REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Akli Mohand Oulhadj Bouira
Faculté des Sciences et des Sciences Appliquées
Département de Génie Electrique

Projet de fin d'étude

En vue de l'obtention du diplôme de Master

OPTION

Systèmes des Télécommunications

Thème :

Réalisation d'un système de dissimulation de données secrètes dans les images (la stéganographie).

Réalisé par :

DEMMOUCHE Sabrina *DJEBRI Leila*

Soutenu le 30/10/2018

Devant le jury composé de :

Mr. B. SAOUD	M.C.B	Présidant	(UAMOB)
Mr. A. BENZAOUI	M.C.B	Encadreur	(UAMOB)
Mr. S. CHELBI	M.C.B	Examinateur	(UAMOB)
Mr. R. KASMI	M.C.B	Examinateur	(UAMOB)

Année universitaire : 2017/2018

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 A. Benzaoui,*** *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.

Dédicace

A mon cher père « Rahimahou Allah » et ma chère mère,

pour l'éducation et le grand amour dont ils m'ont entouré depuis ma naissance.

A tous mes chers frères.

A ma chère sœur.

A toute ma famille.

A tous mes proches.

A mon binôme leila.

A tous mes amis.

A tous ceux que j'aime et qui m'aiment.

Ce mémoire leur est dédié.

Sabrina

DEDICACE

Je dédie ce modeste travail à :

Mes très chers parents qui m'ont aidé et soutenu tout au long de mes études et mon succès :

A la source de mon bonheur, la flamme de mon cœur, celle qui s'est Toujours sacrifiée pour me voir réussir : Maman Hadda que j'adore ''Rahimaha Allah''

A l''homme de ma vie, mon exemple éternel, mon soutien moral et ma Source de joie : Mon père Saïd

Mes chères sœurs : Hayet et Hadjira pour leur amour et leur présence dans ma vie

Mes chers frères : Abderrezak, Nabil, Hamza, Abdellatif pour leur soutien

Ames profs surtout ceux de l'université de brouira et spécialement pour mon encadreur

A mon binôme Sabrina

Ames chères amies pour leur encouragement S.Hannane, T.Hamidda

Et pour tout le reste de ma famille

Table des matières

Chpitre 01: Géneralités sur le traitement d'images

Chapitre 02 : Stéganographie.

Chapitre 03 : Réalisation & Résultats

Liste des figures

Liste des Tableaux

Abréviations

La signification d'une abréviation ou d'un acronyme n'est souvent indiquée qu'à sa première apparition dans le texte. Il existe dans la plupart des cas une abréviation en français et une abréviation en anglais. Toutes les deux sont indiquées une première fois puis nous employons l'abréviation la plus usuelle, qui est le plus souvent l'abréviation en anglais.

Acronymes & Abréviations :

𝒜

ASCII : American **S**tandard **C**ode For **I**nformation **I**nterchange

ℬ

BMP : Bit **M**ap

𝒞

CMY : Cyan **M**agenta **Y**ellow

CIE : Commission **I**nternationale de l'**E**change

𝒟

DCT : Discrète **C**osine **T**ransform

DICOM : Digital **I**maging And **C**ommunications In **M**edecine

DPI : Dots **P**er **I**nch

DWT : Discrète **W**avelet **T**ransform

ℰ

EPS : Enfcapsulated **P**ost **S**cript

𝒢

GIF : Graphics **I**nter change **F**ormats

ℋ

HSL : Hue **S**aturation **L**uminance

ℐ

IBM : International **B**usiness **M**achines

IDCT : Invers **D**iscrète **C**osine **T**ransform

𝒥

JIFF : JPEG **I**mage **F**ile **F**ormat.

JPEG : Joint **P**hotographie **E**xpert **G**roup

ℒ

LSB : Least **S**ignificant **B**it

LZW : Lempel **Z**iv **W**elch

ℳ

MNG : Multiple image **N**etwork **G**raphics

𝒫

PCX : Picture **E**xchange **I**mage **B**itmap **Z**oft

PNG : Portable **N**etwork **G**raphic

PPP : Point **P**ar **P**uce

ℛ

RGB : Rouge, **G**reen, **B**leu

S

SSIS : Spread **S**pectrum **I**mage **S**teganography

𝒯

TIFF : Tagged **I**mage **F**ile **F**ormat

TSL : Teinte **S**aturation **L**uminance

𝒲

W3C : World **W**ide **W**eb **C**onsortium

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 [3].

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 [20].

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 [13].

Il existe des techniques permettant de découvrir le média stéganographié : c'est le cas de la stéganalyse appelée aussi l'analyse stéganographique [20].

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 message 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 message.

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

Le chapitre 1, est réservé à des généralités sur le traitement d'images, nous allons présenter quelques notions de base sur les images numériques.

Le chapitre 2, est consacré à présenter l'art de la dissimulation des informations dans une image et décrivant le principe d'une technique qui détecte l'existence de ces informations (stéganalyse).

Le chapitre 3, va contenir les différents algorithmes proposés et à réaliser ainsi que leurs résultats expérimentaux.

Chapitre I : Généralités sur le traitement d'image.

I.1. Introduction :

L'image est considérée comme l'un des moyens les plus utilisés pour la communication entre les êtres humains. D'où, la richesse de son contenu permet à tout le monde de tout âge et toute culture de se comprendre.

L'image constitue un moyen de communication universel, c'est aussi le moyen le plus efficace pour communiquer, chacun peut analyser l'image à sa manière pour en dégager une impression et d'en extraire des informations précises [1].

Un système de traitement d'image se compose principalement d'un ensemble de fonctions comme l'acquisition d'image, prétraitement pour la diminution de bruit afin d'extraire les informations les plus pertinente [2].

Dans ce chapitre, on va présenter quelques notions de base sur les images numériques tels que : la définition de l'image numérique, sa formation, ses types, ses caractéristiques, ainsi que les différentes formats existantes.

I.2. Image numérique :

Les images manipulées par un ordinateur sont numériques (représentées par une série de bits), contrairement aux images obtenues à l'aide d'un appareil photo, ou dessiner sur papier. La surface de l'image numérique est divisée en éléments de tailles fixes appelés pixels, ayant comme caractéristiques un niveau de gris ou de couleur calculé à partir d'une description de la scène à représenter [1,3,4].

La numérisation d'une image, est une opération qui permet de transformer cette image de son état analogique, en une image numérique ou discrète [5], représentée par une matrice bidimensionnelle de valeurs numérique $I(x, y)$, comme le montre la figure (I.1), où x et y sont des coordonnées cartésiennes d'un point de l'image, et $I(x, y)$ est le niveau d'intensité.

La valeur en chaque point exprime la mesure de l'intensité lumineuse perçue par le capteur [1].

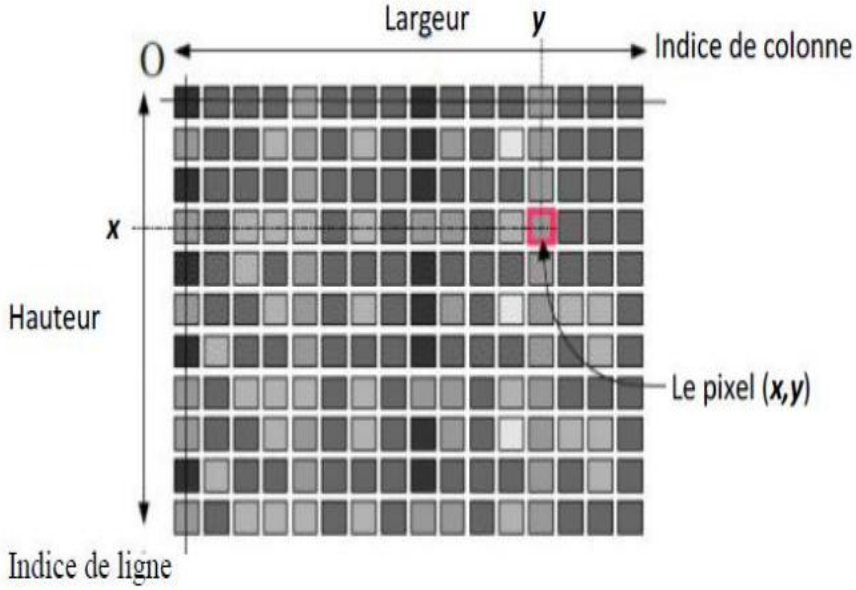


Figure I.1 : Représentation d'une image numérique.

I.3. Formation de l'image numérique :

L'image numérique est constituée d'un ensemble de points discrets. Chacun de ces points se voit affecté par une intensité lumineuse permettant de définir sa couleur. Contrairement aux images optiques qui sont constituées d'une suite continue de tons. Toute image est initialement issue d'un système optique. Pour transformer cette image en une image numérique, il faudra :

- Couper le continue en autant de mesures discrètes : on parle d'échantillonnage.
- Affecter à chacun de ces points de mesure une intensité lumineuse qui traduira une couleur : on parle de quantification [5].

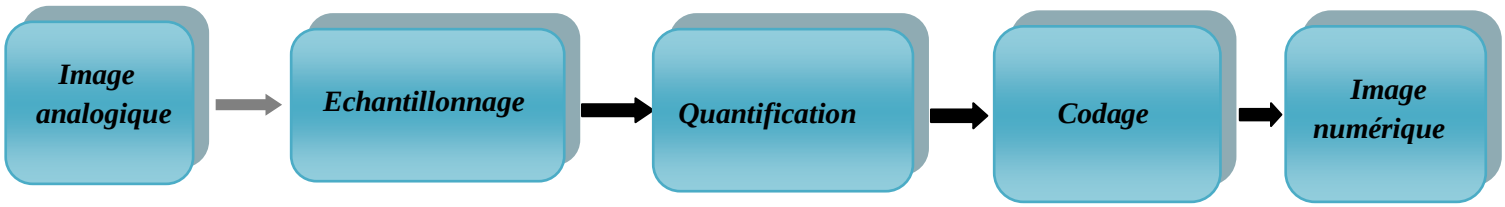


Figure I.2 : Schéma de formation de l'image numérique.

I .3.1 Echantillonnage :

L'échantillonnage est le procédé de discrétisation spatiale d'une image qui consiste à associer à chaque pixel R(x, y) une valeur unique *I(x, y)* [6].

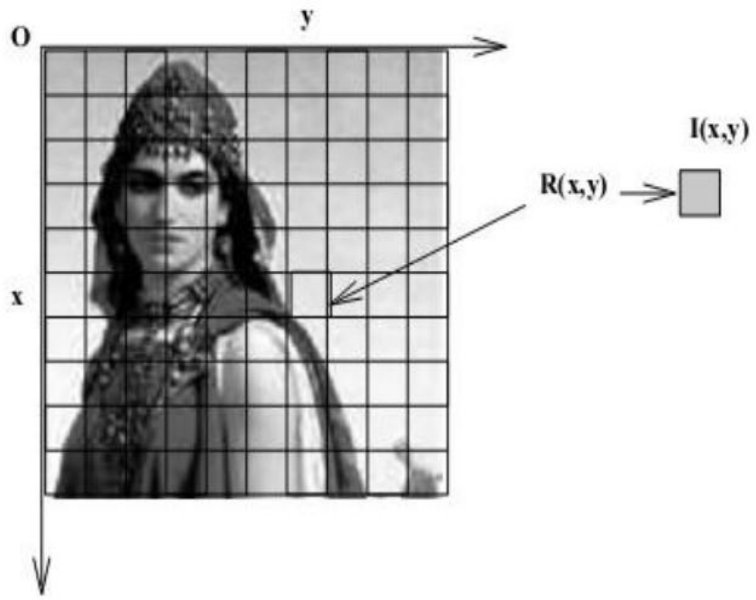


Figure1.3 : Echantillonnage, discrétisation spatiale.

I.3.2 Quantification :

La quantification a pour but de remplacer un nombre infini de valeurs que le *I(x, y)* peut prendre par un nombre fini appelé niveau de quantification, elle remplace la valeur exacte de l'image par une valeur rapprochée et peut également faire apparaitre des distorsions dans les images [6].

I.3.3 Codage des images numériques :

I.3.3.1 Codage en noir et blanc (binaire) :

Chaque pixel soit noir ou soit blanc, donc il faut qu'un seul bit pour coder un pixel (o pour noir et 1 pour blanc). Ce type de codage peut convenir pour un plan ou un texte mais on voit ses limites lorsqu'il est d'une photographie [6].

I.3.3.2 Codage en niveau de gris :

Pour chaque pixel codé sur 2 bits on aura 4 possibilités (noir, gris foncé, gris clair, blanc). En codage sur 8 bits l'image en niveau de gris renferme 256 teintes de gris. Par convention la valeur zéro représente le noir (intensité lumineuse nulle) et la valeur 255

représente le blanc (intensité lumineuse maximale). En effet, chaque entier représentant un niveau de gris est codé sur 8 bits [6].

I.3.3.3 Codage d'une image couleur :

Chaque pixel peut être attribué par 3 valeurs : rouge, vert et bleu (de 0 à 255), chaque couleur est codée sur 1 octet = 8bits, ce qui signifie que chaque pixel est codé sur 3 octets c'est-à-dire 24bits. On peut obtenir une couleur quelconque par addition de ces trois couleurs primaires en proportions convenables [6].

I.4. Types d'images :

I.4.1. Image vectorielle :

L'image vectorielle est une représentation conceptuelle de forme calculée par des formules mathématiques, (exemple, un cercle est déterminé par une formule mathématique qui représente sa forme, sa taille et son emplacement) [4].

Le principe est de représenter les données de l'image par des formules géométriques qui vont être décrites d'un point de vue mathématique. Donc, on stocke la succession d'opérations conduisant au dessin, au lieu de mémoriser une mosaïque de points élémentaires, le dessin est mémorisé par l'ordinateur comme « une droite tracée entre les points (x1, y1) et (x2,y2) », puis « un cercle tracé de centre (x3,y3) et de rayon à 30° de couleur rouge », etc.

Ce type d'image permet de représenter des scènes simples et leur faire subir des transformations (agrandissement, rotation) sans perte de qualité [5].

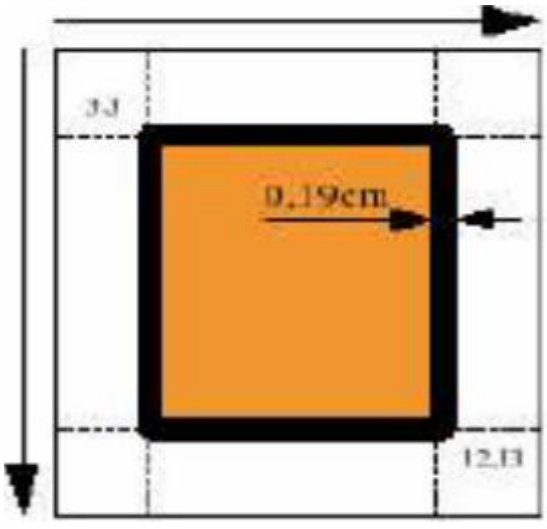


Figure I.4 : Image vectorielle.

- **Applications :**

- Dessin technique.

- Logo et schémas.

- Dessin de référence pour les machines à commandes numériques (gravure,…). [4]

➢ **Avantage :**

- Fichiers de volume peu important.

- Conservation des proportions lors des modifications de taille de l'image.

- Dessin aux contours nets.

➢ **Inconvénients :**

- Moindre possibilités de travail sur les couleurs.

- Pas de travail sur les photos [4].

I.4.2. Image bitmap (matricielle) :

L'image bitmap est représentée par un ensemble de points que l'on appelle pixels. Contrairement aux images vectorielles, ceux ne sont pas des formules mathématiques qui définissent les formes, mais une trame de pixels qui agissent comme un tableau pointilliste [4].

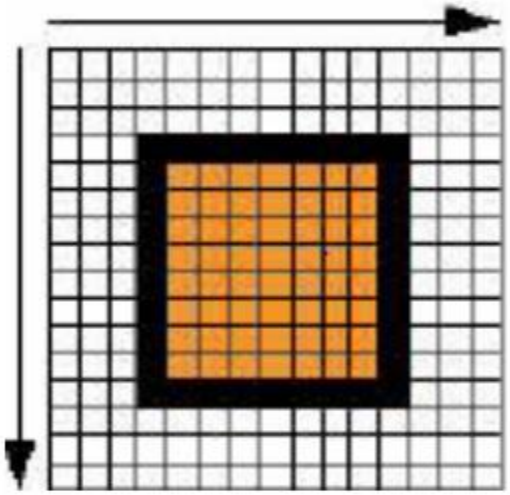


Figure I.5 : Image matricielle [5].

- **Applications :**

- Dessin type artistique.

- Image qualité photo.

- Animation [4].

➢ **Avantage :**

- Simplicité de stockage en mémoire, puisqu'il suffit de coder la succession des valeurs de la matrice.

- Grande facilité de traitement par des algorithmes primitifs au niveau du pixel [2].

➢ **Inconvénients :**

- Fichiers volumineux.

- Ne conserve pas les proportions lors des modifications ex. agrandissement ou rédaction.

- Risque de disparition de pixels lors des modifications de taille [4].

I.4.3. Image multi résolution :

C'est l'image obtenue après l'analyse multirésolution, l'analyse mutirésolution approche le comportement du système psychovisuel humain, c'est une propriété très intéressante pour un système de recherche d'image, d'où chaque image est décomposée en une image d'approximation et plusieurs images de détails à plusieurs niveaux de résolution. L'image d'approximation de basse résolution peut être utilisée comme icône pour représenter l'image d'origine [7].

I.5. Caractéristiques des images numériques :

Comme nous l'avons vu, l'image est un ensemble structuré d'informations, parmi ces caractéristiques nous pouvons citer les paramètres suivants :

- **Pixel :**

Le pixel représente le plus petit point constructif de l'image, c'est la contraction de l'expression anglaise « Picture éléments», c'est une entité calculable, elle peut recevoir une structure et une quantification [3]. D'où l'ensemble de ces pixels est contenu dans un tableau à deux dimensions constituant l'image [8].

La lettre A par exemple, peut être affichée comme un ensemble de pixels dans la figure suivante [1] :

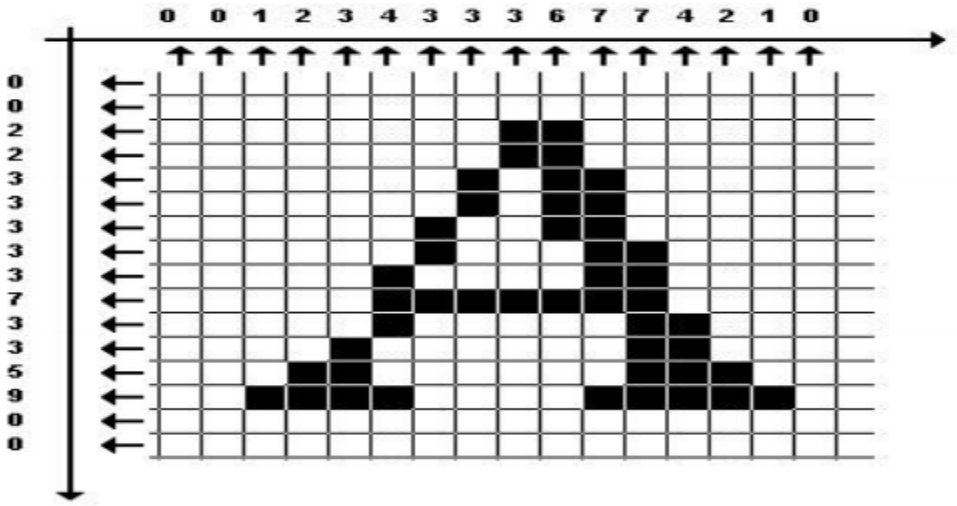


Figure 1.6 : Représentation de la lettre A sous la forme d'un groupe de pixels**.**

- **La dimension (définition) :**

La dimension ou la définition d'une image correspond à la taille de l'image. Cette dernière se présente sous forme de matrice dont les éléments sont des valeurs numériques représentatives des pixels (intensités lumineuses). Le nombre de lignes de cette matrice multiplié par le nombre de colonnes nous donne le nombre total de pixels dans une image [3].

Une image possède 1280 pixels en largeur et 720 en hauteur aura une définition de 1280 pixels par 720, notée 1280 x 720 [2].

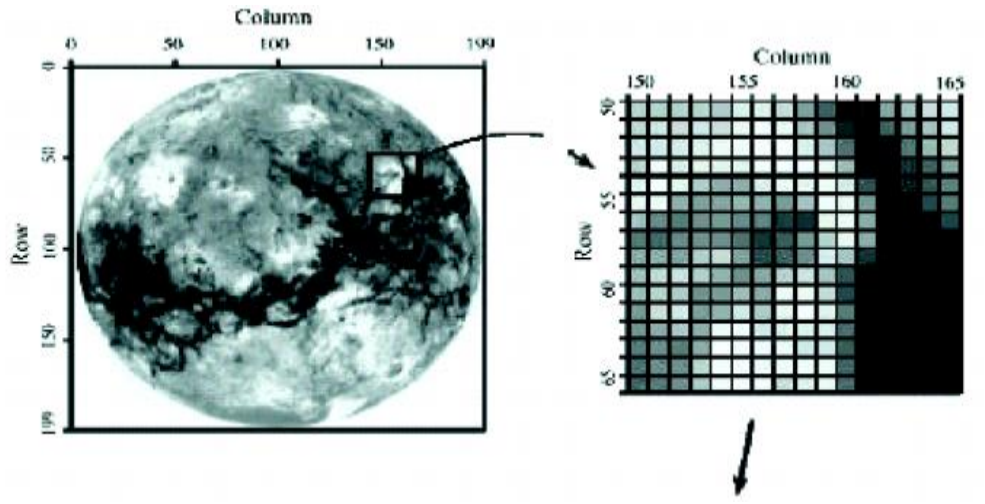


Figure 1.7 : Représentation de dimension d'une image [1].

- **la résolution :**

Elle est déterminée par le nombre de points par unité de surface, exprimée en points par pouce (PPP, en anglais DPI pour Dots Per Inch), d'où le pouce représentant 2.54 cm [2,5]. Ce paramètre est défini lors de la numérisation, et dépend principalement des caractéristiques du matériel utilisé. Plus le nombre de pixels par unité de longueur de l'image à numériser est élevé, plus la quantité d'informations, qui décrit cette image est importante et plus la résolution est élevée [5]. Une résolution de 300 dpi signifie donc 300 colonnes et 300 rangées de pixels sur un pouce carré ce qui donne donc 90000 pixels sur un pouce carré [2].

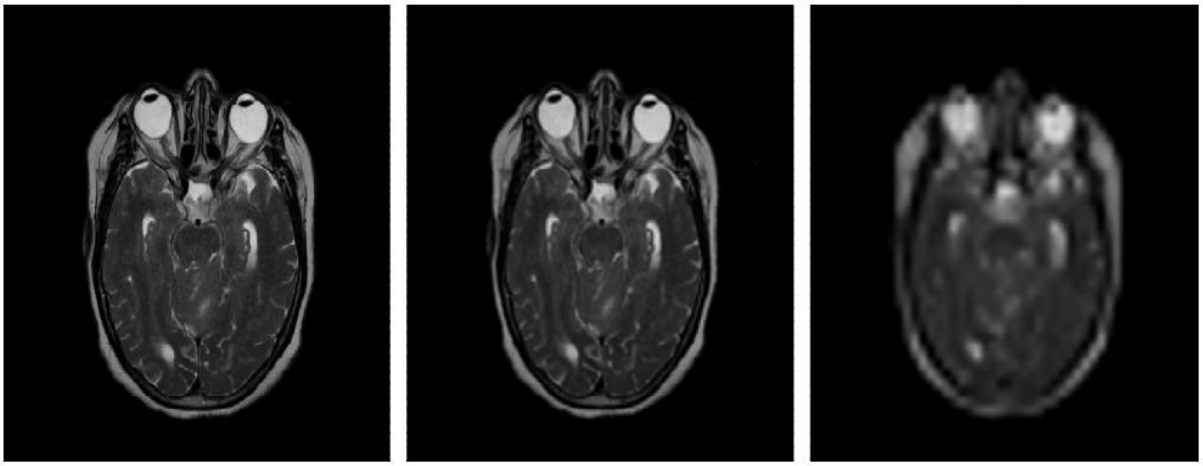
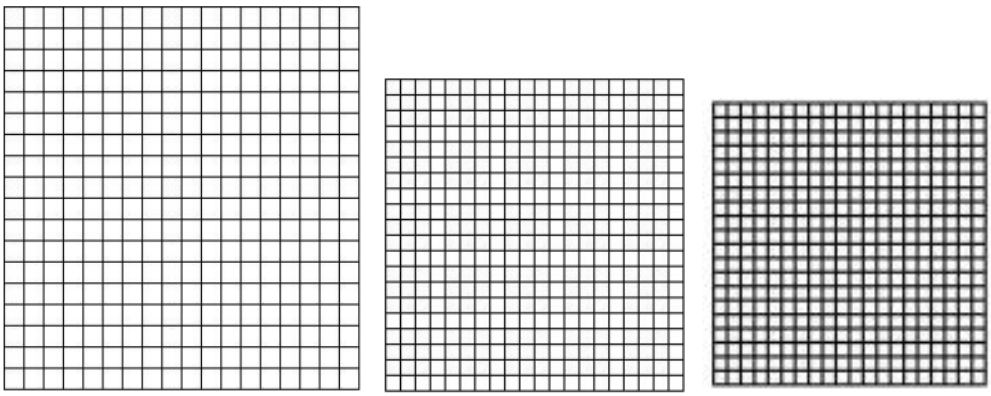


Figure I.8 : La résolution d'une image [2].

Exemple [7] :



Faible résolution Moyenne résolution Forte résolution

- **Le poids :**

Le poids d'une image se mesure en Octects et se détermine en fonction de ces trois paramètres : résolution, dimension, et nombre des couleurs [1].

- **L'Histogramme :**

On appelle histogramme de l'image, la fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image [1].

Donc l'histogramme est un outil privilégié en analyse d'image, parce qu'il représente un résumé simple, mais souvent suffisant du contenu de l'image [8].

Il peut être utilisé pour l'amélioration de la qualité d'une image (rehaussement d'image), en introduisant quelques modifications, afin d'extraire les informations utiles de celle-ci [1].

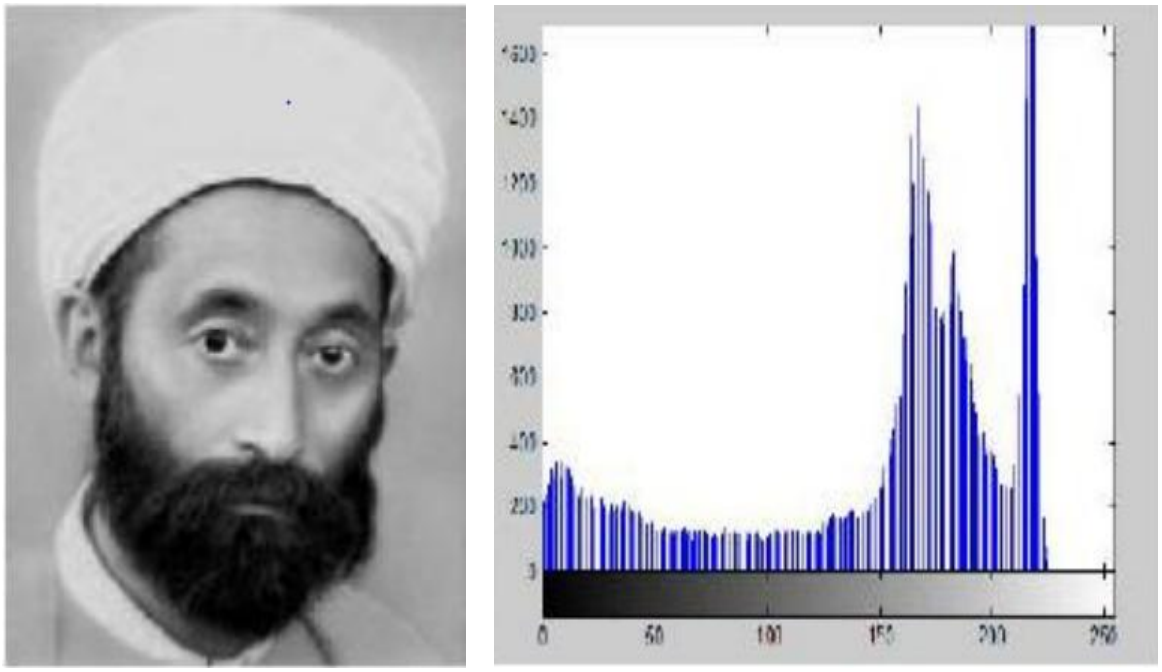


Figure 1.9 : Image et histogramme associé.

- **Contours et textures :**

Les contours sont définis comme étant les frontières existantes entres les objets de l'image, ou d'une autre façon sont la limite entre deux pixels dont les niveaux de gris représentent une différence significative. Alors que les textures décrivent la forme de ceux-ci [1].

Un contour est donc défini comme une zone de l'image où l'intensité des pixels change subitement, cette interruption dans l'image est le passage d'un niveau de gris à un autre, de manière plus ou moins rapide [2]. L'extraction de contour donc consiste à identifier dans l'image les points qui séparent deux textures différentes [1].

Figure 1.10 : Contour d'une image.

I.6. Codage et représentation des couleurs :

Il est essentiel de disposer d'un moyen de choisir une couleur parmi toutes celles utilisable. Bien que la gamme de couleur possible est très vaste et la chaine de traitement de l'image passe par différents périphériques : par exemple un numériseur (scanner), puis un logiciel de retouche d'image et enfin une imprimante. Il est donc nécessaire de pouvoir représenter efficacement la couleur afin de s'assurer de la cohérence entre ces différents périphériques.

On appelle ainsi espace de couleurs la représentation mathématique d'un ensemble de couleurs. Il existe plusieurs, parmi lesquels les plus connus sont [8] :

- **Codage RGB :**

Le mode RGB est idéal pour l'affichage sur l'écran, une image RGB est composée de trois couches *Rouge, Vert, Bleu* [1]. Pour représenter la couleur d'un point, on utilise trois nombres *r, g* et *b,* compris entre 0 et 255, ces nombres correspondent au dosage des trois couleurs de base : (rouge, vert et bleu). Une couleur peut donc être représentée par un point dans un espace à 3D, en portant sur les axes les valeurs de *r, g* et *b* [5].

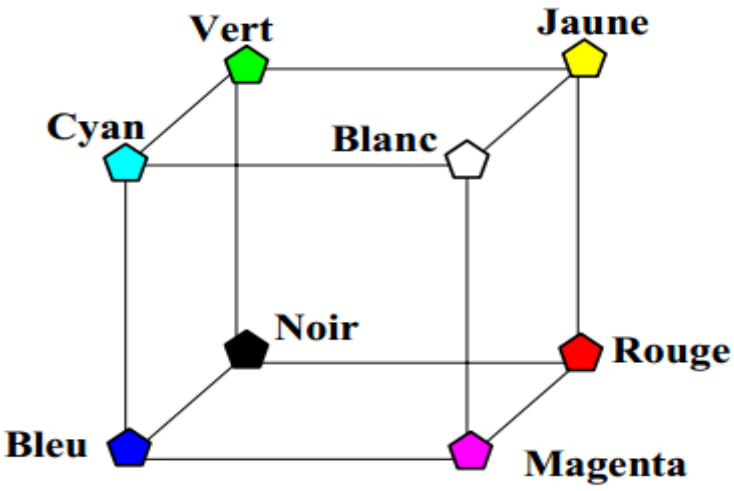


Figure I.11 : Le codage RGB [5].

- **Codage XYZ :**

En 1931, la CIE a décidée de crée un espace dans lequel il n'existerait plus de valeurs négatives, cet espace est nommé XYZ [9]. Donc les primaires [X], [Y] et [Z] ont été de telle sorte que toutes les couleurs soient exprimées par des composantes trichromatiques positives.

On peut noter que l'espace (R,G,B) et l'espace (X,Y,Z) sont reliés entre eux [10], par la relation matricielle suivante [9] :

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = P \text{ x } \begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} X_r & X_g & X_b \\ Y_r & Y_g & Y_b \\ Z_r & Z_g & Z_b \end{bmatrix} \text{ x } \begin{bmatrix} R \\ G \\ B \end{bmatrix} \text{ [9].}$$

La CIE a défini les coordonnées trichromatiques de l'espace (X,Y,Z) :

$$x = \frac{X}{X + Y + Z}$$

$$y = \frac{Y}{X + Y + Z}$$

$$z = \frac{Z}{X + Y + Z}$$

$$x + y + z = 1$$

Comme nous avons *x+y+z=1*, donc on peut déduire *z* à partir de *x* et *y*, ce qui permet de représenter la couleur dans un plan et de construire alors le diagramme de chromaticité (*x,y)*, qui est représenter par la figure suivante [10] :

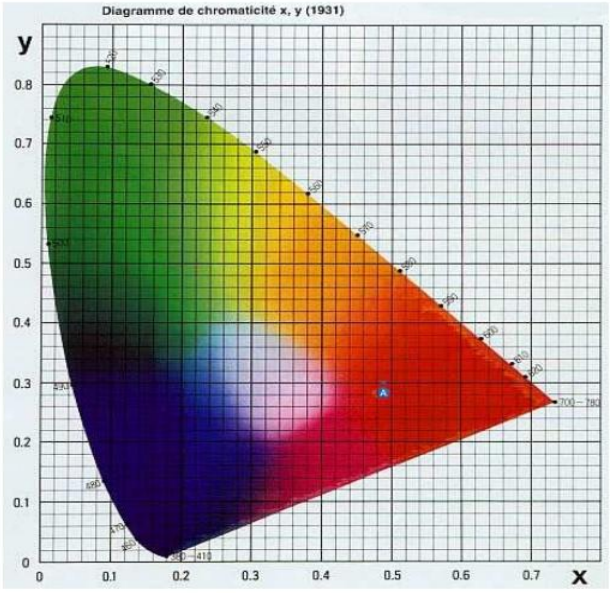


Figure I.12 : Diagramme chromatique défini par les deux variables de chrominance x et y [9].

- **Codage CMY :**

Le codage CMY (Cyan, Magenta, Yellow), est utilisé principalement pour l'impression et basé sur la synthèse soustractive contrairement au RGB [5]. Ce modèle consiste à décomposer une couleur en valeurs de Cyan, de Magenta et de Jaune [8].

- **Le codage HSL (TSL) :**

Le modèle HSL (Hue, Saturation, Luminance, ou en français TSL), est un modèle de représentation dit "naturel", c'est-à-dire proche de la représentation physiologique de la couleur par l'œil humain.

Le modèle HSL consiste à décomposer la couleur selon des critères physiologiques :

- La teinte (en anglais Hue), correspondant à la couleur de base (T-Shirt mauve ou orange).

- La saturation, décrivant la pureté de la couleur, c'est-à-dire son caractère vif ou terne (T-Shirt neuf ou délavé).

- La luminance, indiquant la brillance de la couleur, c'est-à-dire son aspect clair ou sombre (T-Shirt au soleil ou à l'ombre).

La figure suivante illustre une représentation graphique de modèle HSL :

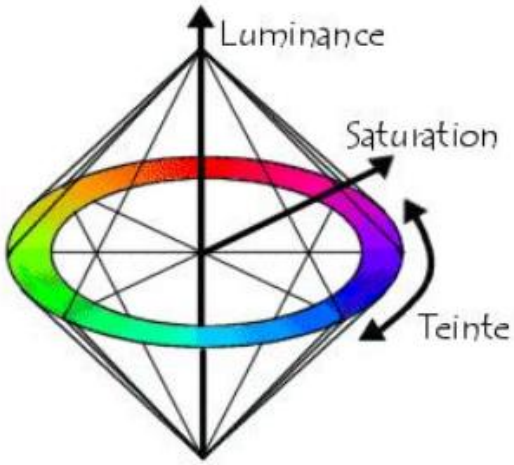


Figure I.13 : Représentation graphique du codage HSL.

Le modèle HSL a été mis en point dans le but de permettre un choix interactif rapide d'une couleur, pour autant il n'est pas adapté à une description quantitative d'une couleur [8].

- **Le codage YUV :**

Le modèle YUV est l'une des méthodes de représentation qui permet la transmission des vidéos. Ce codage détermine un pixel par son niveau de gris (luminance : Y) et deux composantes couleurs (chrominance : U et V) qui demande moins d'informations que la composante Y pour être coder, tandis que le format RGB code chaque pixel grâce aux trois composantes de base [11].

Figure I.14 : L'image originale RGB, et les trois composantes Y, U et V.

On peut obtenir les trois nouvelles composantes à l'aide des équations suivantes [11]:

$$Y = 0.299R + 0.587G + 0.114B$$

$$U = -0.615R - 0.289G + 0.436B = 0.492(B - Y)$$

$$V = 0.615R - 0.515G - 0.100B = 0.877(R - Y)$$

I.7. Déférents formats d'images :

- **Le format BMP :**

Il est créé par Microsoft et IBM. Il a été conçu pour les ordinateurs personnels (PC) et pour une utilisation dans un environnement Windows et OS/2 [12]. C'est un format ouvert et non compressé.

- **Le format GIF (Graphics Interchange Format) :**

Il est développé par Compuserve, il présente deux principaux avantages : portabilité et indépendance vis-à-vis du système d'exploitation, facilité et rapidité de lecture. Le format GIF utilise l'algorithme de compression LZW. Il est mieux adapté aux images ne nécessitant pas une grande palette de couleurs (niveaux de gris ou 256 couleurs). Une des applications où son efficacité est prouvée est le WEB [12].

- **Le format JPEG (Joint photographique Experts Group) :**

Il possède les mêmes avantages que le format GIF. Cependant, il est mieux adapté aux images de couleurs vraies grâce à sa technique de compression JPEG [12].

Il est créé par un consortium industriel, ce format très utilisé sur Internet, permet d'afficher les images en mode 16 millions de couleurs et donc c'est le mode sans perte. Le format JPG peut aussi utilisé pour compacter les images, il utilise un algorithme de compression qui garde la taille des images [1].

- **Le format PCX (Picture Exchange Image Bitmap Zsoft) :**

Il a été crée à l'origine par Zsoft pour un programme de dessin (paint bruch) [1].

- **Le format EPS (Postscript / Encapsulated Postscript) :**

Le Postscript est un langage de description de page conçu pour imprimer des documents indépendamment du périphérique utilisé. Il contient toutes les commandes nécessaires pour dessiner l'image sauvegardée [1].

- **Le format CGM (Computer Graphics Metafile) :**

Les fichiers graphiques CGM restent un moyen privilégié d'échange de dessins vectoriels entre applications, mais il ne traite pas les images Bitmap [1].

- **Le format DICOM :**

Le format DICOM a été publié pour la première fois par le collège américain de radiologie en 1985, il est composé principalement de quatre niveaux d'informations :

1. **Niveau Patient :** contient les informations d'un patient (nom, date de naissance, son sexe….etc.).
2. **Niveau Etude :** contient les données administratives (date d'acquisition, nom de radiologue…etc.). Il est composé d'un groupe de séries.
3. **Niveau Série :** considère l'ensemble des examens médicaux passé pour la même modalité. Il est constitué de plusieurs images.
4. **Niveau image :** il est composé par des attributs d'acquisition, l'identifiant de l'image, son type, etc. [12].

- **le format TIFF :**

Le format TIFF est un format graphique, conçu en 1987, il permet le stockage des images matricielles de taille importante, sans qu'il perdre de qualité et indépendamment des plates formes ou des périphériques utilisés.

Le format TIFF permet de stocker les différents types d'images (noir et blanc, en couleurs réelles ainsi que des images indexées.

- **Le format PNG :**

Le format PNG a été amélioré par le W3C pour le mettre à la place de GIF, Ce dernier n'est pas limité à 256 couleurs de même il est ouvert et permet une bonne compression sans perte. Son utilisation est recommandée pour les petits logos.

On note qu'un autre format qui est nommer MNG est destiné à gérer l'animation et non pas le PNG.

1.8. Conclusion :

Dans ce chapitre, on a essayé de faire un récapitulatif sur les notions élémentaires de traitement d'image, et nous avons présenté les notions de l'image numérique et ses différents caractéristiques (définition, résolution, poids…etc.) ainsi que la représentation des couleurs.

Le chapitre suivant sera consacré à l'étude d'une technique de dissimulation de données secrètes (stéganographie), qui consiste principalement à cacher un message au sein d'un autre message (image), de sorte que l'on ignore l'existence même du secret.

Chapitre 02 : La Stéganographie

II.1 Introduction :

Les avancées technologiques en informatique et télécommunications ont contribué à 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 [13].

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 [14], 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 [15]. Nous nous intéressons sur les images numériques car ce contenu est majoritairement utilisé lors des échanges numériques [14].

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 [15].

Dans ce chapitre, nous allons parler sur la stéganographie, sa définition, son principe, ses différents types et domaines, ainsi que ses caractéristiques…etc. Ensuite nous allons discuter sur la technique de stéganalyse qui consiste à détecter l'existence d'un message secret dans une communication.

II.2 Historique :

Les origines de la stéganographie remontent à l'antiquité. Son utilisation est décrite par deux fois dans l'Enquête d'Hérodote, un premier passage relate qu'*Aristagoras* fit raser la tète de son plus fidèle esclave et y fit tatouer son message. Une fois les cheveux repoussés, l'esclave pouvait s'en aller transmettre le message, un autre passage fait référence à *Demarate*, ancien roi de Sparte exilé en Perse, qui informa Sparte que les perses préparaient une invitation de la Grèce en écrivant le message sur une tablette en bois puis en recouvrant

celle-ci de cire. Cela permet de déjouer une attaque qui survient quatre ans plus tard [16,17,18].

En chine antique, on écrivant les messages secrets sur de très fins rubans de sois, qu'en enrobait ensuite dans les petites boules de cire. Ces boules, avalées ensuite par le messager, pouvaient voyager jusqu'au destinataire, d'une manière totalement discrète [19].

Plus subtile encore, l'invention de l'encre sympathique est attribuée au naturaliste *Pline l'Ancien*, il est toujours utilisé par des organisations mondiales. L'encre sympathique, ou l'encre invisible est un procédé chimique qui consiste a utilisé du jus de citron, du lait ou de chlorate de soude, pour écrire le message secret qui sera invisible à l'œil humain nu. D'où un simple passage sous une source chaude ou un bain dans un réactif chimique, relève le message [19,20].

Il existe une autre technique de dissimulation de message qu'on appelle la stéganographie linguistique, dans laquelle on peut utiliser le langage, l'espace entre les mots, l'orthographe, ou encore les repères au niveau de caractères pour cacher un message secret dans un texte. Parmi ses méthodes on trouve l'acrostiche, qui représente un poème dont la première lettre de chaque vers compose un mot ou une phrase [16,19].

L'apparition de la stéganographie moderne quant à elle peut être attribuée à *G. Simmons* qui est en 1984, énonça le problème des prisonniers, dans ce problème *Simmons* place deux prisonniers qui souhaitent élaborer un plan d'évasion. Cependant tous leurs échanges sont contrôlés par un gardien qui au moindre soupçon placerait un des détenus en zone de confinement. Les deux complices doivent donc trouver un moyen de communiquer sans éveiller les soupçons, c'est ici qu'intervient la stéganographie en leur permettant de dissimuler un message caché à l'intérieur d'un autre qui ne semble pas suspect [21].

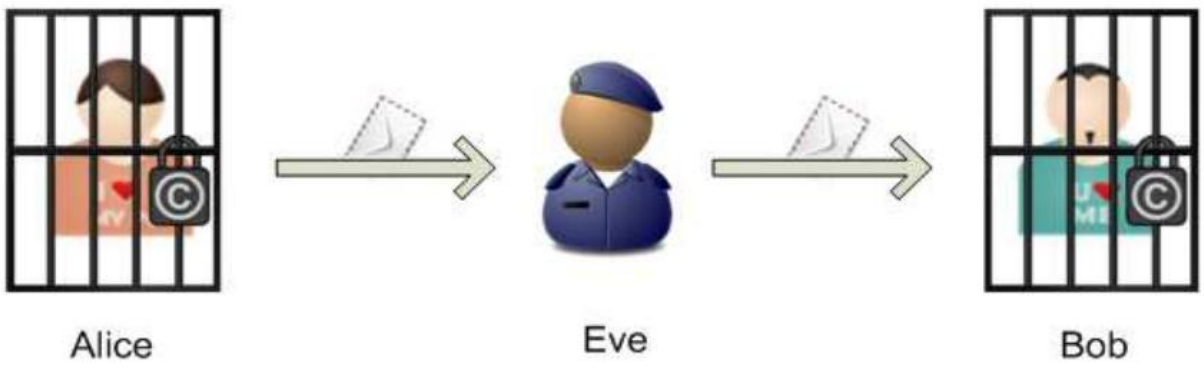


Figure II.1 : Exemple d'une communication secrète.

II.3 Définition :

La stéganographie vient du mot Grec « stéganos » qui veut dire : « dissimulé » et de mot « graphien » signifiant : « écriture », littéralement on traduit par « écriture dissimulée ». Elle consiste à cacher ou dissimuler un message dans un autre, ainsi que le message caché n'est détectable que par la personne connaissant le procédé de dissimulation [22].

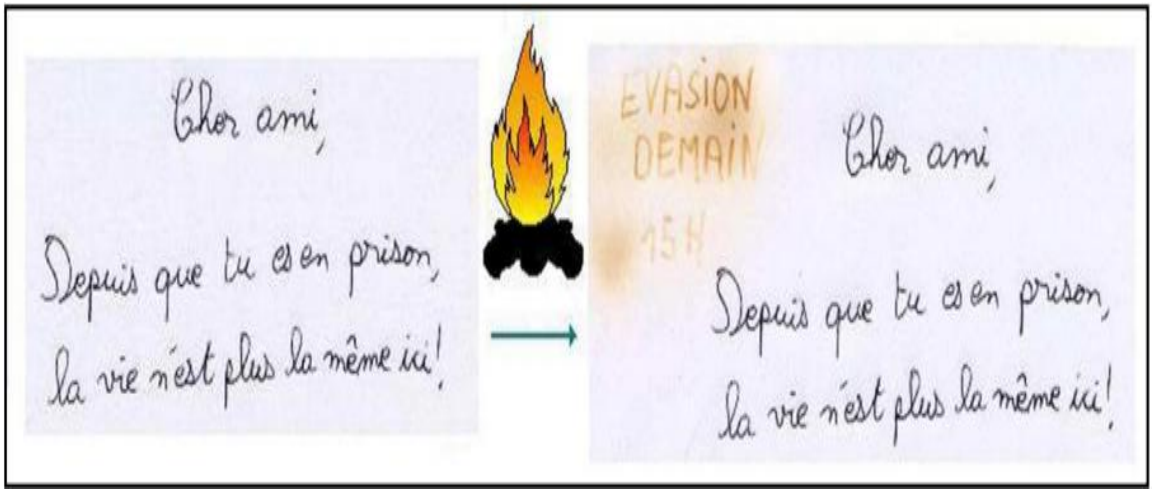


Figure II.2 : Exemple de stéganographie à l'aide de lait [23].

II.4 Principe :

Le principe de la stéganographie est de cacher un message secret, de taille importante dans une image, audio ou une vidéo, appelé média cover (ou original), d'où le média résultant appelé média stégo, ne diffèrent pas beaucoup au média original au moins pour 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.

Nous donnons dans la figure suivante II.3, le principe de la stéganographie, dans le cas où le média original est une image et le message secret une image numérique.

Le processus d'insertion dépend d'une clé secrète qui est une information secrète supplémentaire comme un mot de passe.

On dit qu'un système stéganographique est sécurisé si l'on ne peut pas distinguer la différence entre une image originale est une autre stégo [13].

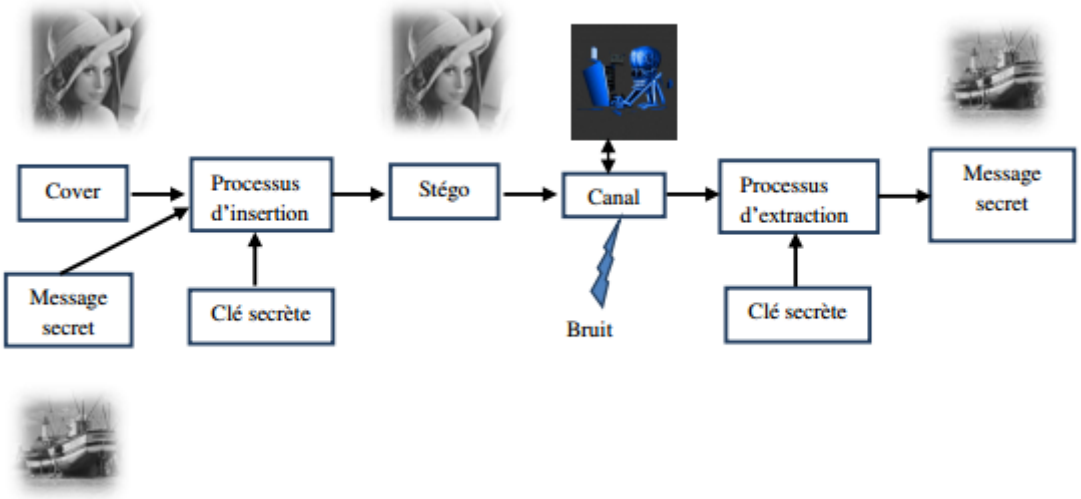


Figure II.3 : principe de la stéganographie.

II.4.1 Structure d'une communication secrète :

Le processus complet de la stéganographie repose sur deux opérations :

- **La dissimulation :**

Elle consiste à insérer l'information dans le medium comme illustre la figure suivante :

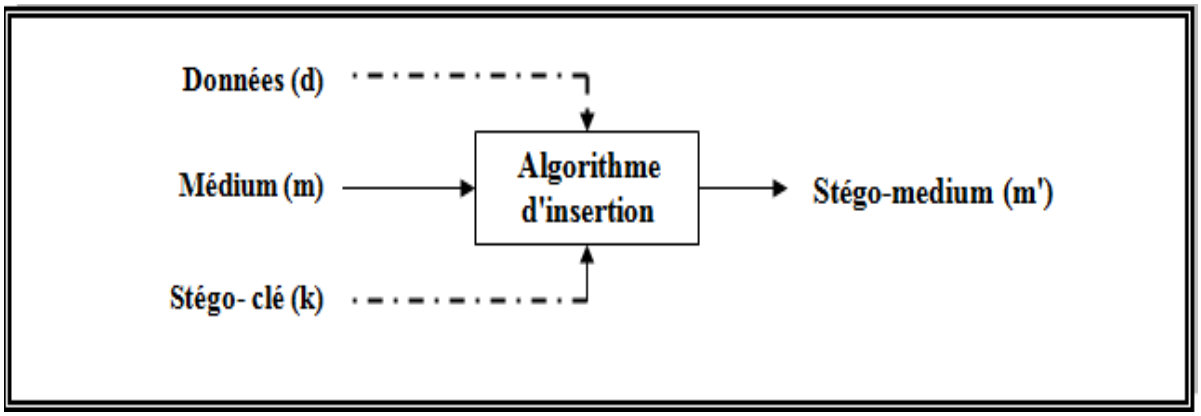


Figure II.4 : dissimulation des données dans le medium [24].

- **L'extraction :**

Consiste à récupérer l'information dissimulée. Le mot détection est également utilisé lorsqu'il s'agit de vérifier la présence d'une information (représentée grâce à un signal, une caractéristique particulière du medium) dans le stégo-medium, sans pour autant vouloir l'extraire comme illustre la figure suivante :

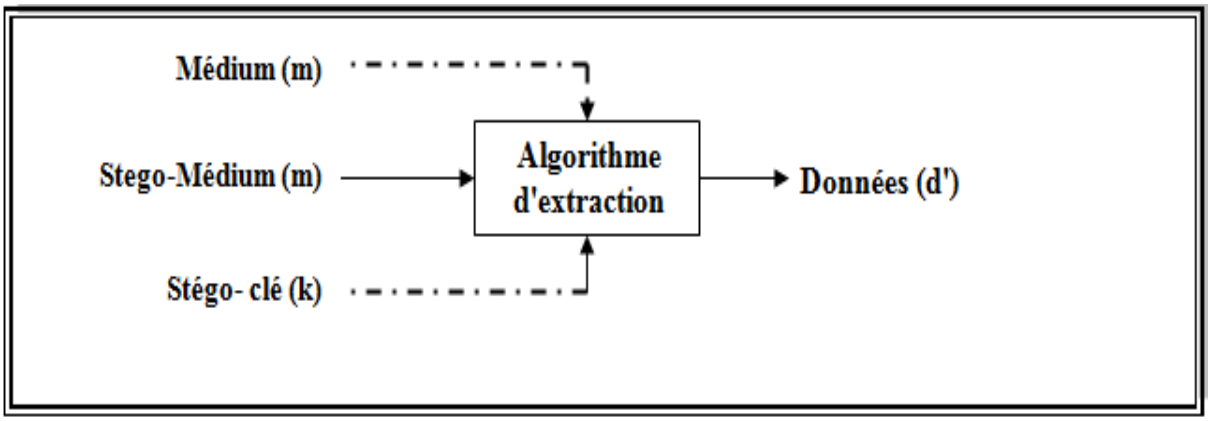


Figure II.5 : Extraction des données du medium [24].

II.4.2 Classification des schémas de stéganographie :

Il existe trois types de protocoles de stéganographie :

- *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 ».
- *La stéganographie à clé secrète :* l'échange de données confidentielles nécessite, au début l'échange d'une clé secrète que l'on ne partagera que avec notre interlocuteur. Il est donc nécessaire d'avoir un canal sécurisé, ou de rencontrer en personne notre interlocuteur, afin d'être certain que cette dernière ne soit pas compromise. Cette clé aura une influence sur la manière de « cacher » l'information.
- *La stéganographie à clé public :* la personne voulant envoyer des données à un autre destinataire, sans éveiller de soupçons, utilisera la clé publique de ce dernier. La clé publique étant à priori connue de tout le monde, il n'y aura pas besoin d'échange préalable « sécurisé ». Le destinataire sera le seul à pouvoir en extraire son contenu à l'aide de sa clé privée [20].

II.4.2.1 Stéganographie pure :

Un système stéganographique est considéré comme pur quand il ne requiert aucun échange préalable de données, comme une clé par exemple. *S. Katzenbeisser* [25] propose la modélisation suivante :

Soit la fonction d'insertion E : C x M $\rightarrow$ C, où :

C est l'ensemble de tous les medias vierges possibles.

M est l'ensemble de messages.

Soit D : C → M, la fonction d'extraction du message. L'émetteur et le récepteur doivent tous les deux posséder les fonctions E et D, mais l'algorithme général n'a pas besoin d'être public.

Le quadruplet S = (C,M,D,E), tel que D(E(c,m)) = m, ∀ m∈ M, et appelé système de stéganographie pur.

II.4.2.2 Stéganographie à clé secrète :

La sécurité du système repose sur le secret de l'algorithme, ce qui va à l'encontre du principe de *Kerchoffs* [25] qui dit que la sécurité d'un algorithme ne doit pas résider que dans un paramétrage par une clé.

La stéganographie est similaire au chiffrement à clé secrète. L'émetteur choisit donc à la fois le medium **m** et la clé secrète **k**. Si le récepteur recevant le stégo-medium **m'**, ne dispose pas de la même clé **k**, il est dans l'incapacité d'extraire le message. Il est donc nécessaire de prévoir une solution pour transmettre la clé de l'émetteur au récepteur, ce qui demande l'existence d'un autre canal sécurisé entre l'émetteur et le récepteur.

Alors on note **K** l'ensemble de toutes les clés d'insertion et d'extraction :

$$E_k : C \times V \times K \rightarrow C$$

$$D_k : C \times K \rightarrow M$$

Le quintuple S = (C, M, K, E_k , D_k), tel que D_k (E_k (c, m)) = m, ∀ m ∈ M et c ∈ C est appelé système de stéganographie à clé secrète.

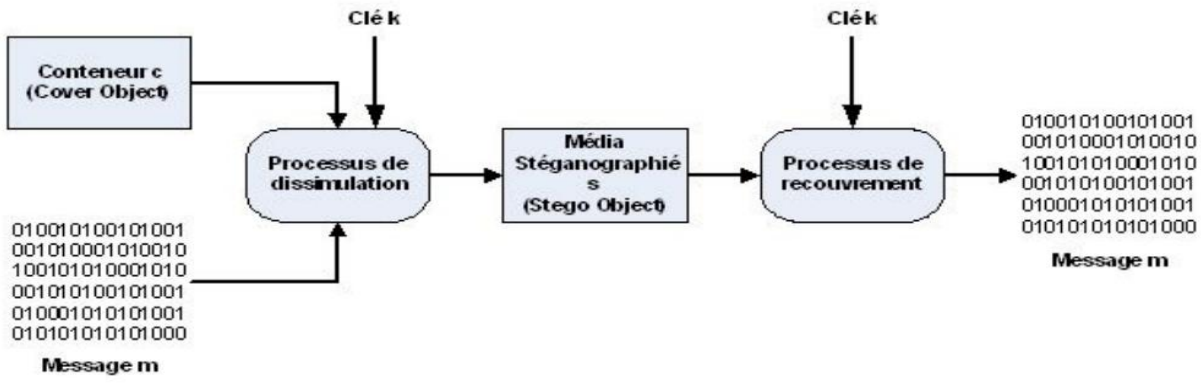


Figure II.6 : schéma qui explique le processus stéganographique [20].

II.4.2.3 Stéganographie à clé publique :

Là, un utilisateur dépose de deux clés, une publique et l'autre privée, la première pour dissimuler le message et la deuxième pour l'extraire.

Nous noterons $K_{pu}(X)$ la clé publique de X et $K_{pr}(X)$ sa clé privée [25].

II.5 Les différents types et supports de stéganographie :

On distingue deux types de stéganographie : la stéganographie linguistique et la stéganographie technique :

II.5.1 La stéganographie linguistique :

La technique linguistique est utilisée pour cacher le message dans un texte de couverture (original), d'une manière non-évidente de sorte que la présence du message est indétectable par un étranger [26].

La littérature de la stéganographie linguistique, dans laquelle les propriétés linguistiques d'un texte sont modifiées pour cacher l'information, est faible par rapport à d'autres médias. Parce qu'il est plus facile d'apporter des modifications aux médias non linguistiques dans lequel le message secret sera indétectable par un observateur [13].

Il existe plusieurs formes de stéganographie linguistique :

a) Sémagramme :

C'est la forme la plus connue [13], elle utilise uniquement des symboles et des signes pour cacher les données [26]. *Alfred de Musset* [13] est le plus intéressé ou l'utilisateur le plus connu de ce procédé, il a entretenu, entre 1833 et 1834, une relation secrète avec *Georges Sand* au travers de poèmes qu'il lui envoyait [13,27]. Cette forme est devisée en deux catégories [26]:

i) Sémagramme visuel : utilise les objets physiques de chaque jour pour transmettre un message, (Ex : le positionnement des articles sur un site WEB particulier).

ii) Sémagramme de texte : ce type est utilisé pour cacher un message en modifiant la forme de texte de l'operateur ou en changeant la taille et le type de police, ou ajouter un espace supplémentaire entre les mots [26].

b) Acrostiche :

Ce procédé consiste à transmettre des informations à travers les premières lettres dans chaque vers de poème et qui, lus de haut en bas, pour former un mot ou une expression. Elle a plusieurs variantes (mot placés dans des vers ou des chapitres,…) [13].

c) Ponctuation :

Les prisonniers de guerre ont utilisé la ponctuation (points et virgules) pour transmettre des messages à leurs familles [13].

d) Nulle :

Les nulles ou les codes camouflés, ayant comme principe de marquer certaines lettres d'un texte par des piqûres d'aiguilles ou encore par la hauteur des lettres. Il suffit alors de rassembler ces lettres marquées pour former un mot ou une expression pour le premier cas, et dans le second cas deux tailles de caractères sont utilisées, le message étant constitué des lettres soit de petites tailles, soit de grandes tailles selon la convention adoptée pour l'échange [13,27].

II.5.2 La stéganographie technique :

La stéganographie technique utilise des outils spéciaux, des dispositifs ou méthodes scientifiques pour cacher un message. Dans ce type, on peut utiliser l'encre invisible, micro points, méthodes informatiques pour garder le secret du message.

Le message de couverture est le porteur du message tel qu'image, vidéo, audio, texte ou un autre support numérique [28]. La couverture est divisée en blocs et bits du message qui sont cachés dans chaque bloc. L'information est encodée en changeant divers propriétés de l'image de couverture. Les blocs de couverture restent inchangés si le bloc de message est zéro [29].

a) Stéganographie de texte :

Dans cette approche, le texte de couverture est produit en générant des séquences de caractères aléatoires, changeant des mots dans un texte, en utilisant des grammaires contextuelles ou en changeant la mise en forme d'un texte existant pour cacher le message. Le texte de couverture généré par cette approche peut se qualifier pour la stéganographie linguistique si le texte est linguistique. Bien que ces méthodes basées sur le texte aient leur

propres caractéristiques uniques pour le texte de couverture, mais souffre de divers problèmes d'un point de vue linguistique et de sécurité [30].

b) Stéganographie de l'image :

Cette technique de stéganographie est la plus populaire en ces dernières années par rapport à d'autres types 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. Un schéma d'image stéganographique est un type de système stéganographique, où le message secret est caché dans une image numérique avec une méthode de dissimulation. Les différentes méthodes de la stéganographie d'image sont [30] :

- Méthode de dissimulation de données : pour utiliser le système il est nécessaire d'avoir un nom d'utilisateur et un mot de passe. Une fois l'utilisateur est connecté dans le système il peut utiliser les données avec la clé secrète pour dissimuler les informations à l'intérieur de l'image choisie [26].
- Méthode d'intégration de données : une clé secrète est nécessaire pour récupérer les données qui ont été intégrées à l'intérieur de l'image. Ces données ne peuvent pas être récupérer de l'image sans la clé secrète, c'est pour assurer l'intégrité et la confidentialité des données. Le message secret qui est extrait du système est transféré dans le fichier texte, puis ce dernier est compressé dans le zip fichier et le fichier texte zip le convertit en codes binaires [26].
- Méthode d'extraction de données : elle consiste a récupéré le message original dissimulé dans l'image d'origine, dont une clé secrète est indispensable pour le décodage et l'extraction [26].

c) Stéganographie audio :

La stéganographie 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 [26].

II.6 Autres types de supports :

- **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.

- **Systèmes 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.

Le système de fichier laisse la possibilité d'utiliser des techniques de stéganographie. Pour cacher des données, il suffit de les stocker dans ce dernier bloc; si la taille de ces données dépassent 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.

Il existe plusieurs outils dans le web de bas niveau comme b map et slacker, permettant d'analyser en détails les blocs utilisés et récupérer l'espace libre.

- **Fichier exécutable :**

Les fichiers exécutables peuvent êtres 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 à besoin. Donc il est possible de bénéficier les parties du code non exécuté [27].

II.7 Caractéristiques :

La stéganographie possède trois grandes caractéristiques qui dirigent son utilisation :

- **La capacité (données utiles) :**

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 du message secret insérés par pixel. Dans le domaine fréquentiel, par exemple insertion des coefficients quantifiés d'une image JPEG, la capacité d'insertion relative peut être exprimée par le nombre des bits du message secret à insérer par chaque coefficient DCT quantifié non-nul [13,19].

- **Sécurité (in-détectabilité) :**

Dans le problème des prisonniers par exemple, la sécurité ou l'in-détectabilité réside dans le fait que le gardien ne peut pas détecter la communication secrète.

Les actions utilisées pour détecter l'existence de stéganographie sont appelées, la stéganalyse. On trouve ainsi dans la littérature aussi bien des travaux portant sur des techniques de stéganalyse [31] que sur des façons de s'en protéger [32].

Donc on dit qu'un système stéganographique est sécurisé quand l'opération de stéganalyse pour détecter la stéganographie a échouée.

- **La robustesse :**

Spécifie la capacité qu'a notre message reste intacte après que le conteneur ait subit des modifications [20].

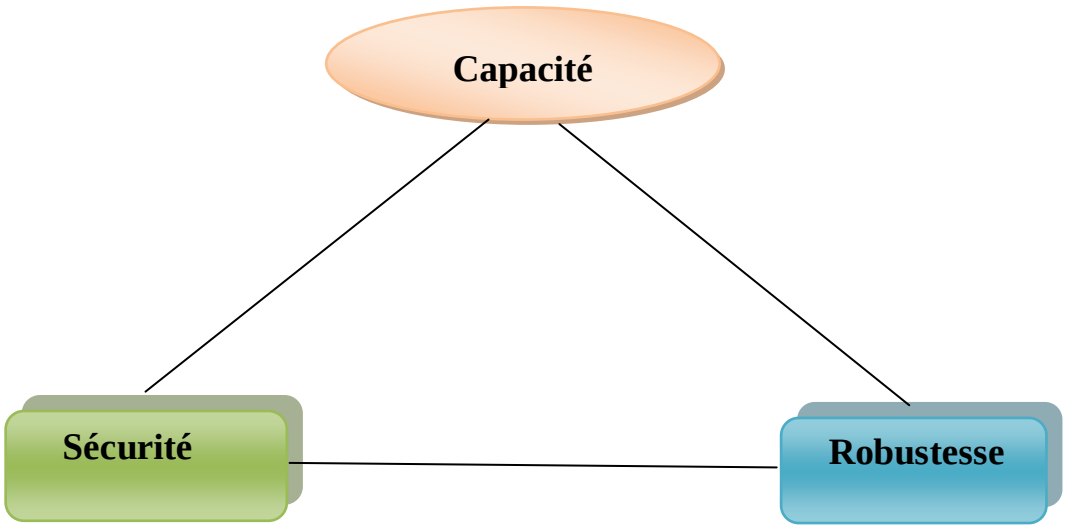


Figure II.7 : Triangle des caractéristiques [20].

En stéganographie, une propriété essentielle est l'in-détectabilité statique puisqu'une personne surveillant le canal de communication ne doit pas pouvoir différencier un médium d'un stégo-médium. De plus, comme le message constitue l'information principale, la capacité doit aussi être assez élevée. Quant à la robustesse, elle constitue une défense contre les modifications subies par le stégo-médium. Néanmoins, la meilleure défense reste l'incapacité de l'adversaire à détecter le message. Ainsi, la plupart du temps, le canal ne modifie pas le stégo-médium et les besoins en robustesse sont minimes. En revanche, des mesures doivent être prises lorsque l'adversaire est actif, soit en termes de robustesse, soit pour contrôler l'intégrité du message afin de détecter un éventuel changement dans celui-ci [33].

II.8 Domaines de la stéganographie :

La stéganographie est composée de deux domaines, le domaine spatial et le domaine fréquentiel. Dans le premier domaine, le message secret est inséré dans les pixels de l'image porteuse tandis que le domaine fréquentiel, les pixels sont transformés en coefficients, et le message secret est inséré dans ces coefficients [13,34,35].

a) Domaine spatial :

La stéganographie spatiale a un principe de faire changer les bits de pixels de l'image pour insérer les bits du message secret. La technique LSB est l'une des techniques la plus

simple et la plus utilisée. Elle consiste à cacher un message secret par l'insertion des bits de ses pixels à la place des bits de poids faible des pixels de l'image, de sorte que les distorsions apportées par le processus d'insertion restent non perceptible. La raison est que les variations de la valeur du LSB sont imperceptibles pour l'œil humain.

La stéganographie par la substitution de LSB et la stéganographie par correspondance de LSB sont des exemples de techniques de stéganographie dans le domaine spatial [13].

Ces techniques sont parmi les plus simples en termes d'intégration et la complexité d'extraction. L'inconvénient le plus influant de ces méthodes est la qualité de bruit additif, qui s'insinue dans l'image qui affecte directement le rapport signal sur bruit maximal et les propriétés statistiques de l'image.

De plus, ces algorithmes d'intégration sont applicables principalement à la compression d'image sans perte régime comme les images TIFF [36].

b) Domaine fréquentiel :

Dans ce domaine, le message est inséré dans les coefficients transformés de l'image, ce qui permet d'apporter plus de robustesse contre les attaques. La stéganographie fréquentielle est considérée comme une technique essentielle de dissimulation de l'information secrète. La stéganographie fréquentielle permet de cacher l'information dans des zones de l'image moins sensibles à la compression [13].

La stéganographie dans le domaine des transformées est majoritairement utilisée dans le cadre de dissimulation effectuée sur le format JPEG/JIFF. Au lieu et à la place d'utiliser les pixels de l'image pour cacher l'information, ce sont les coefficients DCT de la transformée en Cosinus Discrète qui sont utilisés. Comme dans le domaine spatial, la méthode principalement utilisée est celle des modifications de LSB, mais les modifications sont, cette fois, appliquées aux coefficients DCT et non plus aux valeurs des pixels.

L'énorme avantage de ce type de méthode est son large prolifération du format utilisé. En effet, les images aux formats JPEG/JIFF sont de loin des fichiers le plus présents sur le World Wide Web.

La stéganographie dans le domaine des transformées sur support JPEG semble être une solution de choix. Toutefois, la complexité du format JPEG fait que très peu de logiciels dissimulent réellement les données en fin de fichier.

Jsteg fut le premier produit à implémenter cette méthode. Les produits découlant du domaine académique, tels que F5 ou Outguess, suivent la même voie. Un seul produit commercial semble agir dans le domaine des transformées, il s'agit de steganosPrivacy (anciennement Security) [19,20].

II.9 Utilisation de la stéganographie :

1. La stéganographie permet d'envoyer des données et des informations sans être censuré et sans la peur que les messages étant interceptés et retracés jusqu'à nous.

2. Elle est utilisée aussi pour le stockage des informations sur un emplacement. Par exemple, plusieurs sources d'informations comme nos données bancaires privées, certains secrets militaires, peuvent être stockés dans une source de couverture. Lorsque nous somme tenus de révéler l'information secrète dans notre source de couverture, nous pouvons simplement révéler nos informations bancaires et il sera être possible de prouver l'existence des secrets militaires à l'intérieur.

3. La stéganographie peut également être utilisée pour l'application de tatouage, il existe plusieurs techniques stéganographiques qui sont utilisées pour stocker des filigranes dans les données. La principale différance est dans l'intention, alors que l'objectif de la stéganographie est de cacher des données, le tatouage est simplement étendre la source de couverture avec une information supplémentaire. Puisque les gens n'acceptent pas de changements notables dans les images, fichiers audio ou vidéo en raison d'un filigrane, les méthodes stéganographiques peuvent être utilisées pour cacher cela.

4. La stéganographie est utilisée dans le commerce électronique, d'où la plupart des utilisateurs sont protégés par un nom d'utilisateur et un mot de passe dans les transactions électroniques actuelles, sans une véritable méthode de vérification, l'utilisateur est le détenteur de la carte. La numérisation biométrique d'empreintes digitales, combinée avec des identifiants de session uniques intégrés dans l'empreinte digitale d'images via stéganographie, permettent une option très sécurisée pour ouvrir la vérification des transactions de commerce électronique.

5. autrement la stéganographie est utilisé dans le transport de données sensibles qu'on doit passées discrètement [37].

II.10 Les techniques de stéganographie :

Il existe plusieurs techniques de stéganographie, on peut citer :

1. Bit de poids faible (LSB) :

C'est la technique la plus répandue du domaine spatial [38]. Son succès provient d'une grande facilité de mise en œuvre, ce qui permet d'en trouver de nombreuses implémentations.

Sous l'appellation LSB est regroupé tout ce qui a trait à la dissimulation de données par la modification du bit de poids faible d'un élément. Cela va de la valeur d'un pixel, jusqu'à la modification de la valeur d'un coefficient DCT dans le cas de la norme JPEG. Tous se basent sur l'insensibilité du système visuel humain à un faible changement de couleurs [20].

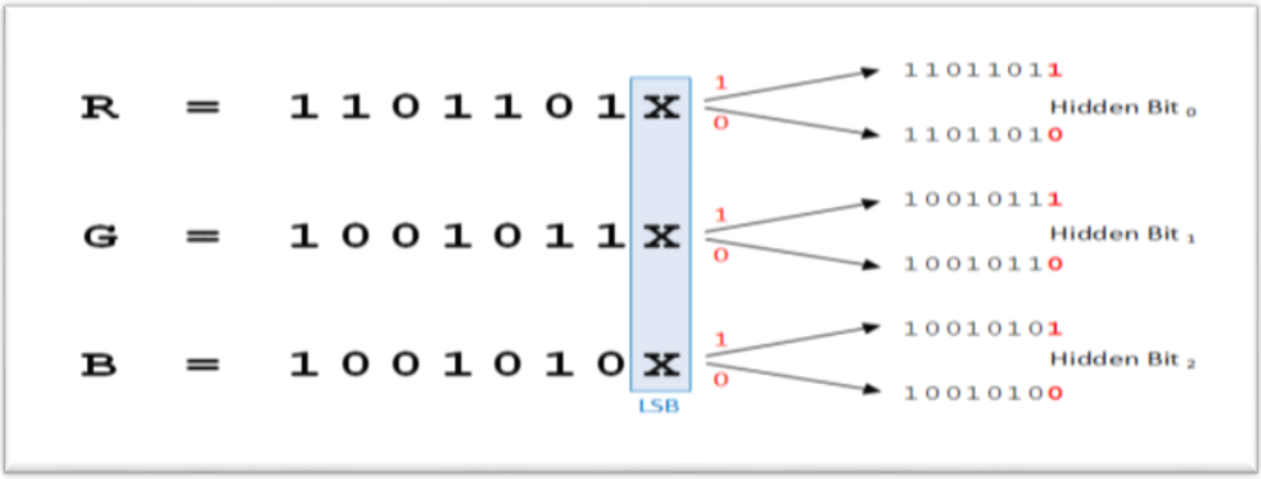


Figure II.8 : Exemple de conversion LSB [38].

2. F5 :

L'algorithme F5 pour les images JPEG est un algorithme par correspondance qui insère les bits du message secret dans les coefficients AC DCT non-nuls. Pour l'insertion, il utilise la technique de codage matriciel, afin de réduire le nombre total de modifications à effectuer sur le support hôte [19]. Le F5 contient deux ingrédients importants :

- Opération d'intégration
- Intégration de la matrice [39].

Image Originale.

Image F5.

Figure II.9 : Exemple d'algorithme F5.

3. Transformée de Fourier (FFT) :

La transformée de Fourier est un outil important de traitement d'images, utilisée pour décomposer une image suivant ses composantes en sinus et cosinus. La sortie de la transformation représente l'image dans le domaine fréquentiel, tandis que l'image d'entrée est dans le domaine spatial équivalent. La transformée de Fourier est utilisée dans une large gamme d'applications telles que l'analyse, le filtrage ou la compression d'images [40].

4. Transformée de Cosinus Discrète (DCT) :

La transformée en cosinus discrète est similaire à la transformée de Fourier discrète. La DCT transforme le signal ou l'image du domaine spatial au domaine fréquentiel. La DCT est utilisée dans la stéganographie comme l'image est divisée en blocs de 8×8 pixels et transforme ces blocs de pixels en 64 DCT, et appliquée à chaque bloc. Grace à la table de quantification, chaque bloc est compressé pour mettre à l'échelle les coefficients DCT et le message est intégré dans ces coefficients. Le tableau de blocs compressés constitue l'image est stocké d'une manière drastiquement réduit la quantité d'espace. Si désiré, l'image est reconstruite grâce à la décompression, un processus qui utilise l'inverse de transformée en cosinus discrète, c'est-à-dire IDCT [41].

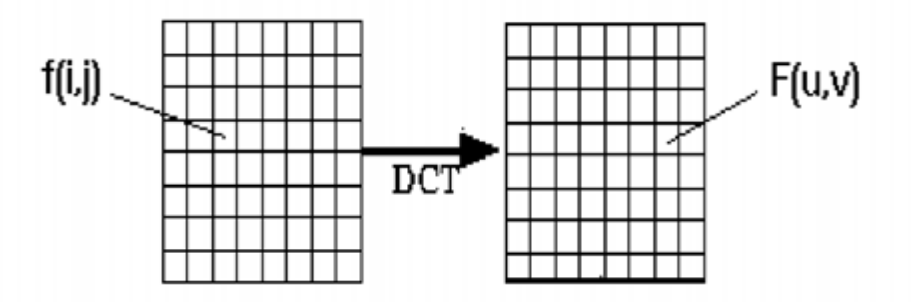


Figure II.10 : Processus de DCT.

5. Transformée en ondelettes (DWT) :

Est un outil très utilisé pour transformer l'image d'un domaine spatial en domaine fréquentiel. Dans le processus de la stéganographie, la DWT identifie la haute fréquence et la basse fréquence de l'information de chaque pixel de l'image. Principalement utilisée pour le traitement des signaux non stationnaires.

Le transformée en ondelettes est basée sur de petites vagues, connues sous le nom de ondelettes, de fréquence différente et de durée limitée. Le DWT est le modèle précis que la DFT ou la DCT et elle à la description de la multi-résolution de l'image [42].

6. Stéganographie par étalement de spectre (SSIS) :

L'algorithme de stéganographie par étalement de spectre (SSIS) est un exemple d'algorithme de stéganographie robuste car il peut supporter une certaine distorsion avant la perte de messages. Cependant, son attractivité à cet égard est attirée par sa grande complexité de calcul.

L'idée principale derrière l'étalement de spectre réside dans la distribution d'informations dans plusieurs fréquences de travail d'un signal donné, (élargissement de la bande de fréquence du signal d'entrée et la redistribution de l'information dans le domaine nouvellement étendu). Cette technique n'est pas nouvelle, son utilisation dans plusieurs technologies de communication est bien établie.

Ses applications principales sont dues au désir de résistance aux signaux de brouillage qui pourraient interférer avec le signal d'entrée sur une gamme de fréquences donnée [43].

Image original.

Image SSIS.

Figure II.11 : Exemple d'Algorithme SSIS.

II.11 Comparaison entre les techniques de la dissimulation de données :

1. Stéganographie vs Cryptographie :

En cryptographie, l'objectif n'est pas de dissimuler des informations dans d'autres, mais plus simplement de rendre l'information que l'on désire transmettre complètement illisible à toute personne ne possédant pas la donnée nécessaire à son décodage [23]. D'autre part la stéganographie permet de cacher le message de sorte qu'il n'y a pas de détection de l'existence du message. Avec la cryptographie, la comparaison est faite entre des parties de texte en clair et des parties du texte chiffré. Dans la steganographie, des comparaisons peuvent être faites entre les milieux de couverture, le stego-media, et les parties possibles du message.

Le résultat final en cryptographie est le texte chiffré, alors que le résultat final en stéganographie est le stego-medium [37].

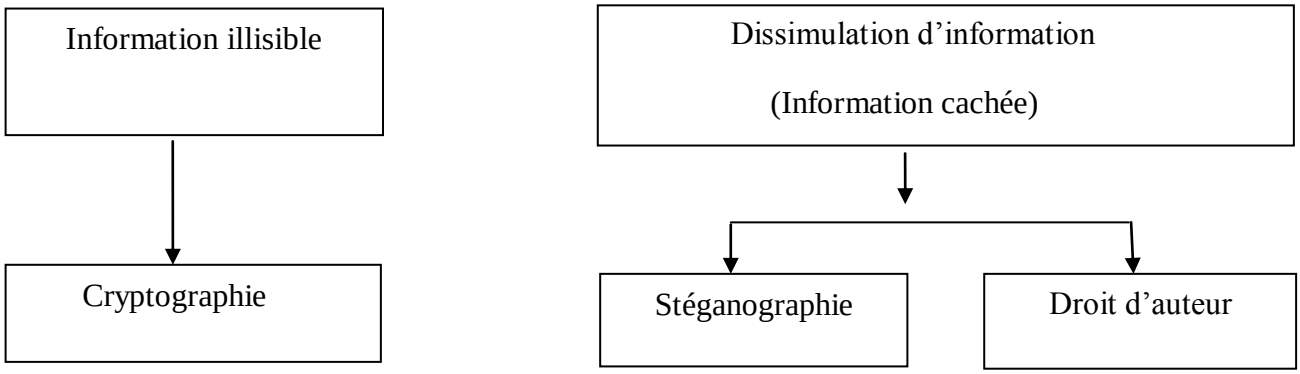


Figure II.12 : Diagramme représentant la dissimulation d'information vs cryptographie [27].

2. Stéganographie vs Marquage :

La stéganographie et le marquage sont deux techniques très proches l'une de l'autre, mais qui n'ont pas les mêmes objectifs, ni les mêmes contraintes.

La différence entre la stéganographie et le marquage, est que dans la stéganographie, l'existence du message caché doit rester secrète alors que pour le marquage seul le message doit rester caché mais son existence (tant qu'on ne peut détecter) peut être connue [22].

Une autre différence très importante entre la stéganographie et le marquage se situe au niveau des attaques qui peuvent avoir lieu contre ces techniques. En stéganographie, le pirate va cacher à lire les données dissimulées dans le document, tandis que dans le cas d'un document marqué il va chercher à laver le document de toute signature possible : c.-à-d. supprimer la marque (ou alors il peut essayer d'usurper l'identité de l'auteur en remplaçant la marque) [23].

II.12 La stéganalyse :

Plusieurs études ont été réalisées pour détecter la présence de données ou d'informations cachées à l'aide d'un algorithme de stéganographie [19,20]. Ce type d'étude forme ce qu'on appel la stéganalyse ou l'analyse stéganographique [20]. Elle correspond à la discipline duale de la stéganographie [19], donc l'analyse stéganographique représente les moyens mis en œuvre pour déceler la présence d'une communication secrète [16].

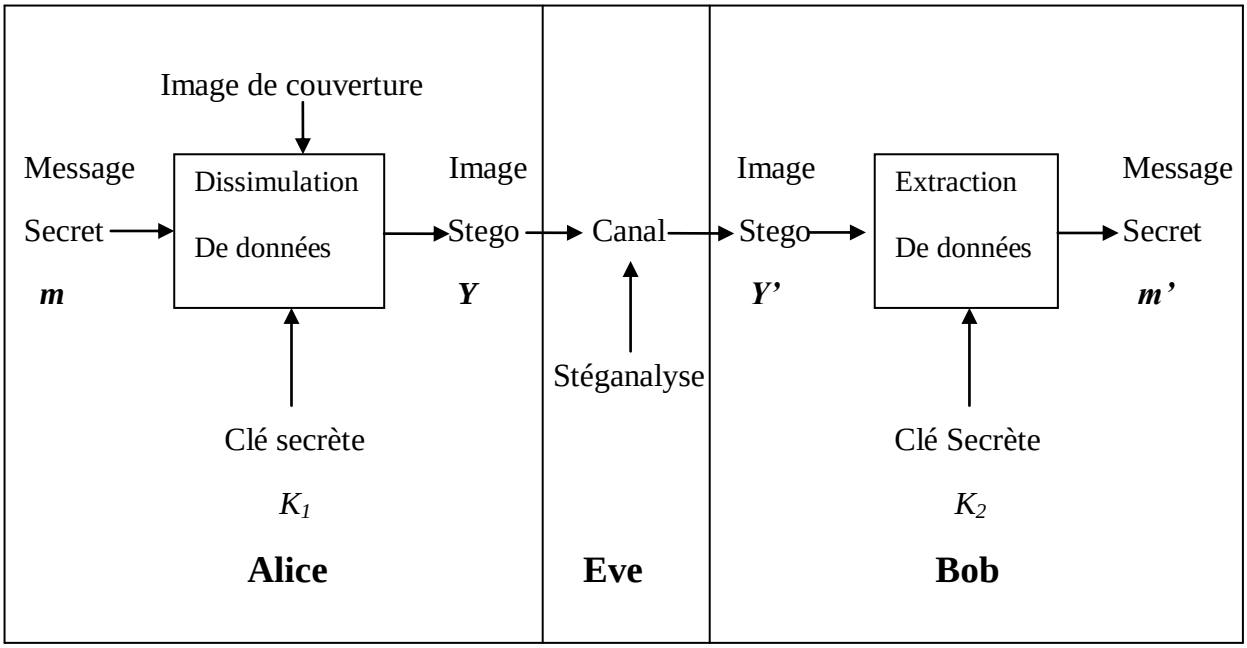


Figure II.13 : problème des prisonniers [20].

II.12.1 Attaque d'un schéma de stéganographie :

La cryptographie est une technique qui sert à récupérer le message, ayant été préalablement crypté, sans connaissance de la clé, tandis que la stéganalyse consiste initialement à la détection de l'existence des données cachées et n'en pas les extraire.

Dans le cas de la stéganographie par modification d'un médium dit empirique qu'on va le citer ensuite (par exemple images numériques naturelles), la stéganalyse revient en pratique à vérifier la statistique du support intercepté, pour déterminer si elle est altérée ou non par un algorithme particulier. De manière plus formelle, pour un support donné $x=(x_1,\ldots,x_n)$, le problème de détection du message secret peut être représenté comme un test entre deux hypothèses [19,20] :

$H_0 = x \sim P_c$

$H_1 = x \sim P_s$

H_0 : Le support x ne contient pas de message caché (cover).

H_1 : Le support x contient un message caché (stego).

La stéganalyse, représentée par la gardienne Eve dans le problème des prisonniers doit donc décider entre ces deux hypothèses pour juger si oui ou non le medium est stéganographié.

Comme indiqué précédemment, il existe trois types de stéganalyse qui différent selon les objectifs recherchés et les moyens utilisés :

- *La stéganalyse à gardien passif :* se contente uniquement de décider si oui ou non le support intercepté est porteur de message caché. En d'autres termes, le rôle du stéganalyse (la gardienne Eve) se limite uniquement à un test d'hypothèses H_0, H_1.
- *La stéganalyse à gardien actif :* peut faire le test d'hypothèse, mais en plus elle a pour objectif d'empêcher la communication de données secrètes. Pour ce faire, la stéganalyse va essayer d'apporter quelques modifications sur le medium intercepté (compression, filtrage...etc.) dans le but de détruire le message caché s'il existe.
- *La stéganalyse à gardien malicieux :* va plus loin que la stéganalyse à gardien passif ou actif. Le but du stéganalyse, pour ce type d'analyse, est de comprendre la technique stéganographique utilisée, et même extraire le message secret. Une fois extrait, la stéganalyse peut contourner le message secret pour ses propres fins. Il peut même réintroduire un autre message falsifié.

Pour ce type de stéganalyse, un protocole de stéganographie à clé publique est proposé, luttant contre la modification et la falsification du message secret [19,20].

II.13 Conclusion :

Le travail présenté dans ce chapitre consiste à expliquer la technique de dissimulation d'informations (stéganographie). L'image est l'une des supports les plus largement utilisés par la stéganographie. La raison de l'importance de ce type de support dans le domaine de dissimulation secrète réside dans les différents types d'images numériques.

Le chapitre qui suit décrit quelques Algorithmes de stéganographie implémentés dans le cadre de notre projet de fin d'études, tel que le LSB.

Chapitre 03 : Réalisations & Résultats

III.1 Introduction :

La stéganographie est l'art et la science de cacher ou dissimuler des informations, dont l'objectif est de transmettre un message de manière dans laquelle aucune personne ne peut détecter l'existence de ce message entre l'émetteur et le récepteur.

Le message secret peut être un texte en clair, un texte chiffré ou des images. L'incorporation du message dans une couverture objet entraine la production d'une image stego, les images sont principalement utilisées comme objets de couverture dans la stéganographie.

Il existe plusieurs techniques de stéganographie de l'image qui sont classées en domaine spatial et domaine fréquentiel (transformé) [44], les techniques du domaine spatial sont des systèmes simples tels que le bit le moins significatif (LSB) [45], d'où le bit le moins significatif est la plus petite valeur d'un nombre binaire. Dans l'algorithme LSB, les données sont cachées dans le moins des parties significatives de l'image de couverture qui sont pas perceptibles lorsqu'elles sont vues avec l'œil humain [44].

Alors que le schéma du domaine fréquentiel est utilisé pour cacher une grande quantité d'informations, il cache les données dans le domaine de fréquence en modifiant la magnitude de toutes les transformées de l'image de couverture. On distingue la Transformée en Cosinus Discret (DCT), et la Transformée en Ondelettes qui sont les principaux types, ces transformations ont tous des coefficients associés à leurs pixels. Les données secrètes sont cachées dans ces coefficients qui définissent également comment l'image ou le fichier devrait être transformé [44].

Dans ce chapitre, on va présenter, tester et comparer les algorithmes de steganographie réalisés au sein de notre projet de fin d'études en commençant par la technique LSB, ensuite les approches proposées à savoir : LSB-Contour et LSB-DCT.

III.2 Algorithmes de Stéganographie :

III.2.1 Domaine spatial :

III.2.1.1Bit de poids faible :

En premier lieu, nous avons essayé de faire un système stéganographique en se basant sur l'algorithme LSB. La technique LSB (Low State Binary) est implémentée dans le domaine spatial. L'utilisation de cette méthode est très simple, aux limites évidentes. Elle consiste à insérer des données uniquement au niveau des bits de poids faible de l'image [46].

La technique d'enrobage dans l'algorithme consiste à remplacer le bit de poids faible du pixel (I (i, j)) par les bits du message un par un. D'où si le message est équivalent à m-bits il y a m-pixels à traiter, dont les bits les moins significatifs seront remplacés par les m bits du message. Le processus d'intégration peut être décrit en utilisant l'équation suivante :

LSB (I (i, j)) =1 et m= 0 ⇨ I_s (i, j) = I (i, j) – 1.

LSB (I (i, j)) = m ⇨ I_s (i, j) = I (i, j).

LSB (I (i, j)) = 0 et m= 1 ⇨ I_s (i, j) = I (i, j) + 1.

- I (i, j) : Le pixel de l'image originale.
- I_s (i, j) : Le pixel de l'image stego qui contient le message secret.
- LSB : Est le bit de poids faible de chaque pixel de l'image.
- m : Le bit de message.

En général, une image p-by-q est simplement une matrice p-by-q, où chaque entrée de la matrice est un entier positif appelé pixel value, qui détermine la couleur de ce pixel. Ces valeurs de pixels sont comprises entre 0 et 2^n-1, pour une image à n bits [47]

Exemple :

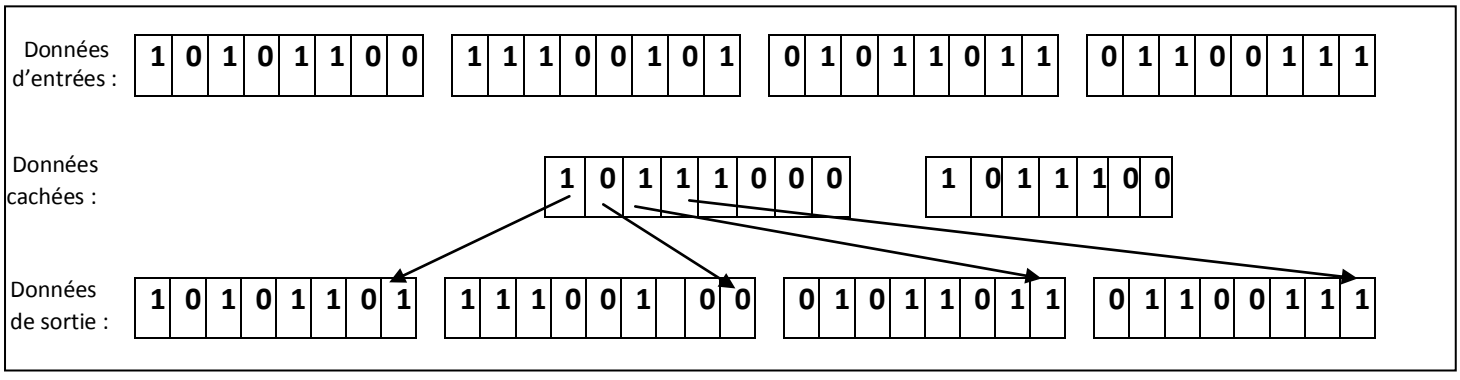


Figure III.1 : Exemple d'insertion du message avec la méthode LSB.

➢ **Algorithme d'insertion :**

C'est l'algorithme le plus simple de la dissimulation, le concept de base de la substitution de bits poids faible inclut l'incorporation des données secrètes aux bits qui ont une pondération minimale de sorte qu'elle n'affecte pas la valeur du pixel d'origine [39].

❖ Voici le schéma d'insertion du message :

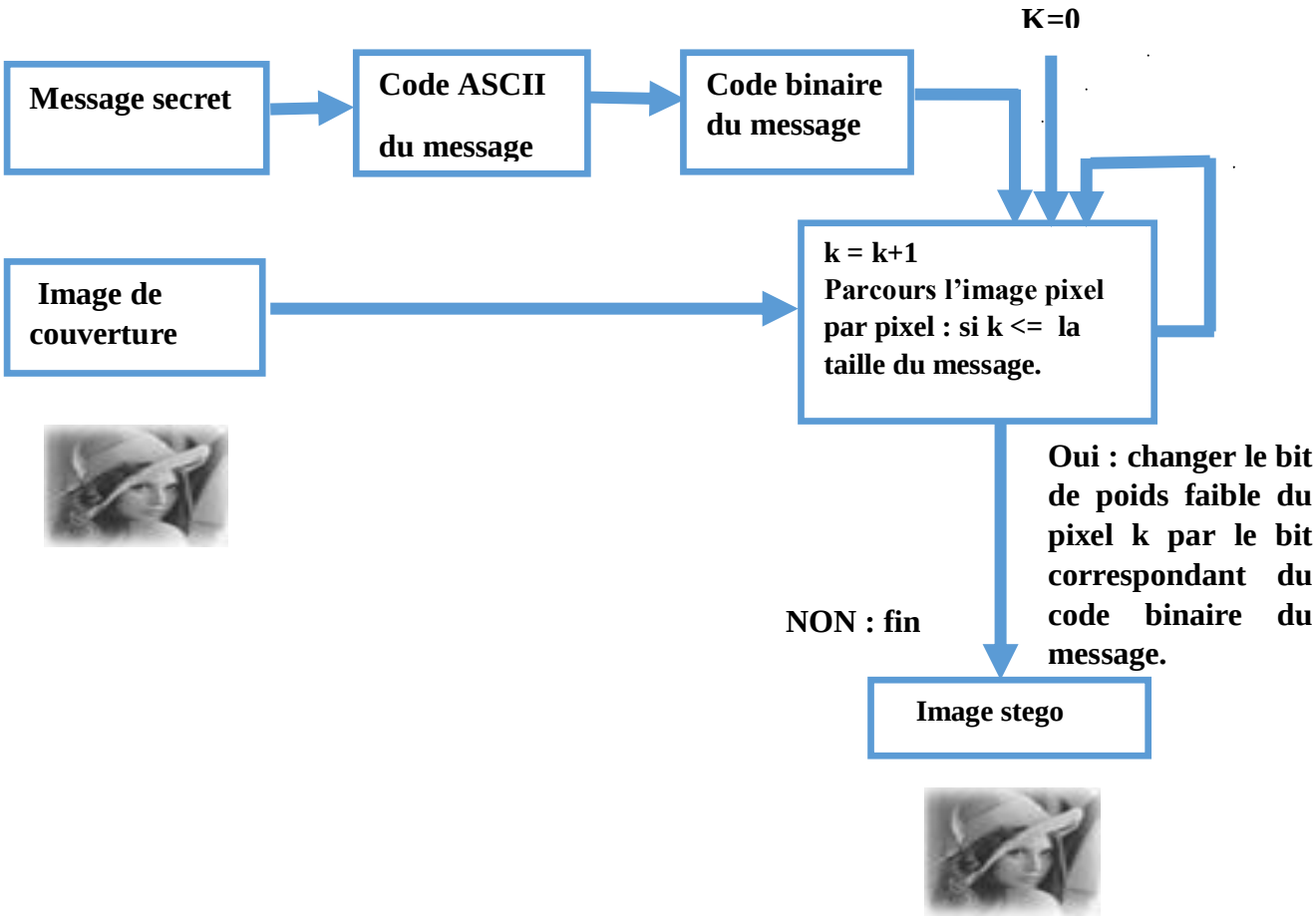


Figure III.2 : Schéma d'insertion du message.

- **Les étapes d'insertion d'un message secret :**

Étape 1: Lisez l'image de couverture et le message texte qui doit être caché dans l'image de couverture.

Étape 2: Convertissez le message texte au format Ascii puis en code binaire.

Étape 3: Calculez le LSB de chaque pixel de l'image de couverture. (Par la division de chaque pixel par 2. Où le reste de cette division représente le bit de poids faible).

Étape 4: Remplacer l'image de couverture du LSB avec chaque bit du message secret un par un.

Étape 5: Ecrire l'image stego.

- **Le Code ASCII (American Standard Code for Information Inter change) :**

C'est un Unicode qui permet de coder les caractères en décimal, ce code est standardisé de 256 caractères.

- **Algorithme d'extraction :**

L'extraction est définie comme les pixels de mappage à l'image. Dans la stéganographie d'image, le processus d'extraction peut être effectué sur un message qui est l'image stego. Le destinataire entre l'image stego et, le cas échéant, la clé stéganographique, dans un algorithme d'extraction qui génère le message secret.

Cet algorithme d'extraction est considéré comme l'inverse de l'algorithme d'intégration, bien que les algorithmes d'intégration et d'extraction puissent être créés de telle sorte que l'algorithme d'extraction ne soit pas réellement l'inverse mathématique de l'algorithme d'incorporation. Plusieurs facteurs influencent sur l'efficacité d'un système stéganographique, dont le plus important est le choix de l'image de couverture [48].

- **Les étapes d'extraction d'un message secret:**

Étape 1: Lisez l'image stego.

Étape 2: Extraire les bits du message un par un, et reconstruire le code binaire de message.

Étape 3: Convertir ce code binaire en code Ascii, puis décoder ce dernier pour obtenir le message caché (caractères).

Exemple 01 :

Voici un exemple d'une image RGB (a) sur laquelle l'algorithme LSB est appliqué, et (b) l'image stego résultante qui contient le message secret. On remarque que l'image stego ressemble à celle de couverture et que l'œil humain ne peut pas détecter la déférence.

(a) Image RGB originale

(b) Image RGB par la méthode LSB.

Figure III.3 : Exemple de LSB.

Exemple 02 :

- Une grille de 3 pixels pour une image 24 bits peut être donnée comme suit :

(01010101 01011100 11011000)

(10110110 11111100 00110100)

(11011110 10110010 10110101)

Lorsque le nombre 300 est inséré dans les bits de poids faible de cette partie de l'image.

C: 10000011

- La grille résultante est la suivante :

(01010101 01011100 11011000)

(10110110 11111100 00110100)

(1101111**1** 1011001**1** 10110101)

Dans l'exemple ci-dessus, le nombre C a été intégré aux 8 premiers octets de la grille et seuls et uniquement 2 bits doivent être modifiés en fonction du message incorporé [46].

- **Inconvénients :**
  - La facilité de détection.
  - N'est utilisé que pour les formats compressés sans perte d'information.

Pour éliminer ces inconvénients, nous avons proposé une nouvelle méthode qui est l'approche LSB-Contour.

III.2.1.2 Approche proposée : LSB-Contour :

III.2.1.2.1 Détection de contours :

Une caractéristique élémentaire et majeure d'une image est les arêtes (contours), d'où les données principales de l'image ont été effectuées par bords. Un bord est défini par la limite avec laquelle il sépare l'intensité supérieure de l'image de celle des intensités inferieures. Les valeurs de bord se présentent de manière aléatoire sur toute la longueur de l'image, et présentent donc une perspective plus sécurisée. La détection des contours pour une image peut aider à la segmentation de l'image, à la compression des données et à la bonne adaptation de la reconstruction d'image [47].

La détection de contour d'une image réduit considérablement la quantité de données et filtre les informations qui peuvent être considérées comme moins pertinentes, préservant ainsi les propriétés structurelles importantes d'une image [48].

La détection de bord vise à identifier des points dans une image numérique à laquelle la luminosité de l'image change fortement ou de manière plus discontinue. Les détecteurs de bord suivants sont pratiques [48] :

- ✓ **Détection de Sobel :**

Les dérivés de premier ordre sont approximés numériquement par les différences. Le détecteur de bord Sobel calcule le gradient en utilisant les différences discrètes entre les lignes et les colonnes. L'opérateur se compose d'une paire de noyaux de convolution 3x3 illustrés à la figure suivante [47] :

-1	0	+1
-2	0	+2
-1	0	+1

+1	+2	+1
0	0	0
- 1	-2	-1

Figure III.4 : Masque pour l'operateur Sobel.

Un noyau est simplement l'autre tourné de 90 degrés. Ces noyaux sont conçus pour répondre le maximum aux arêtes à 45 degrés par rapport à la grille de pixels. Un noyau pour chacune des deux orientations perpendiculaires. Les noyaux peuvent être appliqués séparément à l'image d'entrée pour produire des mesures des composantes de gradient dans chaque orientation (appelez-les Gx et Gy). Celles-ci peuvent alors être combinées ensemble

pour trouver la magnitude absolue du gradient à chaque point et l'orientation de ce gradient. La magnitude du gradient est donnée par [47] :

$$|G| = \sqrt{Gx^2 + Gy^2}$$

Bien que généralement une grandeur approximative soit calculée en utilisant :

$$|G| = |Gx| + |Gy|$$

L'angle d'orientation du bord à l'origine du gradient spécial est donné par :

$$\Theta = \arctan(Gy/Gx) - 3\pi/4$$

- ✓ **Détection de Robert :**

Le détecteur de bord Robert utilise les masques de la figure III.8 pour approcher numériquement les premières dérivées en tant que différences entre les pixels adjacents. Le détecteur de Robert est l'un des détecteurs de bords les plus anciens dans le traitement d'images numériques et c'est aussi le plus simple. Ce détecteur est utilisé considérablement moins que d'autres en raison de sa fonctionnalité limitée, c'est-à-dire symétrique et ne peut pas être généralisé pour détecter des arêtes multiples de 45 degrés [47].

+1	0
0	-1

0	+1
-1	0

Figure III.5 : Masque utilisés pour l'opérateur Robert.

- ✓ **Détection de Prewitt :**

Le détecteur de bord Prewitt utilise les masques de la figure III.9 pour se rapprocher numériquement des premières dérivées Gx et Gy.

Le masque de convolution totale 3x3 est utilisé pour détecter le gradient dans les directions x, y. Le filtre Prewitt est une méthode rapide pour la détection des contours. Il ne convient que pour images sans bruit contrastées [47].

-1	0	+1
-1	0	+1
-1	0	+1

Gx

+1	+1	+1
0	0	0
- 1	- 1	- 1

Gy

Figure III.6 : Masque pour l'opérateur Prewitt.

✓ **Détection de Canny :**

La détection de bord de Canny utilise un algorithme à plusieurs étapes pour détecter une large gamme de bords dans les images. La popularité du détecteur Canny edge peut être attribuée à son optimalité selon les trois critères de bonne détection, bonne localisation et réponse unique à un bord [47].

III.2.1.2.2. Algorithme LSB-Contour :

➢ **Algorithme d'insertion :**

Dans des points de contours d'une image, des pixels ont été sélectionnés afin de cacher les données. Un moyen courant de cacher les données est "Insertion de bits de moindre importance". Cette méthode modifie le bit de poids faible de chaque pixel pour correspondre au message à cacher. La sélection des pixels dans lesquels le message sera inséré est très importante car les pixels modifiés dans les zones de l'image où il y a des pixels qui ressemblent le plus à leurs voisins sont beaucoup plus visibles à l'œil nu. Un seul pixel modifié se distingue parmi ses pixels voisins uniformes, ce qui rend l'image suspecte. Une solution possible à ce problème consiste à sélectionner les pixels de contours de l'image pour masquer le message. Cela ne se remarque pas lorsqu'un seul pixel est modifié lorsque ses pixels environnants lui sont le moins semblables. [48]

- **Les étapes d'insertion d'un message secret :**

Pour insérer un message secret dans une image par l'algorithme LSB-Contour, on applique les étapes suivantes :

Étape 1 : Lecture de l'image d'entrée et du message secret.

Étape 2 : Application de la détection des contours (ex, Sobel) sur l'image : L'algorithme de détection d'arêtes (ex, Sobel) est appliqué sur l'image d'entrée pour obtenir des arêtes dans l'image, l'operateur (ex, Sobel) est utilisé ici pour détecter les contours décrits. L'image

détectée par les contours est une image binaire composée de « 1 » aux pixels de contour et de « 0 » aux pixels non latéraux.

Étape 3 : Conversion du message secret en chaine binaire : Le message secret est d'abord converti en son code ASCII équivalent. Ce code ASCII est converti en chaine binaire, c'est-à-dire sous la forme de "1" et de "0".

Étape 4 : Calcule de la longueur totale du message secret : Le totale de la longueur du message secret est calculée pour être utile au récepteur pour extraire le message secret.

Étape 5 : Incorporation de l'image secrète : les bits du message secret sont insérés dans les LSB des pixels de contour. (Si le pixel courant représente un contour et le nombre du pixel parcouru <= la taille du code binaire du message on remplace le LSB par le bit de code binaire)

Étape 6 : Ecrire stego-image : La sortie est une image contenant un message secret.

- Nous avons illustré les étapes précédentes par le schéma suivant :

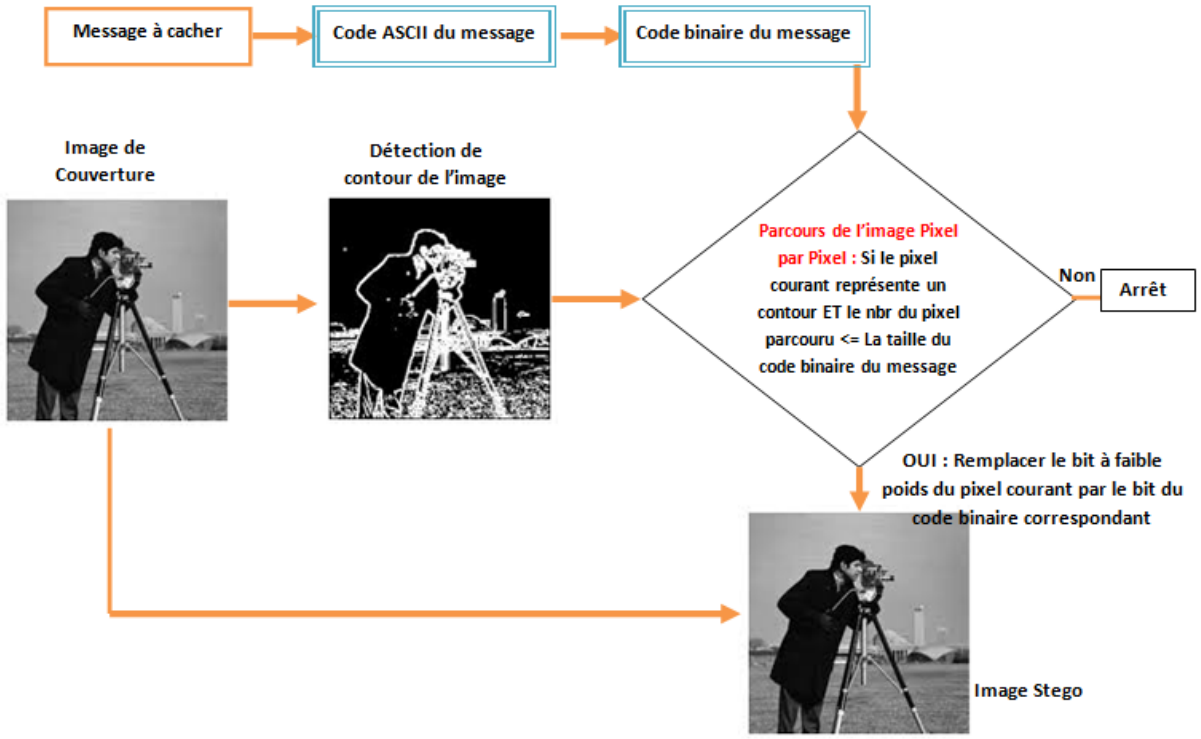


Figure III.7 : Schéma d'insertion du message avec la méthode LSB-Contour.

- **Les étapes d'extraction du message secret :**

Pour récupérer le message secret intégré dansl'image stego, on utilise les étapes suivantes :

Étape 1 : Lecture de l'image stego.

Étape 2 : Détecter les contours dans l'image stego : La méthode d'opérateur Sobel est appliquée pour détecter les contours dans l'image stego-image. Ainsi, obtenir les pixels de contour et non-contour.

Étape 3 : Extraction du la taille des bits du message secret : Le nombre total de bits de longueur de message secret (se trouve dans le pixel de coordonnée (1,1)).

Étape 4 : Extraire le message secret : le message secret est extrait des pixels de contours en utilisant la technique LSB.

Étape 5 : Récupération de l'image : Récupérer des bits de stego-image et convertir la chaine binaire extraite en une valeur ASCII. Ce code ASCII est converti en son caractère correspondant pour former le message complet.

Exemple :

Nous avons une image originale de Lena, lorsque la méthode de détection de contour est appliquée, on obtient la seconde image.

Image originale de Lena.

Détection edge de l'image Lena.

Figure III.8 : Exemple de l'approche LSB- Contour : le code du message secret est inséré dans les pixels de contours.

La méthode proposée dans cette partie (LSB-Contour) permet d'éliminer l'un des inconvénients de LSB Originale qui est la facilité de détection. Mais il nous reste un autre

inconvénient que cette technique ne peut pas le résoudre, et qui réside dans l'inefficacité de la méthode sur les formats compressé avec une perte d'informations. Pour cette raison nous avons proposé une autre technique qui est la LSB-DCT.

III.2.2 Domaine fréquentiel :

III.2.2.1 Transformée en Cosinus Discret :

La technique fréquentielle DCT est protégée contre certaines attaques, surtout lorsque le message est petit. Ceci peut être expliqué par la façon dont elles changent les coefficients dans le domaine de transformation. La stéganographie basée sur la DCT est beaucoup plus puissante et moins vulnérable aux attaques statistiques que les algorithmes opérant dans le domaine spatial [13].

La transformée en cosinus discrète est similaire à la Fourier mais elle n'a pas de composante imaginaire. Pour une image de taille M×N la DCT est donnée par :

$$DCT_{kl} = a_k a_l \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} C_{mn} \cos\frac{\pi(2m+1)k}{2M} \cos\frac{\pi(2m+1)l}{2N}$$

$0 \leq k \leq$ M-1 $\qquad$ $0 \leq l \leq$ N-1

$$a_k = \begin{cases} 1/\sqrt{M} & pour\ k = 0 \\ \sqrt{2/M} & pour\ 1 \leq k \leq M-1 \end{cases} \qquad a_l = \begin{cases} 1/\sqrt{N} & pour\ l = 0 \\ \sqrt{2/N} & pour\ 1 \leq l \leq N-1 \end{cases}$$

Ou DCT_{kl} sont les coefficients DCT de la ligne k et la colonne l et C sont les valeurs des pixels de l'image d'origine de la ligne m et la colonne n.

Pour passer du domaine fréquentiel au domaine spatial, il suffit d'appliquer la transformation inverse du cosinus discrète (IDCT) [13].

- **Algorithme d'insertion du message secret :**

Les coefficients DCT sont utilisés pour la compression [49]. La DCT sépare l'image en plusieurs parties d'une importance différente. Elle transforme un signal ou une image du domaine spatial en domaine fréquentiel. Elle peut séparer l'image en la composant à haute, moyenne et basse fréquences. En sous-bande de basse fréquence, une grande partie de l'énergie du signal est à basse fréquences, qui contient les parties visuelles les plus importantes de l'image alors que les sous-bandes à haute fréquence, les composantes hautes

fréquences de l'image sont généralement supprimées par des attaques de compression et de bruit [49].

Dans l'approche que nous proposons dans le cadre de ce travail, nommée LSB-DCT, nous avons appliqué la DCT sur la matrice Rouge de l'image originale. Nous obtenons une nouvelle matrice qui contient des coefficients au lieu de pixels, ces coefficients contiennent des valeurs positives et des valeurs négatives. Nous avons exploité cette information pour l'insertion du message secret. Notre idée de base consiste à insérer le message secret dans les pixels de l'image originale qui respectent la condition suivante : *si la valeur du coefficient correspondant (obtenu après l'application de la DCT sur la matrice rouge) à ce pixel est inférieure à 0, on fait la substitution LSB.*

- **Insertion du message secret :**

Pour insérer le message secret dans une image on applique les étapes suivantes :

Etape 1 : Lecture de l'image de couverture.

Etape 2 : Extraction de la matrice rouge, puisque l'image est en couleur.

Etape 3 : Lecture du message secret et le convertir en ASCII puis en binaire.

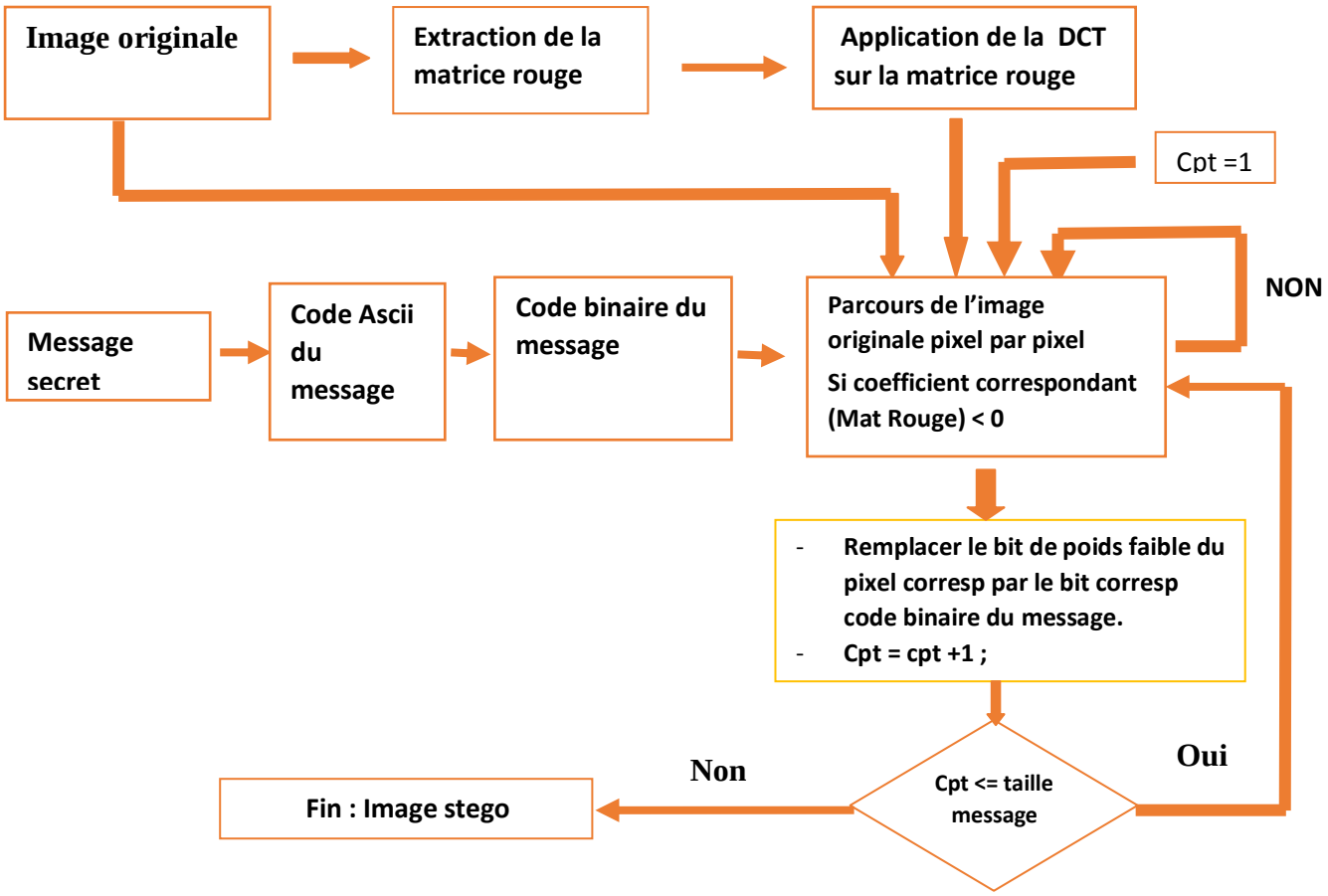
Etape 4 : Application de la DCT sur la matrice rouge.

Etape 5 : Parcours de l'image originale pixel par pixel.

Etape 6 : Si la valeur du coefficient correspondant au pixel parcouru (dans la matrice transformée) est inférieure à 0, on remplace le bit du poids faible du pixel correspondant dans l'image originale par le bit du message correspondant.

Etape 7 : Ecrivez l'image stego.

➢ Nous avons illustré les étapes précédentes par le schéma suivant :



FigureIII.9 : Schéma d'insertion du message secret par la technique LSB-DCT.

- **Extraction du message secret :**

Pour extraire le message caché on applique les étapes suivantes :

Etape 1 : Lire l'image stego.

Etape 2 : Application de la DCT sur la matrice Rouge.

Etape 3 : Parcours de l'image originale pixel per pixel.

Etape 4 : Si la valeur du coefficient qui correspondant au pixel parcouru est inférieure à 0, on récupère la valeur du bit à poids faible.

Etape 5 : Récupérer et convertir chaque 8 bits en caractères.

III.3. Comparaison entre LSB, LSB-Contour et LSB-DCT :

	LSB	**LSB-Contour**	**LSB-DCT**
Insertion de massage	Facile	Complexe	Complexe
Niveau d'insertion dans images	Bits poids faible	Bits poids faible	Bits de poids faible
Détection de stéganalyse	Facile	Difficile	Difficile
Les formats utilisante	Compressé sans perte	Compressé sans perte	Compressé avec et sans perte

Tableau III.1 : Comparaison entre les trois algorithmes.

III.4 Expérimentations & résultats :

III.4.1 Environnement de travail :

Dans cette partie, nous présentons les environnements matériel et logiciel utilisés dans notre travail :

a) Environnement matériel :

Afin de bien réaliser notre projet, nous avons utilisé un ensemble de matériels ayant les caractéristiques suivantes :

Un ordinateur Lenovo caractérisé par :

- Processeur : Intel(R) Core(TM) i3-4005U CPU @ 1.70 GHz
- RAM : 4,00 Go de RAM
- Disque Dur : 500 Go
- Système d'exploitation : Microsoft Windows 7

b) Outils de développements MatlabR2009b :

Nous avons implémenté notre système stéganographique, dans l'environnement de programmation MatlabR2009b, qui permet de manipuler les images avec une grande simplicité.

Matlab est un logiciel de calcul numérique, il a été initialement développé à la fin des années 70, pour permettre aux étudiants de travailler à partir d'un outil de programmation de haut niveau et sans apprendre le Fortan ou le C.

Matlab signifie **Mat**rix **Lab**oratory, il est un langage pour le calcule scientifique, l'analyse de données, leur visualisation, le développement d'algorithmes. Son interface propose d'une part, une fenêtre interactive type console pour l'exécution de commandes, et d'autre part, un environnement de développement intégré (IDE) pour la programmation d'applications [51].

III.4.2 Dissimulation du message par la méthode LSB originale :

Dans la première expérimentation, nous avons utilisé la méthode de stéganographie LSB originale qui consiste à cacher le message dans tous les pixels de l'image (lorsque le compteur est inferieur à la taille de message), quand on a exécuté le code d'insertion nous avons obtenu les résultats suivants :

Figure III.10 : l'image stego résultante de l'application du LSB originale.

Nous remarquons que l'image stego ressemble à l'image originale, et que le changement n'est pas détectable par l'œil humain, car les bits du message secret sont insérés dans les bits de poids faibles de l'image, donc la différence est très petite et indétectable.

Et quand on a exécute le code d'extraction nous avons obtenu le message caché :

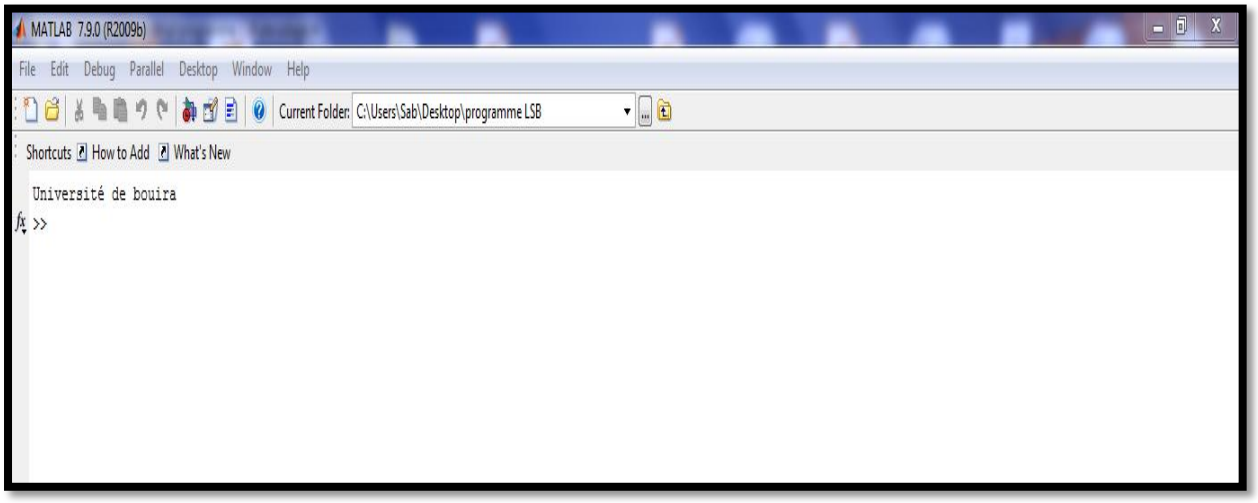


Figure III.11 : Exemple d'extraction de message secret.

III.4.3 Dissimulation du message par la méthode LSB-Contour :

Dans la deuxième expérimentation, nous avons proposé une autre approche qui est plus sécurisée c'est l'approche LSB-Contour qui consiste à dissimuler le message seulement dans les bords (contours) de l'image, lorsque on a exécuté le code d'insertion nous avons obtenu les résultats suivants :

Figure III.12 : Le résultat obtenu de l'application de l'approche LSB-Contour.

Au début nous avons utilisé la méthode de Sobel pour détecter les contours de l'image, ensuite nous avons insérer notre message dans ces contours.

Quand on a appliqué le code d'extraction nous avons récupéré notre message comme il est indiqué dans la figure suivante :

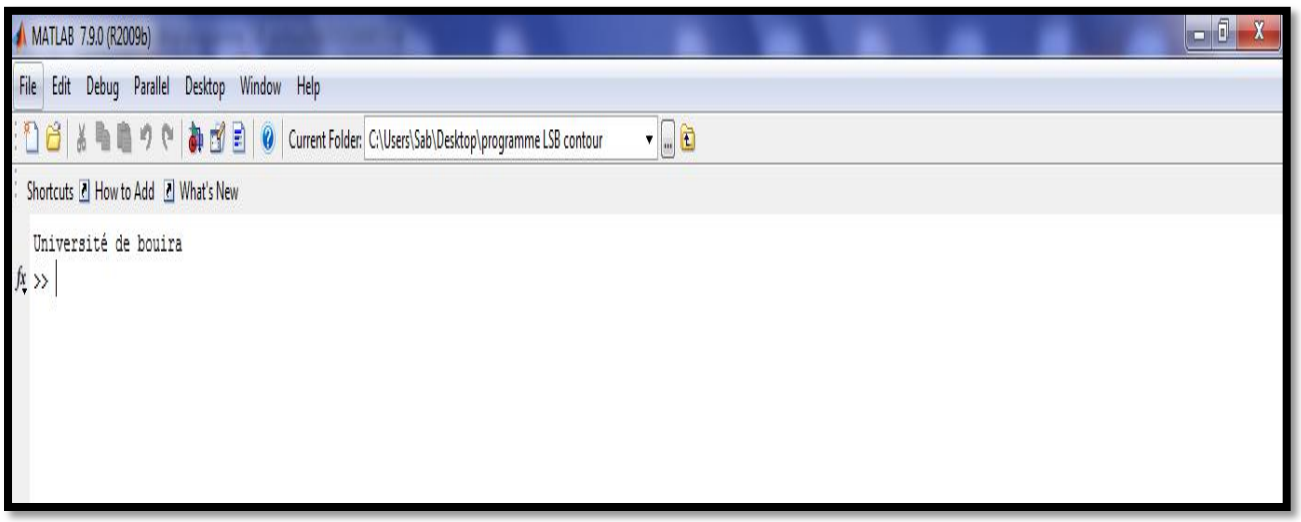


Figure III.13 : Extraction du message secret.

III.4.3 Dissimulation par la méthode LSB-DCT :

Nous avons terminé notre travail par la méthode LSB-DCT, qui consiste à utiliser et exploiter des informations du domaine fréquentiel de l'image pour insérer le message, lorsque on a appliqué cette méthode sur une image JPEG nous avons obtenu les résultats suivant (exécution de code d'insertion) :

Figure III.14 : L'image stego résultante de l'application de la LSB-DCT.

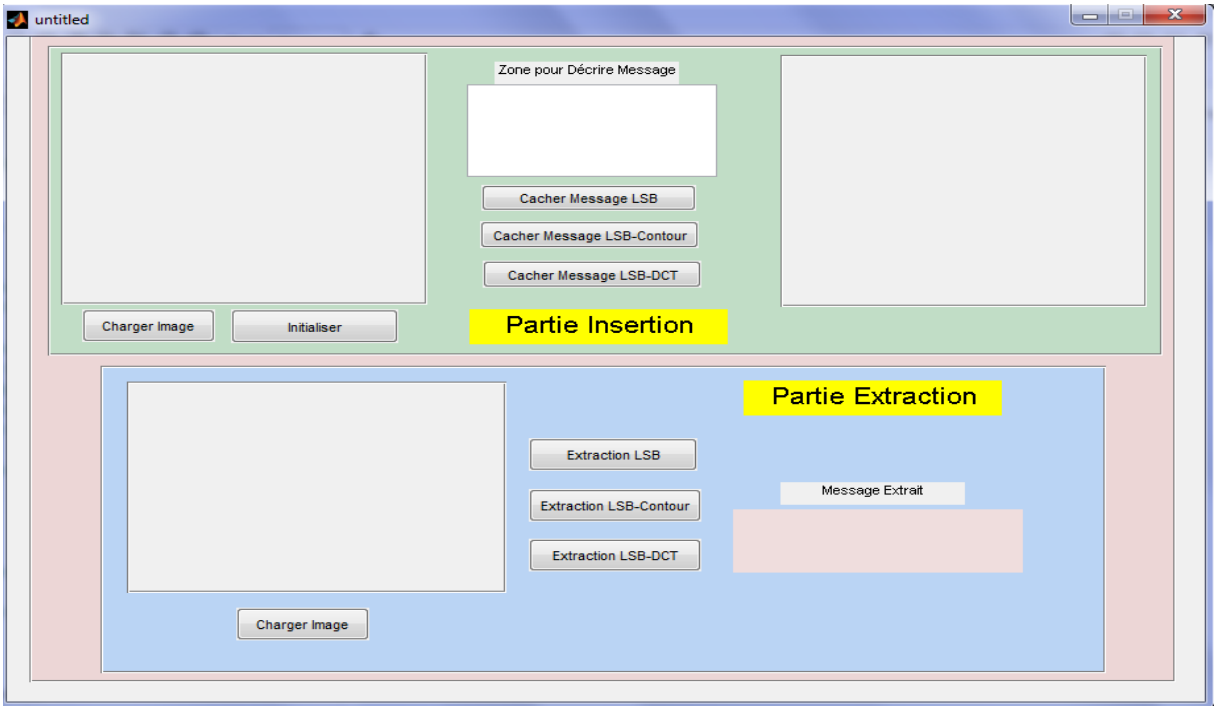
Après l'exécution du code d'extraction nous avons fait sortir notre message caché, comme indiquer dans la figure suivante :

Figure III.15 : Extraction de message par la LSB-DCT.

III.5 Interface Graphique :

Nous avons créé une interface graphique sur Matlab, qui décrit les étapes suivi pour cacher un message secret dans une image de couverture.

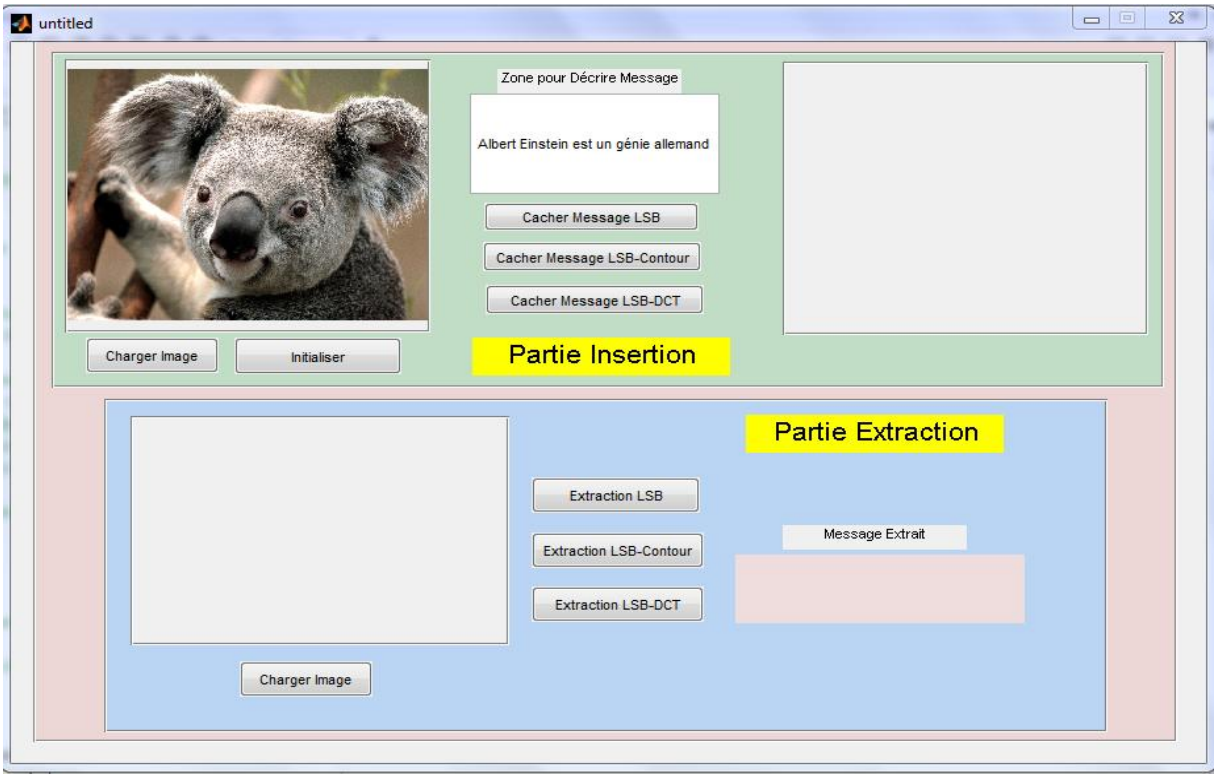
- L'interface Graphique :



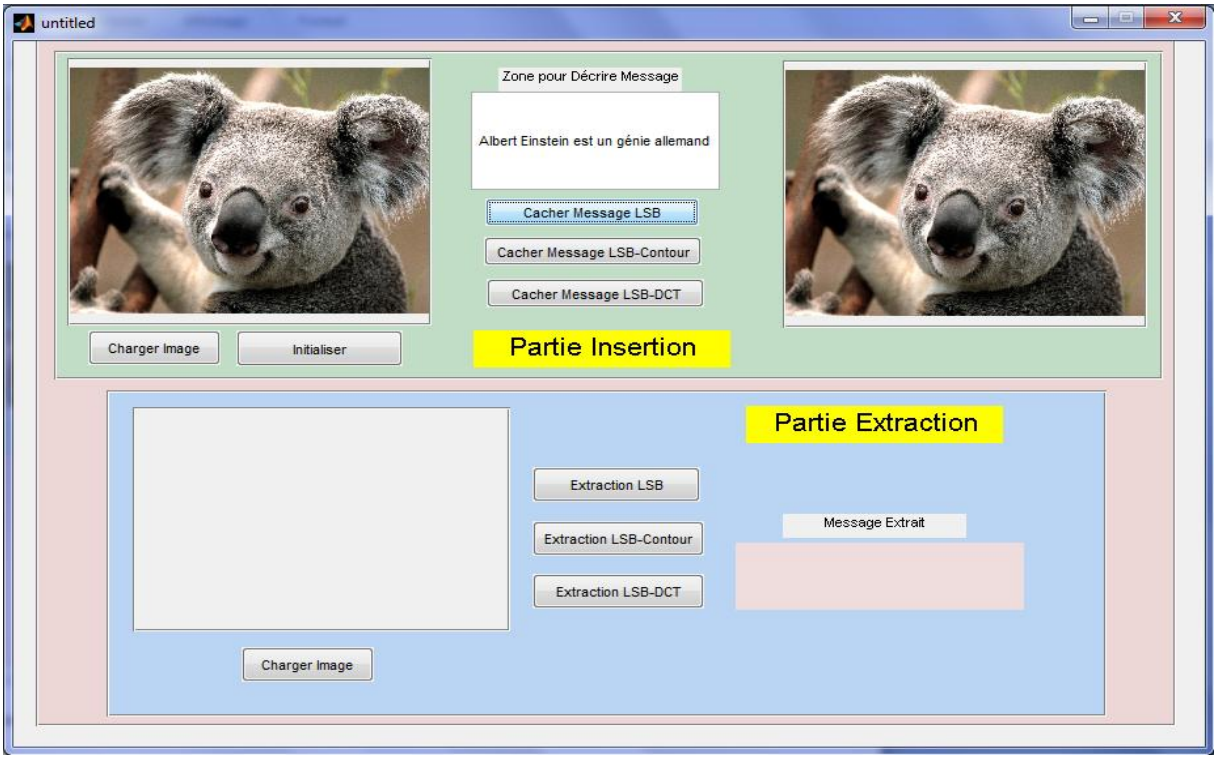
❖ **Processus :**

- **Dissimulation du message par LSB originale :**

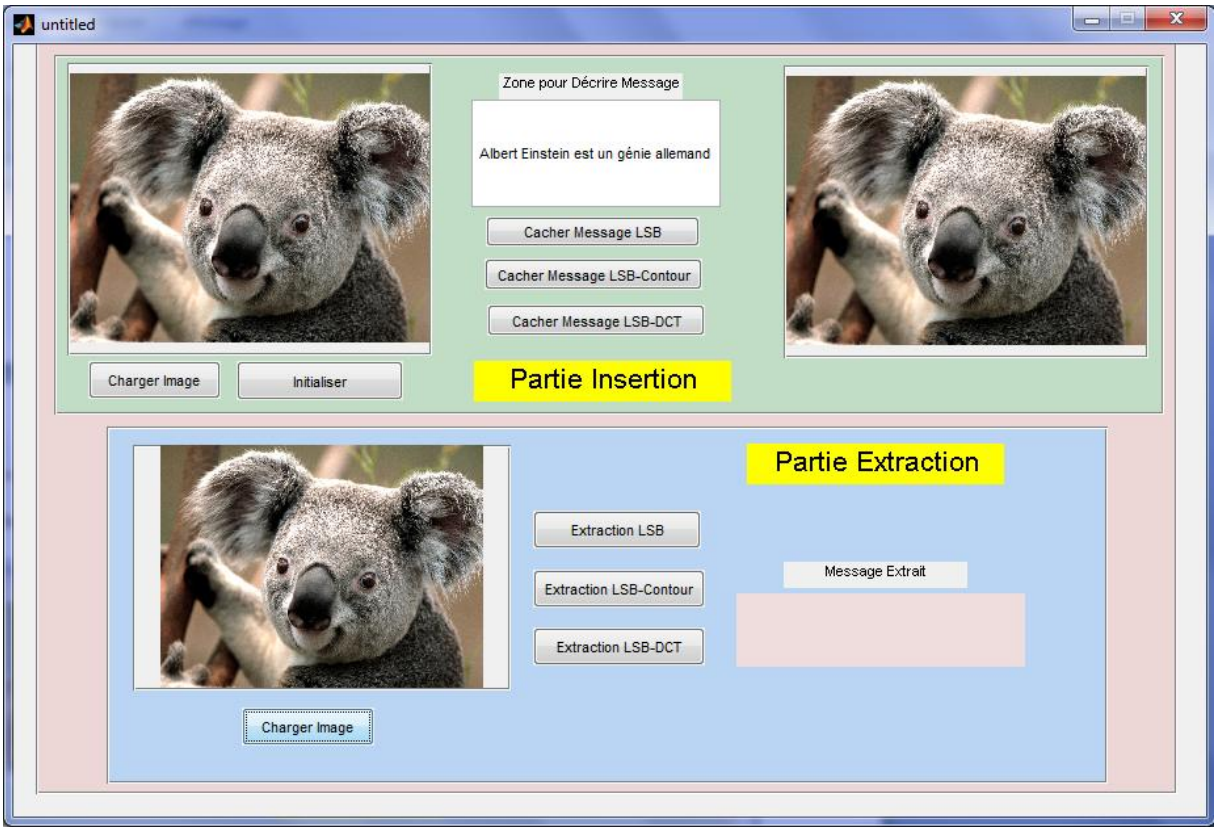
- Chargement de l'image de couverture et écriture du message à cacher :



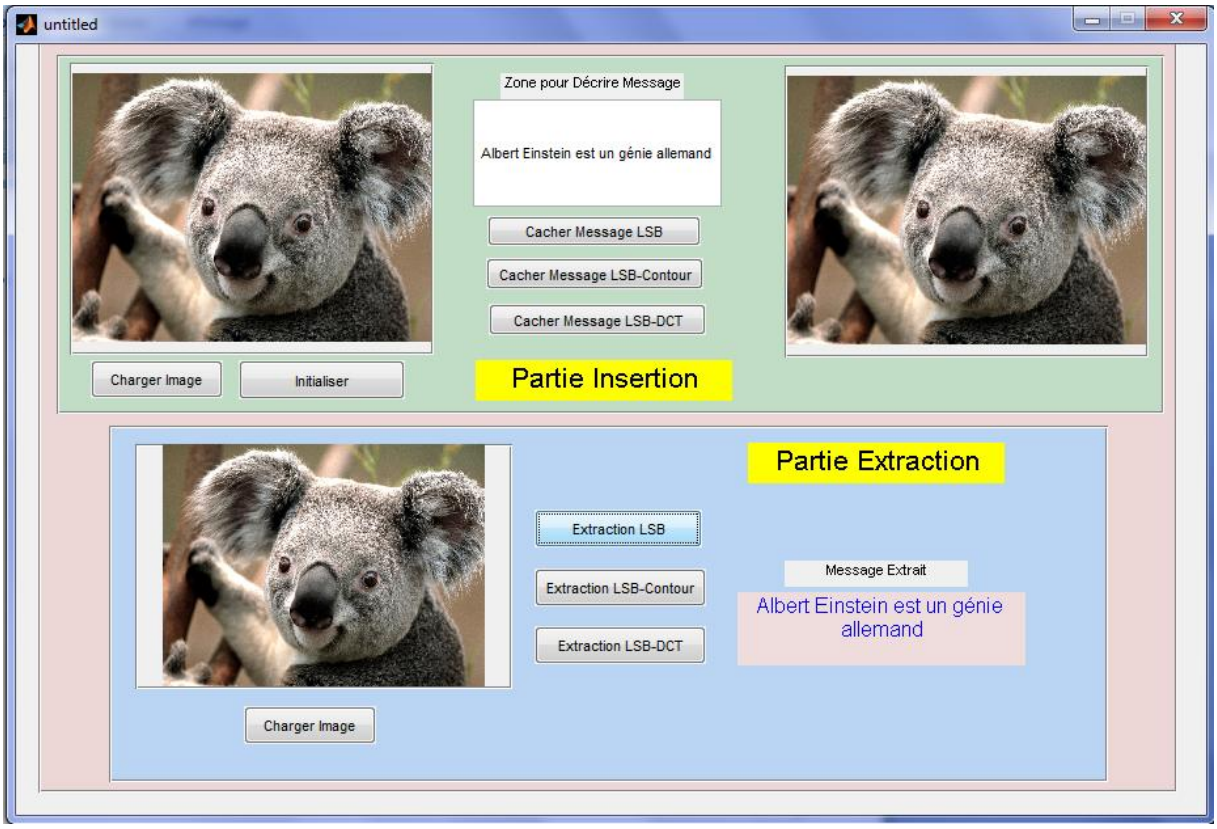
- insertion du message par la méthode LSB :



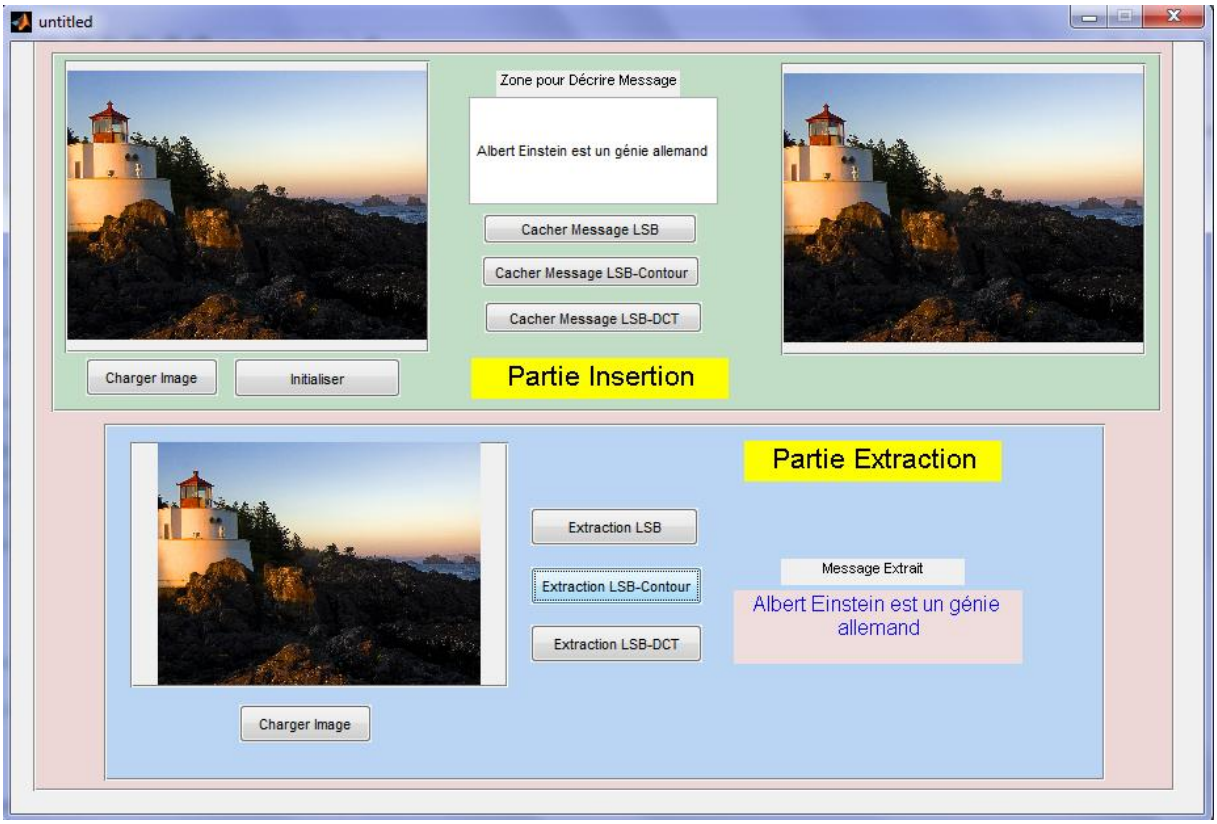
- Chargement de l'image stego :



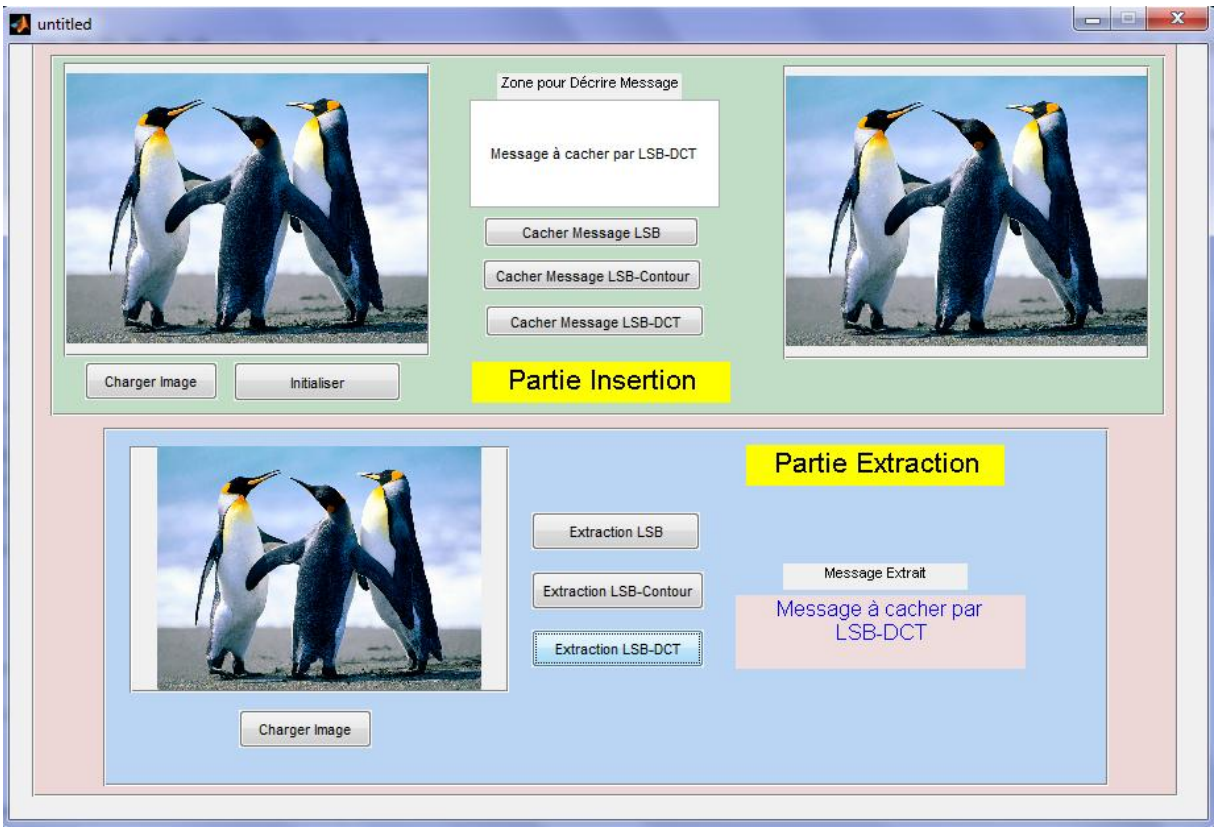
- Extraction du message caché par la méthode LSB :



- **Dissimulation du message par la méthode LSB-Contour :**



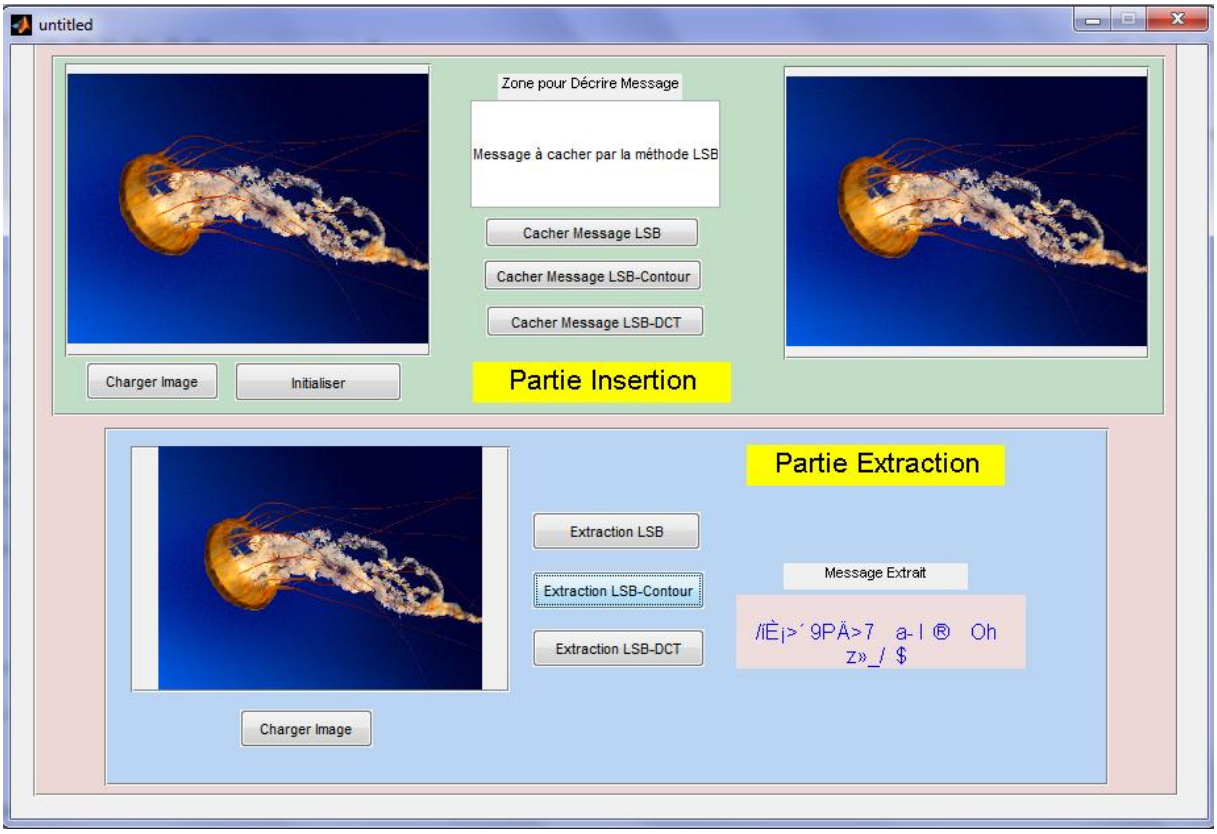
- **Dissimulation du message par la méthode LSB-DCT :**



Remarque :

Pour extraire le message secret de l'image stego, il faut utiliser le même algorithme d'insertion sinon le message va détruit complètement.

Voici un exemple dans lequel l'insertion est faite par l'algorithme LSB, alors que l'extraction est faite par un autre algorithme qui est LSB-Contour :



III.6 Conclusion :

Dans ce chapitre, le travail présenté sert à la dissimulation d'un message secret dans une image numérique. Pour ce faire, nous avons proposé trois systèmes stéganographiques basés sur les algorithmes : LSB, LSB-Contour et LSB-DCT pour l'insertion des bits de message dans les pixels de l'image dans le cas de codage, et l'extraction de ces bits dans le cas de décodage. Nos résultats obtenus sous Matlab indiquent que les Algorithmes utilisés sont efficaces en termes de : non déformation de l'image et difficulté de stéganalyse.

Conclusion Générale & perspectives

Le travail présenté 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 on parle sur le LSB-Contour, et l'autre utilise le domaine fréquentiel on parle sur la DCT.

Le premier chapitre, résume les notions de base de traitement d'images, qui concerne l'image numérique comme sa définition, ses caractéristiques et types, sa formation ainsi que ses formats. Donc une brève explication qui permet de comprendre les outils constituant l'image qui a été considérée dans notre travail comme un support dans lequel nous avons caché des données.

Dans le deuxième chapitre, 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 fonctionne il, et encore on a parlé sur les déférents 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, ou d'une autre articulation c'est l'opération opposite de stéganographie. Alors que dans le dernier chapitre nous avons fait une implémentation et présentation des résultats obtenus à partir des algorithmes de stéganographie LSB, LSB-Contour et la DCT.

Dans des recherches futures, nous allons essayer de réaliser d'autres systèmes de stéganographie en utilisant d'autres techniques comme la DWT (ondelettes), et on va essayer de programmer des algorithmes de stéganalyse pour détecter l'existence d'un message caché, et pourquoi pas, utiliser de nouveaux supports pour cacher notre message tel qu'une vidéo par exemple ou bien dissimuler une image dans une autre image.

Références Bibliographiques :

[1] D. ZEROUAL : « Implémentation d'un environnement parallèle pour la compression d'images à l'aide des fractales ». Thèse de magister, université de Batna (Algérie). Soutenue en 2006.

[2] M. H. BENDAOUD : « développement de méthodes d'extraction de contours sur des images à niveaux de gris ». Thèse de doctorat, université d'Oran (Algérie). Soutenu en 2017.

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

[4] C. TAOUCHE : « Implémentation d'un environnement parallèle pour la compression d'image à l'aide des fractales ». Thèse de magister, université Mentouri Constantine (Algérie). Soutenu en 2005.

[5] N. MOUNIB : « Une approche Co-évolutionnaire proie-prédateur pour le rehaussement d'images ». Thèse de magister, université colonel Hadj Lakhdar-Batna (Algérie). Soutenue le 09/07/2007.

[6] K. HETATACHE : « Développement d'algorithmes de tatouage d'images basés sur la SVD et les transformations discrètes ». Thèse de magister, université Ferhat Abbas-Setif (Algérie). Soutenue le 29/12/2014.

[7] S. V. Mallat : « A théory for multirésolution signal décomposition : The wavelet representation ». IEEE *Transaction on Pattern Analysis and Machine Intelligence*, 11(7): 674-693, July 1989.

[8] M. BENABDELLAH : « Outils de compression et de crypto-compression : application aux images fixes et vidéo ». Thèse de doctorat, université Mohammed V-AGDAL-Rabat (Maroc). Soutenu le 20/06/2007.

[9] C. MEURIE : « Segmentation d'images couleur par classification pixellaire et hiérarchie de partitions ». Thèse de doctorat, université de CAEN/ Basse-Normandie (France). Soutenue le 25/10/2005.

[10] A. POREBSKI : « Sélection d'attributs de texture couleur pour la classification d'images. Application à l'identification de défauts sur les décors verriers imprimés par sérigraphie ». Thèse de doctorat, université de Lille 1 (France). Soutenue le 20/11/2009.

[11] E. DABELLANI : « Méthodologie de conception d'architectures reconfigurables dynamiquement, application au transcodage vidéos ». Thèse de doctorat, Université de Lorraine (France). Soutenu le 02/12/2013.

[12] R. CHBEIR : « Modélisation de la description d'images : Application au domaine médical ». Thèse de doctorat, l'Institut National des Sciences Appliquées de Lyon (France). Soutenu le 14/12/2001.

[13] 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.

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

[15] 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.

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

[17] Hérodot : « L'Enquête » : Livres I à IV, vol. 1 de collection folio. Traduit par A. Barguet. Editions Gallimard, 1985.

[18] Hérodot : « L'Enquête » : Livre V à IX, vol .1 de collection folio. Traduit par A. Barguet. Editions Gallimard, 1990.

[19] 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.

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

[21] G.J. Simmons : « the prisoners' problem and the subliminal channel ». In David CHAUM, éditeur, « *Advance in Cryptograph* », page 51-67. Springer US, 1984.

[22] M. Bouab : «Tatouage d'image basé sur des propriétés psycho visuelle ». Mémoire de magister, option : électronique, Université Mentouri Constantine (Algérie), 2006.

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

[24] J. Barbier : « Analyse de canaux de communication dans un contexte non coopératif ». Thèse de doctorat, école supérieure et d'application des transmissions école polytechnique, Laboratoire de virologie et cryptologie. Soutenue le 28/11/2007.

[25] F. Raynal : « Etudes d'outils pour la dissimulation d'information : Approches Fractales, protocoles D'évaluation et protocoles cryptographiques ». Thèse de doctorat, Université de Paris XI (France). Soutenue le 01/03/2002.

[26] N. Kaur, S. Behal : « A Survey on Various Types of Steganography and Analysis of Hiding Technique ». International Journal of Engineering Trends and Technology (IJETT), volume (11), Number 8, p-389, May 2014.

[27] L. Laimeche : « Détection des informations cachées dans les images numériques basées loi de ZIPF ». Mémoire de magister, Université de Tébessa (Algérie). Soutenu le 10/01/2010.

[28] AL-Shatnawi, M. Attalah, and Bader m. Alfawwaz : «An Integrated Image Steganography System With Improved Image Quality». Applied Mathematical Sciences, vol.71(7) (2013) : 3545-3553.

[29] B. Souvik and G. Sanyal : « A Robust Image Steganography Using DWT Difference Modulation (DWTDM) ». International Journal of Computer Network & Information security 4.7 (2012).

[30] H. Singh, P. K. Singh, K. Saroha : «A Survey on Text Based Steganography ». Proceeding of the 3rd National conference, INDIAcom-2009 computing for nation development, February 26-27, 2009 Bharati Vidyapeeth's Institute of computer Applications and Management, New Delhi.

[31] A. D. Ker : « Steganalysis of LSB matching in grayscale images ». IEEE *Signal Processing Letters*, 12 (6) : 441-444, Juin 2005.

[32] N. Provos : « Defending against statistical steganography ». in proceedings of the 10th conference on USENIX security symposium, vol (10), SSYM'01, Washington, D. C. USENIX Association,2001.

[33] A. Ali. Pacha, N. Hadj-Said, A. Belgoraf, A. M'hamed : « stéganographie : Sécurité par Dissimulation ». Revue de l'information scientifique et technique, vol (6), Numéro 1, p 90-103, 2006.

[34] S. Saejung, A. Boondee, J. Preechasuk, C. Chantrapornchai : « On the comparison of digital image steganography algorithm based on DCT and wavelet». In computer science and Engineering conference (ICSEC), p 328-333, (2013).

[35] S. Goal, A. Rana, M. Kaur : « Comparison of image steganography technique ». International Journal of computers and Distributed Systems, Vol 3, Issue I, (2013).

[36] G. S. Sravanthi, B. Sunitha Devi, S. M. Riyazoddin, M. Janga Reddy : « A spatial Domain Image Steganography Technique Based on Plan Bit Substitution Method ». Global Journal of Computer Science and Technology Graphics & Vision, vol (12), Issue 15, Version 1.0, 2012.

[37] A. Kumar, Km. Pooja : « Steganography ADATA Hiding Technique ». International Journal of computer Applications (0975-8887), vol (9), Numéro 7, Novembre 2010.

[38] H. Kaur, J. Rani : «A survey on different techniques of steganography ». Conf. ICAET, Punjab, India, 2016.

[39] P. Malathi, T. Gireesh Kumar : « Relating the embedding efficiency of LSB steganography techniques in spatial domain ». 6th International Conference on Advances In Computing & Communications, ICACC 2016, 6-8 septembre 2016, Cochin, India.

[40] J. A. Mazumde, K. Hemachandrane : «Study of Image Steganography Using LSB, DFT and DWT ». International journal of computer & Technology, 2013.

[41] A. Kaur, M. Kaur : « Improved Security Steganography Mechanism of Text in Video Using Steganographic Technique ». Int. J. Adv. Res. Comput. Sci. Softtw. Eng, vol. 7782, no. 5, pp. 44-51, (2014).

[42] M. Dixit, N. Bhide, S. Khankhoje, and R. Ukarande : « Video Steganography ». Int. Cnf. Parvasive Comput, vol 00, no. c, pp. 1-4, (2015).

[43] L. Marvel, C. G. J. Boncelet, C. T. Retter : « Spread Spectrum Image Steganography ». IEEE Transactions on Image processing, vol (8), 1999.

[44] S. O. Akimola, A. A. Olatidoye : « On The Image Quality And Encoding Times Of LSB, MSB And Combined LSB-MSB Steganography Algorithms Using Digital Images ». International Journal Of Computer Science & Information Technology (TJCSIT), vol(7), no 4, August 2015.

[45] B. S. Champakamala, K. Padmini, D. K. Radika : « Least Significant Bit algorithm for image steganography ». International Journal of Advenced Computer Technology, vol(3), No 4.

[46] T. Vanita, D. S. Anjalin, B. Rshni, D. S. Sweeta : « A Review On Steganography – Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm ». International Journal Of Innovative Research in Computer and communication Engineering, vol(2), Issue 5, Octobre 2014.

[47] S. Sarkar, A. Basu: « Comparison of various edge detection techniques for maximum data hiding using LSB Algorithm ». International Journal of computer Science and information Technologies, vol 5(3), 2014, 4722-4727.

[48] N. S. Meshram, S. Dubey : « Image Steganography Using LSB and Edge-Detection Technique ». International Journal Of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, vol(2), Issu 3, july 2012.

[49] S. R. Gouda : « Least significant Bit (LSB) and Discrete cosines transform (DCT) Based Steganography ». International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS), vol(2), Issue 1, (Jan-Feb 2015), pp31-36.

[50] V. Lokeswara Reddy, A. Subramanyam, P. Chenna Reddy: « Implementation of LSB Steganography and its Evaluation for Various File Formats ». Int. J Advanced Networking and Applications, vol(2), Issue 5, pages: 868-872, (2011).

[51] https://www.mathworks.com/matlabcentral/''

[52] A. Capri : « Caractérisation des objets dans une image en vue d'une aide à l'interprétation et d'une compression adaptée au contenu : application aux images échographiques ». Thèse de doctorat, Université D'Orléans (France), soutenu en 2007.

[53] N. Merzougui : « Un algorithme évolutionnaire pour la segmentation d'images basé sur le diagramme de Voronoï ». Mémoire de magister, Université Kasdi Merbah-Ouargla (Algérie), soutenue le 28/06/2012.

[54] A. Dirami : « Segmentation d'images bruitées utilisant la dérivée topologique ». Thèse de doctorat, Université Mouloud Mammeri-Tizi Ouzou (Algérie).

[55] J.-P. Cocquerez, S. Philipp : « Analyse d'images : filtrage et segmentation ». Masson, 1995.

[56] S. A. Khayam : « The Discret Cosinus transform (DCT) : Theory and Application ». support de cours (Tutorial). Department of electrical & computer Engineering, Michigan State University (USA), 2003.

[57] N. Brahimi : « Développement et implémentation des algorithmes de compression d'images basés sur des transformées entières ». Mémoire de magister, Université Ferhat Abbas-Setif (Algérie), soutenue le 13/01/2011.

Annexe A

Généralités sur la segmentation d'image

A.1 Introduction :

L'objectif de l'analyse d'image réside dans la description et quantification (nombre, densité) de déférents objets constituant l'image étudiée. L'analyse est utilisée dans de nombreux domaines tels que la médecine. D'où les notions de segmentation et de description objective des composants qui forment l'image donnent à l'expert un complément d'informations lui permettant d'étayer son diagnostic [52].

La segmentation est le cœur d'un système d'analyse automatique d'images. Elle intervient dans de nombreuses applications importantes, comme l'indexation d'une base de données d'images. Elle est en fait un traitement de bas niveau qui consiste à partitionner une image en régions appartenant à une même scène [53]. Dans la majorité des travaux publiés, les méthodes de segmentation sont classées en deux grandes catégories : les approches basées contours et les approches basées régions [54].

Nous nous intéressons dans cette section sur la première catégorie qui est l'approche basée contours.

A.2 définition de la segmentation :

La segmentation est définit comme le partitionnement d'une image en régions homogènes, c'est l'une des techniques les plus importantes utilisées dans plusieurs taches de traitement d'images et de reconnaissance de formes [54]. Elle a comme objectif de rassembler les pixels de l'image étudiée en régions selon des critères prédéfinis.

Nous pouvons adopter la définition suivante pour la segmentation :

« la segmentation est un traitement de bas niveau qui consiste à créer une partition de l'image A en sous-ensembles R_i, appelés régions tels qu'aucune région ne soit vide, l'intersection entre deux régions soit vide et l'ensemble des régions recouvre toute l'image. Une région est un ensemble de pixels connexes ayant des propriétés communes qui les différencient des pixels des régions voisines. » [55].

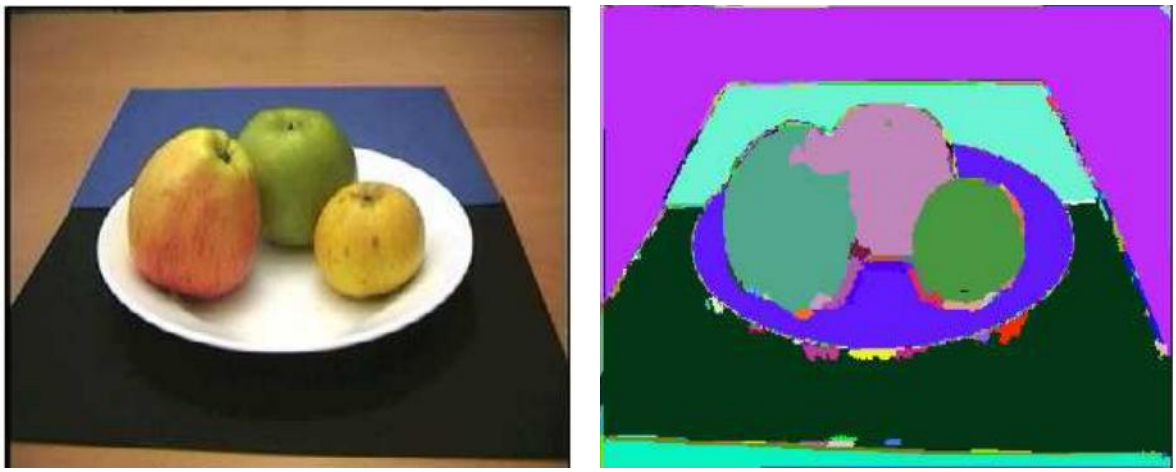


Figure A.1 : Exemple de segmentation d'une image couleur.

Sur cette image, on voit bien que chaque objet de l'image se voit attribué par une couleur, d'où la séparation en régions dites homogènes. Cependant on voit qu'il peut y avoir des défauts de reconnaissance et donc y avoir des confusions entre les régions comme c'est le cas ici entre la pomme du milieu et celle se situant à sa gauche car elles ont une zone en violet commune.

A.3 différentes approches de la segmentation :

Dans le but d'analyser une image, la segmentation est considérer comme une étape primordiale [52]. Dans la littérature, nous avons trouvé plusieurs méthodes de segmentation qui s'intègrent dans quatre approches principales [52, 53].

- Une approche globale de l'image.
- La recherche de « frontières », (approche par contours).
- La recherche de « régions », (approche par régions).
- Approche coopérative.

Comme nous avons dit précédemment nous intéressons à l'approche par contours.

A.4 Approche contour :

La segmentation par approche contour consiste à éliminer tous les motifs de l'image à faible variation des niveaux de gris ou de couleurs pour laisser seulement les lignes de séparation entre les régions homogène. Pour ce faire, différentes opérations de filtrage par convolution ou de filtres différentiels comme le gradient ou le Laplacien peuvent être utilisés en produisant de fortes valeurs aux points où la variation des niveaux de gris ou de couleurs

est élevée. La dérivée permettre la détection de ces variations qu'il est possible d'exploiter sous deux formes [54].

Dans la segmentation par approches contours, il y a deux problématiques à résoudre, à savoir :

- Caractériser la frontière entre les régions :

Figure A.2 : Détection de contours sur Lena.

- Fermer les contours :

Figure A.3 : Illustration de contours à fermer sur Lena.

A.5 Approche gradient :

Ce type de détecteur se base sur la première dérivée de l'image I en chacun de ses points dans les deux directions horizontale et verticale. Un point de contour aura une amplitude A(i,j) et une direction Dir(i,j).

Voici une illustration montrant le gradient d'une image découpée en deux zones distinctes :

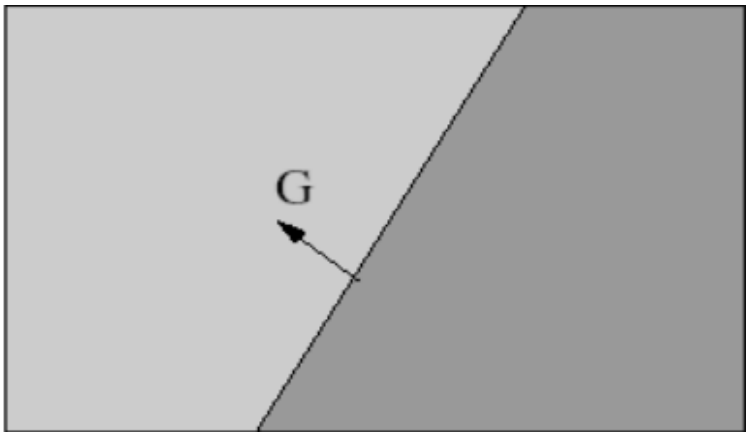


Figure A.4 : Gradient d'une image à 2 régions.

Le gradient n'est autre qu'une dérivée vectorielle de l'image et permettant de détecter les contours du fait que les contours correspondent à des discontinuités d'ordre 0 de la fonction d'intensité.

La détermination des points contours est ramenée à la recherche de filtre linéaire permettant d'estimer le gradient en chaque point. Plusieurs operateurs sont ainsi apparus dans la littérature parmi lesquels nous pouvons citer les masques de Sobel, Prewitt, Robert,...etc. [53].

✓ Le masque le plus intuitif à mettre en œuvre est un masque à deux éléments :

-1	1

L'origine de ce masque est le point -1.

✓ En faisant subir une rotation de $\pi/2$ au premier masque, il apparait le filtre suivant dont l'origine est le point 1 :

1
-1

La figure suivante propose une illustration de l'application de ces masques :

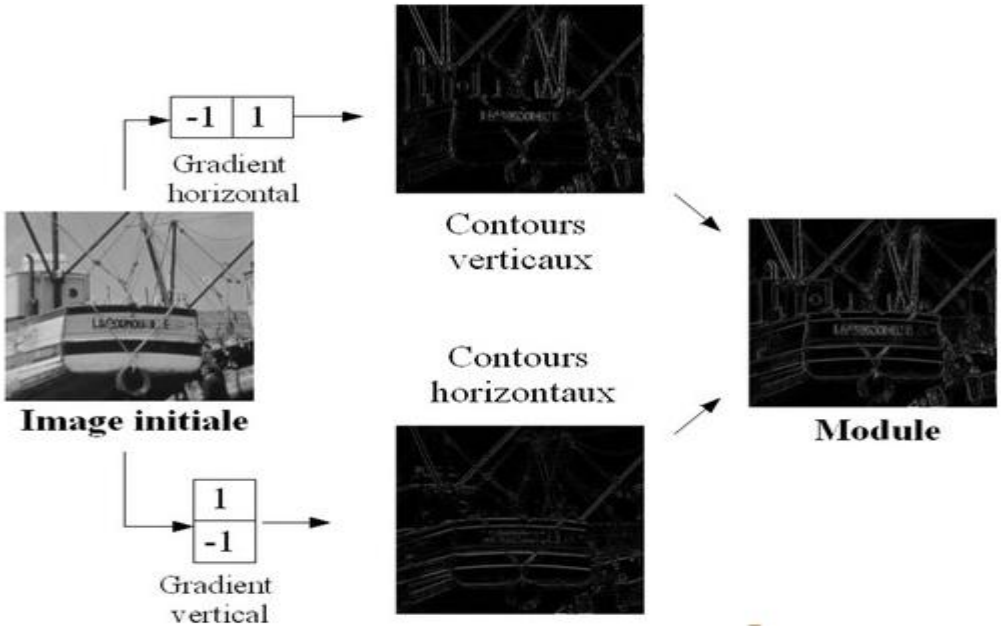


Figure A.5 : Illustration de l'application des masques du gradient.

- **Pré filtrage par l'operateur de Sobel :**

Pour filtrer nos images, nous devons utiliser des filtres que l'on appelle filtres étroits dont l'approche la plus courante est le filtre gradient dans lequel l'operateur de Sobel est utilisé.

On rappelle que le gradient, en un pixel d'une image numérique, est un vecteur caractérisé par son amplitude et sa direction. L'amplitude est directement liée à la quantité de variation locale des niveaux de gris. La direction du gradient est orthogonale à la frontière qui passe au point considéré. La méthode la plus simple pour estimer un gradient est donc de faire un calcul de variation monodimensionnelle.

On a alors le schéma suivant :

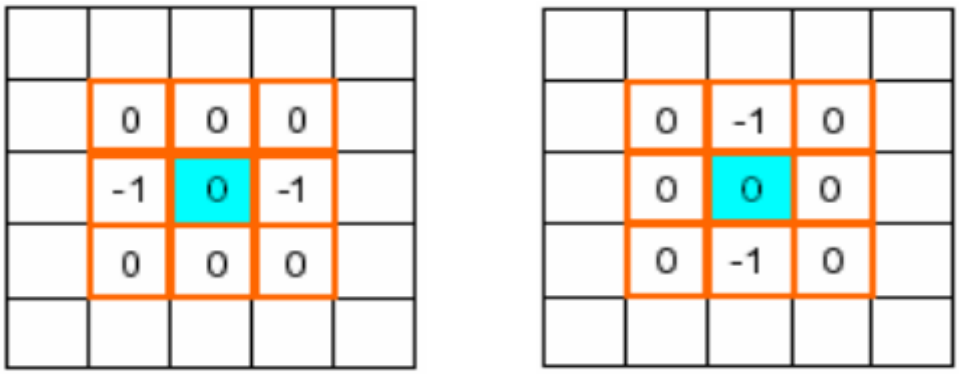
$$G_d(x,y) = (I * W_d)(x,y)$$

Où Wd désigne l'opérateur de dérivation dans la direction d et * le produit de convolution.

Il existe de très nombreux operateurs différents (Roberts, Sobel, Prewitt, Kirsch,....) qui ont les mêmes propriétés. En chaque point (x,y) de l'image, on peut donc calculer le vecteur

gradient, sa direction maximise la dérivée directionnelle et sa norme est la valeur de cette dérivée.

Appliqué à une image, considérée comme une fonction de deux variables, on peut définir deux dérivées partielles, suivant x et suivant y :

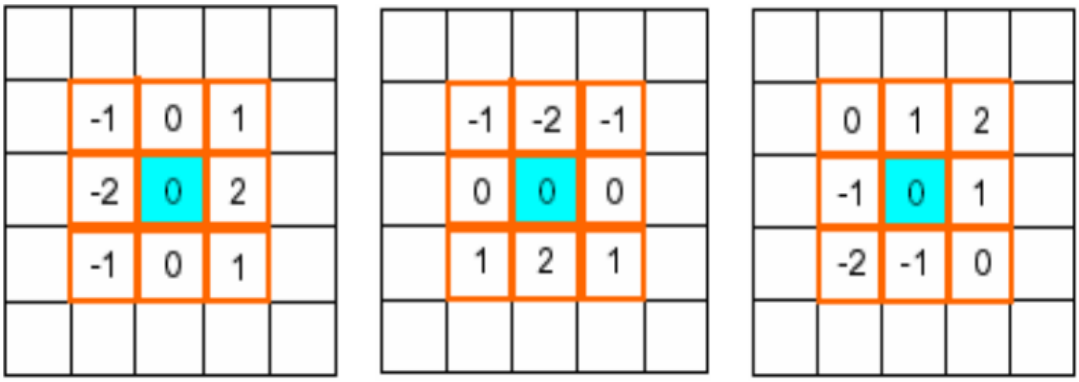


Dérivée horizontale Dérivée verticale

Figure A.6 : Dérivées partielles selon x et y.

Lorsque la dérivation a augmenté le bruit, il a été nécessaire de créer des filtres plus robustes comme celui de Sobel. Ce dernier permet d'utiliser des masques de dérivation dans les directions horizontales, verticales et obliques.

Voici les trois masques de dérivation de l'operateur de Sobel :



Horizontale **Verticale** **Oblique**

Figure A.7 : Les trois masques de dérivation de Sobel.

Une fois l'image filtrée par cet opérateur, on peut appliquer la méthode de détection de contours que l'on a choisis.

La figure suivante illustre l'application des masques de Sobel :

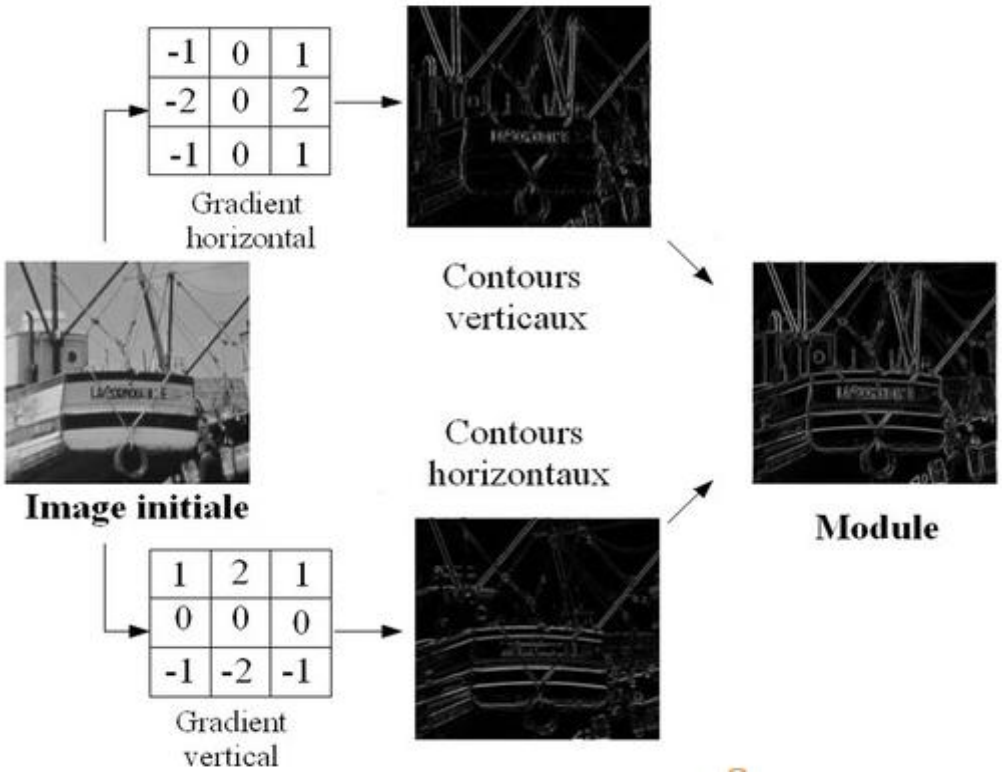


Figure A.8 : Illustration de l'application des masques de Sobel.

- **Filtre de Prewitt :**

Un autre filtre existe est celui de Prewitt :

Les masques dérivateur sont maintenant :

$$G_x = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} * \begin{bmatrix} -1 & 0 & 1 \end{bmatrix}$$

$$G_y = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} * \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$$

$\begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$: Lissage des lignes ou des colonnes.

$\begin{bmatrix} -1 \\ 0 \\ 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 1 \end{bmatrix}$: Dérivée des lignes ou des colonnes.

On combine à la fois un filtrage et une dérivée. Ces méthodes sont moins sensible aux bruit que le calcule direct des dérivées [47].

A.6. Approche Laplacien :

Ce type de détection de contour se base sur la dérivée seconde de l'image. Il est définit par :

$$\Delta^2 = \frac{\delta^2}{\delta x^2} + \frac{\delta^2}{\delta y^2}$$

Contrairement au gradient, le Laplacien permet d'obtenir des contours fermés et d'un pixel d'épaisseur, par contre il a l'inconvénient d'être plus sensible au bruit que le gradient. Le Laplacien est déterminé en chaque point de l'image par filtrage linéaire. Les points contours sont alors assimilés au passage par zéro du Laplacien.

Ces deux méthodes (Approche Gradient et Laplacien) semblent inefficaces si l'amplitude du gradient aux points de contours varie fortement selon les parties de l'image. Il n'existe pas de seuil ***s*** permettant la sélection des points contour sans sélectionner ceux dus au bruit. Le Laplacien augmente le bruit présent dans l'image car il s'agit d'une méthode dérivative [53].

- **Opérateurs discret 2D :**

Contour = passage par laplacien.

Celui-ci peut être estimé grâce à une convolution avec le masque :

0	1	0
1	-4	1
0	1	0

Voici un exemple de segmentation par contour, où l'algorithme Laplacien est appliqué. Les points de contour sont présentés en blanc.

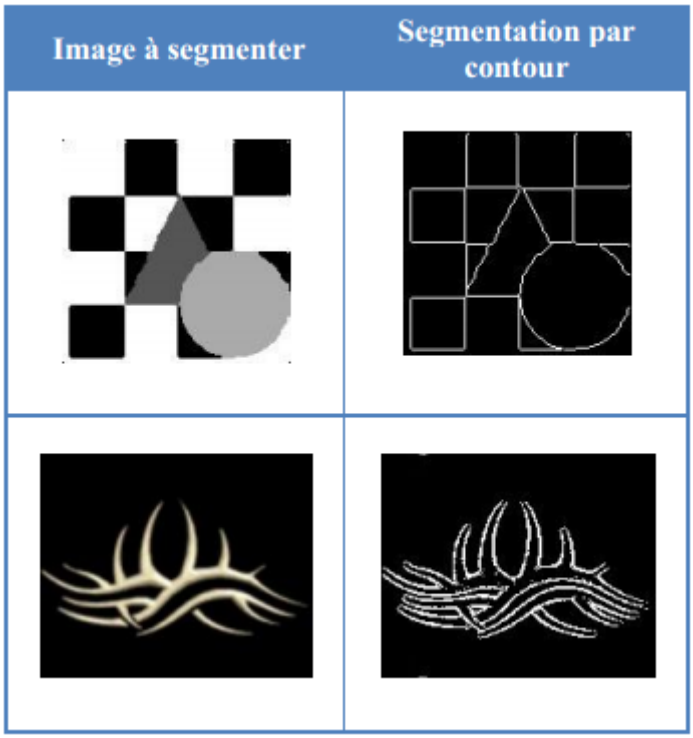


Figure A.9 : Résultats de segmentation par contour (Laplacien).

Annexe B

La transformée Discrète en Cosinus (DCT)

B.1. Introduction :

Les transformations sinusoïdales, telles que les transformations de cosinus discrètes (DCT) et les transformations de Fourier discrètes (DFT), utilisent des transformations indépendantes de l'image. De plus, des algorithmes et des architectures rapides sont disponibles pour DCT et DFT. L'application de la DCT se traduit par des artefacts de blocage moindres dus aux propriétés d'extension de DCT. Elle utilise également des calculs réels, cela rend le matériel DCT plus simple. La DCT est utilisée dans de nombreux domaines comme la compression et la stéganographie. Dans cette section on va parler sur la définition de la DCT et ses deux types, ainsi que ses propriétés.

B.2. La transformée en cosinus discrète (Discret Cosine Transform) :

La DCT est une transformation orthogonale très utilisée en compression d'images et largement acceptée dans les normes multimédias. La DCT appartient à une famille de 16 transformations trigonométriques. La DCT de type 2 transforme un bloc d'image de taille N x N ayant des intensités de pixels s (n_1, n_2) en un tableau de transformées de coefficients S (k_1, k_2), décrit par l'équation suivante:

$$S(k_1,k_2) = \sqrt{\frac{4}{N^2}} C(k_1)C(k_2) \sum_{n_1=0}^{N-1} \sum_{n_2=0}^{N-1} s(n_1,n_2) cos\left(\frac{\pi(2n_1+1)}{2N}\right) cos\left(\frac{\pi(2n_2+1)}{2N}\right) \quad (1)$$

Où k_1,k_2 ,n_1,n_2 = 0,1,...,N −1, et :

$$C(k) = \begin{Bmatrix} 1/\sqrt{2} & pour\ k = 0 \\ 1 & sinon \end{Bmatrix}$$

Le tableau transformé S(k_1,k_2) obtenu par l'équation (1) est également de la taille N x N, identique à celle du bloc d'image d'origine. Il convient de noter ici que les indices de domaine de transformation k_1 et k_2 indiquent les fréquences spatiales dans les directions de n_1 et n_2 respectivement. $k_1 = k_2 = 0$ correspond à la moyenne ou à la composante continue et toutes les composantes restantes correspondent aux fréquences spatiales plus élevées lorsque k_1 et k_2 augmentent.

À partir de considérations informatiques, on peut noter que l'application directe de l'équation ci-dessus pour calculer le tableau transformé nécessite des calculs $O(N^4)$. En utilisant un algorithme analogue à la transformée de Fourier rapide (FFT) pour calculer la DCT, les calculs peuvent être réduits à $O(2N^2 \log N)$. Ces approches informatiques rapides et avec l'utilisation de l'arithmétique réelle ont rendu la DCT populaire pour les applications de compression d'images. Toutes les images naturelles présentant une redondance spatiale, tous les coefficients du tableau transformé ne présentent pas de valeurs significatives. Cela peut être démontré par un exemple. Nous prenons un bloc de 8x8 à partir de l'image de *Lena*, dont les intensités de pixels sont indiquées à la figure B.1.

166	162	162	160	155	163	160	155
166	162	162	160	155	163	160	155
166	162	162	160	155	163	160	155
166	162	162	160	155	163	160	155
166	162	162	160	155	163	160	155
161	160	155	159	154	154	156	154
159	163	158	163	155	155	156	152
159	162	162	160	153	153	153	151

Figure B.1 : Un spécimen de 8 x 8 blocs de *Lena* image.

Nous soustrayons 128 (c'est-à-dire la valeur moyenne d'intensité dans la représentation d'image monochrome de 8 bits) de chaque intensité de pixel et calculons ensuite la DCT pour chaque élément de $S(k_1,k_2)$ en utilisant l'équation (1). Les valeurs de tableau transformées sont présentées dans la figure B.2.

248	19	3	4	-7	9	1	-7
11	-2	3	6	-3	2	5	0
-4	2	-2	-3	0	-1	-1	0
-1	-1	1	1	2	0	-1	0
2	1	0	0	-2	0	3	0
0	0	-1	0	0	0	-1	-1
-3	0	1	0	1	0	0	0
3	0	0	0	-1	0	0	0

.

Figure B.2 : Coefficients DCT pour le bloc 8 x 8.

Il convient de noter que la plupart des coefficients transformés ont des valeurs très faibles et que seuls quelques coefficients ont des grandeurs plus élevées. Cela montre les capacités de compactage énergétique de DCT.

Les images de base DCT peuvent être calculées en utilisant le noyau de transformation, qui est le même pour les transformations DCT directe et en cosinus discrète inverse (IDCT) et est donné par :

$$g(n_1, n_2, k_1, k_2) = h(n_1, n_2, k_1, k_2) = \sqrt{\frac{4}{N^2}}\, C(k_1) C(k_2) cos\left(\frac{\pi(2n_1+1)k_1}{2N}\right) cos\left(\frac{\pi(2n_2+1)k_2}{2N}\right) \quad (2)$$

Pour chaque valeur de k_1 et k_2 (k_1, k_2= 0,1,..., N −1), nous obtenons une image de base de taille N x N en calculant l'équation (2) sur n_1, n_2 = 0,1,...,N -1. Pour une taille de bloc de 4 x 4, nous obtenons donc 16 images de base, chacune de taille 4 x 4.

La sélection des tailles de bloc dans la DCT est une considération importante. Les images doivent être subdivisées de telle sorte que le niveau de redondance entre les sous-images adjacentes soit réduit à un niveau acceptable et que la dimension des sous-images soit un entier de 2. L'augmentation de la taille des blocs réduit la redondance des blocs adjacents et réduit la reconstruction quadratique moyenne de l'erreur en utilisant des coefficients tronqués et quantifiés, mais implique plus de calculs. Les tailles de bloc les plus populaires utilisées dans la compression d'image sont 8 x 8 et 16 x 16.

B.2.1 DCT unidimensionnel :

La définition de la DCT la plus courante d'une séquence 1-D de longueur N est :

$$C(u) = \alpha(u) \sum_{x=0}^{N-1} f(x) cos\left[\frac{\pi(2x+1)u}{2N}\right] \qquad (3)$$

pour *u* = 0,1,2,...,*N-1*. De même, la transformation inverse est définie comme :

$$f(x) = \sum_{u=0}^{N-1} \alpha(u) C(u) cos\left[\frac{\pi(2x+1)u}{2N}\right] \qquad (4)$$

pour *x* = 0,1,2,…N-1. Dans les deux équations (3) et (4), α (u) est défini comme :

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & Pour\ \ u=0 \\ \sqrt{\frac{2}{N}} & Pour\ \ u\neq 0 \end{cases} \qquad (05)$$

Il est clair de (3) que pour $u = 0$, $C(u=0) = \sqrt{\frac{1}{N}} \sum_{i=0}^{N-1} f(x)$. Ainsi, le premier coefficient de transformation est la valeur moyenne de la séquence d'échantillons. Dans la littérature, cette valeur est appelée coefficient DC. Tous les autres coefficients de transformation sont appelés les coefficients AC.

Pour corriger cette idée, ignorez le composant f***(x)*** et α***(u)*** dans (3). L'intrigue de $\sum_{x=0}^{N-1} cos\left[\frac{\pi(2x+1)u}{2N}\right]$ pour N=8 et les valeurs variables de ***u*** sont illustrées à la figure B.3. Conformément à notre observation précédente, la première forme d'onde supérieure gauche (u = 0) donne une valeur constante (DC), alors que toutes les autres formes d'onde (u = 1,2, 7…) donnent des formes aux fréquences progressivement croissantes [56].

Ces formes d'ondes sont appelées la fonction de base du cosinus. Noter que ces fonctions de base sont orthogonales. Par conséquent, la multiplication de toute forme d'onde sur la figure B.3 avec une autre forme suivie d'une somme sur tous les points d'échantillonnage produit une valeur zéro (scalaire), tandis que la multiplication de toute figure de la figure (B.3) suivie d'une somme donne une valeur constante. Les formes d'onde orthogonales sont indépendantes, c'est-à-dire qu'aucune des fonctions de base ne peut être représentée par une combinaison d'autres fonctions de base [56].

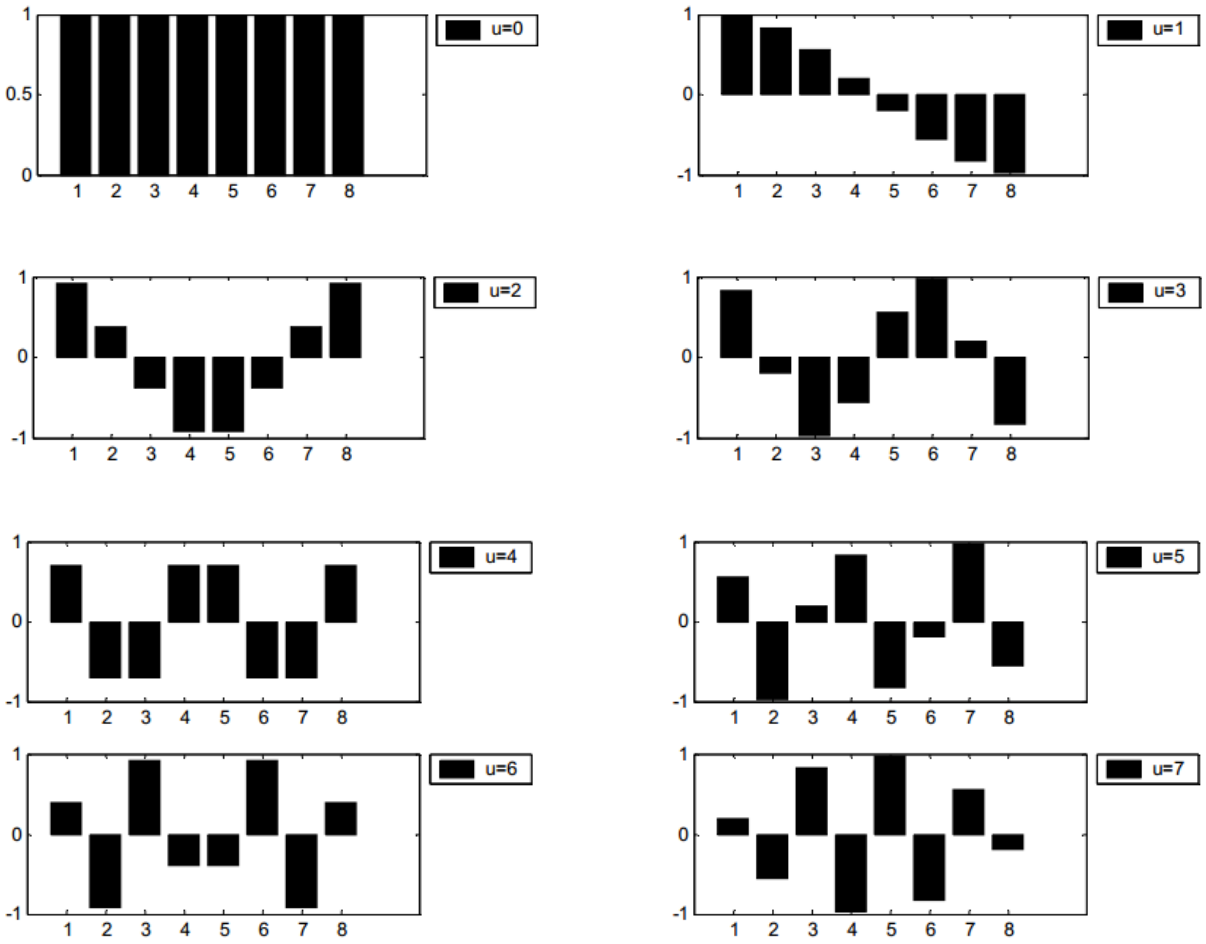


Figure B.3 : Fonction de base en cosinus à une dimension (N = 8).

Si la séquence d'entrée a plus de N points d'échantillonnage, elle peut être divisée en sous-séquences de longueur N et la DCT peut être appliquée indépendamment à ces blocs. Ici, un point très important à noter est que dans ces calculs, les valeurs des points de fonction de base ne changeront pas. Seules les valeurs de f (x) changeront dans chaque sous-séquence. Ceci est une propriété très importante, car elle montre que les fonctions de base peuvent être pré-calculées hors ligne puis multipliées par les sous-séquences. Cela réduit le nombre d'opérations mathématiques (c'est-à-dire les multiplications et les ajouts), rendant ainsi l'efficacité du calcul [56].

B.2.2. DCT bidimensionnel :

La DCT-1D est utilisée en traitement des signaux unidimensionnels tels que les signaux de la parole. Pour cette raison on a besoin d'une version 2D de la DCT pour l'analyse d'un signal bidimensionnel (2D) comme les images.

La DCT-2D est effectuée sur une matrice carrée de *N*x*N* pixel et donne une matrice carrée de *N*x*N* coefficients fréquentiels. Comme pour la DCT-1D, l'élément(0,0) est appelé la composante DC et les autres éléments sont les composantes AC.

Par convention, les 64 valeurs transformées (de chaque bloc de 8x8) sont positionnées d'une certaine manière, ainsi la valeur moyenne de tous les coefficients est placée en haut à gauche de ce bloc. Plus on s'éloigne des coefficients continus plus leurs grandeurs tendent à diminuer, ce qui signifie que la DCT concentre l'énergie d'image en haut à gauche de la matrice transformée, les coefficients en bas et à droite de cette matrice contiennent moins d'information utile [57].

On peut représenter la distribution des fréquences de la DCT d'une matrice de 8x8 éléments par la figure suivante:

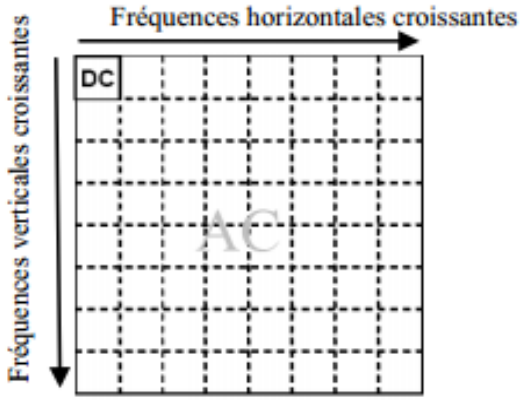


Figure B.4 : Distribution des fréquences de la DCT.

La DCT 2-D est une extension directe du cas 1-D et est donnée par :

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)cos\left[\frac{\pi(2x+1)u}{2N}\right]cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (6)$$

Où *u,v* =0,1,2,...,*N-1* sont des indices des fréquences spatiales dans la direction horizontale et verticale de l'image.

- *f(x,y)* représente la valeur d'un pixel de l'image initiale pour *x* et *y* donnés.
- *C(u,v)* représente les coefficients de la DCT.
- *N* représente la taille du bloc.

Pour *u, v* = 0,1,2,..,*N-1*, et α (*u*) et α (*v*) sont définit dans (5). La transformée inverse est définie comme :

$$f(x,y) = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} \alpha(u)\alpha(v)C(u,v)cos\left[\frac{\pi(2x+1)u}{2N}\right] cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (7)$$

Pour *x, y* = 0,1,2,...,*N-1*. Les fonctions de base 2D peuvent être générées en multipliant les fonctions de base 1D orientées horizontalement (illustrées à la figure B.3) par un ensemble orienté verticalement des mêmes fonctions. Les fonctions de base pour N = 8 sont indiquées. Encore une fois, on peut noter que les fonctions de base présentent une augmentation progressive de la fréquence aussi bien dans le sens vertical que dans le sens horizontal. La fonction de base supérieure gauche résulte de la multiplication de la composante continue de la figure B.5 avec sa transposition. Par conséquent, cette fonction prend une valeur constante et est appelée coefficient DC [56,57].

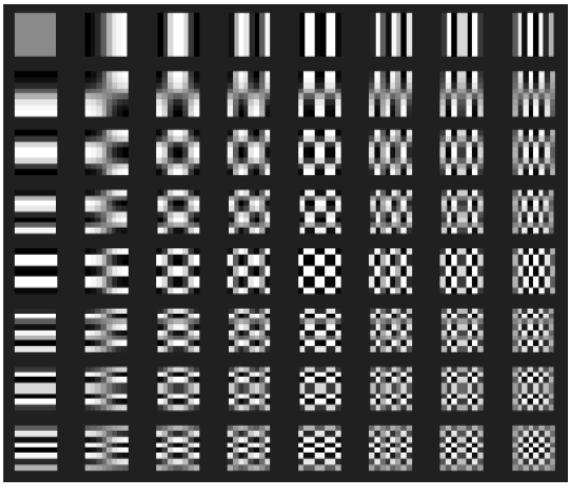


Figure B.5 : Fonctions de base DCT bidimensionnelles (N = 8).

Le gris neutre représente zéro, le blanc représente les amplitudes positives et le noir représente l'amplitude négative.

B.3. Propriétés de la DCT :

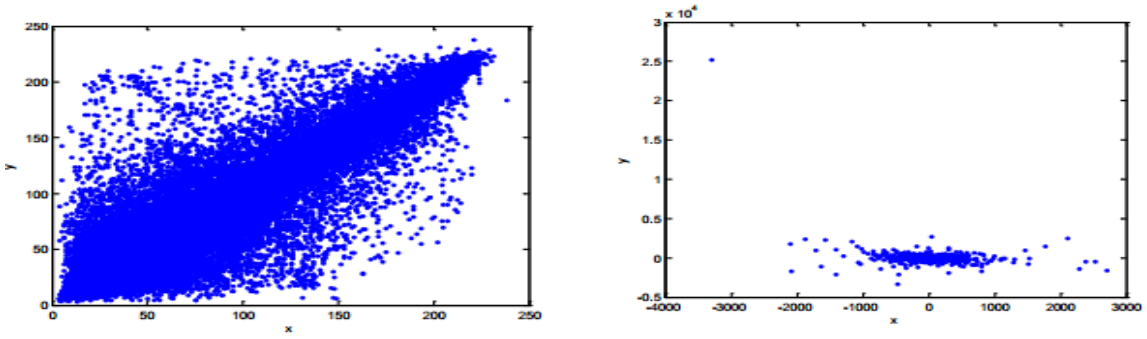
Cette section expose (avec des exemples) quelques propriétés de la DCT qui sont particulièrement importantes aux applications de traitement d'image.

B.3.1. Décorrélation :

L'avantage principal de la transformation d'image est la réduction de redondance entre ces pixels voisins. Ceci mène à des coefficients transformés non-corrélés qui peuvent êtres codés indépendamment.

La figure (B.6) montre une image typique au niveau de gris. L'image est de taille 256x256 avec chaque pixel à niveau de gris codé sur 8 bits pour une gamme de [0-255]. Même avec un grand degré de détails dans beaucoup de régions, la valeur du niveau de gris de n'importe quel pixel indiqué tend à être semblable à ses pixels voisins. Pour illustrer ce rapport, on a tracé les valeurs de niveau de gris des paires de pixels adjacents avant et après l'application de la DCT (figure B.7) [57].

Figure B.6 : Image aux niveaux de gris**.**



(a) (b)

Figure B.7 : les valeurs de niveau de gris des paires de pixels adjacents. (a) avant la DCT. (b) Après la DCT

Chaque point représente un pixel dans l'image, avec la coordonnée 'x' présente son niveau de gris et la coordonnée 'y' présente le niveau de gris de son voisin droit. La relation diagonale forte pour la ligne x=y (figure (b.7(a))) montre la corrélation forte entre les pixels

voisins et lorsque la transformation DCT est appliquée sur l'image entière, le résultat est montré sur la figure (B.7(b)). Les deux pixels sont décorrèlés.

B.3.2 Compactage d'énergie :

L'efficacité d'une transformation peut être mesurée par sa capacité de compactage d'énergie des données d'entrée dans les coefficients. Ceci permet au quantificateur de jeter les coefficients avec des amplitudes relativement petites sans présenter la déformation visuelle dans l'image reconstruite.

Figure B.8 : Saturn et sa DCT.

L'application de la DCT sur cette image fournit un bon compactage d'énergie dans la région de basse fréquence de l'image transformée. La DCT rend un excellent compactage d'énergie pour des images corrélées [57].

B.3.3. Séparabilité :

L'équation de transformation DCT (6) peut être exprimée comme suit:

$$C(u,v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} cos\left[\frac{\pi(2x+1)u}{2N}\right] \sum_{y=0}^{N-1} f(x,y) cos\left[\frac{\pi(2y+1)v}{2N}\right] \qquad (8)$$

Pour $u,v = 0,1,2,...,N-1$.

Cette propriété, appelée séparabilité, a pour avantage principal que C(u,v) peut être calculée en deux étapes par des opérations 1-D successives sur les lignes et les colonnes d'une image. Cette idée est illustrée graphiquement à la figure suivante. Les arguments présentés peuvent être appliqués de manière identique pour le calcul DCT inverse (7) [56].

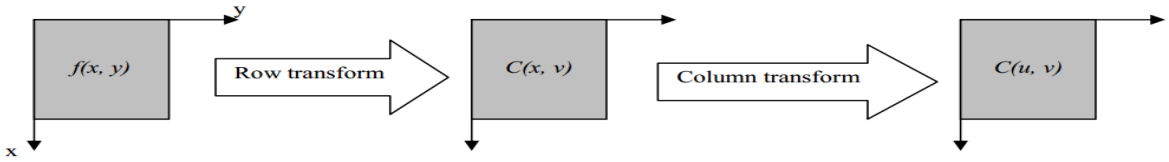


Figure B.9 : Calcul de la DCT 2-D en utilisant la propriété de séparabilité.

B.3.4. Symetrie :

Un autre examen des opérations de ligne et de colonne dans l'équation (8) révèle que ces opérations sont fonctionnellement identiques. Une telle transformation est appelée une transformation symétrique. Une transformée séparable et symétrique peut être exprimée sous la forme.

$$T = AfA \qquad (9)$$

Où A est une matrice de transformation symétrique N x N avec les entrées $a(i,j)$ donnée par :

$$a(i,j) = \alpha(j) \sum_{j=0}^{N-1} cos\left[\frac{\pi(2j+1)i}{2N}\right]$$

Et f est la matrice d'image N x N.

C'est une propriété extrêmement utile, car elle implique que la matrice de transformation peut être pré-calculée hors ligne et ensuite appliquée à l'image, ce qui améliore considérablement l'efficacité du calcul [56].

B.3.5. Orthogonalité :

Pour étendre les idées présentées dans la section précédente, notons l'inverse transformation de (9) comme :

$$f = A^{-1}TA^{-1}$$

Comme discuté précédemment, les fonctions de base DCT sont orthogonales. Ainsi, la matrice de transformation inverse de A est égale à sa transposition, à savoir$A^{-1} = A^{T}$. Donc, et en plus de ses caractéristiques de décorrélation, cette propriété réduit la complexité de calcul préalable [56].

Résumé

Une des préoccupations dans le domaine des communications sécurisées est le concept de la sécurité de l'information. Aujourd'hui, la réalité a encore prouvé que la communication entre deux parties sur de longues distances a toujours été sujette aux risques d'interception.

Devant ces contraintes, de nombreux défis et opportunités s'ouvrent pour l'innovation. Afin de pouvoir fournir une communication sécurisée, cela a conduit les chercheurs à développer plusieurs schémas de stéganographie.

La stéganographie est l'art de dissimuler un message de manière secrète dans un support anodin, dont l'objectif de base est de permettre une communication secrète sans que personne ne puisse soupçonner son existence. Le message est caché dans un medium qui peut être une image (utilisée dans notre travail), texte, audio,...etc. Cependant, de nombreuses techniques ont été développées pour la dissimulation. Les contributions majeures de ce mémoire sont en premier lieu, de présenter trois méthodes de stéganographie permettant de cacher un message dans une image numérique. La première c'est la technique LSB qui consiste à cacher le message dans les bits de poids faible de l'image, la deuxième c'est la technique LSB-Contours et la dernière c'est la technique DCT. Nos résultats expérimentaux effectués sur Matlab montrent l'efficacité de ces trois systèmes stéganographique.

Mot clé : Steganographie, LSB, Transformée en Cosinus Discrète (DCT), bit de poids faible, détection de contour, steganalyse.

Abstract

One of concerns in the field of secure communications is the concept of information security. Today, reality has further proved that long-distance communication between two parts has always been subject to the risks of interception.

Faced with these constraints, many challenges and opportunities open up for innovation. In order to provide secure communication, this has led researchers to develop several steganography schemes.

Steganography is the art of hiding a message secretly in a harmless medium, whose basic purpose is to allow secret communication without anyone being able to suspect its existence. The message is hidden in a medium that can be an image (as used in our work), text, audio, ...etc. However, many techniques have been developed for concealment. The major contributions of this work are, first of all, to present three methods of steganography for hiding a message in a digital image. The first is the LSB technique which consists of hiding the message in the low-end bits of the image, the second is the LSB-Contour and the last is DCT technique. Our experimental results on Matlab show the effectiveness of these three steganographic systems.

Keyword: Steganography, LSB, Discrete Cosine Transform (DCT), least significant bit, contour detection, steganography.