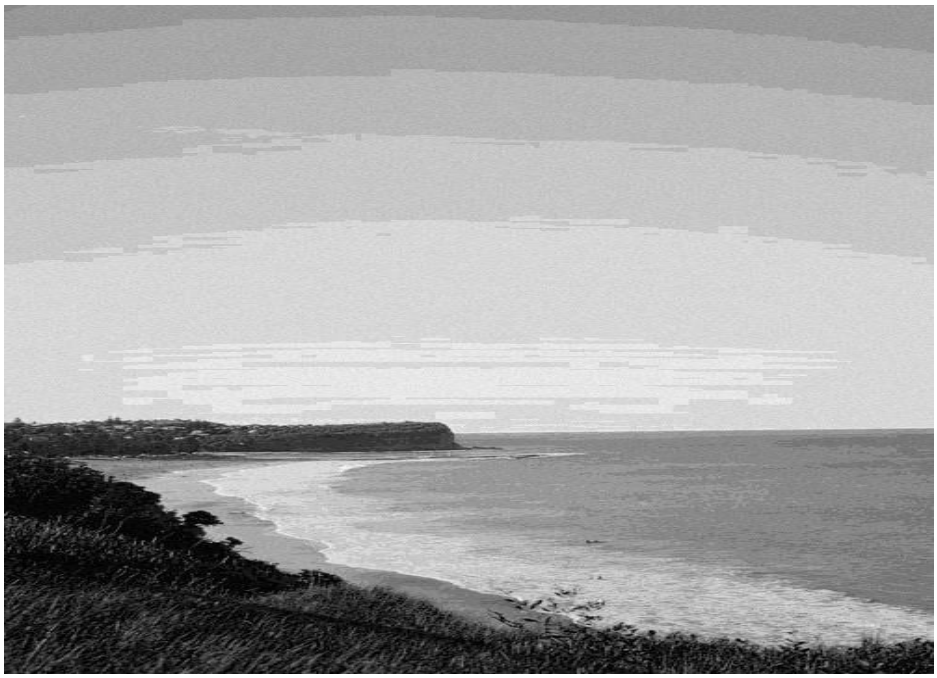


Figure 3.12:image secrète extraite de la méthode LSB.

3.5.2 Méthode LSB basée sur la modulation

Après insérer les deux images originales et secrètes et appliquer la méthode LSB MOD sur les deux images on a comme résultat l’image steganographie et l’image secrète extraite.

Figure 3.13: image stego de la méthode LSB MOD.

Figure 3.14: image extraite de la méthode LSB MOD

3.6Comparaison PSNR.

PSNR est une mesure de distorsion utilisée en image numérique, tout particulièrement en compression d'image. Elle permet de quantifier la performance des codeurs en mesurant la qualité de reconstruction de l'image compressée par rapport à l'image originale.

3.6.1 Méthode LSB

Les valeurs du PSNR présentées dans le tableau 3.2 permettent d'évaluer la qualité des images stéganographies et images secrètes extraitse avec l'algorithme de LSB, par rapport aux images originales et secrète.

Images / PSNRs	(image originale, image stégo)	(image secrète, secrète extraite)
PSNR1	56.1637	41.392

Tableau 3.2 : LSB PSNR résultats

D'après le tableau, on peut conclure que la qualité des images stéganographies et images secrète extraite par rapport aux images originales et secrètes est bon parce que les valeurs de PSNR égale ou supérieure à 38 dB.

3.6.2Méthode LSB MOD

Images / PSNRs	(image originale, image stégo)	(image secret, secrèteextraite)
PSNR1	34.1401	23.8217

Tableau 3.3 : LSB MOD PSNR résultats

Les résultats de PSNR prouvent que la méthode LSB est meilleure que la méthode LSB-modulation

3.7Conclusion

Ce chapitre a été consacré dans un premier temps à présenter les méthodes utilisées dans le cadre de ce travail. Les deux méthodes LSB et LSB-modulation sont les présentées. Nous montrons les résultats trouvés après l'application de ces méthodes et les résultats de PSNR qui clarifient la différence entre les deux méthodes.

Conclusion Générale

Le travail présentée dans ce mémoire, s'inscrit dans le but de la stéganographie et plus précisément l'insertion d'un message secret à l'intérieur d'une image numérique. Dans notre travail, nous avons proposé deux algorithmes de stéganographie pour l'insertion des messages, l'un dans le domaine spatial (LSB), et l'autre dans le domaine fréquentiel .

Le premier chapitre, résume les notions de base de sécurité d'information, nous avons entamé la technique de stéganographie où on a commencé par son historique, d'où elle vient, ensuite sa définition et son principe général permettant de bien avoir le système stéganographique comment il fonctionne, et encore on a parlé sur les différentes techniques et supports utilisés pour réaliser ce type de système, et enfin nous avons terminé notre chapitre par une entrevoir sur la stéganalyse qui consiste à détecter l'existence d'une information cachée.

Le deuxième chapitre, nous avant mis l'accent sur les différentes techniques de dissimulation dans le cas spatial et fréquentiel appliquée.

Dans le troisième chapitre, nous avons essayer de réaliser d'autres systèmes de stéganographie en utilisant d'autres techniques comme LSB, et LSB-MOD et nous avons essayer de programmer des algorithmes de stéganographie pour détecter l'existence d'un message caché.

Les références

[1] M. SAHIR : « Compression des images numériques par la technique des ondelettes ». Thèse de magister, université Ferhat Abbas-Setif (Algérie). Soutenu le 19/06/2011.

[2] I. Bougerne : « la sélection des caractéristiques para llèle pour la stéganalyse ». Thèse de doctorat, Université de Annaba. Soutenue en 2017.

[3] D. Batikh : « Sécurité de l'information par stéganographie basée sur les séquences chaotiques ».Thèse de doctorat, Université de Beyrouth (LIBAN). Soutenue le 18/05/2015.

[4] T. Filler, J. Judas, and J. Fridrich : « Minimizing additive distortion in stéganographie using syndrome. Trellis codes », Information forensics and Security, IEEE Transactions on, vol. 6, no. 3, pp. 920-935, 2011.

[5] C. Cachin : « An Information- Theoretic Model of Steganography ». In Information Hiding – 2ed International workshop, vol. 1525, pp 306-318, Portland Oregan, USA. Springer- Verlag, 1998.

[6] [Cheddad, A., Condell. J., Curran K et McKevitt ,P. (2010). Digital image steganography: Survey and analysis of current methods, Signal Processing 90, pages 727–752.

[7] Saejung, S., Boondee, A., Preechasuk, J. et Chantrapornchai, C. (2013). On the comparison of digital image steganography algorithm based on DCT and wavelet, in Computer Science and Engineering Conference (ICSEC), pages 328–333.

[8] Goel, S., Rana, A., Kaur, M., (2013). Comparison of Image Steganography Technique, International Journal of Computers and Distributed Systems , Numero 3, Issue I.

[9] S. Kouider : « Insertion adaptative en stéganographie : Application aux images numériques dans le domaine spatial ». Thèse de doctorat, Université de Montpellier II (France). Soutenue le 17/12/2013.

[10] I. Bougerne : « la sélection des caractéristiques parallèle pour la stéganalyse ». Thèse de doctorat, Université de Annaba. Soutenue en 2017.

[11] C. Zitzmann : « Détection statique d'information cachée dans des images naturelles ». Thèse doctorat, Université de Technologie De Troyes (France). Soutenue le 24/06/2013.

[12] D. Batikh : « Sécurité de l'information par stéganographie basée sur les séquences chaotiques ».Thèse de doctorat, Université de Beyrouth (LIBAN). Soutenue le 18/05/2015.

[13] A. Adjila : « Signatures numériques pour fichiers audio (audio watermarking) ». Mémoire de magister, Université Kasdi-Merbah Ouargla (Algérie). Soutenue en 2013.

[14] Sharp, T. (2001). An implementation of key-based digital signal steganography. In Information Hiding - 4th International Workshop, volume 2137 de Lecture Notes in Computer Science, IH'01, pages 13–26, Berlin, Heidelberg. Springer-Verlag. Cité page 26. [Sieberg, 2001] Sieberg, D. (2001). Bin Laden exploits tech

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

[16] Westfeld, A. (2001). F5–A Steganographic Algorithm: High Capacity Despite Better Steganalysis. In Information Hiding - 4th International Workshop, volume 2137, pages 289–302, New York, Pittsburgh, PA. Springer-Verlag. Cité pages 24, 27, 33, 41, 59 et 76.

[17] Upham, D. (1992-1997). Jpeg-Jsteg, modification of the independent JPEG's group's JPEG software (release 4) for 1-bit steganography in JFIF output files. Cité pages 27 et 57.

[18] Provos, N. (2001). Defending Against Statistical Steganalysis. In The 10th USENIX Security Symposium, Washington, D.C., USA. Cité page 27

[19] Vasco Pereira and Tiago Sousa, "Evolution of Mobile Communications: from 1G to 4G", in Proc. Of The 2nd International Working Conference on Performance Modeling and Evaluation of Heterogeneous Networks, HET-NETs'04, West Yorkshire, U.K., July 2004

[20] http://studentweb.niu.edu/9/~Z172699/Description.html

[21] Virologie et Cryptologie, B.P. 18, 35 998 Rennes Cedex, 2007.